Énoncés des notes de travail de Grothendieck démontrés en Lean 4, et questions ouvertes

Michel Hua
Chercheur indépendant, Paris
michel@commutator.io

Novembre 2026

Résumé

Les lectures modernisées du fonds Grothendieck de Montpellier reformulent les notes de travail en langage actuel. Elles dérivent de la transcription et peuvent se tromper. Ce texte démontre des énoncés de ces lectures dans soixante-quinze cotes, en algèbre commutative, géométrie algébrique, géométrie affine plane, topologie générale, topologie modérée, théorie des catégories et des groupes, algèbre homotopique, théorie des ordres, algèbre et combinatoire finie. Chaque démonstration suit une preuve vérifiée dans l'assistant de preuve Lean 4 [39], avec sa bibliothèque mathlib [99]. Pour chaque énoncé, le texte donne le contexte du feuillet, la démonstration, les hypothèses superflues ou nécessaires et les corrections apportées à la lecture ou à la page. Il se clôt sur la liste des énoncés que les sections rapportent sans vérification en Lean. Une seconde partie, en anglais, rassemble treize questions ouvertes tirées des mêmes notes.

hexagon:2611.00125v2

Table des matières

Introduction **7**

Tableau récapitulatif **11**

I Cycles algébriques et conjectures standard **17**

1 Cote 11 : la sous-algèbre tautologique des puissances de X, un modèle algébrique **17**

2 Cote 16 : le pseudo-inverse de l'opérateur de Lefschetz, la normalisation de sl(2) et les algèbres de Hodge **22**

3 Cote 98 : une théorie axiomatique des normes, le modèle des G-ensembles ; classes de faisceaux **31**

II Motifs **36**

III Théorie de Hodge **37**

4 Cote 13 : la question du double réseau et le cas de Tate 37

IV Cohomologie étale et ℓ-adique 41

V Groupes p-divisibles et groupes formels 43

VI Algèbre universelle et théories 44

5 Cote 161-2 : monadicité, caractérisation de Gabriel–Ulmer 44

VII Analyse fonctionnelle 47

6 Cote 1 : le système d'inégalités des valeurs singulières, coefficients de Fredholm 47

7 Cote 113 : l'enveloppe de Karoubi et l'invariance de Morita 56

VIII Théorie de la dualité 59

8 Cote 43 : polynômes additifs modulo $F - 1$ et perfection 59

9 Cote 101 : la dualité locale en dimension un pour tous les modules 60

10 Cote 125 : la carte des équivalences et le lemme du feuillet III-18 62

11 Cote 115 : la dualité d'Isbell par le calcul des noyaux 65

IX Descente 67

12 Cote 128 : descente le long d'un conducteur nilpotent, idéaux d'équivalence de rang deux 67

13 La question de Buffalo : une relation d'équivalence finie non effective (Venken, 1971) 75

X Topos et sites 78

14 Cote 161-3 : le topos d'un produit d'espaces 78

15 Cote 37 : le contre-exemple à EGA I 10.10.5 83

XI Variétés abéliennes et schémas de Picard 86

16 Cote 44 : l'intégralité des nombres de Cartan à partir des axiomes 86

17 Cote 50 : la formule des traces dans le cadre axiomatique **87**

18 Cote 63 : les quatre composantes de $j = 0$ ont quatre tangentes en $p = 2$ **89**

19 Cote 100 : un point de dimension un hors d'une famille dénombrable de diviseurs **90**

XII Catégories tensorielles et dualité tannakienne **98**

20 Cote 155 : le produit de Takeuchi comme quotient d'un idéalisateur **98**

21 IHÉS 2ILL5 : objets « sereins » et objets dualisables **99**

XIII Algèbre commutative **101**

22 Cote 21 : injectifs de I-torsion, critère ponctuel pour un champ **101**

23 Cote 22 : produits de modules plats (lemme 3.3, corollaires 3.4 et 3.5), l'obstruction sur $k[[t]]$, un noyau de différentielles **103**

24 IHÉS SGA 6 1/5 : modules à n-présentation finie **109**

25 Cote 67 : modules à involution et triples (P, Q, m) **112**

XIV Catégories et foncteurs **115**

26 Cote 19 : le théorème de comonadicité 1.12, la comonade sur une base produit le théorème de Gabriel–Popescu et les chaînes d'adjoints **115**

27 Cote 133 : le centre et le groupe dérivé vus par deux modules croisés **123**

28 Cote 161-1 : la partie fixe d'une adjonction, les adjonctions idempotentes, les objets locaux **125**

XV Géométrie formelle, modules et représentabilité **133**

29 Cote 39 : le théorème de préparation « formel » ; fonctions implicites dans une classe de séries **133**

30 Cote 41 : continuité de la section générique et ouverture (proposition 1) **136**

31 Cote 42 : familles cohérentes de germes, le lemme 1 et le lemme 2 **138**

XVI K-théorie, classes de Chern et Riemann–Roch **148**

32 Cote 2 : une classe non nulle de classe de Chern totale triviale **148**

33 IHÉS SGA 6 2/3 : le groupe K d'une catégorie triangulée, la formule d'Euler **151**

34 Cote 153 : polynômes à valeurs entières, co-opérations, analyseurs 154

XVII Cohomologie cristalline et de de Rham 161

35 Cote 5 : l'algèbre artinienne universelle à puissances divisées 161

XVIII Schémas en groupes et groupes algébriques 170

36 Cote 10 : les indécomposables de $\mathbb{G}_a \rtimes \mathbb{G}_m$ 170

37 Cote 90 : un groupe plat irréductible dont un saturé n'est pas de type fini 172

38 Cote 40 : la régularité des torseurs sous α_p ne passe pas à la somme 176

39 Cote 46 : relever un cocycle à travers la réduction modulo $\mathfrak{m}$ 179

40 Cote 53 : un monoïde simplifiable est un groupe 186

41 Cote 78 : le critère de fermeture des polygones réguliers sur un anneau, et les 2p-gones en bande 190

42 Cote 64 : la configuration octaédrale en caractéristique 5 193

43 Cote 80 : un contre-exemple au théorème des arrangements cruciaux 195

44 Cote 82 : $\mathfrak{sl}(2)$ et la conique en caractéristique 2, cas déployé 199

45 Cote 84 : le produit des algèbres quadratiques, en coordonnées 201

46 Cote 160 : le déterminant de Moore et les coefficients de Dickson 213

47 Cote 69 : les automorphismes du graphe des vingt-sept droites qui fixent un triangle 215

48 Cote 89 : la relation fondamentale en rang deux 216

XIX Surfaces de Riemann, uniformisation et modules des courbes 222

49 Cote 93 : la différence schwarzienne en dérivées divisées 222

XX Champs, gerbes et catégories fibrées 239

50 Cote 62 : l'invariant j d'une conique munie d'une trisection étale 239

XXI Topologie combinatoire, surfaces et cartes 241

51 Cote 152 : le dictionnaire des graphes circularisés et des contours 241

52 Cote 88 : l'ordre 2ν et la trichotomie des cartes standard 243

53 Cote 73 : les aires des oreilles d'un polygone plan **246**

54 Cote 74 : complexes cubiques généralisés, la réduction à un carré latin et à ses revêtements doubles **251**

55 Cote 76 : l'ordre des sommets ; drapeaux de type H, le lemme de surjectivité **257**

56 Cote 77 : le discriminant universel modulo 2 et modulo 4, la sphère, la symétrie canonique **260**

57 Cote 79 : graphes à homothéties, commutant et étoiles sur $(\mathbf{Z}/n)^2$ **267**

58 Cote 85 : représentations de G_2 et de $\mathbb{D}_\infty$ dans PGL_2, rotation d'ordre 5 **277**

XXII Jeux et combinatoire **289**

59 Cote 68 : les théories de l'orientation et leurs applications de Stokes **289**

XXIII Groupes fondamentaux et théorie de Galois **292**

60 Cote 29 : le critère du déterminant sur l'inertie modérée **292**

61 Cote 145 : l'exposant unité dans le groupe profini libre **296**

XXIV Polyèdres et géométrie convexe **300**

62 Cote 70 : l'icosaèdre en coordonnées universelles, fidèle en toute caractéristique, et sa conique modulo 5 **300**

63 Cote 86 : les cinq trièdres de l'icosaèdre et l'icosaèdre gauche **307**

64 Cote 72 : réalisations par pseudo-réflexions d'un polytope régulier **311**

XXV Théorie de l'homotopie et catégories tests **315**

65 Cote 136 : le lemme binomial des ombres **316**

66 Cote 106 : catégories à cofibrations, factorisation de Brown et critère $(\star\star)$ **318**

67 Cote 114 : les localisateurs fondamentaux et la proposition 4 **322**

68 Cote 118 : produits stables sans asphéricité **324**

69 Cote 158 : monoïdes finis, monoïdes à élément minimal, catégories finies **327**

70 Cote 104 : catégories de modèles, trois exemples, épinglages, un complexe globulaire **330**

XXVI Topologie modérée et espaces stratifiés **341**

71 Cote 121 : la décomposition cellulaire admissible la plus grossière **341**

72 Cote 120 : sommes amalgamées, écraser une partie modérée sur un corps **342**

73 Cote 150 : voisinages coniques, un contre-exemple sur [0, 1] **345**

XXVII Géométrie anabélienne et dessins **349**

74 Cote 146 : les exposants trivialisants de L_i et de L sur $M_{0,n}$ **349**

75 Cote 140-1 : le groupe $H^1(U_{0,3}, \mathfrak{S}_3; \mathbf{G}_m)$ **359**

XXVIII Ordres et géométrie des formes **363**

76 Cote 156-1 : le modèle-segment est un biordre **363**

77 Cote 156-2 : les rives d'une partie fermée **366**

78 Cote 156-3 : l'intermédiarité se lit sur les découpages **366**

79 Cote 156-4 : les parties saturées ne forment pas une algèbre de Boole **369**

Bilan **371**

80 Erreurs, pistes et énoncés restants **371**

Énoncés non vérifiés en Lean **373**

Déclaration sur l'usage de l'intelligence artificielle **377**

Open questions from Grothendieck's Montpellier notes **384**

Open questions from Grothendieck's Montpellier notes **384**

Q1 Why this note **384**

Q2 Étale cohomology and Hodge theory **385**

Q3 Algebraic cycles **388**

Q4 Abelian varieties and reductive groups **390**

Q5 Topoi and stacks **392**

Q6 Moduli of curves and Galois actions **395**

Q7 Pseudoline arrangements **396**

Q8 A problem stated in a lecture **398**

Q9 The large conjectures, and how the notes approach them **399**

Q10 How the list was made, and its limits **405**

Introduction

Ce texte réunit, pour soixante-quinze dossiers (cotes) du fonds Grothendieck de Montpellier, des énoncés de leurs lectures modernisées démontrés en Lean 4. Il se lit seul. Les renvois de la forme « cote, lot n, p. k » ouvrent la page correspondante du PDF du dossier, sur le site de l'université de Montpellier.

Les énoncés qui suivent sont ceux des lectures modernisées, qui restituent en notation actuelle le contenu de la transcription. Chaque démonstration suit une preuve vérifiée mécaniquement en Lean 4, citée en note au titre de la section. Elle établit que l'énoncé tient sous les hypothèses écrites. Elle ne dit pas que la lecture est fidèle à la page.

Ces preuves sont modestes à côté d'autres travaux récents. Le 6 octobre 2026, OpenAI a publié 719 manuscrits produits par un modèle interne, non relus par des pairs, dont une partie s'accompagne de formalisations en Lean 4[1]. Quatre familles de ces manuscrits annoncent des énoncés issus du programme de Grothendieck : l'hypothèse d'homotopie ; la conjecture des sections, p-adique locale, et sur $\mathbb{Q}$ pour les courbes modulaires $X_0(N)$ et $X_1(N)$ de genre au moins deux ; la conjecture de Deligne–Drinfeld sur l'algèbre de Lie de Grothendieck–Teichmüller ; la conjecture de Hodge pour les variétés abéliennes à multiplication complexe et, par des théorèmes de Milne, la conjecture standard de type Hodge pour les variétés abéliennes. Deux seulement sont formalisées, en partie. Pour Deligne–Drinfeld, la formalisation établit la liberté de l'algèbre de Lie des solutions rationnelles de l'antisymétrie, de la relation à trois termes et du pentagone à quatre brins, munie du crochet d'Ihara, avec un générateur en chaque poids impair au moins égal à 3, et l'isomorphisme continu après complétion par le poids. Le transport régularisé et les conséquences pour le complexe des graphes n'y sont pas. Pour l'hypothèse d'homotopie, elle se borne à un théorème intermédiaire, rappelé dans la partie sur l'homotopie. Le projet n'a ni compilé ni vérifié ce code ; ce qui en est dit vient de ses pages de description. Les énoncés de l'annexe sont élémentaires, le plus souvent classiques, et aucun n'est une conjecture de Grothendieck.

Les soixante-quinze cotes sont celles où une lecture énonce un résultat net dans un domaine élémentaire. L'énoncé démontré y est le plus souvent une piste de l'onglet Findings, parfois un énoncé détaché d'une théorie plus vaste (comonades et topos, catégories localement présentables, conjectures standard, localisation homotopique), un lemme de la lecture ou une correction. Dans neuf cotes (19, 63, 80, 90, 118, 150, 156-4, 158 et 160), un contre-exemple réfute une affirmation ou une présomption du feuillet. Le tableau récapitulatif qui suit l'introduction donne le verdict de chaque section. Motifs, catégories tannakiennes, schémas abéliens, dérivateurs et cohomologie étale sont exclus.

Chaque cote a sa section, et les sections suivent l'ordre chronologique des thèmes. Les thèmes sont ceux de la carte des mathématiques du fonds que publie le site (« A map of the

1. `https://github.com/openai/math`, consulté le 10 octobre 2026. La portée des formalisations citées ici est celle que décrivent ses pages `lean/docs/008.md` et `lean/docs/312.md`.

mathematics in the fonds »), qui classe les mots-clés des lectures sous une trentaine de sujets. Une cote est rangée sous le sujet qui porte le plus de ses mots-clés et, à égalité, sous celui dont relève l'énoncé démontré. La date d'un thème est celle de la carte : la moyenne, sur ses cotes, du milieu de leur datation par l'inventaire. Cette moyenne indique une tendance. Dans un thème, les cotes suivent leur propre datation, et les cotes non datées viennent en dernier.

On trouve ainsi, en parties successives : cycles algébriques et conjectures standard (vers 1966), les cotes 11 (§ 1), 16 (§ 2) et 98 (§ 3) ; théorie de Hodge (vers 1967), la cote 13 (§ 4) ; algèbre universelle et théories (vers 1968), la cote 161-2 (§ 5) ; analyse fonctionnelle (vers 1968), les cotes 1 (§ 6) et 113 (§ 7) ; théorie de la dualité (vers 1969), les cotes 43 (§ 8), 101 (§ 9), 125 (§ 10) et 115 (§ 11) ; descente (vers 1969), la cote 128 (§ 12) ; topos et sites (vers 1970), les cotes 161-3 (§ 14) et 37 (§ 15) ; variétés abéliennes et schémas de Picard (vers 1970), les cotes 44 (§ 16), 50 (§ 17), 63 (§ 18) et 100 (§ 19) ; catégories tensorielles et dualité tannakienne (vers 1970), la cote 155 (§ 20) ; algèbre commutative (vers 1970), les cotes 21 (§ 22), 22 (§ 23) et 67 (§ 25) ; catégories et foncteurs (vers 1970), les cotes 19 (§ 26), 133 (§ 27) et 161-1 (§ 28) ; géométrie formelle, modules et représentabilité (vers 1970), les cotes 39 (§ 29), 41 (§ 30) et 42 (§ 31) ; K-théorie, classes de Chern et Riemann–Roch (vers 1970), les cotes 2 (§ 32) et 153 (§ 34) ; cohomologie cristalline et de de Rham (vers 1972), la cote 5 (§ 35) ; schémas en groupes et groupes algébriques (vers 1972), les cotes 10 (§ 36), 90 (§ 37), 40 (§ 38), 46 (§ 39), 53 (§ 40), 78 (§ 41), 64 (§ 42), 80 (§ 43), 82 (§ 44), 84 (§ 45), 160 (§ 46), 69 (§ 47) et 89 (§ 48) ; surfaces de Riemann, uniformisation et modules des courbes (vers 1973), la cote 93 (§ 49) ; champs, gerbes et catégories fibrées (vers 1973), la cote 62 (§ 50) ; topologie combinatoire, surfaces et cartes (vers 1973), les cotes 152 (§ 51), 88 (§ 52), 73 (§ 53), 74 (§ 54), 76 (§ 55), 77 (§ 56), 79 (§ 57) et 85 (§ 58) ; jeux et combinatoire (vers 1974), la cote 68 (§ 59) ; groupes fondamentaux et théorie de Galois (vers 1974), les cotes 29 (§ 60) et 145 (§ 61) ; polyèdres et géométrie convexe (vers 1976), les cotes 70 (§ 62), 86 (§ 63) et 72 (§ 64) ; théorie de l'homotopie et catégories tests (vers 1976), les cotes 136 (§ 65), 106 (§ 66), 114 (§ 67), 118 (§ 68), 158 (§ 69) et 104 (§ 70) ; topologie modérée et espaces stratifiés (vers 1977), les cotes 121 (§ 71), 120 (§ 72) et 150 (§ 73) ; géométrie anabélienne et dessins (vers 1980), les cotes 146 (§ 74) et 140-1 (§ 75) ; ordres et géométrie des formes (1986), les cotes 156-1 (§ 76), 156-2 (§ 77), 156-3 (§ 78) et 156-4 (§ 79). Le rangement suit le vocabulaire de la carte : l'invariance de Morita de la cote 113 relève par exemple de l'analyse fonctionnelle, par le produit tensoriel des catégories linéaires. Trois pièces du fonds Grothendieck–Illusie de l'IHÉS, qui n'ont pas de lecture modernisée, ont leur section : un tapuscrit sur les modules à n-présentation finie en algèbre commutative (§ 24), des notes sur le groupe K d'une catégorie triangulée et de son quotient de Verdier en K-théorie (§ 33), dont les énoncés sont lus sur la transcription, et la définition des objets « sereins » du manuscrit « Motifs » en catégories tensorielles (§ 21).

Quatre thèmes de la carte n'ont aucun énoncé vérifié ici. Chacun garde sa partie, à sa place chronologique : elle le dit, nomme les théories qui manquent à la bibliothèque, donne les cotes du thème et la liste de leurs pistes ouvertes.

Chaque section donne le contexte du feuillet, les définitions que la lecture laisse implicites, l'énoncé tel que la lecture le donne, sa démonstration et des remarques : hypothèses superflues ou nécessaires, contre-exemples, corrections de la lecture ou de la page. Elle se termine par les énoncés de la cote qui ne sont pas démontrés ici. La section 80 fait le bilan des erreurs trouvées et des pistes démontrées.

Le losange $\blacklozenge n$ marque un énoncé lié au théorème numéroté n de la frise des œuvres du site (« The works, on the same years »), qui place ses principaux théorèmes à l'année de l'article

ou de l'exposé qui les démontre. Trois énoncés le portent. Le feuillet 2 de la cote 125 enchaîne cohomologie locale, complétion formelle et dualité. Il relève de la dualité cohérente et de la géométrie formelle (théorème 6, Séminaire Bourbaki n° 149 et 195, EGA III_1) et des théorèmes de Lefschetz par la cohomologie locale (SGA 2, théorème 9). La proposition 2.15 de la cote 21 invoque le critère de Baer sous le nom de « Tohoku », et l'énoncé des pages 14 et 15 de la cote 19 porte sur une catégorie de Grothendieck à générateur ; tous deux relèvent de l'article de Tôhoku (théorème 4). Le lien porte sur le sujet ; aucun de ces énoncés n'est un théorème de la frise.

Le losange rouge ♦ marque les énoncés, démontrés ou non, que l'onglet Findings du site retient comme pistes. Ce sont des énoncés du dossier qui pourraient manquer à la littérature publiée, soit que la recherche n'en ait rien trouvé dans les sources lues (« candidate »), soit qu'elle reste à faire (« unsearched »). Une piste n'est ni un résultat établi ni une affirmation de priorité. Le losange gris ⧫ marque une piste réglée depuis : la recherche a retrouvé l'énoncé dans la littérature, ou, pour la cote 118, l'auteur de la source citée l'a confirmé . Quarante pistes sont démontrées ici, dans les cotes 16, 19 (deux pistes), 37, 39, 40, 44, 46, 67, 68, 70, 72, 73 (trois pistes), 76, 77 (deux pistes), 78, 79 (quatre pistes), 84, 86 (deux pistes), 100, 104, 106, 115, 120 (deux pistes), 121, 133, 145, 154 (sous la forme précisée par l'édition), 156-1, 156-3 et 158 (deux pistes). Quarante-neuf autres ne le sont qu'en partie : celle de la cote 155, sans les produits tensoriels complétés ; celle de la cote 50, la formule des traces pour une forme d'intersection symétrique, dans un cadre à un objet, le corollaire de la page 6 ne suivant pas des axiomes ; celle de la cote 10, les chaînes et le terme dominant de ξ^n, sans la classification ni l'anneau ; celle de la cote 11, dans un modèle algébrique et pour deux partitions de jointure grossière ; une seconde de la cote 11, l'équivalence des pages 37 et 41 sous la forme de l'édition, dans le cas commutatif, sans la seconde assertion de la page 41, la pleine fidélité de $A \mapsto (A(\mathrm{pt}), \Delta)$; celle de la cote 22, pour la topologie discrète seulement ; une seconde de la cote 22, le contre-exemple des différentielles, dans la spécialisation $a_i = 0$ ($i \geq 2$) de la page 28 ; une troisième de la cote 22, la proposition de la page 23 en n variables, sans le « a fortiori » sur k ; celle de la cote 43, la formule de $\mathrm{Ext}^1(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z})$, réduite à son cœur algébrique sur une base affine ; celle de la cote 136, sur les coefficients seulement, sans les modules gradués sur $k\{T\}$; celle de la cote 153, pour K_0 plat sur k_0 ; deux pistes de la cote 16, l'une, le critère de Lefschetz dans un anneau gradué, sans l'existence de la décomposition primitive ni la réciproque (2) $\Rightarrow$ (1), la réciproque (3) $\Rightarrow$ (1) étant fausse hors des projecteurs de la graduation, l'autre parce que l'anneau Φ_0 de la lecture n'existe pas sur $\mathbb{Z}$; celle des extensions χ-scindées de la cote 84, leur produit en coordonnées ; les deux premières pistes de la cote 85, dont la représentabilité n'est pas démontrée, et la troisième, sur un corps, où l'équivalence lue est fausse ; celle de la cote 74, sous une forme reconstruite de la condition (Ka), dont la fin est illisible ; celle de la cote 1, en dimension finie et pour $m \leq 2$; une seconde de la cote 1, les corollaires 2 et 3 des pages 123 et 124, en dimension finie ; une troisième de la cote 1, la sous-additivité de S_p déduite de l'inégalité de déterminants, démontrée pour $n \leq 2$; la quatrième piste de la cote 77, la sphère comme restriction de Weil d'une conique, en coordonnées sur un corps ; la fidélité entière de la cote 70, pour les incidences seulement ; les formules universelles de la cote 70, pour les ordres 3, 4 et 5 seulement ; celle des polygones étoilés de la cote 79, sans le caractère de morphisme de $\lambda \mapsto \nu$ dans le cadre abstrait ni l'existence de ν en un sommet à partir de $G_{0s} \simeq \mathbf{D}_n$; celle de la cote 93, dont la rigidité n'est démontrée que pour $\alpha = 0$; une seconde de la cote 93, le morphisme dérivé défini par un torseur, pour des groupes abéliens et non des faisceaux ; celle des $2p$-gones en bande de la cote 78, pour leur existence seulement ; celle de la cote 64, sur un corps et non sur une base, où l'identification au groupe

octaédral demande en outre 5 inversible ; celle de la cote 140-1, la valeur $\mathbf{Z}/6$ (et $\mathbf{Z}/3$ en caractéristique 2) de $H^1(\mathfrak{S}_3, \mathcal{O}(U_{0,3})^*)$, engendré par la classe tangente, dans un modèle des unités dont l'identification aux unités de $U_{0,3}$ n'est pas démontrée équivariante, sans le passage au groupe de Picard du champ ni le générateur $\mathcal{O}(1)$; celle de la cote 146, au niveau des cocycles pour $n = 4$, 5, 6 et, pour tout n, dans un modèle homogène par des fonctions de poids, sans le dictionnaire avec les fibrés équivariants ; celle de la cote 101, dans le modèle des triplets (M_0, M_1, u) par lequel la page réduit la question ; celle des catégories finies de la cote 158, pour X connexe, l'énoncé lu étant faux sans cette hypothèse ; celle de la cote 21, le critère ponctuel de la proposition 7 sous la forme pseudo-limite de la définition 6, pour un champ scindé, sans l'identification au localisé $X_{(x)}$; celle des formes de $\mathfrak{sl}(2)$ de la cote 82, dans le cas déployé, sans les formes sur une base ; celle du déterminant de Moore de la cote 160, pour E trivialisé ; celle des rives de la cote 156-2, l'injectivité de l'application $(*)$ seulement, sans la bijectivité pour X paracompact ni l'espace découpé ; celle de l'ordre des sommets de la cote 76, sans le retour des ordres compatibles à l'ensemble semi-simplicial, cas Δ_{inj} de l'équivalence de la cote 104 ; celle du groupe $\mathcal{U}_\rho$ de la cote 72, sur les points et en coordonnées, sans le schéma en groupes ni l'énoncé projectif sur une base ; celle des normes axiomatiques de la cote 98, dans le modèle des G-ensembles seulement, sans les schémas ni les revêtements ; celle des réalisations épinglées de la cote 72, pour E libre, sans l'existence locale du point de départ ; celle de la cote 5, l'intégralité et la valuation des q_i seulement, sans l'algèbre universelle ni sa forme normale ; celle de la cote 2 sur φ_K, pour $n \geq 3$ et dans la présentation de CK par $c^1(L)$; celle de la cote 128, les deux relations d'équivalence de la proposition 1 (i) dans le seul cas d'un corps de base, sans la réduction artinienne ; celle de la cote 53, le monoïde simplifiable, pour les points sur un corps algébriquement clos, sans les schémas en monoïdes sur un anneau ni les monomorphismes ; celle de la cote 46, l'injectivité de $H^1(\Gamma, A^*) \to H^1(\Gamma_i, A^*)$ vers le groupe d'inertie, sur un anneau local de corps résiduel infini et pour une inertie d'ordre inversible seulement, sans la base semi-locale ni le groupe de décomposition ; celle de la cote 161-3, la spatialité du locale produit des pages 9 à 14, au niveau des cadres, sans le côté des topos ; celle de la cote 137, la pleine fidélité seulement, sans l'essentielle surjectivité ; celle de la cote 148, l'unicité du recollement seulement, sans le groupoïde de Teichmüller multimarqué lui-même. Sept pistes réglées sont aussi démontrées : entièrement, l'algébricité de l'inverse de la cote 16, le demi-discriminant en rang impair de la cote 77, la distance trois de la cote 79 et la formule du produit de la cote 84, en coordonnées scindées ; en partie, la classification par triplets de la cote 84, pour les algèbres libres, la réponse de la page 35 de la cote 118, dans un modèle des équivalences faibles tronqué en degré 1, et le topos d'un produit de la cote 161-3, dans le modèle des familles de rectangles, sans le dictionnaire avec le 2-produit de topos. Démontrer une piste ne dit pas que l'énoncé manque à la littérature : sur ce point, la piste reste ouverte. Les autres énoncés démontrés sont des résultats classiques, des lemmes ou des corrections de la lecture.

Les résultats principaux sont encadrés. Un énoncé démontré par piste de l'onglet Findings entièrement démontrée y est appelé théorème. Il porte le nom de Grothendieck quand les feuillets l'énoncent ; quand la démonstration établit davantage que la page, la remarque qui suit le dit, et si l'énoncé encadré est la forme générale, son étiquette renvoie à la page sans le nom de Grothendieck. Un énoncé que les feuillets ne font pas, trouvé par l'édition (extension, lemme, reconstruction), ne porte jamais son nom et se dit énoncé de l'édition ; un énoncé qui établit qu'une affirmation de la page ou de la lecture est fausse y est appelé contre-exemple. Les autres énoncés de la lecture gardent le nom d'énoncé.

Une piste restante que les feuillets conjecturent ou demandent est encadrée comme une conjecture de Grothendieck ; une question que pose seulement l'édition ne porte pas son nom. Une piste restante que les feuillets affirment, avec ou sans démonstration, est encadrée comme un théorème de Grothendieck, avec en marge la mention ◊ *non vérifié en Lean* : l'énoncé est rapporté, sa démonstration n'est pas vérifiée.

Sous le titre de chaque partie, quand le fonds en conserve, un paragraphe donne les lettres datées qui situent la partie dans le temps, chacune avec sa cote, son lot et sa page, d'après les registres du site. Dans deux parties, une ligne *Ailleurs* signale des formalisations extérieures au projet qui touchent leur thème.

Ce texte laisse au lecteur trois questions : si l'énoncé démontré est juste tel qu'il est écrit (Lean n'établit que sa validité sous les hypothèses écrites) ; s'il lui manque une hypothèse ou s'il en porte une de trop ; s'il figure déjà dans la littérature, et où. Pour les pistes, seule la troisième se pose. La fidélité de la lecture au feuillet demande le fac-similé et relève d'un autre travail.

Tableau récapitulatif

Une ligne par section, dans l'ordre des parties : la cote, l'énoncé démontré en quelques mots, le verdict, le fichier Lean et la section. *Confirmé tel que lu* : l'énoncé tient sous les hypothèses que la lecture écrit ; *plus général* : il tient sous des hypothèses plus faibles ; *partiel* : une partie seulement est démontrée, ou dans un modèle, ce que la section précise ; *correction de la lecture* : la lecture omettait une hypothèse de la page ou glosait faussement un énoncé juste ; *faux sur la page* : un contre-exemple réfute une affirmation du feuillet ; *conjecture de la page réfutée* : de même pour ce que le feuillet présume sans l'affirmer ; *déjà dans mathlib* : l'énoncé y figure, et le fichier Lean ne fait que l'y rapporter. Une section qui démontre plusieurs énoncés peut porter plusieurs verdicts.

Cote	Énoncé	Verdict	Fichier Lean	§
Cycles algébriques et conjectures standard				
11	La sous-algèbre tautologique des puissances de X, un modèle algébrique	partiel	`Folder11`	1
16	Le pseudo-inverse de l'opérateur de Lefschetz, la normalisation de sl(2) et les algèbres de Hodge	partiel ; correction de la lecture (glose fausse)	`Folder16`	2
98	Une théorie axiomatique des normes, le modèle des G-ensembles ; classes de faisceaux	partiel	`Folder98`	3
Théorie de Hodge				
13	La question du double réseau et le cas de Tate	partiel	`Folder13`	4
Algèbre universelle et théories				
161-2	Monadicité, caractérisation de Gabriel–Ulmer	partiel	`Folder161_2`	5
Analyse fonctionnelle				
1	Le système d'inégalités des valeurs singulières, coefficients de Fredholm	partiel	`Folder1`	6
113	L'enveloppe de Karoubi et l'invariance de Morita	partiel	`Folder113`	7
Théorie de la dualité				
43	Polynômes additifs modulo $F - 1$ et perfection	partiel	`Folder43`	8
101	La dualité locale en dimension un pour tous les modules	confirmé tel que lu	`Folder101`	9
125	La carte des équivalences et le lemme du feuillet III-18	partiel	`Folder125`	10
115	La dualité d'Isbell par le calcul des noyaux	confirmé tel que lu	`Folder115`	11
Descente				
128	Descente le long d'un conducteur nilpotent, idéaux d'équivalence de rang deux	partiel	`Folder128`	12
Topos et sites				
161-3	Le topos d'un produit d'espaces	partiel ; confirmé tel que lu	`Folder161_3`	14
37	Le contre-exemple à EGA I 10.10.5	plus général	`Folder37`	15
Variétés abéliennes et schémas de Picard				
44	L'intégralité des nombres de Cartan à partir des axiomes	correction de la lecture (glose fausse)	`Folder44`	16
50	La formule des traces dans le cadre axiomatique	correction de la lecture (hypothèse omise)	`Folder50`	17

Cote	Énoncé	Verdict	Fichier Lean	§
63	Les quatre composantes de $j = 0$ ont quatre tangentes en $p = 2$	faux sur la page (contre-exemple) ; correction de la lecture (glose fausse)	`Folder63`	18
100	Un point de dimension un hors d'une famille dénombrable de diviseurs	partiel	`Folder100`	19
Catégories tensorielles et dualité tannakienne				
155	Le produit de Takeuchi comme quotient d'un idéalisateur	partiel	`Folder155`	20
Algèbre commutative				
21	Injectifs de I-torsion, critère ponctuel pour un champ	partiel	`Folder21`	22
22	Produits de modules plats (lemme 3.3, corollaires 3.4 et 3.5), l'obstruction sur $k[[t]]$, un noyau de différentielles	partiel	`Folder22`	23
IHÉS SGA 6 1/5	Modules à n-présentation finie	confirmé tel que lu ; plus général	`IhesSGA6_1_5`	24
67	Modules à involution et triples (P, Q, m)	plus général	`Folder67`	25
Catégories et foncteurs				
19	Le théorème de comonadicité 1.12, la comonade sur une base produit le théorème de Gabriel–Popescu et les chaînes d'adjoints	partiel ; faux sur la page (contre-exemple)	`Folder19`	26
133	Le centre et le groupe dérivé vus par deux modules croisés	partiel	`Folder133`	27
161-1	La partie fixe d'une adjonction, les adjonctions idempotentes, les objets locaux	plus général	`Folder161_1`	28
Géométrie formelle, modules et représentabilité				
39	Le théorème de préparation « formel » ; fonctions implicites dans une classe de séries	plus général	`Folder39`	29
41	Continuité de la section générique et ouverture (proposition 1)	plus général	`Folder41`	30
42	Familles cohérentes de germes, le lemme 1 et le lemme 2	plus général	`Folder42`	31
K-théorie, classes de Chern et Riemann–Roch				
2	Une classe non nulle de classe de Chern totale triviale	partiel	`Folder2`	32
IHÉS SGA 6 2/3	Le groupe K d'une catégorie triangulée, la formule d'Euler	confirmé tel que lu ; partiel	`IhesSGA6_2_3`	33
153	Polynômes à valeurs entières, co-opérations, analyseurs	plus général ; partiel	`Folder153`	34
Cohomologie cristalline et de de Rham				
5	L'algèbre artinienne universelle à puissances divisées	partiel	`Folder5`	35

Cote	Énoncé	Verdict	Fichier Lean	§
Schémas en groupes et groupes algébriques				
10	Les indécomposables de $\mathbb{G}_a \rtimes \mathbb{G}_m$	partiel	`Folder10`	36
90	Un groupe plat irréductible dont un saturé n'est pas de type fini	faux sur la page (contre-exemple)	`Folder90`	37
40	La régularité des torseurs sous α_p ne passe pas à la somme	plus général	`Folder40`	38
46	Relever un cocycle à travers la réduction modulo $\mathfrak{m}$	partiel	`Folder46`	39
53	Un monoïde simplifiable est un groupe	partiel	`Folder53`	40
78	Le critère de fermeture des polygones réguliers sur un anneau, et les 2p-gones en bande	plus général	`Folder78`	41
64	La configuration octaédrale en caractéristique 5	plus général	`Folder64`	42
80	Un contre-exemple au théorème des arrangements cruciaux	faux sur la page (contre-exemple)	`Folder80`	43
82	$\mathfrak{sl}(2)$ et la conique en caractéristique 2, cas déployé	partiel	`Folder82`	44
84	Le produit des algèbres quadratiques, en coordonnées	partiel	`Folder84`	45
160	Le déterminant de Moore et les coefficients de Dickson	confirmé tel que lu ; faux sur la page (contre-exemple)	`Folder160`	46
69	Les automorphismes du graphe des vingt-sept droites qui fixent un triangle	partiel	`Folder69`	47
89	La relation fondamentale en rang deux	plus général	`Folder89`	48
Surfaces de Riemann, uniformisation et modules des courbes				
93	La différence schwarzienne en dérivées divisées	partiel	`Folder93`	49
Champs, gerbes et catégories fibrées				
62	L'invariant j d'une conique munie d'une trisection étale	partiel	`Folder62`	50
Topologie combinatoire, surfaces et cartes				
152	Le dictionnaire des graphes circularisés et des contours	partiel	`Folder152`	51
88	L'ordre 2ν et la trichotomie des cartes standard	partiel	`Folder88`	52
73	Les aires des oreilles d'un polygone plan	confirmé tel que lu	`Folder73`	53
74	Complexes cubiques généralisés, la réduction à un carré latin et à ses revêtements doubles	correction de la lecture (hypothèse omise)	`Folder74`	54
76	L'ordre des sommets ; drapeaux de type H, le lemme de surjectivité	confirmé tel que lu	`Folder76`	55

Cote	Énoncé	Verdict	Fichier Lean	§
77	Le discriminant universel modulo 2 et modulo 4, la sphère, la symétrie canonique	plus général	`Folder77`	56
79	Graphes à homothéties, commutant et étoiles sur $(\mathbf{Z}/n)^2$	plus général	`Folder79`	57
85	Représentations de G_2 et de $\mathbb{D}_\infty$ dans PGL_2, rotation d'ordre 5	partiel	`Folder85`	58
Jeux et combinatoire				
68	Les théories de l'orientation et leurs applications de Stokes	confirmé tel que lu	`Folder68`	59
Groupes fondamentaux et théorie de Galois				
29	Le critère du déterminant sur l'inertie modérée	confirmé tel que lu	`Folder29`	60
145	L'exposant unité dans le groupe profini libre	plus général	`Folder145`	61
Polyèdres et géométrie convexe				
70	L'icosaèdre en coordonnées universelles, fidèle en toute caractéristique, et sa conique modulo 5	partiel	`Folder70`	62
86	Les cinq trièdres de l'icosaèdre et l'icosaèdre gauche	confirmé tel que lu	`Folder86`	63
72	Réalisations par pseudo-réflexions d'un polytope régulier	partiel	`Folder72`	64
Théorie de l'homotopie et catégories tests				
136	Le lemme binomial des ombres	plus général	`Folder136`	65
106	Catégories à cofibrations, factorisation de Brown et critère $(\star\star)$	plus général	`Folder106`	66
114	Les localisateurs fondamentaux et la proposition 4	correction de la lecture (hypothèse omise)	`Folder114`	67
118	Produits stables sans asphéricité	confirmé tel que lu ; faux sur la page (contre-exemple)	`Folder118`	68
158	Monoïdes finis, monoïdes à élément minimal, catégories finies	correction de la lecture (glose fausse) ; faux sur la page (contre-exemple)	`Folder158`	69
104	Catégories de modèles, trois exemples, épinglages, un complexe globulaire	partiel	`Folder104`	70
Topologie modérée et espaces stratifiés				
121	La décomposition cellulaire admissible la plus grossière	confirmé tel que lu	`Folder121`	71
120	Sommes amalgamées, écraser une partie modérée sur un corps	plus général	`Folder120`	72

Cote	Énoncé	Verdict	Fichier Lean	§
150	Voisinages coniques, un contre-exemple sur [0, 1]	faux sur la page (contre-exemple)	`Folder150`	73
Géométrie anabélienne et dessins				
146	Les exposants trivialisants de L_i et de L sur $M_{0,n}$	partiel	`Folder146`	74
140-1	Le groupe $H^1(U_{0,3}, \mathfrak{S}_3; \mathbf{G}_m)$	partiel	`Folder140_1`	75
Ordres et géométrie des formes				
156-1	Le modèle-segment est un biordre	confirmé tel que lu	`Folder156_1`	76
156-2	Les rives d'une partie fermée	partiel	`Folder156_2`	77
156-3	L'intermédiarité se lit sur les découpages	confirmé tel que lu	`Folder156_3`	78
156-4	Les parties saturées ne forment pas une algèbre de Boole	conjecture de la page réfutée	`Folder156_4`	79

Partie 1

Cycles algébriques et conjectures standard

Le 27 août 1965, il énonce pour Serre les conjectures standard A, A′, A″ et B (14, lot 3, p. 43). La cote 16 garde deux lettres à John Coates, datées de sa main du 6.1.1966 et du 4.1.1967 (16, lot 3, p. 47, 16, lot 3, p. 43). La première donne des formes équivalentes de la conjecture C ; la seconde situe la conjecture de l'indice et l'indépendance des conjectures à l'égard de la polarisation. Les anneaux gradués étudiés ici sont rangés dans le même dossier.

Ailleurs : le dépôt d'OpenAI cité dans l'introduction annonce la conjecture de Hodge rationnelle pour les variétés abéliennes à multiplication complexe. Il en tire, par des théorèmes de Milne, la conjecture standard de type Hodge pour les variétés abéliennes en toute caractéristique, qui est la conjecture B de la lettre à Serre, celle de positivité (14, lot 3, p. 44). Ces énoncés ne sont ni relus ni formalisés ; trois manuscrits voisins, sur les classes de Weil et les surfaces K3, ont été retirés le 7 octobre 2026. La cote 16 ne donne lieu ici qu'à des énoncés d'algèbre, sur l'opérateur Λ et sur les algèbres de Hodge d'ordre 2, sans lien de démonstration avec ces conjectures.

1 Cote 11 : la sous-algèbre tautologique de $H^*(X^k)$, un modèle algébrique [2]

La cote 11, *Formalisme des correspondances*, cinquante-sept pages que l'inventaire date « à partir de 1961 », se clôt sur la sous-algèbre de $H^*(X^k)$ engendrée par les images inverses y_i de la classe d'un point et par les classes des diagonales partielles (pages 50 à 56). La page 50 en donne les relations pour $k = 2$ et $k = 3$ (11, lot 3, p. 50) ; la page 56 encadre la borne $s + s' \leqslant k + 1$ pour deux polydiagonales à s et s' blocs qui se coupent suivant la petite diagonale, trouve la petite diagonale dans le cas d'égalité, la nullité « pour raison de degrés » si $k > s + s'$, et laisse le cas $k = s + s'$ sur un χ biffé suivi d'un point d'interrogation (11, lot 3, p. 56). La lecture rétablit χ par la formule d'intersection en excès et énonce la table de multiplication complète ; cette table est de l'édition. Aucune géométrie n'est formalisée ici : tout se déduit de quelques identités que vérifie la classe de la diagonale.

Conventions. On se donne un anneau commutatif k, une k-algèbre commutative A, un élément $\Delta \in A \otimes A$, une classe $y \in A$, un scalaire χ et une forme linéaire $\int$ sur A, avec

$$(a \otimes 1)\Delta = (1 \otimes a)\Delta, \quad \Delta \text{ symétrique}, \quad m(\Delta) = \chi\, y, \quad (y \otimes 1)\Delta = y \otimes y, \quad y^2 = 0,$$

et, pour les images directes, $\int y = 1$, $\int 1 = 0$, $(\mathrm{id} \otimes \int)\Delta = 1$. Dans une k-algèbre commutative B munie de morphismes $\iota_1, \dots, \iota_k : A \to B$ (par exemple $A^{\otimes k}$), on pose $y_i = \iota_i(y)$ et $\delta_{ij} = (\iota_i, \iota_j)(\Delta)$; ainsi $\delta_{ii} = \chi\, y_i$. Pour une partie V et une racine $r \in V$, la petite diagonale est $\delta_V = \prod_{v \in V \smallsetminus \{r\}} \delta_{rv}$; elle ne dépend pas de r.

Énoncé (Le modèle)**.** *Soient k un corps, A une k-algèbre commutative de dimension finie, (b_i) et (b_i') deux bases duales pour $(a, b) \mapsto \int ab$, $\varepsilon : A \to k$ une augmentation de noyau nilpotent, et y tel que $ay = \varepsilon(a)\, y$, $\int y = 1$, $\int 1 = 0$, $\varepsilon(y) = 0$. Alors $\Delta = \sum_i b_i \otimes b_i'$ vérifie les identités ci-dessus, avec $\chi = \dim A$.*

2. Preuve vérifiée : `lean/Grothendieck/Folder11.lean`.

C'est le cas pair d'une algèbre à dualité de Poincaré, où $\chi = \dim H^*(X)$; le cas des classes de degré impair, avec signes, n'est pas formalisé (Lean : `model`).

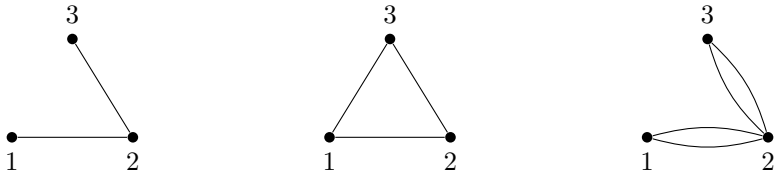
Énoncé (Grothendieck, page 50). *Pour $k = 2$: $y_1\delta = y_2\delta = y_1y_2$ et $\delta^2 = \chi\, y_1y_2$. Pour $k = 3$, avec $\delta = \delta_{\{1,2,3\}}$: $\delta_{12}\delta_{23} = \delta_{12}\delta_{13} = \delta_{23}\delta_{13} = \delta$, $\delta_{ij}^2 = \chi\, y_iy_j$, $\delta_{ij}\, y_i = y_iy_j$, $\delta\, y_i = y_1y_2y_3$, $\delta^2 = 0$ et $\delta_{ij}\,\delta = \chi\, y_1y_2y_3$.*

Lean : `table_two`, `table_three`.

Théorème 1.1 (D'après les pages 54 et 56, règle des multigraphes, énoncé de l'édition ♦). *Soit E une famille finie d'arêtes, boucles et arêtes multiples permises, sur un ensemble fini V qu'elle rend connexe, et $\delta_E = \prod_{(i,j)\in E} \delta_{ij}$. Alors $|V| \leqslant |E| + 1$, et δ_E vaut δ_V si $|E| = |V| - 1$, $\chi \prod_{v\in V} y_v$ si $|E| = |V|$, et 0 si $|E| > |V|$.*

Démonstration. Par récurrence sur $|E|$. Sans arête, V est un point et $\delta_E = 1 = \delta_V$. Une boucle en i vaut $\chi\, y_i$; on la retire sans rompre la connexité, et l'on conclut par $y_i\,\delta_V = \prod_{v\in V} y_v$ et $y_i^2 = 0$. Une arête (i, j) avec $i \neq j$ autorise le transfert : la première identité donne $\delta_{ij}\,\iota_j(a) = \delta_{ij}\,\iota_i(a)$, donc, multiplié par δ_{ij}, tout produit de classes reste le même quand on y remplace l'indice j par i. On contracte ainsi l'arête : le reste devient un multigraphe connexe sur $V \smallsetminus \{j\}$, avec une arête et un sommet de moins, des arêtes parallèles à (i, j) devenant des boucles. Il reste à voir que δ_{ij} fait repasser de $V \smallsetminus \{j\}$ à V dans chacun des trois cas, ce que donnent le transfert, la symétrie de Δ et $y_i\,\delta_{ij} = y_iy_j$. □

Pour $k = 3$, trois relations de la page 50 se lisent sur trois multigraphes connexes à trois sommets, avec deux, trois et quatre arêtes :



$\delta_{12}\delta_{23} = \delta$ $\qquad$ $\delta_{13}\,\delta = \chi\, y_1y_2y_3$ $\qquad$ $\delta^2 = 0$

Corollaire (Grothendieck, page 56, et la table de l'édition). *Soient R et R' deux partitions des k indices, à s et s' blocs, dont la borne supérieure est la partition grossière, et $\delta_R = \prod_{P\in R} \delta_P$. Alors $s + s' \leqslant k + 1$, et $\delta_R\,\delta_{R'}$ vaut la petite diagonale si $s + s' = k + 1$, $\chi\, y_1 \cdots y_k$ si $s + s' = k$, et 0 si $s + s' < k$. Avec un bloc marqué d'un point, $y_j\,\delta_R\,\delta_{R'}$ vaut $y_1 \cdots y_k$ si $s + s' = k + 1$ et 0 sinon ; avec deux, le produit est nul.*

Les arêtes de R et R' joignant chaque bloc à son plus petit élément sont au nombre de $2k - s - s'$, et forment un multigraphe connexe : le théorème 1.1 donne tout (Lean : `graph_rule`, `product_rule`, `product_rule_pointed`).

Énoncé (D'après la page 54, réduction aux blocs de R'', énoncé de l'édition). *Soient R et R' deux partitions des indices, et R'' une partition moins fine que l'une et l'autre dont chaque bloc est connexe pour la relation « être dans un même bloc de R ou de R' » (c'est la borne supérieure de R et R'). Pour un bloc C de R'', soient b et b' les nombres de blocs de R et de R' contenus dans C. Alors $b + b' \leqslant |C| + 1$, et $\delta_R\,\delta_{R'} = \prod_{C\in R''} c_C$, où c_C vaut δ_C si $b + b' = |C| + 1$, $\chi \prod_{v\in C} y_v$ si $b + b' = |C|$, et 0 si $b + b' < |C|$. Plus généralement, pour toute partie M d'indices marqués, $\prod_{m\in M} y_m \cdot \delta_R\,\delta_{R'}$ est le produit sur les blocs C de : c_C si C ne contient aucune marque ; $\prod_{v\in C} y_v$ s'il en contient une et si $b + b' = |C| + 1$; 0 sinon. En particulier, deux marques dans un même bloc de R'' donnent 0.*

Les classes $\varepsilon_{R,J}$ de la lecture sont les $y_j\,\delta_R$ pour $j \in J$, puisque $y_j\,\delta_J = \prod_{i\in J} y_i$; l'énoncé, avec $M = \{j, j'\}$, donne donc la proposition de la lecture tout entière, pour des partitions quelconques. On regroupe les blocs de R et de R' selon le bloc de R'' qui les contient : les arêtes en étoile de ceux qui tombent dans C sont au nombre de $2|C| - b - b'$ et rendent C connexe (une chaîne de la relation ne sort pas du bloc de son origine), et le théorème 1.1 s'applique bloc par bloc ; une marque y_m se range dans le facteur de son bloc, où $y_m\,\delta_C = \prod_{v\in C} y_v$, $y_m^2 = 0$ et $y_m \prod_{v\in C} y_v = 0$ concluent (Lean : `join_rule`, `join_rule_marked`, `join_rule_two_marks`). La borne supérieure R'' est donnée par ses propriétés, non construite.

Énoncé (Page 56, stabilités, en un facteur)**.** *Dans $B \otimes A$, l'image directe $\mathrm{id} \otimes \int$ par la projection qui oublie le dernier facteur $*$ annule les classes qui ne le font pas intervenir, et envoie $x\,y_*$ et $x\,\delta_{i*}$ sur x ; l'image inverse envoie δ_{ij} sur δ_{ij} et y_i sur y_i.*

Lean : `push_old`, `push_point`, `push_diag`, `pull_d`.

Remarques. La règle tient plus généralement que la table de la lecture : pour tout multigraphe connexe, dans toute algèbre où vivent une classe de la diagonale et une classe de point. Le coefficient χ du cas $s + s' = k$, biffé sur la page, est bien celui que la lecture rétablit. La nullité de l'image directe d'une classe qui n'implique pas le facteur oublié demande $\int 1 = 0$, ce que donne en géométrie la raison de degré.

Ne sont pas démontrés ici : le cadre géométrique et la formule d'intersection en excès ; l'engendrement par $\boxtimes$ de la conclusion encadrée ; la catégorie des correspondances d'une théorie bivariante (pages 2 à 18), les sous-foncteurs stables (pages 20 à 24), les signes de Koszul des pages 26 à 30 et la Proposition de la page 39, la seconde mouture (pages 41 à 47) hors de l'équivalence de la sous-section suivante.

Algèbres bivariantes simpliciales et algèbres de Poincaré (pages 37 et 41)

La page 33 définit la catégorie $\mathcal{C}$ des algèbres bivariantes : une k-algèbre A munie d'une forme $\kappa_A : A \to k$ (sa *jauge*), un morphisme $A \to B$ étant un couple (f_*, f^*) d'un homomorphisme d'algèbres $f^* : B \to A$ et d'une application linéaire $f_* : A \to B$ qui vérifie la formule de projection $f_*(f^*(y)\,x) = y\,f_*(x)$ et $\kappa_B f_* = \kappa_A$. Une *algèbre de Poincaré* est une telle algèbre, de dimension finie sur le corps k, où $(x, y) \mapsto \kappa(xy)$ est non dégénérée. Une *algèbre bivariante simpliciale* est un foncteur contravariant $I \mapsto A(I)$ des ensembles finis non vides, avec toutes les applications, vers $\mathcal{C}$: pour $\alpha : I \to J$, une image inverse $\alpha^* : A(I) \to A(J)$ et une image directe $\alpha_* : A(J) \to A(I)$, fonctorielles, avec la formule de projection et la conservation des jauges. Les pages 37 et 41 affirment, sans démonstration et avec « à vérifier », que l'évaluation en un point est une équivalence avec les algèbres de Poincaré. La lecture restreint l'énoncé aux objets *spéciaux*, sans quoi il est faux (l'objet constant $I \mapsto P$ a la même valeur en un point que $I \mapsto P^{\otimes I}$). On le démontre sous cette forme, dans le cas commutatif : algèbres commutatives sans graduation, c'est-à-dire, pour la cohomologie, le cas où tous les degrés sont pairs et où il n'y a pas de signe de Koszul.

Théorème 1.2 (Grothendieck, pages 37 et 41, forme de l'édition, cas commutatif ♦)**.** *Soit k un corps. Disons qu'une algèbre bivariante simpliciale A est* spéciale *si $A(\mathrm{pt})$ est une algèbre de Poincaré, si, pour tout I, les deux images inverses définissent un isomorphisme de Künneth $A(I) \otimes A(\mathrm{pt}) \xrightarrow{\sim} A(I \sqcup \mathrm{pt})$, et si les jauges sont multiplicatives : $\kappa_{A(I\sqcup\mathrm{pt})}(a \otimes b) = \kappa_{A(I)}(a)\,\kappa_{A(\mathrm{pt})}(b)$. Alors l'évaluation $A \mapsto A(\mathrm{pt})$ est une équivalence entre la catégorie des*

algèbres bivariantes simpliciales spéciales, avec les transformations naturelles, et la sous-catégorie pleine de $\mathcal{C}$ formée des algèbres de Poincaré, d'inverse $P \mapsto (I \mapsto P^{\otimes I})$. Plus précisément :

1. *dès que B est spéciale, une transformation naturelle $A \to B$ est déterminée par son image inverse en un point, et tout morphisme $A(\mathrm{pt}) \to B(\mathrm{pt})$ de $\mathcal{C}$ est la valeur en un point d'une transformation naturelle $A \to B$, sans hypothèse sur A ;*
2. *pour toute algèbre de Poincaré P, $I \mapsto P^{\otimes I}$, avec pour images inverses les multiplications le long des fibres et pour images directes leurs adjointes, est spéciale et vaut P en un point, à un isomorphisme d'algèbres près qui respecte les jauges.*

Démonstration. L'image directe est l'adjointe de l'image inverse (page 33). Si D est de Poincaré, la forme $\kappa_D(xy)$ identifie D à son dual ; pour un homomorphisme $h : D \to E$, il existe donc une unique application linéaire $h_* : E \to D$ telle que $\kappa_D(y\, h_*(x)) = \kappa_E(h(y)\, x)$, et elle vérifie la formule de projection et $\kappa_D h_* = \kappa_E$ (faire $y = 1$). Réciproquement, tout couple (f_*, f^*) de $\mathcal{C}$ vérifie cette identité : $\kappa_B(y\, f_*(x)) = \kappa_B(f_*(f^*(y)\, x)) = \kappa_A(f^*(y)\, x)$. Dans la sous-catégorie pleine des algèbres de Poincaré, f_* est donc déterminé par f^*.

Les $A(I)$ d'un objet spécial sont de Poincaré. Si B et C sont de Poincaré, $B \otimes C$ l'est pour la jauge produit : l'application $z \mapsto \kappa(z\,\cdot)$ de $B \otimes C$ dans son dual est le composé de l'isomorphisme $B \otimes C \to B^\vee \otimes C^\vee$ que donnent les deux dualités et de l'isomorphisme $B^\vee \otimes C^\vee \simeq (B \otimes C)^\vee$ de la dimension finie, comme on le voit sur les tenseurs purs. L'isomorphisme de Künneth, multiplicatif et compatible aux jauges, transporte la non-dégénérescence ; on conclut par récurrence sur le cardinal de I.

Engendrement. Par la même récurrence, deux homomorphismes de $A(I)$ dans une algèbre qui coïncident sur les images inverses i^* de $A(\mathrm{pt})$ le long des points $i : \mathrm{pt} \to I$ sont égaux : sur $A(I) \otimes A(\mathrm{pt})$, on teste séparément les deux facteurs, et un point de I composé avec l'inclusion $I \to I \sqcup \mathrm{pt}$ est un point de $I \sqcup \mathrm{pt}$.

Fidélité. Si φ et ψ sont deux transformations naturelles $A \to B$ égales en un point, la naturalité donne $\varphi_I^* \circ i^* = i^* \circ \varphi_{\mathrm{pt}}^* = \psi_I^* \circ i^*$ pour chaque point i, d'où $\varphi_I^* = \psi_I^*$ par engendrement, puis $\varphi_{I*} = \psi_{I*}$ puisque $B(I)$ est de Poincaré.

Plénitude. Soit $g = (g_*, g^*)$ un morphisme de $A(\mathrm{pt})$ vers $B(\mathrm{pt})$. On construit par récurrence $h_I : B(I) \to A(I)$ avec $h_I \circ i^* = i^* \circ g^*$ pour chaque point : $h_{I \sqcup \mathrm{pt}}$ est le composé de l'inverse de l'isomorphisme de Künneth de B, de $h_I \otimes g^*$ et de l'homomorphisme de Künneth de A (qui n'a pas à être bijectif). L'engendrement donne la naturalité pour toute application $\alpha : I \to J$, puisque $\alpha \circ i$ est le point $\alpha(i)$. On prend pour φ_{I*} l'adjointe de h_I ; la naturalité des images directes se vérifie en accouplant avec un $y \in B(I)$, ce qui la ramène à celle des images inverses ; en un point, $h_{\mathrm{pt}} = g^*$ et l'adjointe est g_*.

Surjectivité essentielle. Pour P de Poincaré, on pose $A(I) = P^{\otimes I}$ et, pour $\alpha : I \to J$, $\alpha^*(\otimes_i x_i) = \prod_i \iota_{\alpha(i)}(x_i)$, où ι_j place un facteur en position j : c'est la multiplication le long des fibres, avec 1 hors de l'image. Cet homomorphisme envoie $\iota_i(a)$ sur $\iota_{\alpha(i)}(a)$, ce qui donne la fonctorialité par engendrement. La jauge est $\kappa(\otimes_i x_i) = \prod_i \kappa(x_i)$; l'homomorphisme de Künneth envoie $(\otimes_{i \in I} x_i) \otimes y$ sur le tenseur pur prolongé par y, et coïncide avec l'isomorphisme canonique $P^{\otimes I} \otimes P \simeq P^{\otimes (I \sqcup \mathrm{pt})}$; les jauges sont multiplicatives. Les $P^{\otimes I}$ sont alors de Poincaré, les images directes sont les adjointes, fonctorielles par unicité de l'adjointe, et $a \mapsto \iota_0(a)$ est un isomorphisme $P \simeq P^{\otimes \mathrm{pt}}$ qui respecte les jauges, donc un « bon » isomorphisme de $\mathcal{C}$ au sens de la page 33. □

Lean : `adj`, `adj_unique`, `poincare_tensor`, `Special.poincare_all`, `Special.gen`, `faithful`, `full`, `powFun`, `powFun_special`, `essSurj`, `GHom.ofEquiv`, et l'énoncé réuni `evaluation_equivalence` (espace de noms `Folder11.Simplicial`).

Corollaire 1.3 (Grothendieck, page 41, images directes d'une somme ♦). *Soient D, D' des algèbres de Poincaré, E, E' des algèbres jaugées et $h : D \to E$, $h' : D' \to E'$ des homomorphismes. Pour les jauges produits, l'adjointe de $h \otimes h'$ est $h_* \otimes h'_*$. En particulier, si A est spéciale et $\alpha : I \to J$, l'image directe par $\alpha \sqcup \mathrm{id}_{\mathrm{pt}} : I \sqcup \mathrm{pt} \to J \sqcup \mathrm{pt}$, lue à travers les isomorphismes de Künneth, est $\alpha_* \otimes \mathrm{id}$; il en va de même de l'image inverse, $(\alpha \sqcup \mathrm{id})^* = \alpha^* \otimes \mathrm{id}$.*

Démonstration. Sur les tenseurs purs, $\kappa\big((y \otimes y')(h_* x \otimes h'_* x')\big) = \kappa_D(y\, h_* x)\, \kappa_{D'}(y'\, h'_* x') = \kappa_E(h(y)\, x)\, \kappa_{E'}(h'(y')\, x')$, et l'on conclut par bilinéarité et unicité de l'adjointe, $D \otimes D'$ étant de Poincaré. Dans l'objet spécial, $(\alpha \sqcup \mathrm{id})^*$ envoie $a \otimes b$ sur $\alpha^*(a) \otimes b$, parce que $(\alpha \sqcup \mathrm{id}) \circ \mathrm{incl}_I = \mathrm{incl}_J \circ \alpha$ et que le point ajouté va sur le point ajouté. Pour l'image directe, on accouple avec $w \in A(I) \otimes A(\mathrm{pt})$, ce qui est licite puisque $A(I \sqcup \mathrm{pt})$ est de Poincaré et que l'homomorphisme de Künneth est surjectif ; la formule de projection, la multiplicativité des jauges et l'identité $\kappa(\alpha^*(a)\, c) = \kappa(a\, \alpha_*(c))$ ramènent l'égalité aux tenseurs purs. □

Lean : `adj_tensor`, `SFun.sumPt`, `SFun.pull_sumPt`, `Special.gauge_kun`, `push_sumPt`. Le cas général $\alpha \sqcup \beta$ s'en déduit par récurrence, puisque toute somme $I' \sqcup I''$ s'obtient en ajoutant des points un à un ; cette récurrence, lourde dans le squelette, n'est pas écrite.

Contre-exemple 1.4 (l'objet constant, de l'édition ♦). *Soit P une algèbre de Poincaré différente de k (l'application $k \to P$ n'est pas surjective). L'objet constant $C : I \mapsto P$, où toutes les images inverses et directes sont l'identité et toutes les jauges κ, est une algèbre bivariante simpliciale de valeur P en un point. Elle n'est pas spéciale, et aucune transformation naturelle de $I \mapsto P^{\otimes I}$ vers C n'est surjective en un point. En particulier les deux objets ne sont pas isomorphes, bien qu'ils aient la même valeur, et l'isomorphisme $P^{\otimes \mathrm{pt}} \simeq P$ n'est la valeur d'aucune transformation naturelle : sans le mot « spéciale », l'énoncé des pages 37 et 41 est faux, et la plénitude ci-dessus demande que le but soit spécial.*

Démonstration. Il existe $a \in P$ avec $\kappa(1)\, a \neq \kappa(a) \cdot 1$: si $\kappa(1) \neq 0$, tout a hors de k convient ; sinon, la non-dégénérescence appliquée à $1 \neq 0$ donne a avec $\kappa(a) \neq 0$. L'homomorphisme de Künneth de C est la multiplication $P \otimes P \to P$, qui identifie $a \otimes 1$ et $1 \otimes a$; or $(\mathrm{id} \otimes \kappa)$ les sépare. Si φ est une transformation naturelle de $I \mapsto P^{\otimes I}$ vers C, la naturalité pour les deux points $0, 1$ de $\{0, 1\}$ donne $\iota_0 \circ \varphi^*_{\mathrm{pt}} = \varphi^*_{\{0,1\}} = \iota_1 \circ \varphi^*_{\mathrm{pt}}$; si φ^*_{pt} est surjective, $\iota_0(a) = \iota_1(a)$ dans $P \otimes P$, ce que contredit la forme linéaire $x_0 \otimes x_1 \mapsto \kappa(x_1)\, x_0$. □

Lean : `constFun`, `exists_ne_of_poincare`, `constFun_not_special`, `constFun_not_full` (espace de noms `Folder11.Simplicial`).

Remarques. La pleine fidélité ne demande que la spécialité du but : la source est une algèbre bivariante simpliciale quelconque. La catégorie des ensembles finis non vides est remplacée par son squelette, les ensembles $\{0, \ldots, n\}$, et la spécialité par la seule décomposition $I \sqcup \mathrm{pt}$, dont les autres se déduisent par récurrence. La condition $(\alpha \sqcup \beta)_* = \alpha_* \otimes \beta_*$ de la page 41 n'est pas dans la définition : les images directes étant déterminées par les images inverses, elle en découle (corollaire ci-dessous). La multiplicativité des jauges est une hypothèse de l'édition, que vérifie le modèle $H^*(X^I)$; sans elle, rien n'assure que $A(I)$ soit de Poincaré. Ne sont pas

formalisés : le cas gradué, avec les signes de Koszul des pages 28 et 30 ; et la seconde assertion de la page 41, ci-dessous.

Conjecture (Grothendieck, page 41, la classe de la diagonale)**.** *Le foncteur $A(\cdot) \mapsto (A(\mathrm{pt}), \Delta)$, avec $\Delta = \delta_*(1)$ de degré $d(A)$, est pleinement fidèle vers les algèbres jaugées munies d'un tel Δ.*

La page laisse « à préciser » les axiomes sur Δ ; la lecture les identifie aux identités en zigzag d'une algèbre de Frobenius. Faute d'axiomes écrits, l'énoncé n'est pas démontré ici. On se reportera aux notes de Grothendieck (11, lot 3, p. 41).

2 Cote 16 : le pseudo-inverse de l'opérateur de Lefschetz, la normalisation de $\mathfrak{sl}_2$ et les algèbres de Hodge [3]

La cote 16, *Formalisme algébrique des correspondances et algèbres de Poincaré-Hodge (cf conjectures standard) : notes manuscrites (s.d.), tapuscrit annoté (s.d.), lettres (1966-1967)*, compte cinquante-cinq pages datées « 1966-1967 ». Elle s'ouvre sur un cahier, « Sur certains anneaux gradués » (pages 2 à 17), qui cherche à quelles conditions l'opérateur Λ et les projecteurs de la décomposition primitive appartiennent à un anneau gradué $\mathcal{E}$ muni d'un L de degré 2. La page 9 fixe Λ par les relations (6.7) (16, lot 1, p. 9), que la page 13 reprend sous le numéro (6.15). La même page pose sur une algèbre extérieure le modèle $L_0 x = \xi_0 x$, $\Lambda_0 x = \xi_0^* \lrcorner\, x$, et écrit que « Λ_0 est l'opérateur associé défini par (6.15) » (16, lot 1, p. 13). Le dossier ne mentionne jamais $\mathfrak{sl}_2$. La lecture compare les deux normalisations de Λ ; cette comparaison, purement algébrique, est démontrée ici.

Conventions. Les relations (6.7) sont

$$L\Lambda = 1 - \sum_{0 \leqslant i \leqslant n} \pi_{i,0}, \qquad \Lambda L = 1 - \sum_{n \leqslant i \leqslant 2n} \pi_{i,0},$$

où $\pi_{i,0}$ est la projection de M^i sur sa partie primitive (pour $i \leqslant n$) ou sur le sommet de chaîne correspondant (pour $i \geqslant n$). Pour la normalisation de Hodge, on se donne un anneau commutatif R, une algèbre de Lie sur R contenant un triplet (H, Λ, L) tel que $[H, \Lambda] = 2\Lambda$, $[H, L] = -2L$ et $[\Lambda, L] = H$, et une représentation M ; on note Λy, Ly, Hy l'action. Un vecteur $x \neq 0$ est *primitif de poids* μ si $\Lambda x = 0$ et $Hx = \mu x$. Avec la convention $[L, \Lambda] = H$ de la lecture, une classe de degré i a pour poids $i - n$; on a pris ici l'opposé, de sorte qu'une classe primitive de degré i a pour poids $\mu = n - i$.

Énoncé (Page 9, la comparaison de la lecture)**.** *Le Λ de (6.7) n'est pas celui de la théorie de Hodge, qui agit sur $L^k P^i$ par des scalaires entiers non triviaux : sur une classe primitive x de degré i, on a $\Lambda L x = (n - i)\, x$, et non x.*

Énoncé (Énoncé de l'édition, le commutateur, d'après (6.7))**.** *Avec un Λ normalisé en pseudo-inverse par (6.7), le commutateur vaut*

$$[L, \Lambda] = \sum_{n \leqslant i \leqslant 2n} \pi_{i,0} - \sum_{0 \leqslant i \leqslant n} \pi_{i,0}$$

et ne retient que les extrémités des chaînes.

3. Preuve vérifiée : `lean/Grothendieck/Folder16.lean`.

Énoncé (Page 13, le modèle extérieur)**.** *Soient M_0 libre de base $e_1, \dots, e_{2n}$ sur R, $\xi_0 = \sum_{j=1}^{n} e_{2j-1} \wedge e_{2j}$ et $\xi_0^* = \sum_{j=1}^{n} e_{2j-1}^* \wedge e_{2j}^*$. Sur l'algèbre extérieure ΛM_0, $\Lambda_0 L_0(1) = \langle \xi_0^*, \xi_0 \rangle = n$, alors que (6.15) exige 1 ; l'identification des deux Λ_0 ne vaut donc que pour $n = 1$.*

Lemme 2.1. *Soit x un vecteur primitif de poids μ et $x_k = L^k x$. Pour tout $k \geqslant 0$,*

$$Hx_k = (\mu - 2k)\, x_k, \qquad \Lambda x_{k+1} = (k+1)(\mu - k)\, x_k;$$

en particulier $\Lambda L x = \mu x$.

Démonstration. La relation $[H, L] = -2L$ donne $H(Ly) = L(Hy) - 2Ly$ pour tout y, d'où la première formule par récurrence sur k, à partir de $Hx = \mu x$. La relation $[\Lambda, L] = H$ donne $\Lambda(Ly) = L(\Lambda y) + Hy$. Montrons par récurrence que $\Lambda x_k = k(\mu - k + 1)\, x_{k-1}$ pour $k \geqslant 1$, et $\Lambda x_0 = 0$. C'est vrai pour $k = 0$ par primitivité. Si c'est vrai pour k, alors

$$\Lambda x_{k+1} = L(\Lambda x_k) + Hx_k = \big(k(\mu - k + 1) + \mu - 2k\big)\, x_k = (k+1)(\mu - k)\, x_k.$$

Pour $k = 0$, c'est $\Lambda L x = \mu x$. □

Démonstration de la comparaison de la page 9. Pour une classe primitive x de degré i, de poids $\mu = n - i$, le lemme 2.1 donne $\Lambda L x = (n - i)\, x$ et, plus généralement, Λ agit sur $L^{k+1}x$ par l'entier $(k+1)(n-i-k)$. Supposons de plus R intègre, M sans torsion, et $\Lambda L x = x$, comme (6.7) le demande au bas d'une chaîne. Alors $(\mu - 1)\, x = \Lambda L x - x = 0$ avec $x \neq 0$, donc $\mu = 1$, c'est-à-dire $i = n - 1$. □

Démonstration de la formule du commutateur. Dans tout anneau où L et Λ vérifient (6.7), on soustrait les deux relations : $L\Lambda - \Lambda L = \sum_{n \leqslant i \leqslant 2n} \pi_{i,0} - \sum_{0 \leqslant i \leqslant n} \pi_{i,0}$. □

Démonstration de la formule du modèle extérieur. Notons ι_α la contraction par une forme linéaire α, antidérivation de ΛM_0 telle que $\iota_\alpha(v) = \alpha(v)$ pour $v \in M_0$, et convenons que la contraction par $\alpha \wedge \beta$ est $\iota_\beta \circ \iota_\alpha$. Alors $L_0(1) = \xi_0$ et

$$\Lambda_0 L_0(1) = \sum_{j,l=1}^{n} \iota_{e_{2j}^*}\, \iota_{e_{2j-1}^*}\big(e_{2l-1} \wedge e_{2l}\big).$$

On a $\iota_{e_{2j-1}^*}(e_{2l-1} \wedge e_{2l}) = e_{2j-1}^*(e_{2l-1})\, e_{2l} - e_{2j-1}^*(e_{2l})\, e_{2l-1} = \delta_{jl}\, e_{2l}$, puis $\iota_{e_{2j}^*}(\delta_{jl}\, e_{2l}) = \delta_{jl}$. La somme vaut donc n, c'est-à-dire $n \cdot 1 \in \Lambda^0 M_0 = R$. Si R est de caractéristique nulle et $n \neq 1$, $n \cdot 1 \neq 1$, et $\Lambda_0 L_0(1) \neq 1$. □

Remarque. Le Λ de $\mathfrak{sl}_2$ ne vérifie la relation $\Lambda L x = x$ de (6.7) que sur les classes primitives de degré $n - 1$; ailleurs les deux normalisations diffèrent d'un facteur entier. Le pseudo-inverse évite ce facteur, et le dossier peut ainsi rester sur $\mathbb{Z}$.

Remarque. Le calcul confirme la correction que la lecture apporte à la page 13 : la contraction $\xi_0^* \lrcorner -$ n'est pas l'opérateur que caractérisent les relations (6.15) dès que $n \geqslant 2$. L'erreur est sur la page ; elle est sans effet sur la Proposition qui suit, qui n'utilise que (6.15).

Le n° 4 remplace les conditions sur le module par la condition interne $(4.4)_i$ (16, lot 1, p. 6) ; le n° 5, écrit sur un feuillet « 5 bis », en tire que les π_i sont dans $\mathcal{E}$ (16, lot 1, p. 7) ; la page 8 spécialise à $v_i = L^{n-i}$ sous le numéro $(6.3)_i$ (16, lot 1, p. 8).

Conventions. On se donne un anneau E (le sur-anneau $\mathcal{F}$ de la lecture), une famille $(\pi_a)_{a\in\mathbb{Z}}$ d'idempotents orthogonaux de E, nuls hors de $[0,2n]$, de somme 1, et un sous-anneau $\mathcal{E}\subset E$. Un élément x est *homogène de degré* d si $\pi_b\,x\,\pi_a=0$ dès que $b\neq a+d$. Aucun module n'intervient, et $\mathcal{E}$ n'est qu'un anneau : tout se passe sur $\mathbb{Z}$.

Énoncé (Pages 6 à 8, les projecteurs de la graduation ♦). *Supposons que, pour tout $i\leqslant n$, il existe $v_i\in\mathcal{E}$ homogène de degré $2n-2i$ et $w_i\in\mathcal{E}$ homogène de degré $-(2n-2i)$ tels que $(w_iv_i-1)\,\pi_i=0$ et $(v_iw_i-1)\,\pi_{2n-i}=0$. Alors tous les π_a sont dans $\mathcal{E}$. En particulier, si $L\in\mathcal{E}$ est homogène de degré 2 et si L^{n-i} admet dans $\mathcal{E}$ des inverses w_i au sens de $(6.3)_i$, les π_a sont dans $\mathcal{E}$.*

Lemme 2.2. *Si x est homogène de degré d, alors $x\,\pi_a=\pi_{a+d}\,x\,\pi_a$ pour tout a. Si A et B sont des parties finies de $\mathbb{Z}$, $a_0\in A$, $a_0+d\in B$, et si a_0 est le seul $a\in A$ tel que $a+d\in B$, alors*

$$\Big(\sum_{b\in B}\pi_b\Big)\,x\Big(\sum_{a\in A}\pi_a\Big)=\pi_{a_0+d}\,x\,\pi_{a_0}.$$

Un produit d'homogènes de degrés d et e est homogène de degré $d+e$, et L^k est de degré $2k$ si L est de degré 2.

Démonstration. On écrit $x\,\pi_a=\big(\sum_b\pi_b\big)x\,\pi_a=\sum_b\pi_b\,x\,\pi_a$, où seul le terme $b=a+d$ subsiste (s'il sort de $[0,2n]$, $\pi_{a+d}=0$ et les deux membres sont nuls). Le second énoncé se développe en une double somme dont seul le terme (a_0+d,a_0) subsiste. Pour le produit, $\pi_b\,xy\,\pi_a=\pi_b\,x\,\pi_{a+e}\,y\,\pi_a$, nul si $b\neq a+e+d$; 1 est de degré 0 par orthogonalité, d'où les puissances par récurrence. □

Démonstration. Montrons par récurrence sur $i\leqslant n+1$ que $\pi_a\in\mathcal{E}$ dès que $a<i$ ou $a>2n-i$. Pour $i=0$, ces π_a sont nuls. Supposons-le pour un $i\leqslant n$. Alors

$$\varphi_i=\sum_{i\leqslant a\leqslant 2n}\pi_a=1-\sum_{0\leqslant a<i}\pi_a,\qquad \psi_{2n-i}=\sum_{0\leqslant a\leqslant 2n-i}\pi_a=1-\sum_{2n-i<a\leqslant 2n}\pi_a$$

sont dans $\mathcal{E}$. Le lemme 2.2, appliqué à v_i (le seul $a\geqslant i$ tel que $a+2n-2i\leqslant 2n-i$ est $a=i$) puis à w_i, donne

$$v_i'=\psi_{2n-i}\,v_i\,\varphi_i=\pi_{2n-i}\,v_i\,\pi_i\in\mathcal{E},\qquad w_i'=\varphi_i\,w_i\,\psi_{2n-i}=\pi_i\,w_i\,\pi_{2n-i}\in\mathcal{E}.$$

Comme $\pi_{2n-i}\,v_i\,\pi_i=v_i\,\pi_i$ et $\pi_i\,w_i\,\pi_{2n-i}=w_i\,\pi_{2n-i}$ (même lemme),

$$w_i'v_i'=\pi_i\,w_i\,\pi_{2n-i}^2\,v_i\,\pi_i=\pi_i\,(w_iv_i\pi_i)=\pi_i^2=\pi_i,\qquad v_i'w_i'=\pi_{2n-i}\,(v_iw_i\pi_{2n-i})=\pi_{2n-i},$$

donc π_i et π_{2n-i} sont dans $\mathcal{E}$, ce qui est l'hypothèse au rang $i+1$. Au rang $n+1$, tout a vérifie $a<n+1$ ou $a>n-1$. Le cas $v_i=L^{n-i}$ suit, L^{n-i} étant dans $\mathcal{E}$ et de degré $2n-2i$. □

Remarque. L'argument de la page 7 vaut tel qu'il est écrit, sans hypothèse de réalisation : il suffit que $\mathcal{E}$ soit un sous-anneau et que les π_i existent dans le sur-anneau. Cela démontre la première partie de la piste, l'appartenance des projecteurs de la graduation. Celle de Λ et des projecteurs primitifs $\pi_{i,\alpha}$ n'est pas démontrée ici. Les formules des pages 10 à 12 les écrivent comme produits d'éléments de $\mathcal{E}$, et leur appartenance est immédiate ; il resterait à vérifier qu'elles satisfont (6.7) et donnent les projecteurs de la décomposition primitive, ce qui demande la décomposition elle-même.

La lecture garde $\Phi_0 = \mathbb{Z}[L_0, \Lambda_0] \subset \mathrm{End}(\Lambda M_0)$, avec M_0 un $\mathbb{Z}$-module libre et Λ_0 *au sens de (6.15)*, pour réparer l'identification de la page 13. Sur $\mathbb{Z}$, ce Λ_0 n'existe pas.

Contre-exemple 2.3 (Page 13, sur $\mathbb{Z}$ ♦). *Soient $M_0 = \mathbb{Z}^{2n}$, $n \geqslant 2$, $\xi_0 = \sum_{k=1}^{n} e_{2k-1} \wedge e_{2k}$ et $\mathrm{vol} = e_1 \wedge \cdots \wedge e_{2n}$. Il n'existe aucun $y \in \Lambda M_0$ tel que $\xi_0^n \wedge y = \mathrm{vol}$. En particulier, pour toute application w de ΛM_0 dans lui-même, $L_0^n\big(w(\mathrm{vol})\big) \neq \mathrm{vol}$: la condition $(6.3)_0$ est fausse dans le modèle extérieur sur $\mathbb{Z}$.*

Démonstration. Posons $a_k = e_{2k-1} \wedge e_{2k}$. Deux produits de deux vecteurs commutent dans ΛM_0 (chaque vecteur traverse l'autre paire avec deux changements de signe), et $a_k \wedge a_k = 0$. Par récurrence sur le nombre de termes, $\xi_0 \wedge \xi_0 = c + c$ pour un $c \in \Lambda M_0$: si S est une somme partielle avec $S \wedge S = c + c$, alors $(a+S)^2 = a^2 + aS + Sa + S^2 = (aS + c) + (aS + c)$. Donc $\xi_0^n \wedge y = \xi_0^{n-2} \wedge (c + c) \wedge y = z + z$ avec $z = \xi_0^{n-2} c\, y$. Soit ϕ la forme linéaire sur ΛM_0 qui prend la composante de degré $2n$ et la lit sur la base vol de $\Lambda^{2n} M_0$; $\phi(\mathrm{vol}) = 1$. Si $\xi_0^n \wedge y = \mathrm{vol}$, alors $1 = \phi(z + z) = 2\,\phi(z)$ dans $\mathbb{Z}$, ce qui est impossible. Enfin $L_0^n(x) = \xi_0^n \wedge x$, et l'on prend $y = w(\mathrm{vol})$. □

Remarque. En fait $\xi_0^n = n!\,\mathrm{vol}$, et $L_0^n \colon \Lambda^0 M_0 \to \Lambda^{2n} M_0$ est la multiplication par $n!$; seule la parité est démontrée ici, et elle suffit. D'après la Remarque de la page 12, un Λ_0 vérifiant (6.15) donne $(L_0^n \Lambda_0^n - 1)\,\pi_{2n} = 0$, c'est-à-dire $L_0^n(\Lambda_0^n\,\mathrm{vol}) = \mathrm{vol}$, ce que l'énoncé exclut. Pour $n \geqslant 2$, l'anneau $\Phi_0 = \mathbb{Z}[L_0, \Lambda_0]$ de la lecture ne peut donc pas être pris dans $\mathrm{End}_{\mathbb{Z}}(\Lambda M_0)$, et la décomposition primitive y fait défaut. Pour $n = 2$, $e_1 \wedge e_2 \wedge \xi_0 = \mathrm{vol}$ et $\xi_0 \wedge \xi_0 = 2\,\mathrm{vol}$, de sorte que la composante de $e_1 \wedge e_2$ sur $\mathbb{Q}\,\xi_0$ le long de P^2 vaut $\frac{1}{2}\,\xi_0$ (calcul fait à la main). L'obstacle disparaît sur $\mathbb{Q}$. La correction que la lecture apporte à la page 13 vaut pour l'identification des deux Λ_0, mais le choix de $\mathbb{Z}$ comme anneau de base du modèle ne convient pas.

Lemme 2.4 (Pages 14 et 15, l'étape algébrique de l'unicité). *Dans un anneau, si $\Lambda L \Lambda = \Lambda$, $\Lambda' L \Lambda' = \Lambda'$, $\Lambda L = \Lambda' L$ et $L\Lambda = L\Lambda'$, alors $\Lambda = \Lambda'$.*

Démonstration. $\Lambda = (\Lambda L)\Lambda = \Lambda'(L\Lambda) = \Lambda'(L\Lambda') = \Lambda'$. □

Le lemme 2.4 dit qu'un pseudo-inverse est déterminé par les deux idempotents ΛL et $L\Lambda$; ni l'existence de l'homomorphisme $\Phi_0 \to \mathcal{E}$ ni son unicité ne sont démontrées ici.

Les pages 24 à 28, sous le titre « Algèbres de Hodge d'ordre 2 » (16, lot 2, p. 24), dégagent l'ossature d'un anneau de cohomologie de surface à partir de trois données ; la page 26 la reformule en faisant de la polarisation un paramètre (16, lot 2, p. 26).
Conventions. Soient k un anneau commutatif, V et W des k-modules, $\check{V} = \mathrm{Hom}_k(V, k)$, φ une forme bilinéaire alternée sur V, $\psi \colon V \times V \to W$ bilinéaire alternée (c'est-à-dire $\psi \colon \Lambda^2 V \to W$) et Q une forme bilinéaire symétrique sur W. Soit $A = k \oplus V \oplus (k\xi \oplus W) \oplus \check{V} \oplus k\xi^2$, de composantes $H^0, \ldots, H^4$, muni du produit de la page 24 : 1 est unité ; $xy = \varphi(x,y)\,\xi + \psi(x,y)$ pour $x, y \in V$; $x(c\xi + w) = (c\xi + w)x$ est la forme $t \mapsto c\,\varphi(t,x) + Q(\psi(t,x), w)$, soit $x\xi = \tilde{\varphi}(x)$ et $xw = \rho(w,x)$ dans les notations de la page ; $xy' = -y'x = y'(x)\,\xi^2$ pour $y' \in \check{V}$; $\xi \cdot \xi = \xi^2$, $\xi w = w\xi = 0$ et $ww' = Q(w,w')\,\xi^2$; les produits de degré total supérieur à 4 sont nuls, et l'on étend par bilinéarité. Un élément est *pair* s'il est dans $H^0 \oplus H^2 \oplus H^4$, *impair* s'il est dans $H^1 \oplus H^3$. On pose

$$\chi(x,y,z,t) = \varphi(x,y)\,\varphi(z,t) + Q\big(\psi(x,y), \psi(z,t)\big),$$

de sorte que $(xy)(zt) = \chi(x,y,z,t)\,\xi^2$; $\chi(x,y,z,t) = \chi(z,t,x,y)$ par symétrie de Q, et χ change de signe quand on échange x et y, ou z et t.

Théorème 2.5 (Grothendieck, pages 24 à 28, algèbres de Hodge d'ordre 2 ♦). *1. Quels que soient φ, ψ, Q, le produit est bilinéaire, admet 1 pour unité et est anti-commutatif au sens gradué : les éléments pairs sont centraux, deux éléments impairs anticommutent, et le carré d'un élément impair est nul. Le produit $H^1 \times H^2 \to H^3$ est le seul pour lequel $t(xh) = (tx)h$ quels que soient $t, x \in V$ et $h \in H^2$.*

2. *Le produit est associatif si et seulement si, pour tous $x, y, z, t \in V$,*

$$\varphi(x,y)\varphi(t,z) + Q\big(\psi(x,y),\psi(t,z)\big) = \varphi(t,x)\varphi(y,z) + Q\big(\psi(t,x),\psi(y,z)\big).$$

3. *Si k est un corps et V de dimension finie, $\xi^2 \colon H^0 \to H^4$ est toujours un isomorphisme, et $\xi \colon H^1 \to H^3$ en est un si et seulement si φ est non dégénérée : la condition de Lefschetz équivaut à la non-dégénérescence de φ.*
4. *Si k est un corps, les accouplements $H^0 \times H^4 \to H^4$ et $H^1 \times H^3 \to H^4$ sont toujours non dégénérés, et $H^2 \times H^2 \to H^4$ l'est si et seulement si Q l'est : la condition de Poincaré équivaut à la non-dégénérescence de Q.*

Démonstration. (1) Chaque composante du produit est bilinéaire, et l'unité se lit sur la définition. Si a est pair, les seuls termes de ab où l'ordre compte sont $Q(w,w')$, symétrique, et les produits xh et hx, égaux par définition. Si $a = x + y'$ et $b = z + u'$ sont impairs, $ab = \varphi(x,z)\,\xi + \psi(x,z) + \big(u'(x) - y'(z)\big)\xi^2$, qui change de signe quand on échange a et b, φ et ψ étant alternées, et qui s'annule pour $a = b$. Enfin $t(xh) = (xh)(t)\,\xi^2$, et pour $h = c\xi + w$,

$$(tx)h = \big(\varphi(t,x)\,\xi + \psi(t,x)\big)(c\xi + w) = \big(c\,\varphi(t,x) + Q(\psi(t,x),w)\big)\xi^2;$$

l'égalité pour tout t détermine la forme xh, qui est celle de la définition.

(2) Par bilinéarité, il suffit de vérifier l'associativité sur des éléments homogènes. Les triples où figure un élément de H^0 sont associatifs par l'unité, et ceux de degré total supérieur à 4 donnent 0 des deux côtés. Restent le triple $H^1 \times H^1 \times H^1$, à valeurs dans H^3, et les trois triples formés de deux éléments de V et d'un de H^2, à valeurs dans H^4. Ces derniers sont associatifs quelles que soient les données : pour $t, x \in V$ et $h \in H^2$, $t(xh) = (tx)h$ par (1) ; $(xh)t = -t(xh) = -(tx)h = (xt)h$, puisque $tx = -xt$; $x(ht) = x(th) = (xt)h$; et $(hx)t = (xh)t$, $h(xt) = (xt)h$ par symétrie de Q. Pour $x, y, z \in V$, $(xy)z$ et $x(yz)$ sont des formes sur V, que l'on évalue en t par (1) : $\langle t, (xy)z\rangle = \langle t, z(xy)\rangle = \chi(t,z,x,y)$ et $\langle t, x(yz)\rangle = \chi(t,x,y,z)$. L'associativité équivaut donc à $\chi(t,z,x,y) = \chi(t,x,y,z)$ pour tous x, y, z, t ; comme $\chi(t,z,x,y) = \chi(x,y,t,z)$, c'est l'identité de l'énoncé.

(3) On a $\xi^2 \cdot c = c\,\xi^2$, et $\xi x = x\xi = \tilde{\varphi}(x)$ est la forme $t \mapsto \varphi(t,x)$. L'application linéaire $\tilde{\varphi} \colon V \to \check{V}$ est injective si et seulement si φ sépare à droite, ce qui, φ étant antisymétrique, revient à la non-dégénérescence. Comme $\dim \check{V} = \dim V$, injective équivaut à bijective.

(4) On a $c \cdot d\xi^2 = cd\,\xi^2$ et $x \cdot y' = y'(x)\,\xi^2$; sur un corps, un vecteur annulé par toutes les formes linéaires est nul, sans hypothèse de dimension, et une forme nulle sur tout V est nulle. Enfin $(c\xi + w)(c'\xi + w') = \big(cc' + Q(w,w')\big)\xi^2$. Si Q est non dégénérée et si $cc' + Q(w,w') = 0$ pour tous c' et w', le choix $c' = 1$, $w' = 0$ donne $c = 0$, puis $Q(w,w') = 0$ pour tout w' donne $w = 0$. Inversement, si l'accouplement est non dégénéré, un w tel que $Q(w,\cdot) = 0$ est orthogonal à tout H^2, donc nul. Les deux formes étant symétriques, séparer d'un côté suffit. □

Énoncé (Page 26, la forme χ et la reformulation). *1. Pour tous $x, y, z, t \in V$, $((xy)z)t = \chi(x,y,z,t)\,\xi^2$, que le produit soit associatif ou non.*

2. *L'identité d'associativité équivaut à $\chi(x,y,y,t) = 0$ pour tous x, y, t, et entraîne que χ s'annule dès que deux de ses arguments sont égaux : la forme χ est alternée.*
3. *Soient k un corps, V de dimension finie, $\tilde{W}$ un k-espace muni d'une forme bilinéaire symétrique $\tilde{Q}$, $\alpha\colon \Lambda^2 V \to \tilde{W}$ linéaire et $\xi \in \tilde{W}$ tel que $\tilde{Q}(\xi,\xi) = 1$. Posons $W = \xi^\perp$, $\varphi(x,y) = \tilde{Q}(\alpha(x\wedge y),\xi)$, $\psi = \alpha - \varphi\,\xi$ et $Q = \tilde{Q}|_W$. Alors ψ est à valeurs dans W, $\alpha = \varphi\,\xi + \psi$ et $\tilde{Q}(\alpha(x\wedge y),\alpha(z\wedge t)) = \chi(x,y,z,t)$. L'algèbre de Hodge de (φ,ψ,Q) est associative si et seulement si $\tilde{Q}(\alpha(x\wedge y),\alpha(y\wedge t)) = 0$ pour tous x, y, t ; elle vérifie la condition de Lefschetz si et seulement si φ est non dégénérée, et la condition de Poincaré si et seulement si $\tilde{Q}$ est non dégénérée.*

Démonstration. (1) Par (1) du théorème 2.5, $(xy)z = z(xy)$ est la forme $s \mapsto \chi(s,z,x,y)$, donc $((xy)z)t = -t((xy)z) = -\chi(t,z,x,y)\,\xi^2 = \chi(z,t,x,y)\,\xi^2 = \chi(x,y,z,t)\,\xi^2$.

(2) Écrivons l'identité $\chi(x,y,t,z) = \chi(t,x,y,z)$. Pour $z = y$, elle donne $\chi(x,y,t,y) = \chi(t,x,y,y) = 0$, d'où $\chi(x,y,y,t) = -\chi(x,y,t,y) = 0$. Pour $t = x$, elle donne $\chi(x,y,x,z) = \chi(x,x,y,z) = 0$, d'où aussi $\chi(x,y,z,x) = 0$; avec (t,z) remplacé par (z,y), elle donne $\chi(x,y,z,y) = \chi(z,x,y,y) = 0$. Les cas $\chi(x,x,z,t)$ et $\chi(x,y,z,z)$ sont nuls par alternance de φ et ψ. Réciproquement, si $\chi(x,y,y,t) = 0$ pour tous x, y, t, le développement de $\chi(x, y+z, y+z, t) = 0$ donne $\chi(x,y,z,t) = -\chi(x,z,y,t)$, et alors

$$\chi(x,y,t,z) = -\chi(x,t,y,z) = \chi(t,x,y,z).$$

(3) $\tilde{Q}\big(\xi, \alpha - \tilde{Q}(\xi,\alpha)\,\xi\big) = \tilde{Q}(\xi,\alpha)\big(1 - \tilde{Q}(\xi,\xi)\big) = 0$, donc ψ est à valeurs dans W, et $\alpha = \varphi\,\xi + \psi$ par définition. Comme $\psi(x,y)$ et $\psi(z,t)$ sont orthogonaux à ξ et $\tilde{Q}(\xi,\xi) = 1$, le développement de $\tilde{Q}(\varphi(x,y)\,\xi + \psi(x,y), \varphi(z,t)\,\xi + \psi(z,t))$ donne $\chi(x,y,z,t)$. L'associativité suit alors de (2) du théorème et de (2) ci-dessus, la condition de Lefschetz de (3). Pour la condition de Poincaré, il reste par (4) à voir que $\tilde{Q}$ est non dégénérée si et seulement si Q l'est. Tout $v \in \tilde{W}$ s'écrit $v = \tilde{Q}(\xi,v)\,\xi + v'$ avec $v' = v - \tilde{Q}(\xi,v)\,\xi \in W$. Si $w \in W$ est orthogonal à W, alors $\tilde{Q}(w,v) = \tilde{Q}(\xi,v)\,\tilde{Q}(w,\xi) + \tilde{Q}(w,v') = 0$ pour tout v, et $w = 0$ si $\tilde{Q}$ est non dégénérée. Si $v \in \tilde{W}$ est orthogonal à $\tilde{W}$, alors $\tilde{Q}(\xi,v) = 0$, donc $v \in W$ est orthogonal à W, et $v = 0$ si Q est non dégénérée. □

Remarque. Les énoncés tiennent tels que la page les écrit, et la formalisation dit d'où vient chacun. L'associativité ne contraint que le triple $H^1 \times H^1 \times H^1$: les autres sont associatifs parce que la dualité impose le produit $H^1 \times H^2 \to H^3$. C'est le sens précis de la phrase de la page selon laquelle V, W, φ, ψ, Q permettent de « reconstituer H^* à isom. canonique près ». La construction et l'associativité valent sur tout anneau commutatif. Seule la condition de Lefschetz demande que V soit de dimension finie, pour passer de l'injectivité de $\tilde{\varphi}$ à sa bijectivité ; la condition de Poincaré n'en demande aucune. L'identité d'associativité est exactement l'alternance de la forme χ que la page 26 dit alternée ; la note marginale de la page 24, en partie illisible, rattache déjà l'identité à la forme $xyzt$. Dans la reformulation, c'est $\tilde{Q}(\xi,\xi) = 1$ qui scinde $\tilde{W}$ en somme orthogonale $k\xi \oplus \xi^\perp$ et rend équivalentes les non-dégénérescences de $\tilde{Q}$ et de Q.

Remarque. Le modèle de ces algèbres est la cohomologie rationnelle d'une surface kählérienne compacte X, ou d'une surface projective lisse en cohomologie ℓ-adique, avec ξ la classe d'une polarisation normalisée par $\int_X \xi^2 = 1$: $V = H^1$, W est la partie primitive $\xi^\perp$ de H^2, $\varphi(x,y) = \int_X \xi xy$ et $Q(w,w') = \int_X ww'$. La condition de Lefschetz du théorème 2.5 est alors le théorème de Lefschetz difficile en degré 1, et la condition de Poincaré la dualité de Poincaré en degré 2 ; sur $\mathbf{R}$, les relations bilinéaires de Hodge–Riemann fixent en outre la signature de Q selon les

types de Hodge, donnée que l'algèbre abstraite ne retient pas. Ce dictionnaire est de l'édition. La preuve vérifiée établit le théorème 2.5 et l'énoncé de la page 26 pour des données (φ, ψ, Q) quelconques, sur tout anneau commutatif pour la construction et l'associativité, sur un corps pour les deux non-dégénérescences ; elle ne parle ni de surfaces ni de cohomologie. Les périodes et les structures de Hodge de la même époque sont dans la partie « Théorie de Hodge » (cotes 13 et 18), la borne de poids et de niveau de la cote 12 dans la partie « Motifs ».

La lettre datée de sa main « 6.1.1966 », sans doute par lapsus pour janvier 1967 puisqu'elle suit celle du « 4.1.67 » (16, lot 3, p. 43), montre que $C(X)$ suit de $D(X)$ et de l'existence d'isomorphismes algébriques $H^{2n-i}(X) \to H^i(X)$ quelconques (16, lot 3, p. 47).
Conventions. Soient K un corps ($\mathbb{Q}_\ell$), $F \subset K$ un sous-corps ($\mathbb{Q}$), $V = H^i(X)$ et $W = H^{2n-i}(X)$ des K-espaces, V de dimension finie. « Algébrique » est lu comme l'appartenance à des ensembles donnés d'applications : un sous-anneau $\mathcal{A}_V$ de $\mathrm{End}_K(V)$, stable par multiplication par les éléments de F, et des parties $\mathcal{A}_{WV}$ de $\mathrm{Hom}(W, V)$ et $\mathcal{A}_{VW}$ de $\mathrm{Hom}(V, W)$, telles que $g \circ h \in \mathcal{A}_{WV}$ pour $g \in \mathcal{A}_V$, $h \in \mathcal{A}_{WV}$, et $h \circ k \in \mathcal{A}_V$ pour $h \in \mathcal{A}_{WV}$, $k \in \mathcal{A}_{VW}$. L'hypothèse $D(X)$ est lue comme : les coefficients du polynôme caractéristique de tout $g \in \mathcal{A}_V$ sont dans F.

Théorème 2.6 (Grothendieck, pages 47 et 48, *proposition*, b) $\Rightarrow C$ ♦). *Si $u \in \mathcal{A}_{WV}$ est un isomorphisme quelconque et si $v \in \mathcal{A}_{VW}$ (l'application induite par L^{n-i}) est un isomorphisme, alors il existe $v' \in \mathcal{A}_{WV}$ avec $v' \circ v = \mathrm{id}_V$ et $v \circ v' = \mathrm{id}_W$: l'inverse de L^{n-i} est algébrique.*

Lemme 2.7 (Cayley–Hamilton). *Si $w \in \mathcal{A}_V$ est inversible, son inverse est dans $\mathcal{A}_V$.*

Démonstration. Le polynôme caractéristique P de w est à coefficients dans F par l'hypothèse $D(X)$, et il annule w par Cayley–Hamilton. Son terme constant c_0 est, au signe près, le déterminant de w ; il n'est pas nul. Écrivons $P = XQ + c_0$. Alors $Q(w)\, w = w\, Q(w) = -c_0$, et $w^{-1} = -c_0^{-1} Q(w)$. Cet élément est dans $\mathcal{A}_V$, qui est un sous-anneau stable par multiplication par F, puisque Q est à coefficients dans F. □

Démonstration. $w = u \circ v$ est dans $\mathcal{A}_V$, et inversible comme composé de deux bijections. Le lemme 2.7 donne $g \in \mathcal{A}_V$ avec $g \circ w = \mathrm{id}_V$; on pose $v' = g \circ u \in \mathcal{A}_{WV}$. Alors $v' \circ v = g \circ w = \mathrm{id}_V$, et pour $y = v(x)$, $v(v'(y)) = v\big((v' \circ v)(x)\big) = y$: v' est aussi inverse à droite, v étant surjective. □

Remarque. L'argument de la lettre vaut tel quel, avec la relation de Cayley–Hamilton écrite en $w = uv$, comme la lecture la rétablit ; le tapuscrit l'écrit en u avec les coefficients de w. L'hypothèse que u soit un isomorphisme sert seulement à rendre w inversible. Que v, induit par L^{n-i}, en soit un aussi est l'axiome de Lefschetz de la cohomologie, que la lettre suppose.

Ne sont pas démontrés ici : le théorème de Lefschetz difficile par $\mathfrak{sl}_2$ et la représentation de $\mathfrak{sl}_2$ engendrée par (L_0, Λ_0) ; dans le théorème du n° 6, l'existence de la décomposition primitive et la réciproque (2) $\Rightarrow$ (1) (pages 9 à 12), la réciproque (3) $\Rightarrow$ (1) étant réfutée pour l'inverse de L ; l'existence et l'unicité de l'homomorphisme $\Phi_0 \to \mathcal{E}$ et le corollaire de la page 16 ♦ ; le contre-exemple de la page 21 ; dans les algèbres de Hodge, l'exemple $\chi = \varphi^2$ de la page 28 et la question, restée sans réponse, de la finitude d'une orbite sous u ; les pages 2 à 5, 29 à 46 et 48 à 54, dont les sections hyperplanes, le corollaire de la page 48, les variantes de la page 49 et le lemme.
Conventions. On lit la décomposition primitive dans l'anneau E lui-même, sans module : $p_{j,\beta}$ est le projecteur sur $L^\beta P^j \subset M^{j+2\beta}$, pour $0 \leqslant j \leqslant n$ et $0 \leqslant \beta \leqslant n - j$, de sorte que le $\pi_{i,\alpha}$ de la lecture est $p_{i-2\alpha,\alpha}$ si $i \leqslant n$, et que $\pi_{2n-i,\alpha}$ est $p_{i-2\alpha,\, n-i+\alpha}$. On demande : les $p_{j,\beta}$ sont des idempotents orthogonaux de somme 1 ; $\pi_a p_{j,\beta} = p_{j,\beta} \pi_a$ vaut $p_{j,\beta}$ si $a = j + 2\beta$ et 0 sinon ;

$Lp_{j,\beta} = p_{j,\beta+1}L$ pour $\beta < n-j$ et $Lp_{j,n-j} = 0$; enfin $p_{j,\beta} \in L^\beta p_{j,0} E$, ce qui dit que l'image est $L^\beta P^j$ et non un supplémentaire quelconque. C'est la décomposition que le dossier « admet » (structure `DecompositionPrimitive`).

Théorème 2.8 (Grothendieck, pages 4 à 17, critère de Lefschetz dans un anneau gradué ♦). *Soient E un anneau gradué par des idempotents orthogonaux π_a de somme 1 ($0 \leqslant a \leqslant 2n$), $\mathcal{E} \subset E$ un sous-anneau, $L \in \mathcal{E}$ de degré 2, et, pour $i \leqslant n$, $w_i \in \mathcal{E}$ de degré $-(2n-2i)$ avec $(w_i L^{n-i} - 1)\pi_i = 0$ et $(L^{n-i} w_i - 1)\pi_{2n-i} = 0$, c'est-à-dire $(6.3)_i$. Alors, sans module sous-jacent et sur* **Z** *:*

1. *les projecteurs π_a de la graduation sont dans $\mathcal{E}$;*
2. *tous les projecteurs $p_{j,\beta}$ de la décomposition primitive sont dans $\mathcal{E}$;*
3. *$\Lambda = \sum_j \sum_{\beta<n-j} L^\beta w_j L^{n-j-\beta-1} p_{j,\beta+1}$ est dans $\mathcal{E}$, de degré -2, et vérifie (6.7) : $L\Lambda = 1 - \sum_j p_{j,0}$ et $\Lambda L = 1 - \sum_j p_{j,n-j}$.*

Démonstration de la page (pages 4 à 12). Le n° 4 remplace les conditions portant sur un module par la condition interne $(4.4)_i$ (pp. 4 à 6) ; le n° 5, sur le feuillet « 5 bis » (p. 7), en tire $\pi_i \in \mathcal{E}$ par $v_i' = \pi_{2n-i} v_i \pi_i$ et $w_i' = \pi_i w_i \pi_{2n-i}$, dont les produits sont π_i et π_{2n-i}. Le n° 6 prend $v_i = L^{n-i}$ et obtient les $\pi_{i,\alpha}$ et $\pi_{2n-i,\alpha}$ par une double récurrence descendante, formules (6.9) et (6.10) (p. 11), puis Λ par (6.11) à (6.13) (pp. 11 et 12) ; la décomposition primitive y est admise. La liste d'énoncés de la page 9 est biffée et renumérotée, et l'implication marquée « Démonstration à fournir » (p. 12) est hors des clauses encadrées.

◊ non vérifiée en Lean

Démonstration. (1) est le n° 5 (`projecteurs_mem`, `projecteurs_mem_lefschetz`). Tout le reste repose sur un calcul de bloc : pour $\beta \leqslant n-j$,

$$L^\beta \, w_j \, L^{n-j-\beta} \, p_{j,\beta} = p_{j,\beta}.$$

En effet $p_{j,\beta} = L^\beta p_{j,0}\, y$, donc $L^{n-j-\beta} p_{j,\beta} = L^{n-j} \pi_j \, p_{j,0}\, y$, puis $w_j L^{n-j} \pi_j = \pi_j$ ramène à $p_{j,0}\, y$, et L^β redonne $p_{j,\beta}$ (`inverse_bloc`). Par ailleurs $L^k p_{j,\beta}$ vaut $p_{j,\beta+k} L^k$ tant que $\beta + k \leqslant n-j$ et 0 au-delà (`pow_mul_of_le`, `pow_mul_eq_zero`) ; en particulier $L^{n-j+1} p_{j,0} = 0$, les $p_{j,0}$ projettent sur des classes primitives.

(2) Récurrence sur le degré primitif j, qui est la récurrence descendante du dossier sur α. Si $a = j + 2\beta \leqslant n$, posons $S_j = \sum_{j'<j} \sum_{\beta'} p_{j',\beta'}$, dans $\mathcal{E}$ par récurrence. Dans $\pi_a(1 - S_j)$ ne restent que les blocs de degré a et de degré primitif $j' \geqslant j$; pour $j' > j$, l'exposant $n - j - \beta$ dépasse la longueur restante de la chaîne et $L^{n-j-\beta}$ les tue. Le calcul de bloc donne alors la formule (6.9)

$$p_{j,\beta} = L^\beta \, w_j \, L^{n-j-\beta} \, \pi_a \, (1 - S_j) \in \mathcal{E} \qquad (\texttt{formule_bas}).$$

Si $a \geqslant n$, soit $i = 2n - a = j + 2\beta''$ avec $\beta'' = n - j - \beta$; alors $L^{a-n} p_{j,\beta''} = p_{j,\beta} L^{a-n}$ et $L^{a-n} w_i \pi_a = \pi_a$, d'où la formule (6.10)

$$p_{j,\beta} = L^{a-n} \, p_{j,\beta''} \, w_i \, \pi_a \in \mathcal{E} \qquad (\texttt{formule_haut}),$$

avec $p_{j,\beta''}$ déjà obtenu, puisque $i \leqslant n$ (`projecteurs_primitifs_mem`).

(3) Chaque terme de Λ est un produit d'éléments de $\mathcal{E}$, de degré $2\beta - 2(n-j) + 2(n - j - \beta - 1) = -2$ (`homogene_pseudoInverse`). Par le calcul de bloc, $L \cdot L^\beta w_j L^{n-j-\beta-1} p_{j,\beta+1} = p_{j,\beta+1}$: $L\Lambda$ est la somme des blocs qui ne sont pas en bas de chaîne, soit $1 - \sum_j p_{j,0}$ (`mul_`

`pseudoInverse`). De même $p_{j,\beta+1}L = Lp_{j,\beta}$ donne $L^\beta w_j L^{n-j-\beta-1} p_{j,\beta+1} L = p_{j,\beta}$ pour $\beta < n-j$: ΛL est la somme des blocs qui ne sont pas en haut de chaîne, soit $1 - \sum_j p_{j,n-j}$ (`pseudoInverse_mul`). Le tout est rassemblé dans `critere_lefschetz`. □

Remarque. L'énoncé tient sur **Z** et pour un sous-anneau quelconque, sans module, et sans que les relations $(L^{n-i}w_i - 1)\pi_{2n-i} = 0$ servent au-delà du n° 5 et de la formule (6.10). La récurrence double du dossier se réduit à une récurrence simple, une fois les π_a connus. Pour Λ sur un bloc du bas, la formule affichée par la lecture, $\Lambda\pi_{i,\alpha} = w_{i-2\alpha}L^{n-i+\alpha}\pi_{i,\alpha}$, est de degré -2α et non -2 : il y manque un facteur $L^{\alpha-1}$ à gauche, et la forme juste est $\Lambda\pi_{i,\alpha} = L^{\alpha-1}w_{i-2\alpha}L^{n-i+\alpha}\pi_{i,\alpha}$, qui coïncide avec celle de la lecture pour $\alpha = 1$; la formule pour les blocs du haut est juste telle quelle. Ne sont pas démontrés : l'existence de la décomposition primitive à partir de (6.3), que le dossier admet ; la réciproque (2) ⇒ (1) du théorème de la page 9 ; la caractérisation de la *Remarque* en L et Λ seuls ($\pi_{i,\alpha} = L^\alpha \Lambda^{n-i+2\alpha} L^{n-i+\alpha}(\cdots)$). La réciproque (3) ⇒ (1) est traitée ci-dessous.

La page 9 annonce aussi la réciproque (3) ⇒ (1) : si tous les projecteurs $\pi_{i,\alpha}$ de la décomposition primitive sont dans $\mathcal{E}$, les conditions de Lefschetz $(6.1)_i$ et $(6.2)_i$ valent, l'inverse de L^{n-i} étant dans $\mathcal{E}$, et les π_i sont dans $\mathcal{E}$. La page 12 marque une implication « Démonstration à fournir ». De celle-ci, seule la moitié qui porte sur les projecteurs tient.

Énoncé (Page 9, (3) ⇒ (1), les projecteurs ♦). *Avec les conventions précédentes, si tous les $p_{j,\beta}$ sont dans le sous-anneau $\mathcal{E}$, tous les π_a y sont aussi.*

Démonstration. On a $\pi_a = \pi_a \sum_{j,\beta} p_{j,\beta} = \sum_{j+2\beta=a} p_{j,\beta}$, puisque $\pi_a p_{j,\beta}$ vaut $p_{j,\beta}$ si $a = j + 2\beta$ et 0 sinon (`DecompositionPrimitive.proj_eq_sum`, `projecteurs_mem_of_primitifs`). □

Contre-exemple 2.9 (page 9, (3) n'entraîne ni (1) ni (2) ♦). *Soient R un anneau commutatif non nul (**Z** par exemple), $E = M_2(R)$ et $n = 1$, avec $M^0 = Re_1$, $M^1 = 0$, $M^2 = Re_2$, soit $\pi_0 = e_{11}$, $\pi_2 = e_{22}$, $\pi_1 = 0$, et $L = e_{21}$, de degré 2. La décomposition primitive est $P^0 = Re_1$, $LP^0 = Re_2$, $P^1 = 0$, soit $p_{0,0} = e_{11}$, $p_{0,1} = e_{22}$, $p_{1,0} = 0$. Dans E, $L\colon M^0 \to M^2$ a pour inverse $w_0 = e_{12}$, de degré -2, et (6.3) vaut. Soit $\mathcal{E}$ le sous-anneau des matrices triangulaires inférieures. Il contient L, tous les π_a et tous les $p_{j,\beta}$: (3) est satisfaite. Mais aucun $w \in \mathcal{E}$ ne vérifie $wL\pi_0 = \pi_0$, et aucun $\Lambda \in \mathcal{E}$ ne vérifie $L\Lambda = 1 - p_{0,0} - p_{1,0}$.*

Démonstration. Le coefficient $(1,1)$ de $wL\pi_0 = w\, e_{21}\, e_{11}$ est w_{12}, qui est nul dans $\mathcal{E}$, alors qu'il vaut 1 dans π_0. De même, le coefficient $(2,2)$ de $L\Lambda = e_{21}\Lambda$ est $\Lambda_{12} = 0$, alors qu'il vaut 1 dans $1 - e_{11} = e_{22}$. Les vérifications de `Graduation` et de `DecompositionPrimitive` se font coefficient par coefficient (`graduation_c`, `decomposition_c`, `reciproque_trois_un_fausse`). □

Remarque. Les projecteurs ne voient pas l'inverse de L. L'hypothèse (3) ne dit rien des éléments de degré négatif de $\mathcal{E}$, alors que (1) et (2) en exigent. L'échec ne tient ni à **Z** ni aux dénominateurs : le contre-exemple vaut sur un corps. La réciproque (3) ⇒ (1) n'est donc vraie que pour sa partie « les π_i sont dans $\mathcal{E}$ ». Pour obtenir (1), il faut ajouter à (3) l'appartenance à $\mathcal{E}$ d'un inverse de L^{n-j} sur chaque P^j, c'est-à-dire, à peu de chose près, (6.3) elle-même.

Théorème (Grothendieck, page 49, variantes en dimension critique ♦). *Les deux variantes A'^0 et A''^0 de la condition A^0 en dimension critique, qui portent sur les classes devenant algébriques sur une section hyperplane, entraînent ensemble A^0. Ainsi $C(X)$ équivaut à $C(Y) + A'^0(X \times X) + A''^0(X \times X)$ et, par descente le long d'une chaîne de sections hyperplanes Y, Z, et ainsi de suite, à ces deux seules conditions sur $X \times X$, $Y \times Y$, $Z \times Z$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (page 49). Elle factorise l'opérateur de la dimension critique à travers la section hyperplane, selon la parité de la dimension, sans achever l'argument.

Énoncé (Énoncé de l'édition, page 49, le dédoublement de la condition critique)**.** *Soient des k-modules et des sous-modules de classes algébriques. En dimension paire, si φ^* est surjectif, L_Y un isomorphisme, toute classe algébrique de $H^{2m+2}(X)$ l'image par φ_* d'une classe algébrique (A''^0), L_Y^{-1} conserve les classes algébriques ($A^0(Y)$) et x est algébrique dès que $\varphi^* x$ l'est (A'^0), alors toute classe algébrique de $H^{2m+2}(X)$ est $L^2 = \varphi_* L_Y \varphi^*$ d'une classe algébrique. En dimension impaire, la même conclusion pour L inversible demande que la projection $\varphi^* L^{-1} \varphi_*$ conserve les classes algébriques, ce qui découle déjà de $A^0(X)$.*

L'idée est simple : on remonte une classe algébrique de $H^{2m+2}(X)$ en une classe de Y par A''^0, on l'abaisse de deux degrés par L_Y^{-1} (c'est là que sert $A^0(Y)$), on la relève sur X par φ^* et l'on conclut par A'^0. En dimension impaire, il n'y a pas de L_Y à inverser, et la seule façon de revenir est l'inverse de L lui-même : la réduction tourne en rond. Le point ouvert du problème 5 de l'article sur les problèmes est de savoir si $A^0(Y_T)$, pour une section hyperplane de $X \times X$, est fourni par la récurrence. Lean : `split_even`, `split_odd`, `split_odd_circular`.

3 Cote 98 : une théorie axiomatique des normes, le modèle des G-ensembles ; classes de faisceaux [4]

La cote 98, *Schémas de Hilbert. Normes : notes manuscrites (s.d.)*, que l'inventaire date « [à partir de 1966-1967] », pose aux pages 10 et 11 une axiomatique des normes dans une catégorie à sommes finies : une classe $\mathcal{N}$ de morphismes stable par identités, composition, changement de base, sommes et quotients $(X_Y^n)/H$, $H \subset \mathfrak{S}_n$ ((i) à (v)) ; un degré multiplicatif, invariant par changement de base, additif, avec $\deg\big((X_Y^n)/H \to Y\big) = \operatorname{card}(E^n/H)$ si $\deg u = r$ et $E = \{1, \dots, r\}$ ((i bis) à (v bis)) ; des sections canoniques $\mathrm{Can}_{X/Y} : Y \to \mathrm{Sym}_Y^r(X)$ avec $\mathrm{Can}_{X/X} = \mathrm{id}$, le diagramme de transitivité de la page 11, le changement de base et l'additivité ((i ter) à (iv ter)) (98, lot 1, p. 10, 98, lot 1, p. 11). Dans l'exemple I, les G-ensembles, u est de degré r si toutes ses fibres ont r éléments, et $\mathrm{Can}_{X/Y}(y)$ est la classe de la « suite de ses éléments rangés dans un ordre quelconque » ; la page dit (i) à (v) et (i bis) à (v bis) « trivialement vérifiées », ajoute qu'« on vérifie aussitôt » (i ter) à (iv ter), et aucun exemple n'est vérifié pour (ii ter).

Théorème 3.1 (D'après les pages 10 à 12, exemple I ♦)**.** *Les applications dont toutes les fibres sont finies de même cardinal r, munies de ce cardinal comme degré, satisfont (i) à (v) et (i bis) à (v bis) ; la fibre de $(X_Y^n)/H \to Y$ en y est en bijection avec E^n/H. Avec $\mathrm{Sym}_Y^r(X)$ formé des couples (y, m), m multi-ensemble de r points de $u^{-1}(y)$, et $\mathrm{Can}_{X/Y}(y)$ le multi-ensemble des points de la fibre, (i ter) à (iv ter) sont satisfaits, et Can est compatible à l'action de G quand u est équivariant.*

L'énoncé tient : voir `hasDeg_comp`, `hasDeg_quotPow`, `can_comp`, `can_pullback`, `can_sum` et `can_smul` dans `Folder98.lean`. Pour (ii ter), la fibre de vu au-dessus de z est la réunion disjointe des fibres de u au-dessus des s points de la fibre de v. Le groupe ne joue aucun rôle au-delà de l'équivariance de Can. Ne sont pas démontrés : l'exemple II (morphismes finis localement libres et norme de la page 2) et la transitivité des normes des pages 6 à 8 ; l'exemple III est traité ci-dessous.

4. Preuve vérifiée : `lean/Grothendieck/Folder98.lean`.

La page 13 précise l'exemple III. Un groupe discret Γ opère sur un espace X ; pour E un Γ-ensemble, $\Phi(E) = X \times^\Gamma E$ est le quotient de $X \times E$ par l'action diagonale. La page *suppose* que Φ transforme les morphismes de degré r en morphismes de degré r, affirme qu'il transforme les morphismes canoniques en morphismes canoniques, et s'interrompt. On lit « non ramifié » comme dans la lecture : tout point de X a un voisinage U tel que $gU \cap U = \varnothing$ pour $g \neq 1$.

Théorème 3.2 (D'après la page 13, exemple III ♦). *Soit Γ opérant sur X par homéomorphismes, tout point ayant un voisinage disjoint de ses translatés, et $f : E \to F$ une application Γ-équivariante entre Γ-ensembles discrets. Alors* (a) *$\Phi(f) : \Phi(E) \to \Phi(F)$ est un revêtement, et si toutes les fibres de f ont r éléments, toutes celles de $\Phi(f)$ aussi (il suffit pour cela que l'action sur X soit libre) ;* (b) *$\Phi(E \sqcup F) \simeq \Phi(E) \sqcup \Phi(F)$;* (c) *$\mathrm{Sym}^r_F(E)$ est un Γ-ensemble, $\mathrm{Can}_{E/F}$ est équivariant, l'application $[x, (e', m)] \mapsto ([x, e'], [x, m])$ est une bijection $\Phi(\mathrm{Sym}^r_F(E)) \to \mathrm{Sym}^r_{\Phi(F)}(\Phi(E))$, et elle envoie $\Phi(\mathrm{Can}_{E/F})$ sur $\mathrm{Can}_{\Phi(E)/\Phi(F)}$.*

Démonstration. (a) Les points de $\Phi(E)$ au-dessus de $[x, e']$ sont les $[x, i]$ avec $f(i) = e'$, et $i \mapsto [x, i]$ est injective si l'action est libre : $[x, i] = [x, j]$ donne g avec $gx = x$ et $gj = i$, donc $g = 1$. Pour le revêtement, on prend U ouvert autour de x, disjoint de ses translatés. L'application $y \mapsto [y, e']$ est ouverte, puisque le quotient par un groupe l'est, et son image V de U est un voisinage ouvert de $[x, e']$. L'image réciproque de V est la réunion disjointe des $U_i = \{[y, i] : y \in U\}$, $f(i) = e'$, et $\Phi(f)$ envoie chaque U_i bijectivement sur V. La fibre vide, $f^{-1}(e') = \varnothing$, donne une image réciproque vide. (b) On envoie $[x, e]$ dans le facteur où tombe e. (c) L'application est bien définie car $[gx, ge] = [x, e]$; elle est injective par la liberté, surjective parce que tout point au-dessus de $[x, e']$ s'écrit $[x, i]$, et $\Phi(\mathrm{Can})([x, e'])$ a pour image le multi-ensemble des $[x, i]$, $f(i) = e'$, qui est la fibre de $\Phi(f)$. □

Voir `hasDeg_phi`, `isCoveringMap_phi`, `Phi.sumEquiv`, `can_smul'`, `Phi.symComp_bijective` et `phi_can` dans `Folder98.lean`. L'hypothèse que la page pose, la conservation des degrés, est démontrée ; elle n'exige que la liberté de l'action, et le revêtement vaut pour toute application équivariante, de degré constant ou non. N'est pas démontré : que $X/H' \to X/H$ soit un revêtement de groupe H/H', c'est-à-dire l'identification $X/H \simeq \Phi(\Gamma/H)$ par laquelle ce revêtement devient $\Phi(\Gamma/H' \to \Gamma/H)$, ni que l'image de Φ satisfasse les axiomes dans la catégorie des espaces.

Classes de faisceaux sur les extensions du corps de base (pages 28 à 30)

Plus loin, la cote se demande quand deux faisceaux, définis sur X après deux extensions différentes du corps de base k, doivent être tenus pour le même. La définition 1 de la page 28 dit F_1 sur $X \otimes_k K_1$ et F_2 sur $X \otimes_k K_2$ *k-équivalents* s'il existe une extension K' de k et des k-plongements $u_i : K_i \to K'$ tels que $F_1 \otimes_{K_1} K'$ et $F_2 \otimes_{K_2} K'$ soient isomorphes. C'est une relation d'équivalence, dit la page, « en vertu de la transitivité de l'extension des scalaires » et parce que deux extensions de k peuvent toujours être « dominées » par une troisième (98, lot 2, p. 28). La proposition 1, pour X de type fini, ramène tout aux extensions de type fini : un faisceau est équivalent à un faisceau défini sur une sous-extension de type fini, et deux faisceaux cohérents équivalents ainsi définis le deviennent déjà sur une extension de type fini. Les classes forment un ensemble $\mathfrak{F}(X/k)$, qui est, pour k fixé, un « foncteur contravariant en X » (98, lot 2, p. 29). Le corollaire 5 prend enfin une extension $\widetilde{K}$ algébriquement close de degré de transcendance infini : $\mathfrak{F}(X/k)$ est l'ensemble des classes de faisceaux cohérents sur $X \otimes_k \widetilde{K}$ modulo l'action de $\mathrm{Aut}(\widetilde{K}/k)$ (98, lot 2, p. 30).

Conventions. On ne manipule ni schémas ni faisceaux. Les extensions de k et leurs k-plongements forment une catégorie C ; à chaque K est attaché l'ensemble $\Phi(K)$ des classes d'isomorphisme de faisceaux sur $X \otimes_k K$, et à chaque plongement $u : K \to K'$ l'extension des scalaires $\Phi(K) \to \Phi(K')$, compatible à la composition. Dans ce cadre, la définition 1 se lit telle quelle.

Théorème 3.3 (D'après les pages 28 à 30)**.** (a) *Si deux plongements $A \to B$, $A \to B'$ se prolongent toujours en des plongements $B \to D$, $B' \to D$ qui coïncident sur A, la k-équivalence est une relation d'équivalence.* (b) *Une image inverse $\Phi \to \Psi$ compatible à l'extension des scalaires respecte la k-équivalence.* (c) *Supposons les deux moitiés de la proposition 1, que toute extension de type fini se plonge dans $\widetilde{K}$ et que deux plongements d'une même extension de type fini dans $\widetilde{K}$ diffèrent d'un automorphisme de $\widetilde{K}$. Alors toute classe a un représentant sur $\widetilde{K}$, et deux faisceaux F, G sur $X \otimes_k \widetilde{K}$ sont k-équivalents si et seulement si $F \simeq \sigma(G)$ pour un $\sigma \in \mathrm{Aut}(\widetilde{K}/k)$.*

Démonstration. (a) Supposons $(K_1, F_1) \sim (K_2, F_2)$ réalisé dans K' et $(K_2, F_2) \sim (K_3, F_3)$ réalisé dans K''. Les deux plongements de K_2 dans K' et K'' se prolongent en $K' \to D$, $K'' \to D$ qui coïncident sur K_2. Dans D, l'image de F_1 est celle de F_2 par le premier chemin, celle-ci est l'image de F_2 par le second, et c'est l'image de F_3. (b) On applique l'image inverse à l'isomorphisme sur K'. (c) Pour un faisceau F sur K, défini sur $K_0 \subset K$ de type fini, on plonge K_0 dans $\widetilde{K}$ et l'on amalgame K et $\widetilde{K}$ au-dessus de K_0. Si F et G sur $\widetilde{K}$ sont équivalents, on les descend sur K_1 et K_2 de type fini, on les rend isomorphes sur K'' de type fini, et l'on plonge K'' dans $\widetilde{K}$. Les deux plongements de K_1 dans $\widetilde{K}$, le donné et celui qui passe par K'', diffèrent d'un automorphisme σ_1 ; de même pour K_2 avec σ_2. On obtient $F \simeq \sigma_1\sigma_2^{-1}(G)$. La réciproque prend $K' = \widetilde{K}$, avec l'identité et σ. □

Remarque. La raison donnée par la page ne suffit pas telle quelle. Que deux extensions de k soient dominées par une troisième ne donne pas la transitivité : il faut dominer les deux extensions K' et K'' de K_2 par une extension de K_2, de façon que les deux plongements de K_2 coïncident, faute de quoi les deux images de F_2 dans D n'ont pas de raison d'être isomorphes. Pour des corps, un quotient de $K' \otimes_{K_2} K''$ par un idéal maximal convient, comme le note la lecture. Au corollaire 5, la surjectivité n'utilise que la première moitié de la proposition 1 et le plongement dans $\widetilde{K}$; l'injectivité utilise les deux moitiés et l'homogénéité de $\widetilde{K}$, qui n'est vraie que pour les extensions de type fini et explique le détour par la proposition 1.

La figure 1 reprend la démonstration de (a). Le losange central doit commuter : D est une extension de K_2, et non seulement de k.
Voir `kEquiv_equivalence`, `kEquiv_map`, `corollaire5_surj` et `corollaire5_iff` dans `Folder98.lean`. Ne sont pas démontrés : la proposition 1, renvoyée par la page à un « Chap. V, § 1 » qu'on n'identifie pas, ni les deux propriétés de $\widetilde{K}$, classiques (prolongement à des bases de transcendance de même cardinal infini, puis aux clôtures algébriques) et prises ici pour hypothèses.

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (D'après les pages 9 à 16, forme corrigée par l'édition, théorème de Griffiths par voie ℓ-adique ♦)**.** *En toute caractéristique, soient X projective lisse de dimension $2n$ et un pinceau de Lefschetz, de section hyperplane générique Y. Supposons a) un scindage de type Lefschetz de l'inclusion de Y par une correspondance algébrique, et b) qu'aucune pièce de $\mathrm{Coker}(H^{2n-1}(X) \to H^{2n-1}(Y))$ ne soit de coniveau $n-1$. Alors un cycle de X dont la restriction à Y est algébriquement équivalente à zéro est homologiquement nul à torsion près,*

◊ non vérifié en Lean

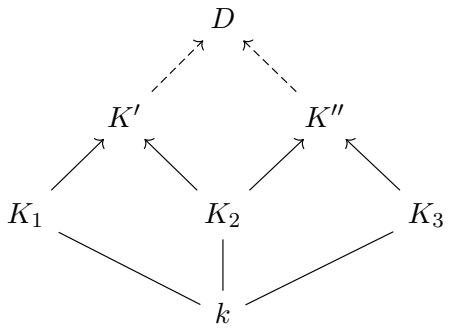


FIGURE 1 – Transitivité de la k-équivalence. $F_1 \sim F_2$ est réalisée dans K', $F_2 \sim F_3$ dans K'' ; les plongements en tirets de K' et K'' dans D coïncident sur K_2, de sorte que les deux images de F_2 dans D sont la même. Deux plongements quelconques de K' et K'' dans une extension commune de k ne le garantissent pas.

et $\mathrm{Grif}(Y) \otimes \mathbf{Q}$ *a un sous-quotient qui s'envoie sur les classes algébriques primitives de* X.

Les feuillets en esquissent une démonstration incomplète (pages 9 à 15) : le n° 4 renvoie à des « calculs explicites essentiellement triviaux », et l'argument est de la lecture. La page dit « sous-espace » là où l'argument ne donne qu'un sous-quotient. L'hypothèse a) est un cas des conjectures standard, et b) n'est démontrée qu'en caractéristique nulle. Mathlib n'a pas la cohomologie ℓ-adique ni l'application d'Abel–Jacobi. On se reportera aux notes de Grothendieck (36, lot 1, p. 9).

Théorème (Grothendieck, pages 60 à 70, défaut des cycles invariants en H^1 ♦). *Soient X projectif et régulier sur un trait strictement hensélien S, avec $\mathcal{O}_S \simeq f_*\mathcal{O}_X$, et n premier à p. On a une suite exacte $0 \to {}_n\Gamma \to H^1(X, \mu_n) \to H^1(X_{\bar\eta}, \mu_n)^I \to \mathrm{Ker}(w_n) \to 0$, où Γ est le groupe des diviseurs portés par la fibre spéciale modulo X_0 et $w : \Gamma \to \mathrm{NS}(X_0)$. À la limite, $H^1(X, \mathbf{Z}_\ell(1)) \to H^1(X_{\bar\eta}, \mathbf{Z}_\ell(1))^I$ est injectif de conoyau $R \otimes \mathbf{Z}_\ell$, où $R = \mathrm{Ker}\, w$ est cyclique d'ordre divisant le pgcd des multiplicités d_i des composantes de X_0, et c'est un isomorphisme quand X_η a un 0-cycle de degré 1.*

◊ non vérifié en Lean

Le tapuscrit des pages 60 à 63 l'énonce ; le manuscrit des pages 64 à 70 le démontre, la torsion de $\mathrm{Ker}\, w$ étant renvoyée à Raynaud et tenue « au moins modulo résolution des singularités ». Celle-ci est démontrée en caractéristique nulle (Hironaka) et en dimension au plus trois sur un corps parfait de caractéristique positive (Cossart–Piltant), et reste ouverte en caractéristique positive à partir de la dimension quatre ; ces trois énoncés figurent, sans démonstration, dans le dépôt Formal Conjectures [58]. Mathlib n'a pas la cohomologie étale ni le groupe de Néron–Severi. On se reportera aux notes de Grothendieck (36, lot 3, p. 60).

Théorème (Grothendieck, pages 73 à 76, orthogonalité sur une base adique régulière ♦). *Soient $X = \mathrm{Spec}\, A$ une base noethérienne régulière complète pour la topologie J-adique, $Y = V(J)$ et $U = X - Y$. Soient G, G' des schémas en groupes commutatifs plats sur X dont les restrictions A_U, A'_U à U sont des schémas abéliens, ξ une correspondance divisorielle sur $A_U \times A'_U$, $H \subset G_Y$ un sous-groupe plat à torsion ℓ^ν finie et $T' \subset G'_Y$ un tore. Alors $\varphi_\xi(T_\ell(\tilde H)|_U, T_\ell(\tilde T')|_U) = 0$ en tout point de U : l'orthogonalité de la partie torique et de la partie de torsion finie pour l'accouplement de Weil ne demande pas un anneau de valuation discrète.*

◊ non vérifié en Lean

La réduction à un anneau de valuation discrète à corps résiduel fini et l'argument des poids de Frobenius (pages 74 à 76) sont lus en grande partie à travers des mots incertains ou illisibles, et

l’équivariance galoisienne du lemme sur les corps finis est ajoutée par l’édition. SGA 7, IX, donne l’orthogonal exact sur un trait. Mathlib n’a pas les schémas abéliens ni l’accouplement de Weil. On se reportera aux notes de Grothendieck (36, lot 4, p. 73).

Partie 2

Motifs

Aucun énoncé de ce thème n'est démontré ici. Les cotes de ce thème supposent les correspondances algébriques et une catégorie de motifs, que mathlib ne définit pas.

Cotes rangées sous ce thème par la carte : 12, 162-6.

Théorème (Grothendieck, pages 115 à 119, poids et niveau d'une immersion ♦). *Soient $f : X \to Y$ une immersion de source régulière et n la dimension de l'adhérence de $f(X)$. Les constituants de $R^i f_* \mathbb{Q}_\ell$ sont de poids $\leq 2\inf(i, n)$ et de niveau $\leq \inf(i, n-1)$. Le dossier tient l'énoncé sous réserve de la résolution, de la pureté et des conjectures de Weil.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 115, 117 et 119). Un constituant de poids w est de niveau $\leq \nu$ quand ses valeurs propres de Frobenius sont divisibles par $q^{(w-\nu)/2}$, ou, côté Hodge, quand ses types (p, q) vérifient $p, q \geq (w-\nu)/2$; la borne $\inf(i, n-1)$ est inférieure d'une unité au niveau $2n-i$ que permet H^i d'une variété lisse de dimension n quand $i \geq n$. Les tableaux qui mènent à l'encadré sont écrits vite et surchargés, et l'énoncé repose sur l'encadré seul ; le passage des termes E_2 à l'aboutissement (proposition 4.2 a) de la page 112) n'est pas écrit. Les structures de Hodge et les périodes sont l'objet de la partie « Théorie de Hodge » (cotes 13 et 18). Mathlib n'a pas les poids des faisceaux ℓ-adiques. On se reportera aux notes de Grothendieck (12, lot 6, p. 115).

Sur $\mathbf{C}$, pour une immersion ouverte $j : X \to Y$, l'édition démontre l'énoncé, sous une forme plus précise, par un argument qui n'est pas sur les feuillets et que Lean ne vérifie pas. Soient $y \notin X$, $\pi : \tilde{Y} \to Y$ une résolution qui est un isomorphisme au-dessus de X, $D = \pi^{-1}(Y - X)$ à croisements normaux simples, $F = \pi^{-1}(y)$ et $F_q = F \cap D^{(q)}$; alors $\dim F_0 \leq n-1$ et $\dim F_q \leq n-q$. La suite spectrale des poids, $E_1 = H^{k-q}(F_q)(-q) \Rightarrow H^k(X \cap B_y)$ (celle de Durfee [45] quand $(Y - X) \cap B_y = \{y\}$; dans le cas général la structure de Hodge mixte vient des modules de Hodge mixtes de Saito [111], et la forme de la suite spectrale n'est pas vérifiée ici), où B_y est une petite boule autour de y, et le théorème 8.2.4 (i), (ii) de Hodge III [40] pour les F_q compacts placent les types de Hodge de $(R^i j_* \mathbf{Q})_y = H^i(X \cap B_y)$ dans la boîte $p, q \in [\max(0, i-n+1), \min(i, n)]$. On retrouve les poids de la page, et le niveau est au plus $\min(i, 2n-1-i) \leq \min(i, n-1)$ pour $i \leq 2n-1$ (au-delà, H^i est nul) ; c'est l'analogue local de 8.2.4 (ii). La majoration des termes E_2 des feuillets laisse passer le niveau n en $E_2^{n,0} = H^n(\pi^{-1}(y))$, et c'est la dimension $n-1$ de la fibre qui l'exclut. La borne est atteinte : le cône sur une variété projective lisse V de dimension $n-1$ telle que $h^{i,0}(V) \neq 0$ (une surface K3 pour $n = 3$) a le niveau i pour $i \leq n-1$ et le niveau $n-1$ en $i = n$; pour $n = 2$ et V une courbe de genre ≥ 1, la fibre de $R^2 j_*$ au sommet est $H^1(V)(-1)$, de poids 3 et de niveau 1. Cette boîte n'a été trouvée imprimée que pour les singularités isolées, où elle découle de la semi-pureté et de la dualité (Friedman et Laza, théorème 2.6 et définition 2.7 [51]). Pour un morphisme propre de fibres de dimension d, le gain d'une unité disparaît : une famille lisse de courbes a déjà un H^1 de niveau $1 = d$; la version relative que la page esquisse avec $n = d_y(f)$, suivie d'un point d'interrogation, ne peut donc pas garder $n-1$ si $d_y(f)$ est la dimension de la fibre.

Partie 3

Théorie de Hodge

4 Cote 13 : la question du double réseau et le cas de Tate[5]

La cote 13, *Groupe de Galois motivique*, est datée de 1965. Aux pages 45 à 49, Grothendieck passe en revue les foncteurs de réalisation des motifs et demande de chacun s'il est pleinement fidèle. La question centrale est celle de la page 47 : sur une extension algébrique k de $\mathbf{Q}$, le foncteur qui envoie un motif M sur sa réalisation de de Rham $T_{DR}(M)$, sa réalisation de Betti $T_B(M)$ et l'isomorphisme de comparaison φ entre elles, sans filtration ni structure de Hodge, est-il pleinement fidèle ? C'est la forme de de Rham–Betti de ce qu'on appelle aujourd'hui la conjecture des périodes de Grothendieck (Bost et Charles 2016, § 2.2 [22]). Elle est ouverte.
L'image à garder. Dans $V \otimes \mathbf{C}$ cohabitent deux structures rationnelles : le réseau de Betti V, rationnel sur $\mathbf{Q}$, et le réseau de de Rham, rationnel sur $\overline{\mathbf{Q}}$. La page traduit le second dans le groupe de Galois motivique G : il s'écrit $g(V_{\overline{\mathbf{Q}}})$ pour un élément $g \in G(\mathbf{C})$, la position relative des deux réseaux. Un élément de V invariant par tout G est dans les deux réseaux à la fois ; la question est de savoir si ce sont les seuls. Elle s'écrit

$$V^G \;\subset\; V \cap g(\overline{V}) \qquad \text{une égalité pour tout } V\,?$$

Les rationnels communs aux deux réseaux mesurent les relations algébriques entre périodes : plus les périodes sont transcendantes, moins il y en a.

La page fait deux affirmations sans les démontrer. L'inclusion vaut toujours : la note de la lecture insiste sur son sens. Et le rang un marche : « s'il est de dim. 1, c'est une puissance de Tate, et ça marche » (13, lot 3, p. 47). Les deux sont démontrées ici, dans des modèles choisis par l'édition.

Énoncé (Grothendieck, page 47, l'inclusion $V^G \subset V \cap g(\overline{V})$)**.** *Soient un groupe Γ agissant sur un ensemble M, deux parties $B \subseteq \Lambda$ de M et $g \in \Gamma$. Un élément de B fixé par tout Γ appartient à $B \cap g \cdot \Lambda$.*

Ici B joue le réseau de Betti V, Λ l'espace $\overline{V} = V \otimes \overline{\mathbf{Q}}$ et $g \cdot \Lambda$ le réseau de de Rham. La démonstration tient en une ligne : si x est fixé par tout le groupe, $g^{-1}x = x$, qui est dans $B \subseteq \Lambda$, donc $x \in g \cdot \Lambda$. Elle passe par la description de $V \cap T'(V)$ que donne la page 33 : x appartient à $B \cap g \cdot \Lambda$ si et seulement si $x \in B$ et $g^{-1}x \in \Lambda$ (`mem_inter_smul_iff`). Lean : `invariants_subset_inter_smul`.

Énoncé (Grothendieck, page 47, le cas de Tate (forme reconstituée par l'édition))**.** *Supposons π transcendant. Pour tout entier n, les rationnels q tels que $q = (2\pi i)^n \alpha$ pour un $\alpha \in \mathbf{C}$ algébrique sont tous les rationnels si $n = 0$, et le seul 0 si $n \neq 0$.*

Pourquoi c'est le cas de Tate. Le motif de Tate $\mathbf{Q}(n)$ a pour réseau de Betti la droite $\mathbf{Q} \subset \mathbf{C}$ et pour réseau de de Rham la droite $(2\pi i)^n\,\overline{\mathbf{Q}}$: sa seule période est $(2\pi i)^n$. Son groupe de Galois motivique est $\mathbf{G}_m$, qui agit par la puissance n-ième ; les invariants V^G sont donc toute la droite

5. Preuve vérifiée : `lean/Grothendieck/Folder13.lean`.

si $n = 0$ et zéro sinon. L'énoncé dit que $V \cap g(\overline{V})$, l'ensemble des rationnels qui sont aussi dans la droite de de Rham, est exactement cela : l'égalité $V^G = V \cap g(\overline{V})$ vaut en rang un. Cette traduction est le modèle de l'édition ; la page n'écrit ni les deux droites ni le groupe.

Démonstration. Pour $n = 0$, tout rationnel q s'écrit $q = 1 \cdot q$, et q est algébrique. Pour $n \neq 0$, supposons $q = (2\pi i)^n \alpha$ avec $q \neq 0$. Alors $\alpha \neq 0$ et $(2\pi i)^n = q\,\alpha^{-1}$ est algébrique, comme produit d'algébriques. Si une puissance entière non nulle de z est algébrique, z l'est : pour un exposant positif, z est racine de $X^n - z^n$ au-dessus d'un corps de nombres ; pour un exposant négatif, on passe à l'inverse (`isAlgebraic_of_zpow`). Donc $2\pi i$ est algébrique, et $\pi = 2\pi i \cdot (2i)^{-1}$ aussi, puisque i est racine de $X^2 + 1$ (`isAlgebraic_I`). C'est contraire à l'hypothèse. Lean : `tate`.

Ce qui est démontré, et ce qui ne l'est pas. La transcendance de π (Lindemann, 1882) est une hypothèse explicite du théorème : mathlib, à la révision épinglée, a la partie analytique du théorème de Lindemann–Weierstrass et l'irrationalité de π, mais pas sa transcendance. Le reste est démontré sans hypothèse. Le cas de rang un est donc celui qui « marche » parce que la seule période est $(2\pi i)^n$, dont on connaît la transcendance ; dès le rang deux, pour une courbe elliptique, les périodes et quasi-périodes donnent un degré de transcendance attendu égal à 4 sans multiplication complexe, ce qui reste ouvert (Chudnovsky établit le cas à multiplication complexe, de degré 2, en 1980 : § 2 A, théorèmes 1 et 3 [31]). Ne sont pas formalisés : l'identification de $\mathbf{Q}(n)$ aux deux droites, le groupe H des pages 33 et 34, que la partie « Théorie de Hodge » encadre plus bas, et la question générale de la page 47, qui est la conjecture des périodes. On se reportera aux notes de Grothendieck (13, lot 2, p. 33, 13, lot 3, p. 47).

Périodes et groupe de Galois motivique. Les cotes 13 et 18 lisent une catégorie de motifs par ses foncteurs fibres. D'après la lecture de la cote 13, la lettre à Mumford du 1er novembre 1965 (pages 13 à 19) construit l'espace $\mathcal{J}$ des structures de Hodge de groupe G donné, réunion d'orbites ouvertes de $G(\mathbf{R})$, qu'on appelle aujourd'hui un domaine de Mumford–Tate ; la page 16 note qu'il n'est pas en général riemannien symétrique, mais fibré au-dessus d'un tel espace en espaces homogènes projectifs complexes, donc simplement connexe. Les pages 26 à 31 posent, pour $k \subset \mathbf{C}$, $G = \mathrm{Aut}^{\otimes}(T_B)$ et le torseur $P = \mathrm{Isom}^{\otimes}(T_B \otimes_{\mathbf{Q}} k, T_{DR})$ sous G_k, dont l'isomorphisme de comparaison est un point complexe, la matrice des périodes : c'est le torseur des périodes, et G le groupe de Galois motivique quand la catégorie est tannakienne, hypothèse que le dossier fait sans l'écrire. La cote 18 compare les réseaux de Betti entiers en plusieurs places archimédiennes. Sur le même axe, la section 2 démontre les énoncés algébriques des algèbres de Hodge d'ordre 2, et la partie « Motifs » encadre la borne de poids et de niveau de la cote 12. Pistes de l'onglet Findings pour ces cotes, hors de portée de Lean pour l'instant :

— Cote 18 : pour un motif sur $k \simeq \mathbb{C}$ défini sur un corps de type fini k_0, la comparaison des réseaux de Betti entiers en différentes places archimédiennes donne un 1-cocycle de $\mathrm{Gal}(k/k_0)$ dans $G(k)$, dont la classe ne dépend pas de la place. En détail : pour M défini sur k_0 de type fini, $k \simeq \mathbf{C}$, et deux topologies archimédiennes v, w de k, la comparaison des réseaux $M_v^{\mathbf{Z}}$, $M_w^{\mathbf{Z}}$ dans $\prod_{\ell \leq \infty} M(\ell)$ donne un élément de $G(\mathbb{A}_{\mathbf{C}})/G(\hat{\mathbf{Z}})$ dont la composante archimédienne est dans $G(k)$, et $\sigma \mapsto \varphi_{v,\infty}(\sigma)$ un 1-cocycle de $\mathrm{Gal}(k/k_0)$ dans $G(k)$, d'où un G-torseur sur k_0 ; la lecture borne aussi par $(n-1)\dim G$ le degré de transcendance de la configuration de n places. La comparaison n'est pas triviale parce que deux variétés conjuguées peuvent ne pas être homéomorphes (Serre 1964 [113]). La page 61 encadre une formule de conjugaison que la lecture remplace par la formule de cobord de la version barrée. La lecture de la page est à vérifier sur le fac-similé. Mathlib n'a pas les motifs, les réseaux de Betti ni la cohomologie galoisienne non abélienne. On se reportera aux notes de Grothendieck (18, lot 3, p. 46). ♦

— Cote 18, pages 35 et 37 : la page tient qu'un motif sur $\mathbf{R}$ de Frobenius réel trivial est engendré par les twists pairs $\mathbf{Q}(-2n)$. L'édition relève que c'est faux tel quel : H^2 de $\mathbf{P}^1_{\mathbf{C}}$ vu comme $\mathbf{R}$-schéma contient $\mathbf{Q}(-1) \otimes \varepsilon$, ε le motif d'Artin de signe de $\mathbf{C}/\mathbf{R}$, où F_∞ agit par $+1$. Reste vrai que $F_\infty = 1$ équivaut à la réalité des périodes ; la classe corrigée est celle des motifs engendrés par les

$\mathbf{Q}(-n) \otimes \varepsilon^n$. On se reportera aux notes de Grothendieck (18, lot 2, p. 35).

Théorème (Grothendieck, pages 33 et 34, invariants d'un double réseau ♦). *Soient une catégorie tensorielle munie d'un foncteur fibre T sur k, d'un foncteur fibre T' sur une extension K et d'un $\otimes$-isomorphisme φ entre eux sur une extension commune L. Les éléments de V qui sont dans la K-structure $T'(V)$ sont exactement les invariants V^H du sous-groupe k-algébrique H de $G = \mathrm{Aut}^{\otimes}(T)$ engendré par l'image dans G de l'image fermée $R \subset G_K$ de $\mathrm{Spec}(L \otimes_K L) \to P \times_k P \to G_K$, $(s,u) \mapsto s^{-1}u$, sans point base sur le torseur $P = \mathrm{Isom}^{\otimes}(T_K, T')$.*

◊ non vérifié en Lean

Le sous-groupe H se lit sur la suite de flèches

$$\mathrm{Spec}(L \otimes_K L) \longrightarrow P \times_k P \xrightarrow{(s,u)\mapsto s^{-1}u} G_K \longrightarrow G,$$

où R est l'image fermée du composé des deux premières et H le sous-groupe de G engendré par l'image de R.

Les feuillets en esquissent une démonstration incomplète (pages 33 et 34). La lecture écrit $T_K \times T_K$ où la page a $T_k \times T_k$. Pour $k = \mathbf{Q}$, $T = T_B$, $T' = T_{DR}$ et $K = L = \overline{\mathbf{Q}}$, P est le torseur des périodes, et le cas correspondant est publié : le torseur des périodes Ω_M de Bost et Charles (2016, définition 2.3 [22]) est le torseur engendré par l'adhérence de Zariski du point des périodes dans $\mathrm{Iso}(M_{dR}, M_B \otimes \overline{\mathbf{Q}})$, contenu dans le torseur tannakien découpé par les classes de Grothendieck (lemme 2.5) ; Kreutz, Shen et Vial (prépublication [87], proposition 3.1) montrent que, sur $\overline{\mathbf{Q}}$, Ω_M est le torseur de de Rham–Betti de M, dont le groupe a pour invariants les classes de de Rham–Betti, et que l'égalité tombe pour un corps de définition $K \neq \overline{\mathbf{Q}}$ (remarque 3.2). La forme de la page, pour une tour $k \subset K \subset L$ quelconque et une catégorie tensorielle quelconque, avec les invariants pris dans V lui-même, n'a pas été trouvée dans les sources lues.

Le corollaire de la page 34, que la lecture écrit « pleinement fidèle si et seulement si $V^H = V^G$ pour tout V » où la page a « fid. plat », dit que H est un sous-groupe épimorphique de G au sens de Bien et Borel (1992) [16], et non que $H = G$: un sous-groupe parabolique vérifie déjà $V^H = V^G$ pour toute représentation. Cette remarque est de l'édition.

La question des pages 47 et 48, si $M \mapsto (T_{DR}(M), T_B(M), \varphi)$, sans filtration ni structure de Hodge, est pleinement fidèle sur une extension algébrique de $\mathbf{Q}$, réduite par la page à $\overline{\mathbf{Q}}$, est la pleine fidélité de la réalisation de de Rham–Betti (Kreutz, Shen et Vial, conjecture 4.1 [87]). Elle est démontrée pour les variétés abéliennes : c'est le théorème 5.4 de Kreutz, Shen et Vial, qu'ils attribuent à André, Bost et Wüstholz. Bost et Charles énoncent la conjecture des périodes de Grothendieck sous une autre forme : l'isomorphisme de comparaison est Zariski-dense dans le torseur des périodes motiviques. On ne sait pas si les deux formes sont équivalentes. En admettant les conjectures standard, la leur entraîne la pleine fidélité (Bost et Charles 2016, conjecture 2.12 et proposition 2.13 [22]). La forme $V^G = V \cap g(\overline{V})$ de la page 48, qui identifie le groupe au H des pages 33 et 34, est de la lecture. Mathlib n'a pas les catégories tannakiennes ni les torseurs de foncteurs fibres. On se reportera aux notes de Grothendieck (13, lot 2, p. 33, 13, lot 3, p. 47).

Le cas elliptique, énoncé en Lean. La page 12 de la cote 18 demande, pour une courbe elliptique sur $\overline{\mathbf{Q}}$, si le corps engendré par le point de comparaison est de degré de transcendance 4 ou seulement 2 (18, lot 1, p. 12). Le fichier `lean/Grothendieck/Folder18.lean` énonce, sans la démontrer, la réponse attendue, qui est le cas elliptique de la conjecture des périodes (Bost et Charles 2016, conjecture 2.12 [22]). Pour un réseau d'invariants g_2, g_3 algébriques et sans multiplication complexe, les périodes ω_1, ω_2 et les quasi-périodes $\eta_i = 2\zeta(\omega_i/2)$ seraient algébriquement indépendantes sur $\mathbf{Q}$ (`EllipticPeriodConjecture`). La fonction ζ y est définie par sa série, comme mathlib définit $\wp$, sans que soient démontrées sa convergence ni la relation

$\zeta' = -\wp$. Avec multiplication complexe, le degré vaut 2 (Chudnovsky 1980, § 2 A, théorèmes 1 et 3 [31]) ; sans, la question reste ouverte. L'énoncé est une proposition et non un axiome, de sorte qu'aucune preuve n'en dépend.

Partie 4

Cohomologie étale et ℓ-adique

Aucun énoncé de ce thème n'est démontré ici. Les cotes de ce thème supposent le site étale d'un schéma et sa cohomologie, que mathlib ne contient pas.

Cotes rangées sous ce thème par la carte : 31, 33, 60.

Exemple (Grothendieck, pages 38 à 58, moyenne sur l'inertie et dualité ♦). Soit E_η un faisceau ℓ-adique au point générique d'une courbe sur $\mathbf{F}_p$. En remplaçant chaque fibre ramifiée E^{I_x} par la moyenne de E sur l'inertie modulo un sous-groupe ouvert qui agit de façon unipotente, on obtient un faisceau virtuel $E_\eta^\natural$ dont la fonction L est additive et locale en (E, x). Son dual de Verdier est $\check{E}_\eta^\natural(1)[2]$ augmenté des termes locaux $\mu_x(E) = \alpha_x(E_\eta)^\vee - \alpha_x(\check{E}_\eta)(1)$; la page 52 demande si $\delta^\natural(E_\eta)^2 = q^{\chi^\natural(E_\eta)}$ pour E_η autodual de poids ρ.

◊ non vérifié en Lean

En termes actuels, la fibre moyennée $E^{\natural(x)}$ est l'espace des invariants de l'inertie dans la représentation de Weil–Deligne de E restreinte au groupe de décomposition en x, l'opérateur de monodromie N étant oublié, c'est-à-dire dans sa semi-simplifiée ; cette traduction est de la lecture. La lecture montre aussi, par le théorème de monodromie ℓ-adique que la page suppose sans le nommer, que $\mu_x(E) = 0$ pour tout E_η : les termes correctifs de la page s'annulent, et la question de la page 52 reçoit la réponse oui. Cet argument est de l'édition et n'est pas vérifié en Lean ; l'équation fonctionnelle de la fonction L ainsi formée n'a pas été cherchée dans la littérature sur les constantes locales. Les connexions et la monodromie en caractéristique 0 sont l'objet de la section 49 (connexions projectives) et des énoncés de la cote 162-5 (partie « Catégories et foncteurs »). Mathlib n'a pas les faisceaux ℓ-adiques, leurs fonctions L ni la dualité de Verdier. On se reportera aux notes de Grothendieck (60, lot 2, p. 38).

Théorème (Grothendieck, pages 64 à 70, majoration de la dimension cohomologique ; voir M. Artin, SGA 4, exposé X, théorème 4.1 (1973) ♦). *Soit φ une fonction sur les points d'un schéma noethérien X telle que $\varphi(x) \geq \mathrm{cd}_\ell(k(x))$ en tout point et $\varphi(y) < \varphi(x) - \mathrm{cd}_\ell(\mathcal{O}_{X,\bar{y}} \otimes k(x))$ pour toute spécialisation stricte y de x. Alors $H^i(X, F) = 0$ pour tout faisceau de ℓ-torsion F et tout i supérieur au supremum de φ sur le support de F.*

◊ non vérifié en Lean

Démonstration de la page (pages 64 à 67). Le résultat est publié par M. Artin dans SGA 4, exposé X, théorème 4.1 (1973) [8] ; l'inventaire date la cote [1963–1973]. Par récurrence noethérienne sur X (p. 66), une suite de composition par des faisceaux élémentaires (p. 64) ramène au cas $F = g_*(G)$, $g : \mathrm{Spec}\, k(x) \to X$, G fini, où $\varphi(F) = \varphi(x)$; la prose de cette réduction est en grande partie illisible. La suite spectrale de Leray de g et la fibre $(R^q g_* G)_{\bar{y}} = H^q(\mathcal{O}_{X,\bar{y}} \otimes k(x), G)$ donnent, par l'hypothèse sur les spécialisations, l'estimation encadrée $\varphi(R^q g_* G) \leq \varphi(x) - q$, et pour $q > 0$ l'hypothèse de récurrence tue $H^p(X, R^q g_* G)$ (p. 67). La page conclut sur un croquis du plan (p, q), sans écrire le dernier pas.

◊ non vérifiée en Lean

Conjecture (Grothendieck, page 84, dimension cohomologique et degré d'imperfection ♦). *En la caractéristique résiduelle ℓ, la borne de la dimension cohomologique d'un schéma affine est gouvernée par le degré d'imperfection $\nu(k)$, défini par $\ell^{\nu(k)} = [k : k^\ell]$, plutôt que par la dimension :* $\mathrm{cd}_\ell(X) \leq \sup(\mathrm{cd}_\ell\, k(x), \nu(V(\ell)) + 3)$, *et* $\mathrm{cd}_\ell(U) \leq \dim A + \nu(k) + \mathrm{cd}_\ell(k)$ *pour*

U ouvert du spectre d'un anneau local hensélien intègre A de caractéristique résiduelle ℓ dont le corps des fractions est de caractéristique 0.

La seconde borne tient, sous une forme plus précise, pour A hensélien, excellent et intègre, de corps résiduel de caractéristique ℓ et de corps des fractions de caractéristique nulle, et U ouvert affine non vide de $\operatorname{Spec} A[1/\ell]$: Gabber et Orgogozo (2008, théorème 6.1) [54] montrent $\operatorname{cd}_\ell(U) = \dim A + \dim_\ell(k)$, où $\dim_\ell$ est la ℓ-dimension de Kato, et $\dim_\ell(k) \leq \nu(k) + \operatorname{cd}_\ell(k)$ découle de leur définition 1.1 ; les mots qui entourent « ouvert » sont illisibles, et rien n'est connu ici pour un U qui rencontre $V(\ell)$. Le rôle de $[k : k^\ell]$ est annoncé, sans borne, dans SGA 4, exposé X, § 3.0 [8]. La première borne, $\sup(\operatorname{cd}_\ell k(x), \nu(V(\ell)) + 3)$, n'a été trouvée dans aucune source lue. Les résultats les plus proches sont locaux ou relatifs : Mathew (2021, démonstration de la proposition 4.5) [96] obtient la même forme, $\operatorname{cd}_\ell \leq d + 1$ pour les ouverts affines de $\operatorname{Spec} R[1/\ell]$ quand $\dim R_\mathfrak{p} + \log_\ell[\kappa(\mathfrak{p}) : \kappa(\mathfrak{p})^\ell] \leq d$ le long de $V(\ell)$, mais pour R intègre, normal et excellent, hensélien le long d'un idéal contenant ℓ ; Gabber et Zavyalov (2026, théorème 1.7) [55] traitent les algèbres affinoïdes, où ℓ est inversible. Les bornes globales imprimées sont plus grossières : SGA 4 donne $\operatorname{cd}_\ell X \leq 2 \dim X + 1$ pour X de type fini sur $\mathbf{Z}$ (exposé X, 6.2 [8]), et Clausen et Mathew $\operatorname{cd}_\ell(X) \leq \dim X + \sup_x \operatorname{cd}_\ell k(x)$ pour X qcqs de dimension de Krull finie (corollaire 3.29 [34]), plus grossière d'un $\dim X$. Le $+2$ de la proposition 5.4.5 de Gabber et Orgogozo porte sur $\dim_\ell(k)$, qui vaut $\nu(k)$ ou $\nu(k) + 1$, et ne se compare pas au $+3$ de la page. La constante 3 paraît être la bonne : pour $\operatorname{Spec} \mathbf{Z}$ et ℓ impair, $\nu(V(\ell)) = 0$ et $\operatorname{cd}_\ell \mathbf{Q} = 2$, tandis que $\operatorname{cd}_\ell(\operatorname{Spec} \mathbf{Z}) = 3$ (SGA 4, exposé X, 6.1 [8] ; la dualité d'Artin–Verdier donne $H^3(\operatorname{Spec} \mathbf{Z}, j_!\mu_\ell) \simeq \mathbf{Z}/\ell$, Milne, II.3.2 et 3.3 [100]) ; la comparaison avec la constante de la page est de l'édition. Mathlib n'a pas la dimension cohomologique étale. On se reportera aux notes de Grothendieck (31, lot 5, p. 84).

Théorème (Grothendieck, page 22, minoration de la dimension cohomologique ♦). *Soit A un anneau local noethérien intègre, de corps des fractions K et de corps résiduel k. Pour tout premier r, $\operatorname{cd}_r(K) \geq \operatorname{cd}_r(k) + \dim A$, sauf peut-être si r est la caractéristique de K, ou si $r = 2$ et qu'un point x de $\operatorname{Spec} A$ a un corps résiduel ordonnable avec $\operatorname{cd}_2 k(x)(\sqrt{-1})$ fini ; la seconde exception disparaît quand A est régulier.*

◊ non vérifié en Lean

Quand r est inversible dans A, l'inégalité est le corollaire 2.4 de SGA 4, exposé X [8], avec l'exception plus grossière « un corps résiduel ordonnable » ; l'exemple de la marge, $\mathbf{R}[X, Y]/(X^2 + Y^2)$ à l'origine, est celui qui suit le théorème 2.3 du même exposé ; quand r est la caractéristique résiduelle et K de caractéristique nulle, elle suit, pour A excellent hensélien, du § 3 de Gabber et Orgogozo (2008) [54]. L'exception plus fine de la page et sa disparition pour A régulier n'ont pas été trouvées ; le livre de Scheiderer [112], qui traite la dimension cohomologique en présence d'ordres, reste à lire ; la marge demande si la restriction est essentielle. Mathlib n'a pas la dimension cohomologique galoisienne. On se reportera aux notes de Grothendieck (31, lot 2, p. 22).

Partie 5

Groupes p-divisibles et groupes formels

Aucun énoncé de ce thème n'est démontré ici. Les cotes de ce thème supposent les groupes de Barsotti–Tate et la théorie de Dieudonné, absents de mathlib.

Cotes rangées sous ce thème par la carte : 129.

Théorème (Grothendieck, page 95, annulation de Ext^2 ♦)**.** *Si 2 est inversible, le faisceau $\mathrm{Ext}^2_{\mathbf{Z}}(G, M)$ est nul pour tout schéma en groupes commutatif fini localement libre G et tout module quasi-cohérent M, ce qui simplifie la théorie des déformations des groupes de Barsotti–Tate pour $p \neq 2$.*

◊ non vérifié en Lean

Breen démontre en 1975 que $\mathcal{E}xt^i(G, H) = 0$ pour $1 < i < 2p - 2$, G fini et plat, H commutatif lisse quasi-projectif, quand les caractéristiques résiduelles sont au moins p et que la multiplication par tout premier $q < p$ est un automorphisme de G ; il note aussi que $\mathcal{E}xt^{2p-2}(\alpha_p, H) \neq 0$ en caractéristique p pour $H = \mathbf{G}_a, \mathbf{G}_m$ [23]. Avec $p = 3$, cela donne l'énoncé de la page pour des coefficients lisses, en particulier les fibrés vectoriels, dès que 2 est inversible ; avec $p = 2$, $\mathcal{E}xt^2(\alpha_2, \mathbf{G}_a) \neq 0$, ce qui va dans le sens de la lecture « si 2 inv. », incertaine. Restent un module quasi-cohérent quelconque et le passage des faisceaux de Breen, faisceautisés pour la topologie étale, aux groupes du site fppf. Mathlib n'a pas les Ext de schémas en groupes finis localement libres. On se reportera aux notes de Grothendieck (129, lot 5, p. 95).

Partie 6

Algèbre universelle et théories

5 Cote 161-2 : monadicité, caractérisation de Gabriel–Ulmer [6]

La cote 161-2, *Algèbre universelle [ou catégories] : notes manuscrites (s.d.)*, cent onze pages que l'inventaire date « [vers 1963-1973] », cherche ce qu'est une espèce de structure algébrique dans une catégorie et comment les modèles déterminent la théorie. Deux feuilles de travail, pages 33 et 34, notent le critère de reconnaissance d'un foncteur « tripleable », avec trois noms que la transcription lit avec doute, « Beck, Barr, Linton » (161-2, lot 2, p. 33), puis le critère de descente pour un morphisme de topos, conclu par « $B_\pi \xrightarrow{\simeq} B$ (th) » (161-2, lot 2, p. 34). La page 60 énonce un corollaire sur les catégories cocomplètes, « Ce sont ces E qu'il faudrait appeler « accessibles » » (161-2, lot 3, p. 60), que la page 61 démontre (161-2, lot 4, p. 61). La page 77 établit, pour les théories définies par limites finies, le lemme $\mathrm{Ind}(\Sigma) \simeq S$ (161-2, lot 4, p. 77).

Conventions. Les notations de la section 26 valent ici : pour une adjonction $f \dashv g$, $f : A \to B$, $h : A \to \varphi$-**Coalg** est le foncteur de comparaison vers les coalgèbres de $\varphi = fg$; dualement, pour $F \dashv U$, $U : A \to B$, le foncteur de comparaison va de A dans les algèbres de la monade $\mathbb{T} = UF$. Une double flèche est *réflexive* si ses deux flèches ont une section commune, *coréflexive* si elles ont une rétraction commune.

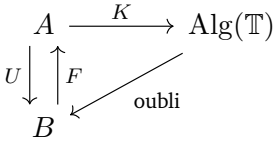
Énoncé (Théorème de monadicité, page 33 ; théorème de Beck)**.** *Un foncteur $U : A \to B$ admettant un adjoint à gauche F est monadique ($A \simeq \mathrm{Alg}(\mathbb{T})$, $\mathbb{T} = UF$) si U est conservatif et si A a et U préserve les coégalisateurs des paires réflexives.*

Lemme 5.1. *Soit $f \dashv g$ une adjonction, $f : A \to B$. Si f est conservatif, si A a les noyaux des doubles flèches coréflexives et si f y commute, le foncteur de comparaison h est une équivalence.*

Démonstration. Pour toute coalgèbre (X, a), la double flèche $(\eta_{gX}, g(a))$ est coréflexive (lemme 26.2) ; elle a donc un noyau, auquel f commute. Le lemme 26.3 (3) conclut. C'est le dual du théorème de monadicité « grossier » de Beck (Mac Lane 1998, § VI.7 [93]). □

Démonstration du théorème de monadicité. C'est l'énoncé dual. Le foncteur $U^\circ : A^\circ \to B^\circ$ est adjoint à gauche de F° ; la monade UF sur B devient la comonade $U^\circ F^\circ$ sur B°, dont les coalgèbres sont les opposées des $\mathbb{T}$-algèbres, et le foncteur de comparaison devient celui du lemme 5.1. Les coégalisateurs de paires réflexives de A sont les noyaux de paires coréflexives de A°, et U° est conservatif. Le lemme 5.1 s'applique. □

Le diagramme place au-dessus de B le foncteur de comparaison K, $KX = (UX, U\varepsilon_X)$ où ε est la coünité de $F \dashv U$; le théorème dit quand K est une équivalence.



$$\mathbb{T} = UF, \quad \text{oubli} \circ K = U.$$

6. Preuve vérifiée : `lean/Grothendieck/Folder161_2.lean`.

Définition. Soient E une catégorie localement petite et κ un cardinal régulier. Un objet X de E est *κ-présentable* si $\mathrm{Hom}_E(X, -)$ commute aux limites inductives κ-filtrantes, et *présentable* s'il l'est pour un κ ; c'est l'« accessible » de la page. Une sous-catégorie pleine $\mathcal{C}$ de E est *dense* si, pour tout X, la flèche canonique $\varinjlim_{\mathcal{C}_{/X}} Y \to X$ est un isomorphisme ; c'est la condition a) par laquelle la page 56 définit une sous-catégorie « strictement génératrice ». La catégorie E est *localement présentable* si elle est cocomplète et s'il existe un cardinal régulier κ et un petit ensemble d'objets κ-présentables dont tout objet est limite inductive κ-filtrante ; c'est le sens de « E est équivalente à un $\mathrm{Ind}_\pi(\mathcal{C})$, $\mathcal{C}$ petite ».

Énoncé (Corollaire, pages 60 et 61 ; théorème de Gabriel–Ulmer)**.** *Une catégorie localement petite et cocomplète E est localement présentable si et seulement si elle admet une petite sous-catégorie pleine dense formée d'objets présentables.*

Démonstration. Supposons E localement κ-présentable. La sous-catégorie pleine P des objets κ-présentables est essentiellement petite et dense : c'est classique (Gabriel et Ulmer [56] ; Adámek et Rosický [1]). Soit $Q \subseteq P$ une petite sous-catégorie pleine contenant un représentant de chaque classe d'isomorphisme ; l'inclusion $Q \to P$ est une équivalence, et le composé d'une équivalence et d'un foncteur dense est dense, donc Q est dense dans E. Ses objets sont κ-présentables, donc présentables.

Réciproquement, soit P une petite sous-catégorie pleine dense dont chaque objet X est κ_X-présentable pour un cardinal régulier κ_X. Comme P est petite, la famille des κ_X est majorée par un cardinal c. Soit κ_0 le successeur de $\max(c, \aleph_0)$; c'est un cardinal régulier, comme tout successeur d'un cardinal infini. Toute limite inductive κ_0-filtrante étant κ_X-filtrante, chaque $X \in P$ est κ_0-présentable. Une sous-catégorie dense est fortement génératrice (classique). Or une catégorie cocomplète qui admet un petit ensemble fortement générateur d'objets κ_0-présentables est localement κ_0-présentable : c'est le théorème 1.20 d'Adámek et Rosický [1]. Donc E est localement présentable. □

Énoncé (Lemme, page 77)**.** *Soient R une petite catégorie à limites finies, $S = \underline{\mathrm{Hom}}_{\mathrm{lex}}(R, \mathrm{Ens})$ et $\Sigma \simeq R^\circ \subset S$ la sous-catégorie pleine des structures représentables. Le foncteur d'inclusion $\Sigma \to S$ induit une équivalence $\mathrm{Ind}(\Sigma) \simeq S$.*

Démonstration. On identifie S aux préfaisceaux $X : \Sigma^\circ \to \mathrm{Ens}$ exacts à gauche, la catégorie $\Sigma = R^\circ$ ayant les limites inductives finies, et $\mathrm{Ind}(\Sigma)$ à la sous-catégorie pleine des préfaisceaux sur Σ qui sont limites inductives filtrantes de représentables. Il suffit de montrer que ces deux sous-catégories pleines ont les mêmes objets. Un représentable est exact à gauche, et les limites inductives filtrantes commutent aux limites projectives finies dans Ens ; tout ind-objet est donc exact à gauche. Réciproquement, soit X exact à gauche. Tout préfaisceau est la limite inductive des représentables sur sa catégorie des éléments $\Sigma_{/X}$, et celle-ci est filtrante : elle est non vide, car X envoie l'objet initial de Σ sur un point ; deux éléments $x \in X(a)$, $y \in X(b)$ proviennent de $X(a \sqcup b) = X(a) \times X(b)$; deux flèches $u, v : (a, x) \rightrightarrows (b, y)$ sont égalisées par la flèche vers le coégalisateur c de u, v, puisque $X(c)$ est le noyau de $X(u), X(v) : X(b) \rightrightarrows X(a)$, qui contient y. C'est le fait classique que les ind-objets d'une petite catégorie à limites inductives finies sont ses préfaisceaux exacts à gauche (Grothendieck et Verdier, SGA 4, exposé I, § 8 [7]), que la preuve vérifiée invoque. □

Remarque. Le corollaire est le théorème de caractérisation des catégories localement présentables de Gabriel et Ulmer, publié en 1971 [56], dans l'intervalle où l'inventaire date la cote. Il

est démontré ici pour la notion moderne ; le $\mathrm{Ind}_\pi(\mathcal{C})$ de SGA 4 que la page emploie n'est pas formalisé. Le lemme de la page 77 est le cas des limites finies de la dualité de Gabriel–Ulmer.

Remarque. Les deux feuilles de travail des pages 33 et 34 se lisent ensemble : le lemme 5.1, appliqué à l'image inverse u^* d'un morphisme de topos surjectif, conservative et exacte à gauche, présente le topos de base comme catégorie de coalgèbres de u^*u_* (voir la dernière remarque de la section 26) ; c'est une lecture possible du critère de descente de la page 34, que la transcription ne permet pas de reconstituer. Les énoncés encadrés ci-dessous portent sur la logique des topos classifiants : une théorie géométrique a un topos classifiant, ses sous-topos correspondent à ses quotients, et la cohérence du topos traduit la finitude des axiomes. Les sous-catégories réflexives de la section 28 en sont le cadre : un sous-topos est une sous-catégorie réflexive à réflecteur exact à gauche.

Ne sont pas démontrés ici : l'adjonction entre théories de Lawvere et monades (page 33) ; le théorème de la page 54 et le corollaire de la page 55 ; le lemme de la page 59, sur Ind_π et les filtrations cardinales ; le corollaire de la page 77 ; la liste de la page 56 ; la Δ-enveloppe (pages 3 à 31) ; les topos classifiants (pages 17 à 24 et 36 à 52) ; les pages 62 à 76 et 78 à 111, dont le corps universel (pages 92 à 95).

Théorème (Grothendieck, pages 39, 41 et 42, deux topos classifiants non cohérents ♦). *Les sous-topos classifiants des anneaux à spectre irréductible (nilradical premier) et des anneaux à spectre de dimension zéro ne sont pas cohérents : les topologies qui les présentent sur les schémas affines de type fini sur* $\mathbf{Z}$ *ne sont pas quasi-compactes, bien que chacun soit un sous-topos du topos classifiant cohérent des anneaux. La page demande s'ils ont assez de points.*

◊ non vérifié en Lean

Théorème (D'après les pages 47 à 49, anneaux de caractéristique définie ♦). *Les anneaux localement de caractéristique p pour un nombre premier p ou de caractéristique 0 sont classifiés par un sous-topos du topos classifiant des anneaux qui n'est pas cohérent et n'est pas défini par une condition ouverte : c'est la réunion du sous-topos ouvert $X_{\mathrm{car}>0} = \bigcup_p X_{\mathbf{Z}/p}$ et du sous-topos non ouvert $X_{\mathbf{Q}} = \bigcap_n X_{\mathbf{Z}[1/n]}$. La réunion de deux sous-topos V, W d'un topos s'obtient par recollement le long d'un ouvert dès qu'il existe des ouverts Z' de V et Z'' de W tels que $Z'' \wedge V$ soit ouvert dans V, $Z' \wedge W$ ouvert dans W, $V = \sup(Z', Z'' \wedge V)$ et $W = \sup(Z'', Z' \wedge W)$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 47 et 48). Le critère de recollement y est un brouillon, mis en forme par l'édition.

Théorème (D'après les pages 92 à 95, le corps universel, forme complétée par l'édition ♦). *Le topos classifiant des corps est le topos des faisceaux sur l'opposée de la catégorie des anneaux commutatifs absolument plats de présentation finie, pour la topologie engendrée par les recouvrements $\mathrm{Spec}\, A_f \sqcup \mathrm{Spec}\, A/f \to \mathrm{Spec}\, A$, le faisceau structural étant le corps générique.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 41, 42 et 92 à 95). L'identification des pseudo-corps aux anneaux absolument plats est de l'édition.

Partie 7

Analyse fonctionnelle

6 Cote 1 : le système d'inégalités des valeurs singulières, coefficients de Fredholm [7]

La cote 1, *Analyse fonctionnelle : notes manuscrites (s.d.), lettre (1953)*, compte cent quarante-neuf pages, que l'inventaire date de 1953. Les pages 70 à 73 sont une mise au net sur les puissances extérieures des opérateurs à trace. La page 71 démontre, pour u, v à trace, l'inégalité $\alpha_n(|u+v|) \leq \sum_p \alpha_p(|u|)\,\alpha_{n-p}(|v|)$ (corollaire 2, formule (14), encadrée), par le développement de $\Lambda^n(u+v)$ en produits $(\Lambda^p u)\wedge(\Lambda^{n-p}v)$. Elle énonce ensuite le théorème 2 pour u, v compacts : la forme produit (15), encadrée, et « plus précisément » le système (16), encadré lui aussi,

$$\sigma_n^m(u+v) \leq \sum_{p=0}^{m} \sigma_n^p(u)\,\sigma_n^{m-p}(v), \qquad 0 \leq m \leq n,$$

où $\sigma_n^m(w)$ est la fonction symétrique élémentaire de degré m des n premières valeurs singulières de w (formule (17)). La marge gauche porte « à réviser » le long du théorème (1, lot 4, p. 71). La page 72 démontre (16) par la proposition 3, $\sigma_n^m(u) = \sup|\alpha_m(v_n u)|$ sur les contractions v_n de rang $\leq n$, et par (14) appliquée à wu et wv (1, lot 4, p. 72). La page 73 juge le système, en mots lus avec doute, « les plus fortes possibles » des inégalités qui majorent les $\rho_i(u+v)$ en fonction des $\rho_i(u)$ et des $\rho_i(v)$ (1, lot 4, p. 73).

La piste porte sur le système (16) tout entier. On le démontre d'abord en dimension finie pour $m \leq 2$ et pour tout n, sur $\mathbb{R}$ comme sur $\mathbb{C}$: pour $m = 0$ les deux membres valent 1, pour $m = 1$ c'est l'inégalité de Ky Fan, et le cas $m = 2$ suit la voie de la page par Λ^2, écrite avec des mineurs d'ordre 2. On démontre aussi que le système, s'il vaut pour tous les $m \leq n$, entraîne la forme produit (15). Le dernier encadré de la section démontre le système pour tous m et n, en dimension finie complexe, d'où (15) pour tout n et la sous-additivité de S_p des pages 128 et 129 ; deux encadrés le suivent, qui l'étendent à la dimension finie réelle et démontrent la proposition 3 comme borne supérieure atteinte.

Conventions. Les espaces E et F sont des espaces préhilbertiens de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$, et $d = \dim E$. Pour $T : E \to F$ linéaire, les valeurs singulières $s_0(T) \geq s_1(T) \geq \cdots$ sont les racines carrées des valeurs propres de T^*T, rangées par ordre décroissant et répétées selon leur multiplicité, prolongées par 0 au-delà de l'indice $d-1$. C'est la définition de la bibliothèque, qui indexe à partir de 0 ; les $\rho_1, \ldots, \rho_n$ de la page sont $s_0, \ldots, s_{n-1}$. On note $(e_j)_{j<d}$ une base orthonormée de vecteurs propres de T^*T, rangée dans le même ordre, de sorte que $T^*Te_j = s_j(T)^2 e_j$, et l'on pose $f_j = s_j(T)^{-1}\,Te_j$, avec $f_j = 0$ lorsque $s_j(T) = 0$. Enfin

$$\sigma_n^m(T) = \sum_{\substack{t\subseteq\{0,\ldots,n-1\}\\ |t|=m}} \prod_{i\in t} s_i(T).$$

Énoncé (Pages 71 et 72, le système (16) pour $m \leq 1$ ♦). *Soient $u, v : E \to F$ linéaires et $n \geq 0$.*

7. Preuve vérifiée : `lean/Grothendieck/Folder1.lean`.

1. *(Ky Fan)* $\sum_{j<n} s_j(u+v) \le \sum_{j<n} s_j(u) + \sum_{j<n} s_j(v)$.
2. *Pour* $m \in \{0,1\}$, $\sigma_n^m(u+v) \le \sum_{p=0}^{m} \sigma_n^p(u)\,\sigma_n^{m-p}(v)$.

Énoncé (Page 71, du système (16) à la forme produit (15))**.** *Soient* $u, v : E \to F$ *linéaires et* $n \ge 0$*. Si* $\sigma_n^m(u+v) \le \sum_{p=0}^{m} \sigma_n^p(u)\,\sigma_n^{m-p}(v)$ *pour tout* $m \le n$*, alors pour tout* $r \ge 0$

$$\prod_{i<n}\bigl(1 + r\,s_i(u+v)\bigr) \le \prod_{i<n}\bigl(1 + r\,s_i(u)\bigr)\prod_{i<n}\bigl(1 + r\,s_i(v)\bigr).$$

En particulier $1 + r\,s_0(u+v) \le (1 + r\,s_0(u))(1 + r\,s_0(v))$.

Lemme 6.1. *Soient* $(y_i)_{i\in I}$ *une famille finie de vecteurs deux à deux orthogonaux, de normes* ≤ 1*, et* z *un vecteur. Alors* $\sum_i |\langle y_i, z\rangle|^2 \le \|z\|^2$.

Démonstration. Posons $c_i = \langle y_i, z\rangle$, $p = \sum_i c_i y_i$ et $S = \sum_i |c_i|^2$. On a $\langle p, z\rangle = \sum_i \bar{c}_i c_i = S$. Par l'orthogonalité, $\langle y_i, p\rangle = c_i \|y_i\|^2$, d'où $\|p\|^2 = \sum_i |c_i|^2 \|y_i\|^2 \le S$. L'inégalité de Cauchy-Schwarz donne $S \le \|p\|\,\|z\|$, donc $S^2 \le \|p\|^2\|z\|^2 \le S\,\|z\|^2$. Si $S > 0$, on divise par S ; si $S = 0$, il n'y a rien à démontrer. □

Lemme 6.2. *Soient* $(s_j)_{j\ge 0}$ *une suite réelle positive et décroissante, et* $c_0, \dots, c_{d-1}$ *des réels de* $[0,1]$ *de somme* $\le n$*. Alors* $\sum_{j<d} s_j c_j \le \sum_{j<n} s_j$.

Démonstration. Posons $\varepsilon_j = 1$ si $j < n$ et $\varepsilon_j = 0$ sinon. Pour tout $j < d$, on a $s_j c_j \le \varepsilon_j s_j + s_n(c_j - \varepsilon_j)$. Si $j < n$, cela s'écrit $s_j(c_j - 1) \le s_n(c_j - 1)$, qui vient de $s_j \ge s_n$ et $c_j \le 1$; si $j \ge n$, cela s'écrit $s_j c_j \le s_n c_j$, qui vient de $s_j \le s_n$ et $c_j \ge 0$. En sommant, $\sum_j s_j c_j \le \sum_{j<\min(n,d)} s_j + s_n\bigl(\sum_j c_j - \min(n,d)\bigr)$. La somme des c_j est $\le n$ par hypothèse et $\le d$ puisque chaque c_j est ≤ 1 ; le second terme est donc ≤ 0, et le premier est $\le \sum_{j<n} s_j$ puisque les s_j sont positifs. □

Lemme 6.3. *Soit* $T : E \to F$ *linéaire. Pour tous* j, $k < d$, $\langle Te_j, Te_k\rangle = s_k(T)^2\langle e_j, e_k\rangle$*. En conséquence* $\|Te_j\| = s_j(T)$, $Te_j = s_j(T)\,f_j$*, les* f_j *sont deux à deux orthogonaux et de normes* ≤ 1*, et* $\langle f_j, Te_j\rangle = s_j(T)$.

Démonstration. On a $\langle Te_j, Te_k\rangle = \langle e_j, T^*Te_k\rangle = s_k(T)^2\langle e_j, e_k\rangle$. Pour $j = k$, cela donne $\|Te_j\|^2 = s_j(T)^2$. Si $s_j(T) = 0$, alors $Te_j = 0 = s_j(T)f_j$; sinon $s_j(T)f_j = Te_j$ par définition. Pour $j \ne k$, $\langle f_j, f_k\rangle$ est un multiple de $\langle Te_j, Te_k\rangle = 0$. La norme de f_j vaut $s_j(T)^{-1}s_j(T)$, c'est-à-dire 1, ou 0 si $s_j(T) = 0$. Enfin $\langle f_j, Te_j\rangle = s_j(T)^{-1}\|Te_j\|^2 = s_j(T)$, les deux membres étant nuls si $s_j(T) = 0$. □

Lemme 6.4 (principe de Ky Fan, majoration)**.** *Soient* $T : E \to F$ *linéaire,* I *un ensemble fini à au plus* n *éléments,* $(x_i)_{i\in I}$ *dans* E *et* $(y_i)_{i\in I}$ *dans* F *deux familles chacune formée de vecteurs deux à deux orthogonaux de normes* ≤ 1*. Alors*

$$\Bigl|\sum_{i\in I}\langle y_i, Tx_i\rangle\Bigr| \le \sum_{j<n} s_j(T).$$

Résultat général, démontré en Lean dans
`Upstream/SingularValuesSigmaTwo.lean` *; la démonstration n'est pas reprise ici.*

Démonstration du premier énoncé. (1) Appliquons le lemme 6.3 à $w = u+v$, et soit I l'ensemble des $j < d$ tels que $j < n$; il a $\min(n, d)$ éléments. Comme $s_j(w) = 0$ pour $j \geq d$, $\sum_{j<n} s_j(w) = \sum_{j\in I} s_j(w) = \sum_{j\in I} \langle f_j, we_j\rangle$, et cette somme est égale à

$$\sum_{j\in I} \langle f_j, ue_j\rangle + \sum_{j\in I} \langle f_j, ve_j\rangle.$$

Les familles (e_j) et (f_j), indexées par I, vérifient les hypothèses du lemme 6.4. Appliqué à $T = u$ puis à $T = v$, il majore les deux sommes en module par $\sum_{j<n} s_j(u)$ et $\sum_{j<n} s_j(v)$.

(2) On a $\sigma_n^0 = 1$, la seule partie à 0 élément étant vide, et $\sigma_n^1(T) = \sum_{j<n} s_j(T)$. Pour $m = 0$, l'inégalité est $1 \leq 1$. Pour $m = 1$, son second membre est $\sigma_n^1(v) + \sigma_n^1(u)$, et c'est (1). □

Démonstration du second énoncé. En développant le produit,

$$\textstyle\prod_{i<n}(1 + ra_i) = \sum_{m=0}^{n} r^m e_m(a_0, \ldots, a_{n-1}),$$

où e_m est la fonction symétrique élémentaire de degré m ; appliqué aux valeurs singulières, cela donne $\prod_{i<n}(1 + rs_i(T)) = \sum_{m\leq n} r^m \sigma_n^m(T)$. Posons $A_m = \sigma_n^m(u)$, $B_m = \sigma_n^m(v)$ et $C_m = \sigma_n^m(u + v)$, tous positifs. L'hypothèse donne

$$\sum_{m\leq n} r^m C_m \leq \sum_{m\leq n} \sum_{p\leq m} r^p A_p\, r^{m-p} B_{m-p}.$$

En échangeant les sommations et en posant $k = m - p$, le second membre est la somme des $r^p A_p\, r^k B_k$ sur les couples (p, k) tels que $p + k \leq n$. Les termes étant positifs, elle est au plus la somme sur tous les couples $p, k \leq n$, qui vaut $\big(\sum_{p\leq n} r^p A_p\big)\big(\sum_{k\leq n} r^k B_k\big)$. Pour $n = 1$, l'hypothèse porte sur $m \in \{0, 1\}$ et c'est le premier énoncé. □

Remarque. Pour $m = 1$, le système (16) est l'inégalité de Ky Fan, publiée en 1951 [49] ; l'inventaire date la cote de 1953. L'inégalité est démontrée ici par la voie classique du principe du maximum, et non par celle des pages 71 et 72, qui passe par les puissances extérieures, le corollaire 2 et la proposition 3 ; pour $m = 1$, la démonstration de la page revient d'ailleurs au même principe : $\alpha_1(|wu|) = \operatorname{Tr}|wu|$ avec w de rang $\leq n$ et de norme ≤ 1. La bibliothèque utilisée définit les valeurs singulières d'une application linéaire entre espaces de dimension finie et en démontre la décroissance, mais elle ne contient ni le principe de Ky Fan ni son inégalité (voir aussi [15]). Le lemme 6.4 ne demande pas que les familles soient orthonormées : il suffit qu'elles soient orthogonales et de normes ≤ 1, et l'on peut donc y prendre la famille (f_j), dont certains termes peuvent être nuls.

Remarque. Le second énoncé est l'implication que la page énonce par « et plus précisément » : le système (16) donne (15) coefficient par coefficient, sans autre hypothèse que la positivité des valeurs singulières. La réciproque n'est pas démontrée ici ; la piste affirme que le système est strictement plus fort que (15), et ce point n'est pas vérifié. Pour $n = 1$, (15) se réduit à $s_0(u + v) \leq s_0(u) + s_0(v)$, qui est l'inégalité triangulaire pour la norme d'opérateur. La ligne coupée au bas de la page 71 mentionne (16) et $n = 1$; le reste de la ligne est illisible.

Théorème 6.5 (Grothendieck, pages 71 et 72, le système (16) pour $m = 2$ ♦). *Soient*

$u, v : E \to F$ linéaires et $n \geq 0$. Alors

$$\sigma_n^2(u+v) \leq \sigma_n^2(u) + \sigma_n^1(u)\,\sigma_n^1(v) + \sigma_n^2(v).$$

Le système (16) vaut donc pour $m \leq 2$ et tout n, et la forme produit (15) pour $n \leq 2$.

Notations. Pour une partie finie I, des familles $(x_i)_{i\in I}$ dans E, $(y_i)_{i\in I}$ dans F et $T, T' : E \to F$, on pose

$$B(T,T') = \sum_{i,j\in I} \big(\langle y_i, Tx_i\rangle\langle y_j, T'x_j\rangle - \langle y_i, Tx_j\rangle\langle y_j, T'x_i\rangle\big),$$

somme des mineurs principaux mixtes d'ordre 2 des matrices $(\langle y_i, Tx_j\rangle)$ et $(\langle y_i, T'x_j\rangle)$, prise sur les couples ordonnés. Pour des familles (g_k), (g'_l), (h_i) d'un même espace, on pose $M_{kl,ij} = \langle g_k, h_i\rangle\langle g'_l, h_j\rangle - \langle g_k, h_j\rangle\langle g'_l, h_i\rangle$, qui est $\langle g_k \wedge g'_l, h_i \wedge h_j\rangle$ au sens de Λ^2, puis $\Lambda_{kl} = \sum_{i,j\in I} |M_{kl,ij}|^2$ et $p_k = \sum_{i\in I} |\langle g_k, h_i\rangle|^2$.

Lemme 6.6 (Lagrange)**.** *Pour des scalaires a_i, b_i indexés par un ensemble fini I, $\sum_{i,j\in I} |a_i b_j - a_j b_i|^2 \leq 2 \sum_i |a_i|^2 \sum_i |b_i|^2$. En particulier $\Lambda_{kl} \leq 2\, p_k\, p'_l$, où p'_l est formé avec (g'_l).*

Résultat général, démontré en Lean dans
`Upstream/SingularValuesSigmaTwo.lean` *; la démonstration n'est pas reprise ici.*

Lemme 6.7 (poids pour σ^2)**.** *Soient K un ensemble fini, $G \subseteq K$, des réels $s_k \geq 0$ et $\theta \geq 0$ avec $s_k \geq \theta$ pour $k \in G$ et $s_k \leq \theta$ pour $k \notin G$. Soient (α_{kl}) symétrique, à coefficients dans $[0,1]$, de diagonale nulle, et $p_k \in [0,1]$ avec $\sum_k p_k \leq |G|$ et $\sum_l \alpha_{kl} \leq (|G|-1)\, p_k$ pour tout k. Alors*

$$\sum_{k,l} \alpha_{kl}\, s_k s_l \leq \Big(\sum_{k\in G} s_k\Big)^2 - \sum_{k\in G} s_k^2.$$

Démonstration. Posons $g = |G|$, $m_k = \min(s_k, \theta)$ et $d_k = s_k - m_k$. On a $0 \leq m_k \leq \theta$, $d_k \geq 0$, $m_k = \theta$ sur G et $d_k = 0$ hors de G ; soit $D = \sum_{k\in G} d_k$. On développe $s_k s_l = m_k m_l + m_k d_l + d_k m_l + d_k d_l$ et l'on majore les quatre sommes. D'abord $\sum \alpha_{kl} m_k m_l \leq \theta^2 \sum_k (g-1) p_k \leq \theta^2 (g-1) g$; si $g = 0$, la somme des p_k est nulle. Ensuite $\sum \alpha_{kl} m_k d_l \leq \theta \sum_l d_l \sum_k \alpha_{lk} \leq \theta \sum_l d_l (g-1) p_l \leq \theta (g-1) D$, car $d_l = 0$ hors de G et $g \geq 1$ dès que G a un élément ; de même pour $\sum \alpha_{kl} d_k m_l$. Enfin $\sum \alpha_{kl} d_k d_l \leq \sum_{k\neq l} d_k d_l = D^2 - \sum_{k\in G} d_k^2$. Le total vaut $g(g-1)\theta^2 + 2(g-1)\theta D + D^2 - \sum_G d_k^2$, et c'est $(g\theta + D)^2 - \sum_G (\theta + d_k)^2$, le second membre. □

Lemme 6.8 (Cauchy–Binet pour les mineurs d'ordre 2)**.** *Dans un anneau commutatif, si $A_{ij} = \sum_k s_k P_{ik} Q_{kj}$ et $C_{ij} = \sum_l t_l P'_{il} Q'_{lj}$, alors*

$$2 \sum_{i,j} (A_{ii} C_{jj} - A_{ij} C_{ji}) = \sum_{k,l} s_k t_l \sum_{i,j} (P_{ik} P'_{jl} - P_{jk} P'_{il})(Q_{ki} Q'_{lj} - Q_{kj} Q'_{li}).$$

Démonstration. On développe le produit de droite en quatre termes ; l'échange de i et j identifie le quatrième au premier et le troisième au deuxième. Le membre de gauche, développé par bilinéarité, donne les mêmes termes. □

Démonstration du troisième énoncé. Si $n = 0$, les deux membres sont nuls. Sinon, soient $w = u + v$, I l'ensemble des $j < d$ tels que $j < n$, $x_i = e_i(w)$ et $y_i = f_i(w)$ pour $i \in I$; ces familles sont orthogonales et de normes ≤ 1 (lemme 6.3), et $|I| \leq n$.

Le cas $T = T' = w$. On a $\langle f_i(w), we_j(w)\rangle = s_i(w)$ si $i = j$ et 0 sinon. Donc $B(w,w) = \sum_{i,j\in I} s_i s_j - \sum_{i\in I} s_i^2 = (\sum_I s_i)^2 - \sum_I s_i^2$, avec $s_i = s_i(w)$. Comme $s_i(w) = 0$ pour $i \geq d$, cette quantité est $(\sum_{i<n} s_i)^2 - \sum_{i<n} s_i^2 = 2\sigma_n^2(w)$.

Bilinéarité. $B(w,w) = B(u,u) + B(u,v) + B(v,u) + B(v,v)$.

Majoration générale. Pour T, écrivons $s_k = s_k(T)$, $e_k = e_k(T)$, $f_k = f_k(T)$, et de même t_l, e'_l, f'_l pour T'. Le développement de x sur (e_k) donne $\langle y, Tx\rangle = \sum_k s_k \overline{\langle f_k, y\rangle}\, \langle e_k, x\rangle$. Le lemme 6.8, avec $P_{ik} = \overline{\langle f_k, y_i\rangle}$ et $Q_{kj} = \langle e_k, x_j\rangle$, donne

$$2B(T,T') = \sum_{k,l} s_k t_l \sum_{i,j\in I} \overline{M^f_{kl,ij}}\, M^e_{kl,ij},$$

où M^f est formé avec (f_k), (f'_l), (y_i) et M^e avec (e_k), (e'_l), (x_i). Par $|ab| \leq (|a|^2 + |b|^2)/2$, on obtient $|B(T,T')| \leq \frac{1}{4}\sum_{k,l} s_k t_l (\Lambda^f_{kl} + \Lambda^e_{kl})$.

Le terme mixte. Le lemme 6.6 donne $\Lambda^f_{kl} \leq 2q_k q'_l$ et $\Lambda^e_{kl} \leq 2p_k p'_l$, où q_k, q'_l, p_k, p'_l sont formés avec les familles correspondantes. D'où $|B(T,T')| \leq \frac{1}{2}\big[(\sum_k s_k q_k)(\sum_l t_l q'_l) + (\sum_k s_k p_k)(\sum_l t_l p'_l)\big]$. Comme dans la démonstration du lemme 6.4, les poids p_k, q_k sont dans $[0,1]$ et de somme $\leq |I| \leq n$, et le lemme 6.2 donne $\sum_k s_k p_k \leq \sigma_n^1(T)$, et de même pour les trois autres sommes. Donc $|B(T,T')| \leq \sigma_n^1(T)\,\sigma_n^1(T')$.

Le terme pur. Prenons $T' = T$ et $\alpha_{kl} = \Lambda^e_{kl}/2$. La matrice (α_{kl}) est symétrique ($M^e_{lk,ij} = -M^e_{kl,ij}$), de diagonale nulle ($M^e_{kk,ij} = 0$) et à coefficients dans $[0,1]$ par le lemme 6.6. Pour ses lignes, on écrit $M^e_{kl,ij} = \langle e_l, z\rangle$ avec $z = \langle e_k, x_i\rangle x_j - \langle e_k, x_j\rangle x_i$; le lemme 6.1 appliqué à la famille (e_l) donne $\sum_l |M^e_{kl,ij}|^2 \leq \|z\|^2$, et $\|z\|^2 \leq |\langle e_k, x_i\rangle|^2 + |\langle e_k, x_j\rangle|^2$ si $i \neq j$, tandis que $z = 0$ si $i = j$. En sommant sur $i \neq j$, $\sum_l \alpha_{kl} \leq (|I| - 1)\, p_k$. Le lemme 6.7, appliqué avec $G = I$ et $\theta = s_{n-1}(T)$ (la suite est décroissante, donc $s_k \geq \theta$ pour $k < n$ et $s_k \leq \theta$ pour $k \geq n$), donne $\sum_{k,l} \alpha_{kl} s_k s_l \leq (\sum_I s_k)^2 - \sum_I s_k^2 = 2\sigma_n^2(T)$. Le même raisonnement vaut pour $\Lambda^f/2$, avec la famille (f_l) dans le lemme 6.1. Donc $|B(T,T)| \leq \frac{1}{2}(2\sigma_n^2(T) + 2\sigma_n^2(T)) = 2\sigma_n^2(T)$.

Conclusion. $2\sigma_n^2(w) = |B(w,w)| \leq 2\sigma_n^2(u) + 2\sigma_n^1(u)\sigma_n^1(v) + 2\sigma_n^2(v)$. Avec le premier énoncé, cela donne (16) pour $m \leq 2$, et le second énoncé donne (15) pour $n \leq 2$, l'hypothèse portant sur $m \leq n \leq 2$. □

Remarque. La démonstration suit la voie de la page 71 par Λ^2 sans construire l'espace hilbertien $\Lambda^2 E$: le produit scalaire $\langle a\wedge b, c\wedge d\rangle = \langle a,c\rangle\langle b,d\rangle - \langle a,d\rangle\langle b,c\rangle$ y est remplacé par les mineurs $M_{kl,ij}$, et la formule de Cauchy–Binet et l'identité de Lagrange tiennent lieu de structure hilbertienne. Le terme mixte $B(u,v)+B(v,u)$ correspond à $u\wedge v + v\wedge u$, et sa borne $2\,\sigma_n^1(u)\sigma_n^1(v)$ est celle que donne la constante $p!\,q!/(p+q)! = 1/2$ de la page pour $p = q = 1$. Le terme pur $|B(T,T)| \leq 2\sigma_n^2(T)$ est la majoration de la proposition 3 pour $m = 2$, restreinte aux contractions de la forme $\sum_i x_i\langle y_i, \cdot\rangle$ à familles orthogonales. L'inégalité de Ky Fan appliquée à $\Lambda^2 T$ n'y suffirait pas : elle majore par la somme des $\binom{n}{2}$ plus grands produits $s_i s_j$, qui peut dépasser $\sigma_n^2(T)$ (pour $n = 3$ et $s = (2,1,1,1)$, elle vaut 6 et $\sigma_3^2 = 5$). La majoration des lignes $\sum_l \alpha_{kl} \leq (|I| - 1)\, p_k$, propre aux vecteurs décomposables, rend possible le lemme 6.7. L'énoncé vaut tel que la page l'écrit pour $m = 2$, sans hypothèse supplémentaire.

Coefficients de Fredholm (pages 123 et 124). Pour un opérateur T, $\alpha_k(T)$ désigne le coefficient de X^k dans $\det(1 + XT)$, c'est-à-dire la trace de $\Lambda^k T$; $|A| = (A^*A)^{1/2}$ et $|A^*| = (AA^*)^{1/2}$. La page 123 encadre le corollaire 2, la page 124 le corollaire 3, pour des opérateurs nucléaires (1, lot 7, p. 123, 1, lot 7, p. 124).

Théorème 6.9 (Grothendieck, pages 123 et 124, corollaires 2 et 3, en dimension finie ♦). *Soient A, B des matrices carrées complexes. Pour tout k,*

$$|\alpha_k(A+B)|^2 \le \alpha_k(|A|+|B|)\,\alpha_k(|A^*|+|B^*|),$$

et $|\det(1+A+B)| \le \frac{1}{2}\big[\det(1+|A|+|B|)+\det(1+|A^*|+|B^*|)\big]$.

L'énoncé tient tel que la page l'écrit (Lean : `corollaire2`, `corollaire3`). La même démonstration donne la forme géométrique, énoncé de l'édition : $|\det(1+A+B)|^2 \le \det(1+|A|+|B|)\det(1+|A^*|+|B^*|)$.

Remarque. La démonstration n'est pas le développement multilinéaire de la page. La matrice par blocs $\left(\begin{smallmatrix} |A| & A^* \\ A & |A^*| \end{smallmatrix}\right)$ est $|H|+H$ pour $H = \left(\begin{smallmatrix} 0 & A^* \\ A & 0 \end{smallmatrix}\right)$, donc positive ; on ajoute celles de A et de B, on restreint aux mineurs principaux, où le complément de Schur et la croissance du déterminant donnent $|\det T_S|^2 \le \det P_S \det Q_S$, puis on applique l'inégalité de Cauchy–Schwarz à la somme des mineurs. Le cas des opérateurs nucléaires n'est pas formalisé.

La sous-additivité de S_p par le déterminant (pages 126 à 139). Pour $0<p<1$, on note $S_p(u)=\sum_i s_i(u)^p$ la somme des puissances p-ièmes des valeurs singulières. Ce n'est pas une norme, et l'inégalité $S_p(u+v)\le S_p(u)+S_p(v)$ n'a rien d'évident. La page 129 dit ne connaître qu'une méthode analytique pour l'obtenir. Pour un réel $s\ge 0$, s^p s'écrit comme une intégrale de $\log(1+vs)$ contre la mesure $v^{-1-p}\,dv$ sur $]0,\infty[$ (lemme 1, p. 128). En sommant sur les valeurs singulières, $S_p(u)$ devient l'intégrale de $\log\det(1+v|u|)$, et l'inégalité de déterminants (15) passe sous l'intégrale (1, lot 7, p. 129). Ainsi la page déduit la sous-additivité de (15), démontrée plus haut pour $n\le 2$ et, en dimension finie complexe, pour tout n dans le dernier encadré de la section.

Théorème 6.10 (D'après les pages 128 et 129, en dimension finie ♦). *Soit $0<p<1$ et $K_p=\int_0^\infty \log(1+t)\,t^{-1-p}\,dt$. Alors $K_p>0$ et $s^pK_p=\int_0^\infty \log(1+vs)\,v^{-1-p}\,dv$ pour tout $s\ge 0$. Si des réels positifs vérifient $\prod_{i<n}(1+ra_i)\le\prod_{i<n}(1+rb_i)\prod_{i<n}(1+rc_i)$ pour tout $r\ge 0$, alors $\sum_{i<n}a_i^p\le\sum_{i<n}b_i^p+\sum_{i<n}c_i^p$. En particulier $\sum_{i<n}s_i(u+v)^p\le\sum_{i<n}s_i(u)^p+\sum_{i<n}s_i(v)^p$ dès que (15) vaut pour cet n, donc pour $n\le 2$.*

La déduction de la page est juste. Lean vérifie la représentation intégrale par changement de variable $t=vs$, sans calculer K_p, qui vaut $\pi/(p\sin\pi p)$; la sous-additivité de S_p en dimension finie complexe, pour tout n, découle du dernier encadré (théorèmes `integral_kernel`, `sum_rpow_le_of_prod_le`, `sum_singularValues_rpow_add_le`).

Ne sont pas démontrés ici : la borne $p!\,q!/(p+q)!$ de la page 71 sur $\|(\Lambda^p u)\wedge(\Lambda^q v)\|_1$ et la formule (14) pour des opérateurs à trace ; la seconde forme de la proposition 3, $\sup\alpha_m(|v_nu|)$, et la proposition 3 sur $\mathbb{R}$ (sur $\mathbb{C}$ en dimension finie, voir plus bas) ; le passage de la dimension finie aux opérateurs compacts entre espaces de Hilbert ; l'assertion de la page 73 sur l'optimalité du système ; la proposition 4 ; les pages 74 et 75, sur la sous-additivité des fonctions concaves des valeurs singulières ; les corollaires 2 et 3 des pages 123 et 124 pour des opérateurs nucléaires ; l'inégalité de Weyl $\sum|\lambda_i|^p\le S_p$ par la formule de Jensen et l'inégalité de Hölder des pages 130 à 139.

Théorème 6.11 (Grothendieck, pages 71 à 73, le système (16), en dimension finie ♦). *Soient E, F des espaces hilbertiens complexes de dimension finie et $u,v : E\to F$ linéaires.*

Pour tous entiers n et m,

$$\sigma_n^m(u+v) \le \sum_{p=0}^{m} \sigma_n^p(u)\,\sigma_n^{m-p}(v).$$

Par conséquent, pour tout n et tout $r \ge 0$, $\prod_{i<n}(1+rs_i(u+v)) \le \prod_{i<n}(1+rs_i(u))\prod_{i<n}(1+rs_i(v))$, et, pour $0<p<1$, $\sum_{i<n} s_i(u+v)^p \le \sum_{i<n} s_i(u)^p + \sum_{i<n} s_i(v)^p$.

L'énoncé tient tel que la page l'écrit, pour tout m, en dimension finie (Lean : `sigma_system`, `prod_one_add_singularValues_add_le`, `sum_singularValues_rpow_add_le`). Pour $m > n$, le premier membre est nul. La démonstration utilise les coefficients $\alpha_m(M) = \sum_{|K|=m} \det M_K$ du paragraphe précédent, pour des matrices carrées quelconques, et quatre lemmes de matrices.

Lemme 6.12. *1. (Sylvester) Pour X de taille $k\times l$ et Y de taille $l\times k$, $\alpha_m(XY) = \alpha_m(YX)$.*

2. Pour des matrices carrées A et D, $\alpha_m\left(\begin{smallmatrix} A & 0 \\ 0 & D\end{smallmatrix}\right) = \sum_{p\le m} \alpha_p(A)\,\alpha_{m-p}(D)$.

3. (Fischer) Si $M = \left(\begin{smallmatrix} A & B \\ B^* & D\end{smallmatrix}\right)$ est positive, $\det M \le \det A \det D$.

4. (Cauchy–Schwarz) Pour X de taille $k\times l$ et Y de taille $l\times k$, $|\det XY|^2 \le \det(XX^*)\det(Y^*Y)$.

Démonstration. (1) Par définition, $\alpha_m(M)$ est le coefficient de X^m dans $\det(1+XM)$, et $\det(1+X\,XY) = \det(1+YX\,X)$ (identité de Sylvester, sur l'anneau des polynômes). (2) Le déterminant d'une matrice diagonale par blocs est le produit des déterminants des blocs : $\det(1+XM)$ est le produit de $\det(1+XA)$ et de $\det(1+XD)$, dont on compare les coefficients. (3) Si $\det A = 0$, un vecteur $z \ne 0$ vérifie $Az = 0$; la positivité de M donne alors $M(z,0) = 0$, et $\det M = 0$. Sinon A est définie positive, $\det M = \det A \det(D - B^*A^{-1}B)$ (complément de Schur), et $D - B^*A^{-1}B$, $B^*A^{-1}B$ sont positives ; la croissance du déterminant (démonstration des corollaires 2 et 3) donne $\det(D - B^*A^{-1}B) \le \det D$. (4) La matrice $\left(\begin{smallmatrix} X \\ Y^*\end{smallmatrix}\right)\left(\begin{smallmatrix} X^* & Y\end{smallmatrix}\right) = \left(\begin{smallmatrix} XX^* & XY \\ Y^*X^* & Y^*Y\end{smallmatrix}\right)$ est positive, et l'inégalité $|\det T|^2 \le \det P \det Q$ de la démonstration des corollaires 2 et 3 s'applique. □

Lemme 6.13 (entrelacement)**.** *Soient $s_0 \ge s_1 \ge \cdots \ge 0$, $S = \operatorname{diag}(s_0,\dots,s_{d-1})$ et Ψ une matrice $d\times d$ telle que $\|\Psi z\|^2 \le \sum_{j<n} |z_j|^2$ pour tout $z \in \mathbb{C}^d$. Alors*

$$\alpha_p(\Psi^* S \Psi) \le \sum_{\substack{t\subseteq\{0,\dots,n-1\} \\ |t|=p}} \prod_{i\in t} s_i.$$

Démonstration. La matrice $N = \Psi^* S \Psi$ est hermitienne positive ; soient $\lambda_0 \ge \cdots \ge \lambda_{d-1} \ge 0$ ses valeurs propres et (b_l) une base orthonormée de vecteurs propres associés. En diagonalisant N par une matrice unitaire U, le lemme 6.12 (1) donne $\alpha_p(N) = \alpha_p(\operatorname{diag}(\lambda))$, c'est-à-dire la fonction symétrique élémentaire de degré p des λ_i. Celle-ci croît avec chacune de ses variables positives ; il suffit donc de montrer que $\lambda_i \le s_i$ si $i < n$ et que $\lambda_i = 0$ si $i \ge n$. C'est l'argument de dimension du principe du min-max. Fixons i et imposons à $z \in \mathbb{C}^d$ les conditions $\langle b_l, z\rangle = 0$ pour $l > i$, et $(\Psi z)_k = 0$ pour $k < i$ si $i < n$, ou $z_k = 0$ pour $k < i$ si $i \ge n$. Cela fait $(d-1-i)+i < d$ équations linéaires : il existe $z \ne 0$ qui les vérifie. D'une part, $\langle z, Nz\rangle = \sum_l \lambda_l |\langle b_l, z\rangle|^2$, où seuls les $l \le i$ comptent et $\lambda_l \ge \lambda_i$, d'où $\langle z, Nz\rangle \ge \lambda_i \|z\|^2$. D'autre part, $\langle z, Nz\rangle = \sum_k s_k |(\Psi z)_k|^2$. Si $i < n$, les termes $k < i$ sont nuls et $s_k \le s_i$ pour $k \ge i$, d'où $\langle z, Nz\rangle \le s_i \|\Psi z\|^2 \le s_i \|z\|^2$. Si $i \ge n$, les z_j d'indice $j < n \le i$ sont nuls, donc $\Psi z = 0$ par l'hypothèse, et $\langle z, Nz\rangle = 0$. On divise par $\|z\|^2 > 0$. □

Démonstration du théorème. Posons $T = u + v$; soient (e_j, f_j) ses vecteurs de Schmidt (conventions du début de la section), et $x_j = e_j$, $y_j = f_j$ pour $j < n$, $x_j = y_j = 0$ pour $n \le j < d$. Pour $w : E \to F$ linéaire, notons C_w la matrice $d \times d$ de coefficients $\langle y_i, w x_j \rangle$.

Le premier membre. Le lemme 6.3 montre que C_T est diagonale, de coefficients $s_j(T)$ pour $j < n$ et 0 ensuite. Ses mineurs principaux sont des produits de coefficients diagonaux, et $\sigma_n^m(T) = \alpha_m(C_T)$, les $s_j(T)$ d'indice $j \ge d$ étant nuls.

Factorisation. Soient $w \in \{u, v\}$, $(e_k(w), f_k(w))$ ses vecteurs de Schmidt et $S_w = \operatorname{diag}(s_k(w))$. En écrivant $x_j = \sum_k \langle e_k(w), x_j \rangle\, e_k(w)$ et $w\, e_k(w) = s_k(w) f_k(w)$, on obtient $\langle y_i, w x_j \rangle = \sum_k \langle y_i, f_k(w) \rangle\, s_k(w)\, \langle e_k(w), x_j \rangle$, c'est-à-dire

$$C_w = (S_w^{1/2} \Phi_w)^* (S_w^{1/2} \Psi_w), \qquad \Phi_w = \big(\langle f_k(w), y_j \rangle\big)_{k,j}, \quad \Psi_w = \big(\langle e_k(w), x_j \rangle\big)_{k,j}.$$

Comme $C_T = C_u + C_v$, on a $C_T = G^* H$, où H (resp. G) est la matrice $2d \times d$ formée des blocs $S_u^{1/2}\Psi_u$ et $S_v^{1/2}\Psi_v$ (resp. $S_u^{1/2}\Phi_u$ et $S_v^{1/2}\Phi_v$) placés l'un sous l'autre.

Cauchy–Schwarz et Fischer. Par le lemme 6.12 (1),

$$\alpha_m(C_T) = \alpha_m(HG^*) = \sum_K \det(H_K G_K^*),$$

où K parcourt les parties à m éléments des deux copies de $\{0, \dots, d-1\}$ et H_K désigne les lignes de H d'indices dans K. Par (4), $|\det(H_K G_K^*)|^2 \le \det(HH^*)_K \det(GG^*)_K$. La matrice $(HH^*)_K$ est positive, et ses lignes se répartissent entre les deux copies ; par (3), $\det(HH^*)_K \le \det(P_H)_K$, où P_H est la partie diagonale par blocs de HH^*, de blocs $S_u^{1/2}\Psi_u\Psi_u^* S_u^{1/2}$ et $S_v^{1/2}\Psi_v\Psi_v^* S_v^{1/2}$. De même pour G. L'inégalité de Cauchy–Schwarz sur la somme en K donne

$$\sigma_n^m(T) \le \alpha_m(P_H)^{1/2}\, \alpha_m(P_G)^{1/2}.$$

Entrelacement. Par (2), $\alpha_m(P_H) = \sum_p \alpha_p(S_u^{1/2}\Psi_u\Psi_u^* S_u^{1/2})\, \alpha_{m-p}(S_v^{1/2}\Psi_v\Psi_v^* S_v^{1/2})$, et par (1), $\alpha_p(S_w^{1/2}\Psi_w\Psi_w^* S_w^{1/2}) = \alpha_p(\Psi_w^* S_w \Psi_w)$. Pour $z \in \mathbb{C}^d$, $(\Psi_w z)_k = \langle e_k(w), \sum_j z_j x_j \rangle$; le lemme 6.1 et l'orthogonalité des x_j, de normes ≤ 1 et nuls pour $j \ge n$, donnent $\|\Psi_w z\|^2 \le \|\sum_j z_j x_j\|^2 \le \sum_{j<n} |z_j|^2$. Le lemme 6.13 donne alors $\alpha_p(\Psi_w^* S_w \Psi_w) \le \sigma_n^p(w)$. Les $f_k(w)$ et les y_j vérifient les mêmes hypothèses, et le même raisonnement vaut pour G. Les deux facteurs sont donc majorés par $\sum_p \sigma_n^p(u)\, \sigma_n^{m-p}(v)$, d'où (16). La forme produit s'en déduit par l'énoncé « du système (16) à la forme produit (15) », et la sous-additivité de S_p par le théorème des pages 128 et 129. □

Remarque. La page majore $\|(\Lambda^p u) \wedge (\Lambda^q v)\|_1$ par $p!\, q!\, \|\Lambda^p u\|_1 \|\Lambda^q v\|_1/(p+q)!$, en déduit la formule encadrée (14), $\alpha_n(|u+v|) \le \sum_p \alpha_p(|u|)\, \alpha_{n-p}(|v|)$, puis (16) par la proposition 3. La démonstration ci-dessus garde le développement de $\Lambda^m(u+v)$, écrit avec des mineurs principaux, mais ne sépare jamais les termes mixtes : la factorisation de C_T à travers $\mathbb{C}^{2d}$ range u et v dans deux blocs, et c'est l'inégalité de Fischer qui les sépare ; la constante $p!\, q!/(p+q)!$ n'apparaît pas. Le lemme 6.13 est la moitié de la proposition 3 qui sert, la majoration de $|\alpha_m|$ d'une compression de w par $\sigma_n^m(w)$, pour des compressions par des familles orthogonales de normes ≤ 1. Lean écrit C_w (`compr`), sa factorisation (`compr_eq`), $\sigma_n^m(T) \le \operatorname{Re} \alpha_m(C_T)$ (`sigma_le_alpha_compr`), les points (1) à (4) du lemme 6.12 (`alpha_mul_comm`, `alpha_fromBlocks_zero`, `det_fromBlocks_le` et sa forme `det_le_det_blockMask`, `norm_det_mul_sq_le`), l'étape de Cauchy–Schwarz et Fischer (`norm_alpha_mul_conjTranspose_le`) et l'entrelacement (`eigenvalues`$_0$`_le_of_conj_diagonal`, `alpha_conj_diagonal_le`, avec l'hypothèse de Bessel `gramMat_bound`). Les lemmes de matrices sont écrits sur $\mathbb{C}$; le cas réel s'en déduit par complexification (énoncé

suivant), et la proposition 3 comme borne supérieure fait l'objet de l'énoncé d'après. Ne sont pas formalisés la formule (14) pour des opérateurs à trace et le passage aux opérateurs compacts, énoncé plus bas.

Théorème 6.14 (Grothendieck, pages 71 à 73, le système (16) sur $\mathbb{R}$ ♦). *Soient E, F des espaces euclidiens réels de dimension finie et $u, v : E \to F$ linéaires. Pour tous entiers n et m, $\sigma_n^m(u+v) \leq \sum_{p=0}^{m} \sigma_n^p(u)\,\sigma_n^{m-p}(v)$; par conséquent la forme produit (15) vaut pour tout n et tout $r \geq 0$, et $\sum_{i<n} s_i(u+v)^p \leq \sum_{i<n} s_i(u)^p + \sum_{i<n} s_i(v)^p$ pour $0 < p < 1$.*

L'énoncé tient tel que la page l'écrit (Lean : `sigma_system_real`, `prod_one_add_singularValues_add_le_real`, `sum_singularValues_rpow_add_le_real`).

Démonstration. On complexifie. Soient M la matrice réelle de u dans des bases orthonormées de E et de F, et $u_{\mathbb{C}} : \mathbb{C}^{\dim E} \to \mathbb{C}^{\dim F}$ l'application de matrice M lue sur $\mathbb{C}$. La matrice de u^*u dans la base orthonormée de E est $M^{\mathsf{T}}M$, celle de $u_{\mathbb{C}}^* u_{\mathbb{C}}$ est $M^*M = M^{\mathsf{T}}M$ lue sur $\mathbb{C}$: les deux opérateurs ont le même polynôme caractéristique, à l'inclusion $\mathbb{R} \subset \mathbb{C}$ près. Les valeurs propres d'un opérateur autoadjoint, rangées par ordre décroissant, sont les racines de ce polynôme ainsi rangées ; le polynôme réel est scindé sur $\mathbb{R}$, et ses racines dans $\mathbb{C}$ sont les mêmes. Donc u^*u et $u_{\mathbb{C}}^* u_{\mathbb{C}}$ ont les mêmes valeurs propres, et $s_i(u_{\mathbb{C}}) = s_i(u)$ pour tout i. Comme $(u+v)_{\mathbb{C}} = u_{\mathbb{C}} + v_{\mathbb{C}}$, le théorème complexe appliqué à $u_{\mathbb{C}}$ et $v_{\mathbb{C}}$ donne (16) ; (15) et la sous-additivité s'en déduisent comme sur $\mathbb{C}$. □

Théorème 6.15 (Grothendieck, page 72, la proposition 3 en dimension finie ♦). *Soient E, F des espaces hilbertiens complexes de dimension finie, $u : E \to F$ linéaire et m, n des entiers. Alors*

$$\sigma_n^m(u) = \max\bigl\{|\alpha_m(wu)| : w : F \to E \text{ linéaire},\ \|w\| \leq 1,\ \operatorname{rang} w \leq n\bigr\},$$

où $\alpha_m(wu)$ est le coefficient de X^m dans $\det(1 + X\,wu)$, calculé dans une base quelconque de E.

L'énoncé tient tel que la page l'écrit, sous la forme de la première égalité, et la borne supérieure est atteinte (Lean : `isGreatest_norm_alpha_comp`, `norm_alpha_comp_le`). La seconde forme, $\sup_w \alpha_m(|wu|)$, n'est pas formalisée.

Démonstration. Le coefficient α_m de la matrice d'un endomorphisme ne dépend pas de la base : un changement de base conjugue la matrice, et le lemme 6.12 (1) s'applique. *Majoration.* Soit w comme dans l'énoncé, et $w^* : E \to F$ son adjoint, contraction de même rang. Soient (e_i, f_i) les vecteurs de Schmidt de w^* et $t_i = s_i(w^*)$; alors $t_i \leq 1$, $t_i = 0$ pour $i \geq n$, et $w^* e_i = t_i f_i$. Dans la base (e_i), la matrice de wu a pour coefficients $\langle e_i, wu\,e_j\rangle = \langle w^* e_i, ue_j\rangle = t_i \langle f_i, ue_j\rangle$; elle s'écrit DN avec $D = \operatorname{diag}(\sqrt{t_i})$ et $N_{ij} = \sqrt{t_i}\langle f_i, ue_j\rangle$, et $\alpha_m(DN) = \alpha_m(ND)$, où $(ND)_{ij} = \langle y_i, ux_j\rangle$ pour $x_j = \sqrt{t_j}\,e_j$ et $y_i = \sqrt{t_i}\,f_i$. Ces deux familles sont orthogonales, de normes ≤ 1 et nulles à partir de l'indice n. Comme dans la démonstration du théorème complexe, la compression $(\langle y_i, ux_j\rangle)$ se factorise en $(S_u^{1/2}\Phi)^*(S_u^{1/2}\Psi)$; l'inégalité de Cauchy–Schwarz sur les mineurs (lemme 6.12 (4), sommée sur les parties K) et le lemme 6.13 appliqué à chaque facteur donnent $|\alpha_m(ND)| \leq \sigma_n^m(u)^{1/2}\,\sigma_n^m(u)^{1/2}$. *Égalité.* Soient (e_j, f_j) les vecteurs de Schmidt de u et $w_0 = \sum_{j<n} e_j \langle f_j, \cdot\rangle$; c'est une contraction par l'inégalité de Bessel, de rang $\leq n$, et la matrice de $w_0 u$ dans la base (e_j) est la compression C_u, diagonale de coefficients $s_j(u)$ pour $j < n$; donc $\alpha_m(w_0 u) = \sigma_n^m(u)$. □

Énoncé (Pages 71 et 72, opérateurs compacts ♦). *Soient u, v des opérateurs compacts entre espaces de Hilbert. Pour $0 \le m \le n$, $\sigma_n^m(u+v) \le \sum_{p=0}^m \sigma_n^p(u)\,\sigma_n^{m-p}(v)$, coefficient par coefficient ; ce système entraîne $\prod_{i\le n}(1+rs_i(u+v)) \le \prod_{i\le n}(1+rs_i(u))\prod_{i\le n}(1+rs_i(v))$ pour tout $r \ge 0$.*

◊ non vérifié en Lean

Démonstration de la page (pages 71 et 72). La page majore $\|(\Lambda^p u)\wedge(\Lambda^q v)\|_1$ par

◊ non vérifiée en Lean

$$\frac{p!\,q!}{(p+q)!}\,\|\Lambda^p u\|_1\,\|\Lambda^q v\|_1$$

et, en développant $\Lambda^n(u+v)$, obtient la formule encadrée (14),

$$\alpha_n(|u+v|) \le \sum_p \alpha_p(|u|)\,\alpha_{n-p}(|v|)$$

(p. 71). La proposition 3 écrit $\sigma_n^m(u)$ comme borne supérieure de $|\alpha_m(wu)|$ sur les w de norme ≤ 1 et de rang $\le n$ (p. 72). La formule (14) appliquée à $wu + wv$, puis la proposition 3, donnent (16), forme précise de (15). La prose de la page 72 est en grande partie illisible, et la page 71 porte en marge « à réviser ». En dimension finie complexe, l'énoncé est le théorème précédent ; pour des opérateurs compacts, il s'en déduirait en approchant u et v par des opérateurs de rang fini, ce que Lean ne fait pas.

7 Cote 113 : l'enveloppe de Karoubi et l'invariance de Morita [8]

La cote 113, *Abelianization : notes manuscrites (s.d.)*, douze pages que l'inventaire date « [à partir de 1982] », construit sous le titre « $\otimes$ dans Cat » le produit tensoriel de petites catégories k-linéaires, et montre qu'il calcule celui de leurs catégories de modules. Sur la page 3, pour P petite catégorie k-additive, P^k est *défini* comme $\mathrm{Hom}_{\mathbf{Z}}(P^\circ, Ab)$, identifié à $\mathrm{Hom}_k(P^\circ, Ab_k)$ avec la parenthèse « ne dépend pas du choix de la str. k-additive ». Le plongement $P \hookrightarrow P^k$ est une « inclusion additive pl. fid. », d'où « $\mathrm{Kar}\,P \approx \mathrm{Ul}\,\mathrm{Proj}(P^k)$ », les deux lettres devant « Proj » n'étant pas identifiées. Une note en marge ajoute « $P \to \mathrm{Kar}\,P$ induit $(\mathrm{Kar}\,P)^k \xrightarrow{\sim} P^k$ » (113, lot 1, p. 3). La lecture modernisée comprend la première équivalence comme $\mathrm{Kar}(P) \simeq \mathrm{Proj}_{\mathrm{tf}}(P^k)$, les projectifs de type fini, et nomme l'ensemble invariance de Morita.

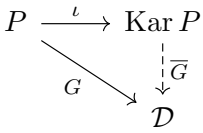
Définition. Soit P une catégorie. Son *enveloppe de Karoubi* $\mathrm{Kar}\,P$ a pour objets les couples (X, e) formés d'un objet X de P et d'un idempotent $e = e^2$ de $\mathrm{End}(X)$, et pour flèches $(X,e) \to (Y,e')$ les $f : X \to Y$ tels que $e'f = f = fe$; la composition est celle de P, et l'identité de (X,e) est e. Le foncteur $\iota : P \to \mathrm{Kar}\,P$ envoie X sur (X, id_X). Une catégorie est *karoubienne* si tout idempotent s'y scinde. Si P est préadditive, $\mathrm{Kar}\,P$ l'est aussi, ses groupes de flèches étant des sous-groupes de ceux de P.

Énoncé (Page 3, la note marginale). *Soient P une catégorie préadditive et $\mathcal{D}$ une catégorie préadditive karoubienne, par exemple Ab ou la catégorie des k-modules. La restriction le long de $\iota^\circ : P^\circ \to (\mathrm{Kar}\,P)^\circ$ est une équivalence de la catégorie des foncteurs additifs $(\mathrm{Kar}\,P)^\circ \to \mathcal{D}$ sur celle des foncteurs additifs $P^\circ \to \mathcal{D}$. Pour $\mathcal{D} = Ab$, c'est l'équivalence $(\mathrm{Kar}\,P)^k \simeq P^k$, avec la définition $P^k = \mathrm{Hom}_{\mathbf{Z}}(P^\circ, Ab)$ de la page.*

Lemme 7.1. *Soient P une catégorie et $\mathcal{D}$ une catégorie karoubienne. La restriction le long de $\iota : P \to \mathrm{Kar}\,P$ est une équivalence de la catégorie des foncteurs $\mathrm{Kar}\,P \to \mathcal{D}$ sur celle des foncteurs $P \to \mathcal{D}$.*

8. Preuve vérifiée : `lean/Grothendieck/Folder113.lean`.

Démonstration. C'est la propriété universelle classique de l'enveloppe de Karoubi, complétion libre par les rétractes : un foncteur $G : P \to \mathcal{D}$ se prolonge en envoyant (X, e) sur l'objet par lequel se scinde l'idempotent $G(e)$, et ce prolongement est unique à isomorphisme unique près. On ne la redémontre pas ici. □



$\overline{G} \circ \iota \simeq G$, $\quad \overline{G}(X, e) =$ l'objet par lequel se scinde $G(e)$.

Lemme 7.2. *Il existe un isomorphisme de catégories* $\mathrm{Kar}(P^\circ) \to (\mathrm{Kar}\, P)^\circ$*, bijectif sur les objets, qui fait commuter les plongements : le composé* $P^\circ \xrightarrow{\iota_{P^\circ}} \mathrm{Kar}(P^\circ) \to (\mathrm{Kar}\, P)^\circ$ *est* ι_P°*.*

Démonstration. Un objet de $\mathrm{Kar}(P^\circ)$ est un couple (X, e) où e est un idempotent de $\mathrm{End}_{P^\circ}(X) = \mathrm{End}_P(X)$; on l'envoie sur l'objet (X, e) de $(\mathrm{Kar}\, P)^\circ$. Une flèche $(X, e) \to (Y, e')$ de $\mathrm{Kar}(P^\circ)$ est une flèche $f : Y \to X$ de P telle que $fe' = f = ef$, c'est-à-dire exactement une flèche $(Y, e') \to (X, e)$ de $\mathrm{Kar}\, P$, ou encore une flèche $(X, e) \to (Y, e')$ de $(\mathrm{Kar}\, P)^\circ$; on l'envoie sur elle-même. Ce foncteur respecte identités et compositions, il est bijectif sur les objets et sur chaque ensemble de flèches. Sur $X \in P$, les deux composés donnent (X, id_X), et sur les flèches l'identité. □

Lemme 7.3. *Pour* $\mathcal{D}$ *karoubienne, la restriction le long de* $\iota_P^\circ : P^\circ \to (\mathrm{Kar}\, P)^\circ$ *est une équivalence de la catégorie des foncteurs* $(\mathrm{Kar}\, P)^\circ \to \mathcal{D}$ *sur celle des foncteurs* $P^\circ \to \mathcal{D}$*.*

Démonstration. Par le lemme 7.2, cette restriction est la composée de la restriction le long de l'isomorphisme $\mathrm{Kar}(P^\circ) \to (\mathrm{Kar}\, P)^\circ$, qui est une équivalence, et de la restriction le long de ι_{P°, qui en est une par le lemme 7.1 appliqué à P°. □

Lemme 7.4. *Toute flèche* $f : (X, e) \to (Y, e')$ *de* $\mathrm{Kar}\, P$ *s'écrit* $f = p' \circ \iota(f) \circ j$*, où* $j : (X, e) \to (X, \mathrm{id})$ *et* $p' : (Y, \mathrm{id}) \to (Y, e')$ *sont les flèches données par* e *et par* e'*.*

Résultat général, démontré en Lean dans
`Upstream/KaroubiAdditiveFunctors.lean` *; la démonstration n'est pas reprise ici.*

Lemme 7.5. *Soient* P *et* $\mathcal{D}$ *préadditives et* $F : (\mathrm{Kar}\, P)^\circ \to \mathcal{D}$ *un foncteur. Si* $F \circ \iota^\circ$ *est additif,* F *l'est.*

Démonstration. Par le lemme 7.4, pour toute flèche $h : (X, e) \to (Y, e')$ de $\mathrm{Kar}\, P$, on a $F(h) = F(j) \circ (F \circ \iota^\circ)(h) \circ F(p')$, les flèches j et p' ne dépendant que de la source et du but de h, et h étant regardée à droite comme une flèche $Y \to X$ de P°. Pour deux flèches h_1, h_2 de même source et de même but, la somme dans $\mathrm{Kar}\, P$ est la somme dans P ; l'additivité de $F \circ \iota^\circ$ et la bilinéarité de la composition dans $\mathcal{D}$ donnent alors $F(h_1 + h_2) = F(h_1) + F(h_2)$. □

Démonstration de l'énoncé. Les foncteurs additifs forment une sous-catégorie pleine de celle de tous les foncteurs. La restriction le long de ι° étant pleinement fidèle sur tous les foncteurs par le lemme 7.3, elle l'est sur les foncteurs additifs, et elle envoie un foncteur additif sur un foncteur additif. Elle est essentiellement surjective : soit $G : P^\circ \to \mathcal{D}$ additif ; par le lemme 7.3, il existe $F : (\mathrm{Kar}\, P)^\circ \to \mathcal{D}$ et un isomorphisme $F \circ \iota^\circ \simeq G$; un foncteur isomorphe à un foncteur additif est additif, donc $F \circ \iota^\circ$ l'est, et F est additif par le lemme 7.5. Les catégories Ab et des k-modules sont préadditives et karoubiennes, tout idempotent y ayant une image. □

Remarque. L'énoncé ne demande ni que P soit petite, ni que le but soit abélien. Il suffit que P soit préadditive et $\mathcal{D}$ préadditive et karoubienne ; l'énoncé vaut en particulier pour les foncteurs additifs à valeurs dans les k-modules.

Remarque. L'enveloppe porte le nom de Karoubi, qui l'emploie en K-théorie en 1968 [78]. L'énoncé est l'invariance de la catégorie des modules par passage à cette enveloppe, déduite de sa propriété universelle. Le nom d'invariance de Morita renvoie à la caractérisation par Morita, en 1958, des anneaux dont les catégories de modules sont équivalentes [101].

Ne sont pas démontrés ici : la forme k-linéaire de l'invariance de Morita ; l'indépendance de la structure k-additive ; l'équivalence $\mathrm{Kar}\, P \simeq \mathrm{Proj}_{\mathrm{tf}}(P^k)$; le théorème de Freyd–Mitchell ; l'énoncé 2-fonctoriel ; les pages 5 à 12 (produit tensoriel, contre-exemple ($\circledast$), produit dérivé).

Partie 8

Théorie de la dualité

Aucune lettre du fonds ne porte sur la cote 125, que l'inventaire date « [avant 1970] ». Deux lettres situent la dualité dans ces années. Le 10 décembre 1965, il envoie à Deligne une démonstration plus simple de la dualité en cohomologie p-adique et sa forme relative (5, lot 3, p. 49). Le 4 août 1969, Hartshorne lui écrit sur les notes de Jouanolou destinées à SGA 5 (37, lot 3, p. 53).

8 Cote 43 : polynômes additifs modulo $F-1$ et perfection [9]

La cote 43, *Dualité des groupes. Jacobiennes généralisées etc*, réunit des liasses sur le corps de classes, les jacobiennes généralisées de Rosenlicht, la dualité de Cartier et les accouplements de Tate et de Lang ; la carte la date de 1964–1965. Aux pages 165 à 169, un lemme identifie $\mathrm{Ext}^1_{S\text{-gr}}(G,\Gamma)$ aux classes primitives de $H^1(G,\Gamma)$, puis la page 169 écrit, pour une base S de caractéristique p (43, lot 9, p. 165) :

$$\mathrm{Ext}^1_{S\text{-gr}}(\mathbb{G}_a,\mathbb{Z}/p\mathbb{Z})\simeq\Gamma(S,\mathcal{O}^{p^{-\infty}}),\qquad \mathcal{O}^{p^{-\infty}}=\varinjlim\big(\mathcal{O}\xrightarrow{x\mapsto x^p}\mathcal{O}\xrightarrow{x\mapsto x^p}\cdots\big).$$

Pour voir d'où vient la perfection, on observe qu'une extension de $\mathbb{G}_a$ par $\mathbb{Z}/p\mathbb{Z}$ sur $S=\operatorname{Spec}R$ est un revêtement d'Artin–Schreier $x^p-x=f(t)$, et elle est compatible à l'addition quand f est un *polynôme additif*, $f(t)=\sum_i a_i t^{p^i}$; deux tels f donnent la même classe quand ils diffèrent d'un g^p-g, g additif. La lecture remarque que, modulo ces g^p-g, tout polynôme additif se ramène à un seul terme $a\,t$ avec a dans la perfection. On démontre ici ce cœur algébrique, sur une base affine quelconque.

Notations. Soient p premier et R un anneau commutatif de caractéristique p. On note $R\{F\}$ le groupe des polynômes additifs $\sum_i a_i t^{p^i}$, suites presque nulles (a_i) d'éléments de R. La composition à gauche par $F:t\mapsto t^p$ envoie $\sum a_i t^{p^i}$ sur $\sum a_i^p t^{p^{i+1}}$, qui est $(\sum a_i t^{p^i})^p$ en caractéristique p ; on pose $D=F-1$, de sorte que $D(f)=f^p-f$. La perfection $R^{p^{-\infty}}$ est l'ensemble des classes de couples (i,a), où (i,a) représente $a^{p^{-i}}$ et $(i+1,a^p)$ s'identifie à (i,a) ; on note $[a]_i$ cette classe.

Théorème (D'après la lecture des pages 165 à 169, S affine ♦). *L'application $\Phi:R\{F\}\to R^{p^{-\infty}}$, $\sum_i a_i t^{p^i}\mapsto\sum_i[a_i]_i$, est un homomorphisme surjectif de groupes, de noyau exactement l'image de $D=F-1$. Elle induit un isomorphisme de groupes*

$$R\{F\}/(F-1)R\{F\}\ \simeq\ R^{p^{-\infty}}.$$

De plus, modulo l'image de D, tout polynôme additif est égal à un seul terme $c\,t^{p^M}$, pour tout M assez grand.

Démonstration. L'application $a\mapsto[a]_i$ est additive : $[a]_i+[b]_i=[a^{p^i}+b^{p^i}]_{2i}=[(a+b)^{p^i}]_{2i}=[a+b]_i$, par la règle de somme de la perfection et l'additivité de Frobenius. Donc Φ est additive.

9. Preuve vérifiée : `lean/Grothendieck/Folder43.lean`.

Elle tue l'image de D : $\Phi(F(a\,t^{p^i})) = [a^p]_{i+1} = [a]_i$, d'où $\Phi \circ F = \Phi$ et $\Phi \circ D = 0$. Elle est surjective, puisque $[a]_n = \Phi(a\,t^{p^n})$.

Pour le noyau, on monte d'un cran : $a\,t^{p^N} - a^p\,t^{p^{N+1}} = -D(a\,t^{p^N})$, et par récurrence $a\,t^{p^N} \equiv a^{p^z}\,t^{p^{N+z}}$ modulo l'image de D pour tout z. Un polynôme $\sum_{i\le N} a_i t^{p^i}$ est donc congru à $c\,t^{p^M}$ pour tout $M \ge N$, avec $c = \sum_i a_i^{p^{M-i}}$: c'est la dernière assertion. Si $\Phi(f) = 0$ et $f \equiv c\,t^{p^M}$, alors $[c]_M = 0$ dans la perfection, ce qui signifie $c^{p^z} = 0$ pour un z. Alors $c\,t^{p^M} \equiv c^{p^z}\,t^{p^{M+z}} = 0$, et f est dans l'image de D. L'isomorphisme s'en déduit par passage au quotient. □

Remarque. Aucune hypothèse de réduction ni de noethérianité n'intervient : les éléments x tels que $x^{p^z} = 0$, qui forment le noyau de $R \to R^{p^{-\infty}}$, sont absorbés par $F - 1$. La parenthèse de la page qui semble évoquer « l'hypothèse noethérienne » n'a donc pas lieu d'être pour ce cœur algébrique. En Lean, $R\{F\}$ est représenté par les suites presque nulles, et l'identification $D(f) = f^p - f$ avec le polynôme est vérifiée dans $R[t]$.

Ne sont pas démontrés ici les deux énoncés suivants de la cote. Le premier est la formule de la page 169 telle qu'elle est écrite : il y faut en outre le lemme des pages 166 à 168 sur les classes primitives, son invariance par homéomorphisme universel, le passage à une base non affine et la représentabilité par des pro-schémas parfaits.

Théorème (Grothendieck, pages 165 à 169, $\mathrm{Ext}^1(\mathbf{G}_a, \mathbf{Z}/p\mathbf{Z})$ et perfection ♦). *Sur une base quelconque S de caractéristique p, $\mathrm{Ext}^1_{S\text{-}gr}(\mathbf{G}_a, \mathbf{Z}/p\mathbf{Z}) \simeq \Gamma(S, \mathcal{O}^{p^{-\infty}})$, sections globales de la perfection $\varinjlim(\mathcal{O} \to \mathcal{O} \to \cdots)$ pour $x \mapsto x^p$. Le foncteur $\mathrm{Ext}^1(\mathbf{G}_a, \mathbf{Z}/p\mathbf{Z})$ est donc représentable parmi les pro-schémas parfaits sur S.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 166 à 168) : ils démontrent le lemme des classes primitives et son invariance par homéomorphisme universel, mais pas la formule elle-même, et le mot « parfaits » est incertain. Mathlib n'a pas les Ext de schémas en groupes. On se reportera aux notes de Grothendieck (43, lot 9, p. 165).

Théorème (D'après les pages 70 à 74, forme corrigée par l'édition, concentration de la cohomologie locale ♦). *Soient A un anneau local régulier de dimension d contenant un corps algébriquement clos k, et G un groupe algébrique commutatif sur k. La cohomologie locale de Zariski $H^i_{\mathfrak{a}}(\mathrm{Spec}\,A, G)$ au point fermé est nulle pour $i \neq d$; elle vaut $G(K)/G(A)$ pour $d = 1$ et $H^{d-1}(\mathrm{Spec}\,A - \mathfrak{a}, U)$ pour $d \ge 2$, où U est la partie unipotente de G. Le foncteur $G \mapsto H^d_{\mathfrak{a}}(G)$ est donc exact sur les suites localement triviales ; cette exactitude sert à définir la jacobienne locale $J_{A/k}$ de la page 74.*

◊ non vérifié en Lean

La clôture algébrique de k est ajoutée par l'édition, et presque tous les mots de la prose sont de lecture incertaine. Mathlib n'a pas la cohomologie locale à valeurs dans un groupe algébrique. On se reportera aux notes de Grothendieck (43, lot 4, p. 70).

9 Cote 101 : la dualité locale en dimension un pour tous les modules [10]

La cote 101, *Cohomologie locale : notes manuscrites (s.d.)*, quarante-deux pages que l'inventaire date « [à partir de 1967-1968] », énonce page 10, pour A local régulier complet de dimension n, $X = \mathrm{Spec}\,A$ et $I = H^n_x(\mathcal{O}_X)$, que les applications de dualité $\varphi^i_F : \mathrm{Ext}^{n-i}(X; F, \mathcal{O}_X) \to$

10. Preuve vérifiée : `lean/Grothendieck/Folder101.lean`.

$\mathrm{Hom}(H^i_x(F), I)$ sont des isomorphismes pour tout $\mathcal{O}_X$-module F, « pas nécessairement quasi-cohérent » (101, lot 1, p. 10). Pour $n = 1$, les pages 10 et 11 le démontrent. Un $\mathcal{O}_X$-module est un triplet (M_0, M_1, u) : un A-module M_0, un K-espace vectoriel M_1 et une application A-linéaire $u : M_0 \to M_1$, avec $H^0_x(F) = \operatorname{Ker} u$ et $H^1_x(F) = \operatorname{Coker} u$. La résolution injective $\mathcal{O}_X \to \underline{K}_X \to \underline{K}_X/\mathcal{O}_X$ donne $\mathrm{Ext}^\bullet(X; F, \mathcal{O}_X)$ comme cohomologie du complexe $\mathrm{Hom}_K(M_1, K) \to \mathrm{Hom}_A(M_0, K/A)$, $g \mapsto g \circ u \bmod A$. La page conclut par trois faits : a) un homomorphisme d'un K-espace vectoriel dans A est nul ; b) $\mathrm{Ext}^1_A(K, A) = 0$, parce que A est complet ; c) K/A est injectif.
Conventions. On travaille dans le modèle de la page, dont on admet la réduction : l'équivalence entre $\mathcal{O}_X$-modules et triplets, et le calcul des Ext par la résolution. Ext^0 est le noyau et Ext^1 le conoyau de $g \mapsto g \circ u \bmod A$.

Le diagramme suivant montre le complexe et les deux applications de dualité du théorème ci-dessous ; la flèche horizontale du milieu est $g \mapsto g \circ u \bmod A$:

$$\begin{array}{ccccccc} \mathrm{Ext}^0 & \hookrightarrow & \mathrm{Hom}_K(M_1, K) & \to & \mathrm{Hom}_A(M_0, K/A) & \twoheadrightarrow & \mathrm{Ext}^1 \\ \downarrow & & & & & & \downarrow \\ \mathrm{Hom}_A(\operatorname{Coker} u, K/A) & & & & & & \mathrm{Hom}_A(\operatorname{Ker} u, K/A) \end{array}$$

Théorème 9.1 (Grothendieck, pages 10 et 11, dimension un ♦). *Soit A un anneau de valuation discrète complet, de corps des fractions K. Pour tout triplet (M_0, M_1, u), les applications $\mathrm{Ext}^0 \to \mathrm{Hom}_A(\operatorname{Coker} u, K/A)$, $g \mapsto (g \bmod A)$, et $\mathrm{Ext}^1 \to \mathrm{Hom}_A(\operatorname{Ker} u, K/A)$, restriction, sont bijectives.*

Démonstration. Soit ϖ une uniformisante. Fait a) : si $g(m) = y \neq 0$, alors $g((\varpi y)^{-1} m) = \varpi^{-1} \in A$, absurde. Fait b) : soit $f : K \to K/A$ linéaire et $c_n \in K$ avec $f(\varpi^{-n}) = c_n \bmod A$. Comme $\varpi f(\varpi^{-n-1}) = f(\varpi^{-n})$, les $d_n = \varpi^n c_n$ vérifient $d_{n+1} - d_n \in \varpi^n A$; par complétude, $d_n - d_0$ converge vers $e \in A$, avec $d_0 + e - d_n \in \varpi^n A$. Pour $c = d_0 + e$, on a $c\,\varpi^{-n} - c_n \in A$ pour tout n, donc $f(x) = cx \bmod A$ pour tout $x = a\varpi^{-n}$. Sur une base de M_1, tout $h : M_1 \to K/A$ se relève ainsi en une application K-linéaire $M_1 \to K$. Fait c) : A est principal et K/A divisible, d'où le critère de Baer.

L'injectivité sur Ext^0 est a) appliqué à une différence. Pour la surjectivité, un $\psi : \operatorname{Coker} u \to K/A$ donne $h : M_1 \to K/A$ nul sur $u(M_0)$, qui se relève par b) en g, et $g \circ u$ est à valeurs dans A. La surjectivité sur Ext^1 est c). Pour l'injectivité, un $h : M_0 \to K/A$ nul sur $\operatorname{Ker} u$ se factorise par $u(M_0) \subset M_1$, s'étend à M_1 par c), se relève par b) en $g : M_1 \to K$, et $h = g \circ u \bmod A$. □

Remarque. L'énoncé tient tel que la page le démontre ; la complétude ne sert qu'en b). La fin de l'argument d'injectivité, en partie illisible sur la page, est rétablie par la lecture dans cet ordre, et Lean la confirme. Les deux pages ne numérotent pas les applications de la même façon. La page 10 les indexe par le degré de cohomologie locale, si bien que φ^1 part de Ext^0 ; la page 11 écrit au contraire $E^0 \xrightarrow{\varphi^0} \mathrm{Hom}(\operatorname{Coker} u, K/A)$. Les noms `phi0` et `phi1` du code Lean suivent la page 11.

La note de la lecture qui cite de mémoire l'équivalence entre $\mathrm{Ext}^1_A(K, A) = 0$ et la complétude est exacte ; c'est la réciproque de b).

Énoncé (Réciproque du fait b), note de la lecture ♦). *Soit A un anneau de valuation discrète, de corps des fractions K. Alors A est complet si et seulement si toute application A-linéaire $K \to K/A$ se relève en une application A-linéaire $K \to K$, autrement dit si et seulement si*

$\mathrm{Hom}_A(K,K) \to \mathrm{Hom}_A(K,K/A)$ *est surjective, ce qui équivaut à* $\mathrm{Ext}^1_A(K,A)=0$ *puisque* K *est injectif.*

Démonstration. Le sens direct est b). Réciproquement, A est séparé pour la topologie $\mathfrak{m}$-adique (Krull). Soit (e_n) une suite de Cauchy, $e_m - e_n \in \varpi^n A$ pour $n \leqslant m$. Pour $x \in K$ et n tel que $\varpi^n x \in A$, la classe de $e_n x$ modulo A ne dépend pas de n, car $(e_m - e_n)x \in \varpi^n x A \subset A$; elle définit une application A-linéaire $f : K \to K/A$. Un relèvement g de f vérifie $g(1) \equiv e_0 \bmod A$, donc $g(1) \in A$, et $g(1) - e_n = \varpi^n\big(g(\varpi^{-n}) - e_n\varpi^{-n}\big) \in \varpi^n A$: la suite converge vers $g(1)$. □

Ne sont pas démontrés ici : l'équivalence entre $\mathcal{O}_X$-modules et triplets, et le calcul des Ext (et, en particulier, l'identification de $\mathrm{Ext}^1_A(K,A)$ au conoyau de $\mathrm{Hom}_A(K,K) \to \mathrm{Hom}_A(K,K/A)$, qui n'est pas formalisée) et des H^i_x dans ce modèle. En dimension 2 la dualité échoue, et la page 14 le découvre (piste `101-sheaf-duality-dim-two-fails`, ci-dessous) :

Contre-exemple (pages 10, 14 et 15, dualité locale en dimension deux ♦). *La première phrase de la page 10 affirme les isomorphismes de dualité locale en toute dimension ; ils tombent en défaut en dimension 2. Soient A un anneau local régulier complet de dimension 2, $f \in \mathfrak{m}$ non nul, $U = X_f$ et $F = j_!\mathcal{O}_U$ sur $X = \mathrm{Spec}\, A$. L'application $A_f = \mathrm{Ext}^0(X; F, \mathcal{O}_X) \to \mathrm{Hom}_A(H^2_x(F), E(k))$ est injective et non surjective : la dualité locale à duaux de Matlis algébriques ne vaut pas pour les $\mathcal{O}_X$-modules non quasi-cohérents.*

◊ non vérifié en Lean

La page 14 conclut « φ n'est pas surjective », souligné deux fois, sans démonstration, et une phrase commencée page 14, achevée page 15, dit qu'il faut des duaux topologiques. Mathlib n'a pas la cohomologie locale ni la dualité de Matlis.

10 Cote 125 : la carte des équivalences et le lemme du feuillet III-18 [11]

La cote 125, *Dualité projective : notes manuscrites (s.d.)*, datée par l'inventaire « [avant 1970] », compte huit feuillets, dont une chemise titrée de sa main « Dualité locale et dualité … projective ». Le feuillet 2 est une carte : six énoncés encadrés, reliés par des doubles flèches verticales, pour $\mathbf{P}^n \supset X^r \supset Y^m$, $r > m > 0$. Le premier énoncé est la suite exacte de cohomologie locale, marquée d'une astérisque ; la flèche du deuxième encadré au troisième porte le seul mot du feuillet, « dualité », entouré (125, lot 1, p. 2). Le feuillet 3 est une page de tapuscrit numérotée III-18, annotée d'une autre main. Elle établit qu'un homomorphisme $u : A^n \to B$ bijectif sur les germes en un point l'est sur un voisinage, avec en marge la justification « puisque Y est noethérien et B de type fini par hypothèse » (125, lot 1, p. 3). La lecture modernisée donne les trois premiers étages de la carte et ce lemme, seules parties du dossier qui ne dépendent ni de la dualité de Serre ni du complété formel ; on les démontre ici.

Énoncé (Feuillet 2, trois premiers étages ♦ 6 ♦ 9). *Soient X une variété projective de dimension r, $Y \subset X$ un fermé de dimension m, F un faisceau cohérent sur X. Les énoncés suivants sont équivalents :*

1. *(premier étage)* $H^p(X - Y, F) = 0$ *pour* $p \geqslant m$ *;*
2. *(deuxième étage)* $H^p_Y(X,F) \to H^p(X,F)$ *est bijectif pour* $p > m$ *et surjectif pour* $p = m$ *;*

11. Preuve vérifiée : `lean/Grothendieck/Folder125.lean`.

3. *(troisième étage)* $\mathrm{Ext}^q_{\mathcal{O}_X}(F, \Omega^r_{X/k}) \to \mathrm{Ext}^q_{\mathcal{O}_{\widehat{X}}}(\widehat{F}, \widehat{\Omega}^r_{X/k})$ *est bijectif pour* $q < r - m$ *et injectif pour* $q = r - m$.

Le deuxième étage est « le premier étage lu à travers la suite exacte » ; le troisième lui est équivalent par la dualité, qui met H^p *et* $\mathrm{Ext}^{r-p}(-, \Omega^r)$ *en accouplement parfait, et « les bornes se répondent comme il faut :* $p \geqslant m$ *d'un côté,* $q < r - m$ *de l'autre, et* $p + q = r$ *».*

On démontre ici la forme abstraite de ces deux passages. Pour le premier, on se donne une suite exacte longue quelconque indexée par les entiers naturels,

$$\cdots \to L^p \xrightarrow{a_p} G^p \xrightarrow{b_p} C^p \xrightarrow{\delta_p} L^{p+1} \xrightarrow{a_{p+1}} \cdots$$

de groupes abéliens, exacte en chaque terme ; L^p tient lieu de $H^p_Y(X, F)$, G^p de $H^p(X, F)$, C^p de $H^p(X - Y, F)$. Pour le second, la dualité de Serre n'est pas démontrée : on l'admet sous la forme que lui prête la lecture : sur le corps k, la flèche de comparaison des Ext en degré $q = r - p$ s'identifie à la transposée ${}^t a_p : (G^p)^\vee \to (L^p)^\vee$ de a_p.

Lemme 10.1. *Soit* $m \in \mathbb{N}$. *On a* $C^p = 0$ *pour tout* $p \geqslant m$ *si et seulement si* a_p *est bijectif pour tout* $p > m$ *et* a_m *est surjectif.*

Démonstration. Supposons $C^p = 0$ pour $p \geqslant m$. Pour $p \geqslant m$, b_p est nul, donc son noyau, qui est l'image de a_p par exactitude en G^p, est G^p tout entier : a_p est surjectif, en particulier pour $p = m$. Soit $p > m$; écrivons $p = q + 1$ avec $q \geqslant m$. Par exactitude en L^{q+1}, le noyau de a_{q+1} est l'image de δ_q, qui est nulle puisque $C^q = 0$: a_p est injectif, donc bijectif.

Réciproquement, supposons a_p bijectif pour $p > m$ et a_m surjectif, et soient $p \geqslant m$ et $c \in C^p$. D'abord a_p est surjectif : si $p > m$ parce qu'il est bijectif, si $p = m$ par hypothèse. Par exactitude en L^{p+1}, $a_{p+1}(\delta_p(c)) = 0$; comme $p + 1 > m$, a_{p+1} est injectif et $\delta_p(c) = 0$. Par exactitude en C^p, il existe $y \in G^p$ avec $c = b_p(y)$, puis, a_p étant surjectif, $x \in L^p$ avec $y = a_p(x)$. Alors $c = b_p(a_p(x)) = 0$ par exactitude en G^p. □

Lemme 10.2. *Soient* k *un corps,* $(a_p : L^p \to G^p)_{p \in \mathbb{N}}$ *des applications* k*-linéaires, et* $m \leqslant r$ *des entiers. Les conditions suivantes sont équivalentes :*

1. a_p *est bijectif pour* $m < p \leqslant r$ *et* a_m *est surjectif ;*
2. ${}^t a_{r-q}$ *est bijectif pour* $q < r - m$ *et* ${}^t a_m$ *est injectif.*

De plus, si $p + q = r$, *on a* $p \geqslant m \Leftrightarrow q \leqslant r - m$ *et* $p > m \Leftrightarrow q < r - m$.

Démonstration. On utilise deux faits classiques d'algèbre linéaire sur un corps, valables en dimension quelconque : une application linéaire a est surjective si et seulement si sa transposée ${}^t a$ est injective, et elle est bijective si et seulement si ${}^t a$ l'est. (Le premier est immédiat dans un sens, et dans l'autre repose sur le fait qu'un sous-espace strict est contenu dans le noyau d'une forme linéaire non nulle ; le second en découle, avec l'énoncé dual : a injective si et seulement si ${}^t a$ surjective, par prolongement des formes linéaires à partir d'un sous-espace.)

Les deux conditions sur a_m se correspondent donc. Pour les autres : si $q < r - m$, l'entier $p = r - q$ vérifie $m < p \leqslant r$, et ${}^t a_{r-q}$ est bijectif puisque a_p l'est ; si inversement $m < p \leqslant r$, l'entier $q = r - p$ vérifie $q < r - m$ et $r - q = p$, et a_p est bijectif puisque ${}^t a_p$ l'est. L'assertion sur les bornes est de l'arithmétique : sous $p + q = r$, $p \geqslant m$ équivaut à $r - q \geqslant m$, soit $q \leqslant r - m$, et de même avec des inégalités strictes. □

Le lemme du feuillet 3 est démontré ici sous sa forme affine : $Y = \mathrm{Spec}\, R$ et le voisinage cherché est un ouvert $D(f)$.

Énoncé (Feuillet 3, III-18, forme affine)**.** *Soient R un anneau noethérien, $\mathfrak{p}$ un idéal premier de R, B un R-module de type fini et $u : R^n \to B$ une application R-linéaire telle que $u_\mathfrak{p} : R_\mathfrak{p}^n \to B_\mathfrak{p}$ soit bijective. Il existe $f \in R \setminus \mathfrak{p}$ tel que $u_f : R_f^n \to B_f$ soit bijective.*

Démonstration. Le module B, de type fini sur un anneau noethérien, est de présentation finie : le noyau d'une surjection $R^s \to B$ est un sous-module de R^s, donc de type fini. Il suffit alors de démontrer l'énoncé classique suivant, où l'anneau commutatif R est quelconque : *si M est de type fini, B de présentation finie et $u : M \to B$ bijective en $\mathfrak{p}$, alors u_f est bijective pour un $f \notin \mathfrak{p}$.*

Le conoyau Q de u est de type fini, quotient de B, et $Q_\mathfrak{p} = 0$ puisque la localisation est exacte. Chacun de ses générateurs $y_1, \dots, y_t$ est donc annulé par un $g_i \notin \mathfrak{p}$, et $g = g_1 \cdots g_t \notin \mathfrak{p}$ annule Q : $Q_g = 0$, c'est-à-dire que $u_g : M_g \to B_g$ est surjective. Son noyau K est de type fini : M_g est de type fini sur R_g, B_g de présentation finie, et le noyau d'une surjection d'un module de type fini sur un module de présentation finie est de type fini (fait classique : si $0 \to K \to M' \xrightarrow{\pi'} B' \to 0$ est exacte, avec M' de type fini et B' de présentation finie, choisissons une surjection $\pi : R^s \to B'$ de noyau N de type fini et relevons-la en $\varphi : R^s \to M'$ avec $\pi'\varphi = \pi$; chaque générateur de M' s'écrit $\varphi(x_j) + k_j$ avec $k_j \in K$, et tout $k \in K$ s'écrit $\varphi(x) + \sum c_j k_j$ où $\pi(x) = \pi'(k) = 0$, de sorte que $K = \varphi(N) + \sum_j Rk_j$). Comme $K_\mathfrak{p}$ est le noyau de $u_\mathfrak{p}$, il est nul ; le même argument donne $h \notin \mathfrak{p}$ tel que $K_h = 0$. Avec $f = gh \notin \mathfrak{p}$, u_f est surjective et injective. □

Remarque. Le passage du premier au deuxième étage vaut pour toute suite exacte longue, avec les bornes du feuillet ; il n'utilise rien de X, de Y ni de F. La dualité étant admise sous la forme d'une transposition, les trois étages encadrés sont cohérents entre eux. La comparaison, sous une borne sur la dimension cohomologique de $X - Y$, de la cohomologie de X à celle de son complété formel le long de Y, qui fait la suite de la carte, a été publiée par Hartshorne en 1970, au chapitre III d'*Ample Subvarieties of Algebraic Varieties* [68] ; l'inventaire date le dossier « [avant 1970] ».

Remarque. Le commentaire de la lecture apparie $p \geqslant m$ avec $q < r - m$. Sous $p + q = r$, $p \geqslant m$ équivaut à $q \leqslant r - m$, de sorte que la plage $p \geqslant m$ répond à toute celle du troisième étage, cas limite injectif compris. L'écart est dans le commentaire ; la carte est juste.

Remarque. Le lemme III-18 est un fait classique : il vaut sur tout anneau commutatif pour une source de type fini et un but de présentation finie. La noethérianité de Y et la finitude de B qu'invoque la marge servent seulement à rendre B de présentation finie.

Ne sont pas démontrés ici : la profondeur le long d'un fermé et le prolongement de type Hartogs ; la dualité de Serre, admise ; les étages 4 et 5 de la carte, qui passent par la complétion formelle ; les annulations pour $\mathcal{O}(n)$; la dimension cohomologique de $P - X$; les Ext des pages 4 et 5 ; le feuillet III-5 (Koszul) ; le lemme III-18 pour les faisceaux.

Théorème (Grothendieck, pages 2, 4 et 7, dimension cohomologique du complémentaire ; voir aussi Hartshorne [68] ♦)**.** *Soient $P \supset X \supset Y$ de dimensions n, r et m, avec $r > m > 0$. L'annulation de $H^p(X - Y, F)$ pour $p \geq m$ et tout F cohérent équivaut, par une dualité avec $\mathrm{Ext}^q(-, \Omega^r)$ sur X et sur son complété formel $\hat{X}$ le long de Y, à ce que $H^q(X, F) \to H^q(\hat{X}, \hat{F})$ soit bijectif pour $q < r - m$ et injectif pour $q = r - m$, pour tout F localement libre.*

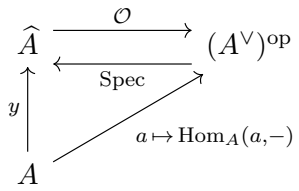
◊ non vérifié en Lean

11 Cote 115 : la dualité d'Isbell par le calcul des noyaux [12]

La cote 115, *« Correspondances » fonctorielles. Dualité des topos*, quatorze pages que l'inventaire date « [à partir de 1982] », attache, aux pages 3 à 5, à un noyau $X \in (A \times B)^\wedge$, préfaisceau contravariant en ses deux variables sur deux petites catégories, deux transformées ${}^sX : \widehat{A}^{\mathrm{op}} \to \widehat{B}$ et ${}^dX : \widehat{B}^{\mathrm{op}} \to \widehat{A}$, reliées par $\mathrm{Hom}_{\widehat{A}}(L, {}^dX(M)) \simeq X(L,M) \simeq \mathrm{Hom}_{\widehat{B}}(M, {}^sX(L))$. La page 7 prend $B = A^{\mathrm{op}}$ et pour noyau le hom de A, que la marge de la page 3 désigne comme l'élément canonique de $(A \times A^{\mathrm{op}})^\wedge$ (115, lot 1, p. 3). La lecture modernisée note $\mathcal{O}$ et Spec les foncteurs que le manuscrit écrit φ_A et Ψ_A.

Théorème 11.1 (Grothendieck, pages 3 à 7, la dualité (dite d'Isbell) comme cas particulier ♦)**.** *Pour tout noyau K sur $A \times B$, ${}^sK$, vu comme foncteur $\widehat{A} \to (\widehat{B})^{\mathrm{op}}$, est adjoint à gauche de ${}^dK$. Pour $B = A^{\mathrm{op}}$ et $K = \mathrm{Hom}_A$, les deux transformées sont exactement $\mathcal{O}(\Phi)(a) = \mathrm{Hom}(\Phi, ya)$ et $\mathrm{Spec}(\Psi)(a) = \mathrm{Hom}(\Psi, \mathrm{Hom}_A(a,-))$, et l'adjonction est $\mathcal{O} \dashv \mathrm{Spec} : \widehat{A} \rightleftarrows (A^\vee)^{\mathrm{op}}$. On a $\mathcal{O}(ya) \simeq \mathrm{Hom}_A(a,-)$, $\mathrm{Spec}(\mathrm{Hom}_A(a,-)) \simeq ya$, et $\mathcal{O}$ transforme les colimites de $\widehat{A}$ en limites de $A^\vee$.*

Le diagramme montre l'adjonction et ses valeurs sur les représentables ; le triangle commute à isomorphisme près :



$$\mathcal{O}(ya) \simeq \mathrm{Hom}_A(a,-), \quad \mathrm{Spec}(\mathrm{Hom}_A(a,-)) \simeq ya.$$

L'énoncé tient tel que la lecture le donne. En Lean, le noyau est un foncteur $K : A^{\mathrm{op}} \to [C, \mathbf{Ens}]$, le cas de la page étant $C = B^{\mathrm{op}}$; l'adjonction générale est `kernelAdj`, la dualité `isbell`, obtenue en posant K égal au foncteur de co-Yoneda, et les deux formules de la page 7 valent par définition (`isbell0_obj_obj`, `isbellSpec_obj_obj`). La question de la piste, savoir si une démonstration publiée obtient ainsi la dualité, relève de la littérature et reste ouverte.

Théorème 11.2 (caractérisation de $\mathcal{O}$ et de Spec par leur restriction le long de y)**.** *Le foncteur $\mathcal{O}$ est l'extension de Kan à gauche le long de y du foncteur $a \mapsto \mathrm{Hom}_A(a,-)$ de A dans $(A^\vee)^{\mathrm{op}}$: tout foncteur $L : \widehat{A} \to (A^\vee)^{\mathrm{op}}$ qui transforme colimites en colimites, c'est-à-dire colimites de $\widehat{A}$ en limites de $A^\vee$, et tel que $L(ya) \simeq \mathrm{Hom}_A(a,-)$ naturellement en a, est isomorphe à $\mathcal{O}$. Dualement, tout foncteur $G : (A^\vee)^{\mathrm{op}} \to \widehat{A}$ qui commute aux limites et vérifie $G(\mathrm{Hom}_A(a,-)) \simeq ya$ naturellement en a est isomorphe à Spec.*

Esquisse. Tout préfaisceau est colimite canonique de représentables, si bien qu'un foncteur commutant aux colimites est déterminé, à isomorphisme près, par sa restriction le long de y ; c'est le théorème de densité de mathlib (`Presheaf.uniqueExtensionAlongULiftYoneda`), repris ici sous la forme `isoOfRestrict`. Il s'applique à $\mathcal{O}$, adjoint à gauche, dont la restriction est $a \mapsto \mathrm{Hom}_A(a,-)$ par le lemme de Yoneda (`isbell0_restrict`, `isbell0_isLeftKanExtension`, `isbell0_unique`). Pour Spec, on passe aux opposés : $G^{\mathrm{op}} : A^\vee \to \widehat{A}^{\mathrm{op}}$ commute aux colimites, $A^\vee$ est la catégorie des préfaisceaux sur A^{op}, dont les représentables sont les $\mathrm{Hom}_A(a,-)$ (`yonedaOpIso`), et l'on conclut de même (`isbellSpec_unique`). □

12. Preuve vérifiée : `lean/Grothendieck/Folder115.lean`.

Remarque. L'adjonction $\mathcal{O} \dashv \mathrm{Spec}$ relève de la section 28 : ses parties fixes $E_0 \subset \widehat{A}$ et $F_0 \subset (A^\vee)^{\mathrm{op}}$, où l'unité et la coünité sont inversibles, sont les objets réflexifs de la dualité d'Isbell, et l'énoncé sur les points fixes de la page 4 de la cote 161-1 les met en équivalence. Le lemme `isbell0_yoneda` et son dual disent que les représentables sont dans ces parties fixes. La page 7 demande si ce sont les seuls et répond « sans doute pas » ; la réponse est juste dès que A n'est pas karoubienne : l'unité d'un rétracte est un rétracte de l'unité, donc un rétracte d'un représentable est réflexif, et un tel rétracte n'est pas toujours représentable. La lecture place de même l'enveloppe de Karoubi de A parmi les objets réflexifs, comme inclusion et non comme égalité. Ces deux points sont de l'édition et ne sont pas vérifiés en Lean. La dualité entre topos et sites des pages suivantes rejoint les sections 26, 28 et 5.

Ne sont pas démontrés ici : la roue des onze catégories de foncteurs de la page 5, l'extension aux familles finies (A_i) et la dualité des topos des pages suivantes. Autres pistes de l'onglet

Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 10 et 11, noyau de l'image réciproque et indice ♦). *Soient $f : X \to Y$ propre sur un corps k, Y irréductible et lisse de point générique η, X_η non vide, et N le pgcd des degrés des 0-cycles de X_η. Il existe une application $H^*(X, G_X) \to H^*(Y, G)$, fonctorielle en le complexe de coefficients étale G, dont le composé avec f^* est $N \cdot \mathrm{id}$. Le noyau de f^* est donc tué par l'indice de la fibre générique, sans hypothèse sur la dimension relative.*

◊ non vérifié en Lean

Le calcul de la page 10 suppose le formalisme de Gysin du § 4 pour des Z_i éventuellement singuliers, que le dossier énonce sans le démontrer. Mathlib n'a pas la cohomologie étale. On se reportera aux notes de Grothendieck (32, lot 1, p. 10).

Théorème (Grothendieck, pages 40 à 43, permanence de la condition de Lefschetz ♦). *Soient X quasi-projectif sur un anneau noethérien et Y un fermé de X tels que la paire (X, Y) vérifie $(\mathrm{LG})_n$: $H^i(X, F) \to H^i(X_{/Y}, F_{/Y})$ est bijectif pour $i \leq n$ et injectif pour $i = n + 1$ pour tout F localement libre. Alors pour tout $f : W \to X$ projectif et plat, la paire $(W, f^{-1}(Y))$ vérifie $(\mathrm{LG})_n$; de même pour la condition Lef de SGA 2, X. Rien n'est demandé aux fibres de f.*

◊ non vérifié en Lean

Démonstration donnée par l'édition, non vérifiée en Lean.

SGA 2 (exposés X et XII) obtient ces conditions par des hypothèses de profondeur sur les fibres. Mathlib n'a pas les complétions formelles ni leur cohomologie. On se reportera aux notes de Grothendieck (58, lot 2, p. 40).

Théorème (Grothendieck, pages 45 à 51, comparaison des Hom hors de Y ♦). *Soient A un anneau local noethérien, quotient d'un anneau régulier et t-adiquement complet, X' son spectre épointé et $Y' = V(t) \cap X'$. Pour F et G cohérents sur X', $\mathrm{Hom}(F, G) \simeq \mathrm{Hom}(\hat{F}, \hat{G})$ le long de Y' dès que G est de profondeur ≥ 2 aux points fermés de $X' - Y'$. Aucune profondeur n'est demandée aux points de Y', alors que SGA 2, X, exemple 2.1 (i), la demande en tout point fermé de X'.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 45 à 51) : la page 47 marque d'un « ? » le pas t-régulier et s'arrête. Mathlib n'a pas les faisceaux cohérents sur un spectre épointé ni leur complétion formelle. On se reportera aux notes de Grothendieck (58, lot 3, p. 45).

Partie 9

Descente

12 Cote 128 : descente le long d'un conducteur nilpotent, idéaux d'équivalence de rang deux [13]

La cote 128, *Descente non plate. Modules formels*, trente et une pages non datées, compare le complexe d'Amitsur d'une extension $A \subset A'$ à celui de sa réduction modulo un idéal nilpotent. Sept pages (12 à 18) y traitent de « résultats auxiliaires sur les relations d'équivalence ». La proposition 1 de la page 12 affirme que, si A'/A est isomorphe au corps résiduel $k = A/\mathfrak{m}$, il n'y a sur $\operatorname{Spec} A'$, au-dessus de $\operatorname{Spec} A$, que deux relations d'équivalence : la plus fine et la moins fine (128, lot 1, p. 12). La page 13 ramène l'énoncé au cas où $A = k$ est un corps et A' une k-algèbre de rang 2, traite $k \times k$ et s'arrête sur « $A' \simeq k[\varepsilon]$ » (128, lot 1, p. 13). On démontre ici ce cas d'un corps et la réduction qui y ramène le cas local, puis, à la fin de la section, le résultat de descente des pages 4 à 9 : la descente plate effective se remonte le long d'un idéal nilpotent contenu dans le conducteur.

Idéaux d'équivalence. Sur un ensemble X, une relation d'équivalence est une partie $R \subset X \times X$ qui contient la diagonale, est stable par l'échange $(x, y) \mapsto (y, x)$ et vérifie : si (x, y) et (y, z) sont dans R, (x, z) aussi. Pour $X = \operatorname{Spec} A$ au-dessus d'un corps k, le produit $X \times_k X$ est $\operatorname{Spec}(A \otimes_k A)$, et un sous-schéma fermé de ce produit est donné par un idéal J de $A \otimes_k A$, d'autant plus petit que le sous-schéma est gros. Les trois axiomes se traduisent alors ainsi (la lecture les énonce après la proposition 3 du n° 1, pages 9 à 11) :

— réflexivité : R contient la diagonale, c'est-à-dire $J \subset \Delta = \operatorname{Ker}(A \otimes_k A \to A,\ a \otimes b \mapsto ab)$;

— symétrie : J est stable par l'échange $a \otimes b \mapsto b \otimes a$;

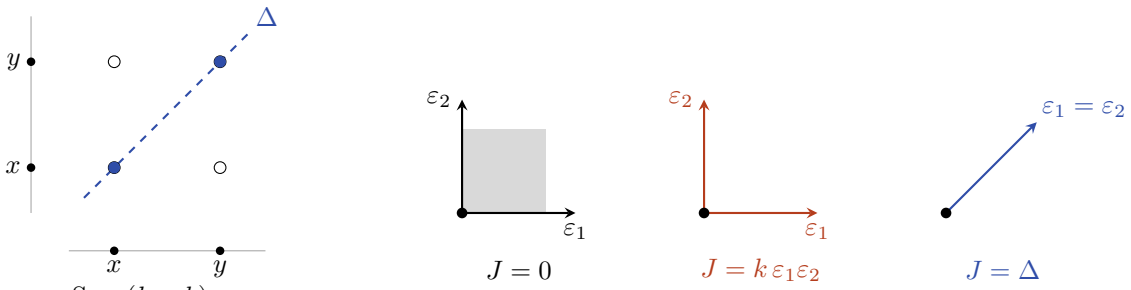
— transitivité : $p_{13}(J) \subset p_{12}(J) + p_{23}(J)$ dans $A \otimes_k A \otimes_k A$, où $p_{12}(a \otimes b) = a \otimes b \otimes 1$, $p_{13}(a \otimes b) = a \otimes 1 \otimes b$ et $p_{23}(a \otimes b) = 1 \otimes a \otimes b$ engendrent des idéaux.

La dernière condition dit que le sous-schéma de X^3 formé des (x, y, z) avec $(x, y) \in R$ et $(y, z) \in R$ s'envoie dans R par $(x, y, z) \mapsto (x, z)$. Les deux idéaux extrêmes sont $J = \Delta$, la diagonale, relation la plus fine, et $J = 0$, le produit tout entier, relation la moins fine.

L'intuition. Une k-algèbre de rang 2 est un « schéma à deux points », au sens géométrique : deux points distincts ($k \times k$), un point double ($k[\varepsilon]$, $\varepsilon^2 = 0$), ou un seul point de degré 2 (une extension quadratique de k). Pour deux points, la question est celle des relations d'équivalence sur un ensemble à deux éléments, et il y en a deux. Pour le point double, on pourrait craindre une relation intermédiaire, qui identifierait le point à lui-même « à l'ordre un » sans l'identifier à son vecteur tangent ; la transitivité l'interdit (figure 2).

Théorème 12.1 (Grothendieck, page 12, proposition 1 (i), cas d'un corps)**.** *Soient k un corps et A une k-algèbre commutative de dimension 2. Les idéaux d'équivalence de $A \otimes_k A$ sont exactement 0 et Δ.*

13. Preuve vérifiée : `lean/Grothendieck/Folder128.lean`.



Spec($k \times k$) :
0 garde les quatre points,
Δ les deux de la diagonale

Spec($k[\varepsilon] \otimes_k k[\varepsilon]$) = Spec $k[\varepsilon_1, \varepsilon_2]/(\varepsilon_1^2, \varepsilon_2^2)$: un seul point,
avec ses directions tangentes ε_1, ε_2 et le terme croisé $\varepsilon_1\varepsilon_2$ (en gris)

FIGURE 2 – Les sous-schémas du carré $\mathrm{Spec}(A \otimes_k A)$ pour les deux modèles de rang 2. Pour $k \times k$, deux points, les relations 0 et Δ sont le carré entier et sa diagonale. Pour $k[\varepsilon]$, un point double, le carré est un seul point épaissi ; Δ ne garde que la direction diagonale, et l'idéal intermédiaire $k\,\varepsilon_1\varepsilon_2$ ôte le seul terme croisé. Il n'est pas transitif : dans $A^{\otimes 3}$, placer le point du milieu à l'origine annule $\varepsilon_1\varepsilon_2$ et $\varepsilon_2\varepsilon_3$, mais pas $\varepsilon_1\varepsilon_3$.

Démonstration. Les deux idéaux 0 et Δ sont d'équivalence : pour Δ, la symétrie vient de la commutativité de A, et la transitivité de l'identité $p_{13}(\delta s) = p_{12}(\delta s) + p_{23}(\delta s)$, où $\delta s = 1 \otimes s - s \otimes 1$, ces éléments engendrant Δ.

Réciproquement, soit J un idéal d'équivalence. Pour $x \in A$ hors de k, $(1, x)$ est une base de A, et $\Delta = A \cdot \delta x$: le A-module Δ est engendré par les δs, et $\delta(c + dx) = d\,\delta x$. Tout élément de J s'écrit donc $a \cdot \delta x = a \otimes x - ax \otimes 1$, et il suffit de montrer que $J = 0$ ou que $\delta x \in J$ pour un tel x.

Si tout élément non nul de A est inversible, un élément non nul $a \cdot \delta x$ de J donne $\delta x = a^{-1} \cdot (a \cdot \delta x) \in J$. Sinon, soit e non nul et non inversible ; il n'est pas dans k, et $e^2 = s + re$ avec $s, r \in k$. Si $s \neq 0$, $e \cdot s^{-1}(e - r) = 1$; donc $s = 0$ et $e^2 = re$.

Si $r \neq 0$, $f = e/r$ est un idempotent hors de k (c'est le cas $k \times k$). Un élément de J s'écrit $t = c\,(1 \otimes f) + d\,(f \otimes f) - (c + d)(f \otimes 1)$. On calcule $(f \otimes 1)\,t = (c + d)\,w_1$ et $(1 \otimes 1 - f \otimes 1)\,t = c\,w_2$, avec $w_1 = f \otimes f - f \otimes 1$ et $w_2 = 1 \otimes f - f \otimes f$. Si $t \neq 0$, l'un des scalaires $c + d$, c est non nul, donc w_1 ou w_2 est dans J. Or $w - \sigma(w) = \delta f$ pour $w = w_1$ comme pour $w = w_2$, où σ est l'échange, et la symétrie donne $\delta f \in J$.

Si $r = 0$, $e^2 = 0$ (c'est le cas $k[\varepsilon]$). Un élément de J s'écrit $t = c\,\delta e + d\,(e \otimes e)$, et $(e \otimes 1)\,t = c\,(e \otimes e)$. Supposons $\delta e \notin J$. Si $c \neq 0$, $e \otimes e \in J$, puis $c\,\delta e = t - d\,(e \otimes e) \in J$, contradiction ; donc $J \subset k\,(e \otimes e)$. Si de plus $J \neq 0$, $e \otimes e \in J$. Soit $\chi : A \to k$ le caractère $c + de \mapsto c$, et $\varphi : A^{\otimes 3} \to A^{\otimes 2}$ le morphisme d'algèbres $a \otimes b \otimes c \mapsto \chi(b)\,a \otimes c$, qui « oublie le point du milieu ». Il annule $p_{12}(e \otimes e) = e \otimes e \otimes 1$ et $p_{23}(e \otimes e) = 1 \otimes e \otimes e$, donc les idéaux $p_{12}(J)$ et $p_{23}(J)$, mais envoie $p_{13}(e \otimes e) = e \otimes 1 \otimes e$ sur $e \otimes e \neq 0$. La transitivité est en défaut ; donc $J = 0$.

Dans tous les cas, $J = 0$ ou $\delta x \in J$ pour un $x \notin k$, et alors $\Delta = A \cdot \delta x \subset J \subset \Delta$. □

Remarque. La démonstration n'utilise ni la clôture algébrique de k, que la page s'accorde en interligne, ni la classification des algèbres de rang 2 : elle couvre d'un coup les extensions quadratiques, séparables ou non. Le cas $k[\varepsilon]$, que la page laisse après « $\varepsilon^2 = 0$ », est celui de la lecture : l'idéal $k\,\varepsilon_1\varepsilon_2$ est réflexif et symétrique, mais pas transitif. Le cas $k \times k$ se règle, lui, par la seule symétrie : les idéaux $k\,(f \otimes (1 - f))$ et $k\,((1 - f) \otimes f)$, réflexifs et transitifs, correspondent aux deux relations non symétriques d'un ensemble à deux éléments.

Portée de la vérification. Lean formalise la définition des idéaux d'équivalence par les trois

conditions ci-dessus, pour A commutative de dimension 2 sur un corps quelconque, et démontre le théorème 12.1 dans les deux sens. L'idéal Δ y est le noyau de la multiplication `Algebra.TensorProduct.lmul'`, et les δs l'engendrent comme A-module par un résultat de mathlib qui sert à définir les différentielles de Kähler.

La partie difficile de la proposition 1 (i) est la réduction du cas général au cas d'un corps. Elle passe par la proposition 3 du n° 1 et son corollaire 2 (pages 9 à 11) : la réduction modulo $\mathfrak{m}$ induit une bijection entre les idéaux d'équivalence de $A' \otimes_A A'$ et ceux de $A'_0 \otimes_k A'_0$, parce que l'idéal d'augmentation se réduit isomorphiquement (lemme du serpent). Cette réduction est démontrée plus bas, pour $I = \mathfrak{m}$ et dans le sens qui sert (théorème 12.4) ; ni la traduction entre idéaux et sous-schémas fermés, ni les points (ii) et (iii) de la proposition ne sont formalisés.
Le critère sur un corps. Prenons $A = k$ et notons, comme dans le théorème 12.1, A l'algèbre finie (le A' de la page). L'hypothèse « $\delta(x)$ engendre l'idéal Δ de $A'' = (A \otimes_k A)/J$ » se lit dans $A \otimes_k A$: $\Delta \subset (\delta x) + J$. L'exactitude de $k \to A \rightrightarrows A''$ dit que $\delta x \in J$ seulement pour $x \in k$. Les feuillets distinguent deux cas : A non radiciel, ramené à k^n où un décompte donne $n = 2$, et A radiciel, ramené à $k \oplus V$ avec $V^2 = 0$, où la page 18 s'arrête sur « il faut prouver » $\dim V = 1$. La démonstration ci-dessous évite cette distinction : elle regarde J point par point.

Théorème 12.2 (Grothendieck, pages 14 à 18, proposition 2, cas d'un corps)**.** *Soient k un corps, A une k-algèbre commutative de dimension finie dont tous les corps résiduels sont k, et $J \subset \Delta$ un idéal de $A \otimes_k A$. On suppose que $\delta x \in J$ entraîne $x \in k$, et que $\Delta \subset (\delta x) + J$ pour tout $x \notin k$. Alors $\dim_k A \leq 2$, c'est-à-dire $\log(A/k) \leq 1$. Si de plus J est un idéal d'équivalence et $\dim_k A = 2$, alors $J = 0$, c'est-à-dire $A'' = A \otimes_k A$.*

Démonstration. Un point $\chi : A \to k$ (un morphisme de k-algèbres, d'idéal $\mathfrak{m}_\chi = \operatorname{Ker} \chi$) donne le morphisme $\varphi_\chi : A \otimes_k A \to A$, $a \otimes b \mapsto \chi(a)\, b$, qui « fixe le premier point en χ ». Il envoie δx sur $x - \chi(x)$, et Δ dans $\mathfrak{m}_\chi$. Pour $0 \neq z \in \mathfrak{m}_\chi$ (donc $z \notin k$) et $y \in \mathfrak{m}_\chi$, écrivons $\delta y = u\, \delta z + j$ avec $j \in J$; en appliquant φ_χ, $y = \varphi_\chi(u)\, z + \varphi_\chi(j)$. Ainsi $\mathfrak{m}_\chi \subset Az + \varphi_\chi(J)$.

Premier cas : $\varphi_\chi(J) = 0$ pour un point χ. Alors tout $z \neq 0$ de $\mathfrak{m}_\chi$ l'engendre. Si $\mathfrak{m}_\chi = 0$, $A = k$. Sinon, soit $z \neq 0$ dans $\mathfrak{m}_\chi$ et $\mathfrak{n}$ un idéal maximal contenant l'annulateur de z ; c'est le noyau d'un point χ'. Pour $w \in \mathfrak{n}$, si $wz \neq 0$, il engendre $\mathfrak{m}_\chi$: $z = bwz$, donc $1 - bw$ annule z et serait dans $\mathfrak{n}$ avec bw, absurde. Donc $\mathfrak{n}z = 0$, et $bz = \chi'(b)\, z$ pour tout b : $\mathfrak{m}_\chi = kz$ et $A = k \oplus kz$.

Second cas : $\mathfrak{m}_\chi \subset \varphi_\chi(J)$ pour tout χ (si $\varphi_\chi(J)$ contient $y_0 \neq 0$, on prend $z = y_0$ ci-dessus). Pour $f \in \Delta$, $f \equiv \delta(\varphi_\chi f)$ modulo $\mathfrak{m}_\chi \Delta$ (où A agit sur le premier facteur) : c'est vrai pour $f = \delta s$, car δ s'annule sur k, et le passage à $a \cdot f$ ajoute $(a - \chi(a)) \cdot f \in \mathfrak{m}_\chi \Delta$. Pour $x \in A$, choisissons $f \in J$ avec $\varphi_\chi(f) = x - \chi(x)$; alors $\delta x = \delta(\varphi_\chi f) \in J + \mathfrak{m}_\chi \Delta$. Ainsi $\Delta \subset J + \mathfrak{m}\Delta$ pour tout idéal maximal $\mathfrak{m}$, puisque tous sont des $\mathfrak{m}_\chi$. Par le lemme de Nakayama, appliqué en chaque idéal maximal au A-module de type fini $(\Delta + J)/J$, $\Delta \subset J$; l'exactitude donne alors $x \in k$ pour tout x, soit $A = k$.

Enfin, si $\dim_k A = 2$ et si J est un idéal d'équivalence, le théorème 12.1 donne $J = 0$ ou $J = \Delta$, et $J = \Delta$ contredirait l'exactitude. □

Remarque. La première assertion n'utilise de J que l'inclusion $J \subset \Delta$: ni la symétrie, ni la transitivité, ni la nilpotence de J que la page souligne sans la justifier. Le décompte « $2(n-1) = n^2 - n$ » du cas non radiciel et le calcul de $\dim V$ de la page 18 sont deux instances du premier cas, $\varphi_\chi(J) = 0$; le second cas est celui où la relation ne relie χ à aucun autre point, ni infinitésimalement.

Portée de la vérification. Lean démontre le théorème 12.2 sous ces hypothèses (`Colength.finrank_le_two`, `Colength.eq_bot_of_finrank_eq_two`, réunis dans `Colength.prop2`) ; l'hypothèse sur les corps résiduels y est écrite « tout idéal maximal est le noyau d'un morphisme $A \to k$ », et le lemme de Nakayama en tout idéal maximal y est `Colength.le_of_forall_le_sup_smul`. La réduction du cas local au cas d'un corps fait l'objet du théorème suivant.
Du cas local au cas d'un corps. Revenons à l'énoncé de la page 14 : A local artinien d'idéal maximal $\mathfrak{m}$, $k = A/\mathfrak{m}$, et A' une A-algèbre finie. Les idéaux d'équivalence de $A' \otimes_A A'$ se définissent comme plus haut, $\otimes_k$ devenant $\otimes_A$, et $\delta x = 1 \otimes x - x \otimes 1$. La page obtient $\mathfrak{m}A' = \mathfrak{m}$ par sa distinction radiciel / non radiciel, en s'appuyant sur la nilpotence de J, puis réduit modulo $\mathfrak{m}$ par la proposition 3 du n° 1 et son corollaire 2 (pages 9 à 11), qui identifient l'idéal d'augmentation Δ à celui de $A'_0 = A'/\mathfrak{m}A'$ et transportent les idéaux d'équivalence. On suit ici la même réduction, mais $\mathfrak{m}A' = \mathfrak{m}$ se lit directement sur l'hypothèse, et l'argument point par point du théorème 12.2 se fait dans A'_0 sans passer par $A'_0 \otimes_k A'_0$.

Théorème 12.3 (Grothendieck, pages 14 à 18, proposition 2 ♦). *Soient A un anneau noethérien, $\mathfrak{m}$ un idéal maximal de A, $k = A/\mathfrak{m}$, et A' une A-algèbre finie dont tout idéal maximal est le noyau d'un morphisme de A-algèbres $A' \to k$ (c'est le cas si A est local artinien d'idéal maximal $\mathfrak{m}$ et si les extensions résiduelles de A' sont triviales). Soit $J \subset \Delta$ un idéal de $A' \otimes_A A'$; on suppose que $\delta x \in J$ entraîne $x \in A$ (exactitude de $A \to A' \rightrightarrows (A' \otimes_A A')/J$), et que $\Delta \subset (\delta x) + J$ pour tout $x \notin A$. Alors :*

1. *$\mathfrak{m}A'$ est contenu dans l'image de A ; si $A \to A'$ est injectif, $\mathfrak{m}A' = \mathfrak{m}$;*
2. *A'/A est de longueur au plus 1 ;*
3. *si de plus J est un idéal d'équivalence et si A'/A est de longueur 1, alors $J = 0$, c'est-à-dire $(A' \otimes_A A')/J = A' \otimes_A A'$.*

Esquisse. Point 1. Tout idéal maximal $\mathfrak{n}$ de A' est le noyau d'un point $\chi : A' \to k$, donc contient $\mathfrak{m}A'$. Si $x \in \mathfrak{m}A'$ n'était pas dans A, on aurait $\delta x \in \mathfrak{m}\Delta \subset \mathfrak{n}\Delta$ (car δ est A-linéaire et nul sur A), où A' agit sur le premier facteur ; l'hypothèse donnerait $\Delta \subset (\delta x) + J \subset J + \mathfrak{n}\Delta$ pour tout $\mathfrak{n}$, donc $\Delta \subset J$ par le lemme de Nakayama en chaque idéal maximal de A' (Δ est de type fini, A' étant noethérien), et l'exactitude mettrait x dans A.

Point 2. Pour un point χ, le morphisme $\varphi_\chi : A' \otimes_A A' \to A'_0$, $a \otimes b \mapsto \chi(a)\,\bar{b}$, envoie δx sur $\bar{x} - \chi(x)$, et l'on refait la démonstration du théorème 12.2 dans la k-algèbre finie A'_0, dont les corps résiduels sont k. Ou bien $\varphi_\chi(J) = 0$ pour un χ, et l'idéal maximal de χ dans A'_0 est simple, d'où $\dim_k A'_0 \leq 2$. Ou bien, pour tout χ, cet idéal est contenu dans $\varphi_\chi(J)$; la congruence $f \equiv \delta(\varphi_\chi f)$ du cas d'un corps est remplacée par : tout $t \in \Delta$ est congru à un δs modulo $\mathfrak{n}_\chi\Delta$ (on écrit $a = \lambda + (a - \lambda)$ avec $\lambda \in A$ relevant $\chi(a)$). Pour $x \in A'$, prenons $f \in J$ avec $\varphi_\chi(f) = \bar{x} - \chi(x)$ et s avec $f \equiv \delta s$; comme φ_χ annule $\mathfrak{n}_\chi\Delta$, $\bar{x} - \bar{s} \in k$, donc $x - s \in A + \mathfrak{m}A'$ et $\delta x \equiv \delta s \equiv f$ modulo $\mathfrak{n}_\chi\Delta$. Ainsi $\Delta \subset J + \mathfrak{n}\Delta$ pour tout $\mathfrak{n}$, puis $\Delta \subset J$ et $A' = A$. Dans le premier cas, soit $z \notin A$: par le point 1, 1 et $\bar{z}$ sont libres dans A'_0, donc en forment une base, et $A' = A + Az + \mathfrak{m}A' = A + Az$; tout élément non nul de A'/A l'engendre, et la longueur vaut au plus 1.

Point 3. Soit $\Theta : A' \otimes_A A' \to A'_0 \otimes_k A'_0$ la réduction modulo $\mathfrak{m}$. Son noyau est contenu dans $\mathfrak{m}(A' \otimes_A A')$ (exactitude à droite du produit tensoriel) ; et comme $\mathfrak{m}A' \subset A$, $\mu(a \otimes b) = (\mu a) \otimes b = 1 \otimes \mu ab$ pour $\mu \in \mathfrak{m}$, de sorte que tout élément t de $\mathfrak{m}(A' \otimes_A A')$ vaut $1 \otimes t'$ où t' est son image par la multiplication : il est nul s'il est dans Δ. Ainsi Θ est injectif sur Δ ; c'est la proposition 3 du n° 1 pour $I = \mathfrak{m}$. Comme Θ commute à l'échange, à la multiplication et aux p_{ij},

$\Theta(J)$ est un idéal d'équivalence (corollaire 2, dans le sens qui sert). La longueur 1 fournit $z \notin A$, et le point 2 donne $\dim_k A'_0 = 2$. Par le théorème 12.1, $\Theta(J) = 0$, d'où $J = 0$ par injectivité, ou $\Theta(J) = \Delta_0$; dans ce cas $\Theta(\delta z) = \Theta(j)$ pour un $j \in J$, donc $\delta z = j \in J$, contre l'exactitude. □

Théorème 12.4 (Grothendieck, pages 12 et 13, proposition 1 (i) ♦). *Soient A un anneau, $\mathfrak{m}$ un idéal maximal, $k = A/\mathfrak{m}$, et $A \subset A'$ une A-algèbre telle que $A'/A \simeq k$ comme A-modules. Les idéaux d'équivalence de $A' \otimes_A A'$ sont exactement 0 et Δ.*

Esquisse. Comme $\mathfrak{m}$ annule A'/A, $\mathfrak{m}A' \subset A$. Soit z relevant $1 \in k$: tout y s'écrit $\lambda + \nu z$ avec $\lambda, \nu \in A$, donc $1, \bar{z}$ engendrent A'_0, et ils sont libres puisque $z \notin A + \mathfrak{m}A'$; $\dim_k A'_0 = 2$. Pour un idéal d'équivalence J, $\Theta(J)$ est un idéal d'équivalence de $A'_0 \otimes_k A'_0$, donc 0 ou Δ_0 (théorème 12.1). Dans le premier cas $J = 0$ par injectivité de Θ sur Δ. Dans le second, tout $d \in \Delta$ a son image dans $\Delta_0 = \Theta(J)$, donc $d - j \in \Delta$ est d'image nulle pour un $j \in J$, et $d = j$: $J = \Delta$. Réciproquement 0 et Δ sont des idéaux d'équivalence, comme sur un corps. □

Remarque. Ni la nilpotence de J, que la page souligne sans la justifier, ni la distinction radiciel / non radiciel, ni la différentielle $d : A' \to \Delta/\Delta^2$ ne servent ; les points 1 et 2 n'utilisent de J que l'inclusion $J \subset \Delta$. L'anneau de base n'a pas à être local ni artinien : il suffit qu'il soit noethérien et que tous les points de A' soient rationnels au-dessus d'un même idéal maximal. La proposition 1 (i) vaut sur un anneau quelconque, sans finitude ; c'est l'énoncé de la page 12, que la page 13 ramène au cas d'un corps sans plus de détail.

Portée de la vérification. Lean démontre le théorème 12.3 sous ces hypothèses (`ColengthLocal.map_le_range` pour le point 1, `ColengthLocal.colength_le_one` pour les points 1 et 2, `ColengthLocal.eq_bot_of_length_eq_one` pour le point 3, réunis pour A local noethérien dans `ColengthLocal.prop2`), la longueur étant `Module.length` ; l'alternative du point 2 est `ColengthLocal.finrank_le_two_or`, la congruence modulo $\mathfrak{n}\Delta$ `ColengthLocal.exists_sub_dl_mem`, la réduction Θ `ColengthLocal.theta`, son injectivité sur Δ `ColengthLocal.eq_zero_of_theta`, et le transport des idéaux d'équivalence `ColengthLocal.isEquivalenceIdeal_map`. Il démontre le théorème 12.4 (`ColengthLocal.prop1_i`, avec `ColengthLocal.isEquivIdeal_bot` et `ColengthLocal.isEquivIdeal_diag`). Ne sont pas formalisés : la proposition 3 du n° 1 et son corollaire 2 pour un idéal nilpotent I quelconque du conducteur (seul le cas $I = \mathfrak{m}$, $\mathfrak{m}A' \subset A$, et le sens de A' vers A'_0 le sont), les points (ii) et (iii) de la proposition 1, et la traduction entre idéaux et sous-schémas fermés.
Descente le long d'un conducteur nilpotent. Revenons aux pages 4 à 9 (128, lot 1, p. 4). Soient $A \to A'$ un morphisme d'anneaux commutatifs et I un idéal de A que $\lambda \mapsto \lambda \cdot 1$ envoie injectivement sur un idéal de A' : I est contenu dans le conducteur, et le carré formé de A, A', $A_0 = A/I$, $A'_0 = A'/IA'$ est cartésien (un carré de Milnor). Une *donnée de descente* sur un A'-module E' relativement à $A \to A'$ est un isomorphisme $\varphi : A' \otimes_A E' \to E' \otimes_A A'$ satisfaisant la condition de cocycle ; on l'écrit ici par la coaction $\psi(e) = \varphi(1 \otimes e) = \sum b_i \otimes e_i$, application A'-linéaire $E' \to A' \otimes_A E'$ soumise à deux conditions : la counité $\sum b_i e_i = e$ et le cocycle $\sum b_i \otimes \psi(e_i) = \sum b_i \otimes 1 \otimes e_i$. Les invariants $E = \{e \mid \psi(e) = 1 \otimes e\}$ forment le H^0 du complexe de descente, et la donnée est *effective* si E est plat sur A et si $A' \otimes_A E \to E'$ est bijectif : elle est alors celle de $A' \otimes_A E$. Un morphisme $\operatorname{Spec} A' \to \operatorname{Spec} A$ est de *descente effective pour les modules plats* si $M \to H^0(A'/A, M)$ est bijectif pour tout A-module plat M et si toute donnée de descente sur un A'-module plat est effective. Une donnée sur E' en induit une sur $E'_0 = A'_0 \otimes_{A'} E'$ relativement à $A_0 \to A'_0$, sa réduction.

Théorème 12.5 (Grothendieck, pages 4 à 7, proposition 2 et corollaire 1 ♦). *Soient $A \to A'$ et I comme ci-dessus, avec I nilpotent.*

1. *Si E' est un A'-module plat muni d'une donnée de descente dont la réduction modulo I est effective, la donnée est effective.*
2. *Si $\operatorname{Spec} A'_0 \to \operatorname{Spec} A_0$ est un morphisme de descente effective pour les modules plats, $\operatorname{Spec} A' \to \operatorname{Spec} A$ l'est aussi.*

Démonstration. On note $\pi : E' \to E'_0$ la réduction, E et E_0 les invariants de E' et de E'_0. Le fait de base est que, IA' étant égal à l'image de I, on a dans $A' \otimes_A N$, pour tout A-module N, $\lambda b \otimes n = 1 \otimes \lambda_b n$ avec $\lambda_b \in I$: tout élément de $IA' \cdot (A' \otimes_A N)$ s'écrit $1 \otimes y$ avec $y \in IN$.

Étape 1 : e est invariant si et seulement si $\pi(e)$ l'est. Si $\pi(e)$ est invariant, $\psi(e) - 1 \otimes e$ s'annule modulo I, donc vaut $1 \otimes y$; en appliquant la counité, $e - e = y$, d'où $y = 0$. C'est le calcul de la page 5, qui n'utilise ni $I^2 = 0$ ni la platitude. Ainsi $E \to E_0$ est surjectif, de noyau IE'.

Étape 2 : par l'effectivité modulo I, E'_0 est engendré par E_0, donc $E' = A'E + IE'$, et $E' = A'E$ par le lemme de Nakayama pour l'idéal nilpotent IA' ; on en tire aussi $IE' = IE$. L'application $A' \otimes_A E \to E'$ est donc surjective.

Étape 3 : elle est injective. Un élément t de son noyau a une réduction dans $A'_0 \otimes_{A_0} E_0$ qui s'envoie sur $\pi(0) = 0$, donc est nulle par l'effectivité modulo I ; t est alors dans $IA' \cdot (A' \otimes_A E)$, de la forme $1 \otimes y$, et son image y est nulle.

Étape 4 : E est plat. D'une part $E/IE \simeq E_0$ est plat sur A_0. D'autre part $I \otimes_A E \simeq I \otimes_{A'} (A' \otimes_A E) \simeq I \otimes_{A'} E' \to E'$ est injectif, E' étant plat sur A' ; c'est le seul usage de cette platitude. Le critère local de platitude pour un idéal nilpotent conclut : si M/IM est plat sur A/I et $I \otimes_A M \to M$ injectif, M est plat. On le démontre sans hypothèse noethérienne, en remontant une filtration $J \subset J + I^{n-1} \subset \cdots \subset A$ de chaque idéal J et en ramenant chaque cran, tué par I, à un module libre.

Pour le point 2, l'effectivité se déduit du point 1 appliqué à la réduction de la donnée. Pour M plat sur A, on applique l'hypothèse à $M_0 = A_0 \otimes_A M$: si $1 \otimes m = 0$ dans $A' \otimes_A M$, alors $m \in IM$, provient de $I \otimes_A M$, qui s'injecte dans $A' \otimes_A M$ par platitude, d'où $m = 0$; et un invariant x de $A' \otimes_A M$ a une réduction de la forme $1 \otimes m_0$, d'où $x - 1 \otimes m = 1 \otimes y$ par l'étape 1 et $x = 1 \otimes (m + y)$. □

Remarque. La page procède autrement : elle traite le cas $I^2 = 0$ par la suite exacte de cohomologie de $0 \to I\, C_D^\bullet \to C_D^\bullet(A'/A, E') \to C_D^\bullet(A'_0/A_0, E'_0) \to 0$, puis raisonne par récurrence sur l'ordre de nilpotence. L'étape 1 montre que cette récurrence n'est pas nécessaire. Comme le note la lecture, les hypothèses $A \simeq H^0(A'/A)$ et $H^1(A'/A) = 0$ de l'énoncé ne servent pas au point 1. Le dernier pas de la page 6, l'isomorphisme $E \otimes_A A' \to E'$, presque illisible, est ici l'étape 3, qui ne demande pas la platitude de E'.

Théorème 12.6 (Grothendieck, page 7, exemple du corollaire 1 ♦). 1. *Si $A \to A'$ est plat, $A' \otimes_A E \to E'$ est bijectif pour toute donnée de descente sur un A'-module E', E désignant ses invariants.*

2. *Si $A \to A'$ est fidèlement plat, $\operatorname{Spec} A' \to \operatorname{Spec} A$ est un morphisme de descente effective pour les modules plats.*
3. *Soient $A \to A'$ et I comme au théorème 12.5, I nilpotent. Si A'_0 est fidèlement plat sur A_0, $\operatorname{Spec} A' \to \operatorname{Spec} A$ est un morphisme de descente effective pour les modules plats.*

Démonstration. Point 1. Soit $f = \psi - (1 \otimes \cdot) : E' \to A' \otimes_A E'$, A-linéaire, de noyau E. Le cocycle dit que $\psi(e)$ est annulé par $A' \otimes f$; A' étant plat, le noyau de $A' \otimes f$ est l'image de $A' \otimes_A E$, qui s'injecte dans $A' \otimes_A E'$. On écrit donc $\psi(e) = j(t)$, avec $j : A' \otimes_A E \hookrightarrow A' \otimes_A E'$, et la counité donne $\theta(t) = e$ pour $\theta : A' \otimes_A E \to E' : \theta$ est surjectif. Pour x invariant, $\psi(\theta(b \otimes x)) = b\psi(x) = b \otimes x = j(b \otimes x)$, donc $j = \psi \circ \theta$, et θ est injectif puisque j l'est.

Point 2. Pour M un A-module, $M \to A' \otimes_A M$ est injectif par fidèle platitude. Si E' est plat sur A', $A' \otimes_A E \simeq E'$ est plat sur A', donc E est plat sur A (la platitude descend le long d'un morphisme fidèlement plat) : la donnée est effective. Enfin, pour la donnée canonique sur $A' \otimes_A M$, d'invariants N, l'application $\iota : M \to N$, $m \mapsto 1 \otimes m$, vérifie $\theta \circ (A' \otimes \iota) = \mathrm{id}$; θ étant bijectif par le point 1, $A' \otimes \iota$ est surjectif, donc ι aussi par fidèle platitude : $M \simeq H^0(A'/A, M)$.

Point 3. C'est le point 2 du théorème 12.5, dont l'hypothèse est donnée par le point 2 appliqué à $A_0 \to A'_0$. □

La démonstration est la descente fidèlement plate classique, écrite directement sur les coactions : elle n'utilise pas la comonadicité de l'extension des scalaires.

Portée de la vérification. Lean définit les données de descente par la coaction (`Descent.DescentDatum`), leurs invariants, l'effectivité (`DescentDatum.IsEffective`), la réduction (`DescentDatum.reduce`) et les morphismes de descente effective pour les modules plats (`IsEffectiveDescentFlat`), et démontre le point 1 (`DescentDatum.isEffective_of_reduce`), le point 2 (`isEffectiveDescentFlat_of_quotient`) et le critère local de platitude (`flat_of_isNilpotent`), pour des anneaux commutatifs quelconques. L'hypothèse sur I y est `IsConductorIdeal`. Il démontre aussi le théorème 12.6 : le point 1 (`DescentDatum.bijective_of_flat`), le point 2 (`isEffectiveDescentFlat_of_faithfullyFlat`, avec `surjective_of_section` et la descente de la platitude `Module.Flat.of_flat_tensorProduct` de mathlib) et le point 3 (`isEffectiveDescentFlat_of_quotient_faithfullyFlat`). Ne sont pas formalisés les corollaires 2 et 3 (énoncé ci-dessous).

Ne sont pas démontrés ici, de la même cote :

Théorème (Grothendieck, pages 8 et 9, corollaires 2 et 3 ♦). *Soient X un préschéma, $\mathcal{I}$ un idéal quasi-cohérent nilpotent de $\mathcal{O}_X$ et $X' = \operatorname{Spec} \mathcal{A}' \to X$ affine, $\mathcal{I}$ s'envoyant isomorphiquement sur un idéal de $\mathcal{A}'$ et X'_0 étant fidèlement plat sur $X_0 = V(\mathcal{I})$. Alors $X' \to X$ est un morphisme de descente effective pour les modules quasi-cohérents plats, et le reste après tout changement de base plat $Y \to X$.*

◊ non vérifié en Lean

Le cas affine, avec l'hypothèse plus faible que $\operatorname{Spec} A'_0 \to \operatorname{Spec} A_0$ soit de descente effective pour les modules plats, est le théorème 12.5, et le cas affine tel qu'énoncé, avec A'_0 fidèlement plat sur A_0, est le point 3 du théorème 12.6. Restent non vérifiés le recollement sur un préschéma et la stabilité par changement de base plat.

Théorème (Grothendieck, pages 19 à 29, descente infinitésimale ♦). *Soient A un anneau semi-local noethérien de radical $\mathfrak{m}$, A' une A-algèbre finie, $A_n = A/\mathfrak{m}^{n+1}$ et $A'_n = A' \otimes_A A_n$. Les trois conditions suivantes, imposées pour tout n, sont équivalentes : $H^1(A'_n/A_n) = 0$; $H^1(A'_n/A_n, \mathrm{GL}_r)$ est trivial ; la descente des modules quasi-cohérents plats le long de $\operatorname{Spec} A'_n \to \operatorname{Spec} H^0(A'_n/A_n)$ est effective. Elles entraînent la descente effective des modules plats de type fini le long de $\operatorname{Spec} A' \to \operatorname{Spec} H^0(A'/A)$.*

◊ non vérifié en Lean

Le théorème lui-même reste non vérifié : mathlib n'a ni la cohomologie d'Amitsur $H^1(A'/A)$ ni le H^1 non abélien $H^1(A'/A, \mathrm{GL}_r)$, et sa démonstration (pages 26 à 29) repose sur le lemme 1 et ses corollaires

2 et 3, que la lecture trouve non démontrés : le cobord multiplicatif d'une unité u est $u^{-1}\partial(u)$, non $\partial(u)$, et le carré de la page 20 ne commute pas. On vérifie ci-dessous les morceaux de la démonstration qui tiennent tels quels (128, lot 1, p. 19).

Rendre une matrice inversible. Le lemme 2 fournit l'hypothèse du corollaire 2 dans la récurrence de la partie a) : toute matrice sur $\widetilde{B}_0 = H^0(A'_0/A_0)$ devient inversible quand on lui ajoute une matrice venue de B. La page le démontre sous deux hypothèses, (i) corps résiduels infinis et (ii) extensions résiduelles radicielles ; la lecture observe que (i) est superflue sous (ii).

Théorème 12.7 (Grothendieck, page 23, lemme 2, sans l'hypothèse (i) ♦)**.** *Soient B un anneau et C une B-algèbre entière n'ayant qu'un nombre fini d'idéaux maximaux. On suppose que deux idéaux maximaux distincts de C induisent des idéaux distincts de B et que chaque extension résiduelle $k(\mathfrak{n})/k(\mathfrak{m})$ est radicielle. Alors pour tout $n \geq 1$ et toute $u \in \mathbb{M}_n(C)$, il existe $v \in \mathbb{M}_n(B)$ telle que $u+\varphi(v)$ soit inversible. En particulier ($n = 1$, N.B. du lemme 1, page 19) $C = C^* + \varphi(B)$.*

Démonstration. Une matrice carrée sur C est inversible si et seulement si son déterminant n'est dans aucun idéal maximal $\mathfrak{n}$; il suffit donc de trouver v telle que $\det(u+v)$ soit non nul dans chaque corps $k(\mathfrak{n}) = C/\mathfrak{n}$. Les idéaux $\mathfrak{m} = \mathfrak{n} \cap B$ sont maximaux (C est entière sur B) et deux à deux distincts, donc deux à deux étrangers : par le lemme chinois, appliqué coefficient par coefficient, on peut prescrire v modulo chacun d'eux. On se ramène ainsi à un seul $\mathfrak{n}$, et à trouver $w \in \mathbb{M}_n(B)$ avec $\det(\bar{u}+\bar{w}) \neq 0$ dans $k(\mathfrak{n})$.

Si $k(\mathfrak{m})$ est infini, on prend $w = t$ scalaire : $\det(t+\bar{u})$ est la valeur en t du polynôme caractéristique de $-\bar{u}$, unitaire, donc non nul, qui n'a qu'un nombre fini de racines dans $k(\mathfrak{n})$, alors que $k(\mathfrak{m}) \to k(\mathfrak{n})$ est injectif. Si $k(\mathfrak{m})$ est fini, il est parfait ; l'extension $k(\mathfrak{n})/k(\mathfrak{m})$, radicielle et algébrique, est alors séparable, donc triviale : $B \to k(\mathfrak{n})$ est surjectif, et on relève $1-\bar{u}$ en w, de sorte que $\bar{u}+\bar{w} = 1$. □

Remarque. Sur un corps résiduel infini, l'hypothèse radicielle ne sert pas, ni la finitude de C : le Lean énonce aussi le lemme sous la forme « à chaque $\mathfrak{n}$, $k(\mathfrak{m})$ est infini ou $B \to k(\mathfrak{n})$ est surjectif ». Pour le N.B. du lemme 1, avec $C = \widetilde{B}_0$ et $B = \overline{B}$, il reste à savoir que $\operatorname{Spec}\widetilde{B}_0 \to \operatorname{Spec}\overline{B}$ est radiciel, ce que la page affirme sans le démontrer.

Descendre relativement à A'/A ou à A'/H^0. Les pages 26 et 27 identifient, entre crochets, la donnée de descente relativement à A'_n/A_n à celle relativement à $A'_n/B^{(n)}$. C'est exact : pour $b \in H^0(A'/A)$, $b \otimes 1 = 1 \otimes b$ dans $A' \otimes_A A'$, et en multipliant par $s \otimes 1$ puis en faisant agir $A' \otimes_A A'$ sur $A' \otimes_A E$, on obtient $bs \otimes e = s \otimes be$; l'application canonique $A' \otimes_A E \to A' \otimes_B E$ a donc un inverse, pour tout A'-module E et tout B entre A et $H^0(A'/A)$. Les complexes d'Amitsur et les données de descente relatives à A'/A et à A'/B coïncident, et $H^0(A'/B) = H^0(A'/A)$.

Portée de la vérification. Lean démontre le lemme 2 sans l'hypothèse (i) (`Infinitesimal.lemme2`, sous la forme générale `Infinitesimal.exists_isUnit_add_map`), le cas $n = 1$ (`Infinitesimal.exists_isUnit_add`), l'identification des produits tensoriels (`Infinitesimal.tensorEquiv`, `Infinitesimal.bijective_mapOfCompatibleSMul`, `Infinitesimal.mem_H0_iff`, avec $H^0(A'/A)$ défini comme égaliseur, `Infinitesimal.H0`), et l'identité $p_2(u)\,p_1(u)^{-1} = 1 + p_1(u)^{-1}(p_2(u) - p_1(u))$ qui fait du cobord multiplicatif une dérivée logarithmique (`Infinitesimal.coboundary_mul_eq`). Ne sont pas formalisés : les H^1 d'Amitsur, additif et non abélien, le lemme 1 et ses corollaires, la récurrence sur n de la partie a), le passage à la limite de la partie b) (Mittag-Leffler, Artin–Rees) et la partie c) ; le théorème encadré ci-dessus reste donc non vérifié.

13 La question de Buffalo : une relation d'équivalence finie non effective (Venken, 1971) [14]

Cette section ne porte pas sur une cote du fonds. Elle répond à une question que Grothendieck a laissée ouverte deux fois. En 1961, dans le troisième exposé sur la construction des schémas, il écrit qu'il ne sait pas si une relation d'équivalence finie, sans hypothèse de platitude, est toujours effective, même sur un corps [122]. Le 11 juillet 1973, à la fin d'une séance de son cours de Buffalo, il la donne encore comme problème ouvert, en ajoutant qu'il attend une réponse négative et que la question est « très élémentaire ». La réponse était imprimée depuis deux ans : c'est le corollaire 3.1 d'une note de Jacques Venken aux *Comptes rendus* [123], dont le titre parle de descente des modules plats et qui, de ce fait, semble être passée inaperçue.

L'idée. On reprend le vocabulaire de la section 12. Soit A une algèbre de dimension finie sur un anneau k et $J \subset A \otimes_k A$ un idéal d'équivalence : il est contenu dans le noyau de la multiplication, stable par l'échange des facteurs, et vérifie la condition de transitivité. Le quotient de $\operatorname{Spec} A$ par la relation est le spectre de l'anneau des invariants

$$A^J = \{\, a \in A : a \otimes 1 - 1 \otimes a \in J \,\}.$$

Les éléments $b \otimes 1 - 1 \otimes b$, pour b invariant, engendrent un idéal $J_{A^J} \subset J$, celui de la relation « avoir la même image dans le quotient ». La relation est *effective* quand les deux coïncident, c'est-à-dire quand elle est exactement la relation définie par son propre quotient. Pour une relation finie et plate, c'est toujours le cas (SGA 3, exposé V [6]). La question est de savoir si la platitude est nécessaire. Comme tout est de dimension finie, la réponse est une affaire d'algèbre linéaire : il suffit d'exhiber un élément de J qui n'est pas dans J_{A^J}, et pour le montrer, une forme linéaire qui s'annule sur J_{A^J} et pas sur cet élément.

L'exemple de Venken. Soit B le quotient de $k[M, N, X, Y, Z, W]$ par l'idéal engendré par

$$M^2,\ MN,\ N^2,\ X^3,\ Y^3,\ Z^3,\ W^3,\ YZ,\ NY,\ MZ,\ NXY,\ MYW$$

et par tous les monômes de degré 3 en X, Y, Z, W ; on note les classes en minuscules. C'est une algèbre locale, de base les 33 monômes qui échappent à ces relations, tous de degré au plus 3. Venken considère la sous-algèbre engendrée par m, n, mx, nw et $my - nz$, et la relation d'équivalence sur $\operatorname{Spec} B$ dont l'idéal est

$$I_V = \big(a \otimes 1 - 1 \otimes a : a = m, n, mx, nw, my - nz\big) + (mxy \otimes w) \subset B \otimes_k B.$$

Les premiers générateurs disent que deux points ont les mêmes valeurs de $m, n, mx, nw, my{-}nz$; le dernier ajoute une condition qui n'est pas de cette forme.

Énoncé (Venken 1971, corollaire 3.1, sous la forme démontrée en Lean)**.** *Soit k un anneau commutatif non nul, et B, I_V comme ci-dessus.*

1. *I_V est un idéal d'équivalence : il est contenu dans le noyau de la multiplication $B \otimes_k B \to B$, il est stable par l'échange des facteurs, et $p_{13}(I_V) \subset p_{12}(I_V) + p_{23}(I_V)$ dans $B \otimes_k (B \otimes_k B)$.*

14. Preuve vérifiée : `lean/Grothendieck/EffectiveVenken.lean`.

2. *Ses invariants forment le sous-module engendré par les dix éléments*

$$1,\ m,\ n,\ mx,\ nz - my,\ nw,\ mx^2,\ my^2,\ nz^2,\ nw^2.$$

3. *$mxy \otimes w$ appartient à I_V mais pas à l'idéal engendré par les $b \otimes 1 - 1 \otimes b$, b invariant. La relation n'est donc pas effective.*

Le point 2 contient une petite surprise : la sous-algèbre de Venken a pour base les six éléments 1, m, n, mx, nw et $my - nz$, et les invariants de la relation sont plus nombreux. Les quatre éléments de degré 3, mx^2, my^2, nz^2 et nw^2, sont invariants sans appartenir à cette sous-algèbre. Cela ne change pas la conclusion, mais il faut les connaître pour la démontrer, puisque l'idéal J_{A^J} dépend de tous les invariants.

Démonstration. Tout se ramène à des identités entre éléments de $B \otimes_k B$, et l'on travaille dans la base des 33×33 produits $u \otimes v$ de monômes de base. La table de multiplication de B est calculée une fois, et Lean la vérifie terme à terme.

Réflexivité. Chaque générateur de I_V s'envoie sur 0 par la multiplication : $a \cdot 1 - 1 \cdot a = 0$, et $mxy \cdot w = mxyw = 0$ puisque MYW est dans l'idéal.

Symétrie et transitivité. L'échange envoie $a \otimes 1 - 1 \otimes a$ sur son opposé, qui est dans I_V ; pour l'image $w \otimes mxy$ du dernier générateur, on exhibe une combinaison explicite des générateurs de I_V à coefficients dans $B \otimes_k B$ qui lui est égale (neuf termes). De même, chaque image par p_{13} d'un générateur est écrite comme combinaison explicite d'images par p_{12} et p_{23} (vingt termes en tout). Ce sont des certificats : trouver la combinaison demande un calcul, la vérifier n'est qu'un développement.

Les invariants. Que les dix éléments soient invariants se vérifie de la même façon, par des combinaisons explicites. L'inclusion inverse est la partie délicate : il faut montrer qu'aucun autre élément de B n'est invariant. On utilise vingt-trois formes linéaires ψ_p sur $B \otimes_k B$, à coefficients entiers, qui s'annulent sur I_V. Si $b = \sum_s c_s\, s$ est invariant, alors $\psi_p(b \otimes 1 - 1 \otimes b) = 0$ pour tout p, et ces vingt-trois équations linéaires en les coefficients c_s forcent b à être une combinaison des dix éléments. Les formes et les combinaisons sont à coefficients entiers et l'argument ne divise jamais : c'est pourquoi l'énoncé vaut sur tout anneau commutatif non nul.

La non-effectivité. Soit φ la forme linéaire sur $B \otimes_k B$, à seize coefficients non nuls, tous entiers, que fournit le calcul. On vérifie qu'elle s'annule sur tous les produits $(u \otimes v)(b \otimes 1 - 1 \otimes b)$, pour u, v monômes de base et b l'un des dix invariants ; elle s'annule donc sur l'idéal J_{A^J} qu'ils engendrent. Et $\varphi(mxy \otimes w) = 1$. Donc $mxy \otimes w \notin J_{A^J}$, alors que $mxy \otimes w \in I_V$ par définition. □

Comment la preuve a été trouvée, et ce qu'elle vérifie. Les combinaisons et les formes linéaires ont été obtenues par une élimination de Gauss sur $\mathbf{Q}$, dans la base des monômes, dont tous les pivots valent ± 1 ; c'est ce qui permet des certificats à coefficients entiers, valables sur tout anneau. Lean ne refait pas l'élimination : il vérifie les certificats, chacun par un calcul sur des listes d'entiers que le noyau évalue (`decide +kernel`, sans `native_decide`). Découpées par degré, ces vérifications prennent une à deux minutes. La démonstration n'utilise que les trois axiomes standard de Lean. Venken, lui, démontre la non-effectivité par la cohomologie d'Amitsur : $mxy \otimes w$ définit une classe non nulle dans $H^1(B/A, \mathbb{G}_a)$. Le certificat φ joue ici le rôle de cette classe.

Ce qui n'est pas formalisé. Les dimensions des deux idéaux en degré 4 (269 et 268 sur

un corps) ne sont pas démontrées en Lean ; seule la forme qui les sépare l'est. Les énoncés de Venken sur la descente des modules plats, et la traduction entre idéaux d'équivalence et relations d'équivalence dans la catégorie des schémas, ne le sont pas non plus. Un second exemple, de longueur 15 (ou 16 en caractéristique 2) en deux variables, obtenu en restreignant la relation de Raicu sur le plan à un sous-schéma fini, est démontré à la main dans la note `grothendieck-effective.pdf` ; il n'est pas formalisé. Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 17 à 23, factorisation radicielle-étale ♦). *Soit $f : X \to Y$ fini et universellement ouvert, Y localement noethérien, dont toutes les fibres ont le même nombre de points géométriques. Alors f se factorise en un morphisme radiciel fini surjectif $X \to X^{ét}$ suivi d'un revêtement étale fini $X^{ét} \to Y$, universel parmi les Y-morphismes de X vers les Y-schémas étales.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : la section ouverte et fermée de la page 19 est marquée « [vérif] », la prose des lemmes des pages 18, 20, 21 et 22 est illisible, et la page 23 s'arrête sur « À formuler ».

Théorème (D'après les pages 4 à 7, forme complétée par l'édition, quotient d'une déformation nilpotente ♦). *Soit $R \rightrightarrows X$ une relation d'équivalence plate dont la réduction $R_0 \rightrightarrows X_0$ modulo un idéal nilpotent est effective, de quotient fpqc quasi-séparé $X_0 \to Y_0$. Alors R est effective, son quotient Y est un épaississement nilpotent de Y_0 et $X \to Y$ est plat.*

◊ non vérifié en Lean

La page porte la conclusion et la méthode, le relèvement par l'annulation de $\check{H}^0(X_0/Y_0, \mathcal{H}^1)$; les hypothèses, en grande partie illisibles, sont reconstituées par l'édition, de même que la réduction au cas $\mathcal{J}^2 = 0$ et la platitude.

Théorème (Grothendieck, pages 26 à 29, descente générique ♦). *Soient S noethérien, $T \to S$ plat de type fini et F une catégorie fibrée sur les S-schémas de type fini pour laquelle les morphismes plats surjectifs sont de F-descente (pleine fidélité seulement). Un isomorphisme $\varphi : p_1^* X \simeq p_2^* X$ défini sur un ouvert dense de $T \times_S T$ et vérifiant la condition de cocycle sur un ouvert dense de $T \times_S T \times_S T$ se prolonge, après restriction de T à un ouvert dense, en une donnée de descente qui coïncide avec φ là où les deux sont définies.*

◊ non vérifié en Lean

Démonstration de la page (pages 26 à 29). On réduit $\mathcal{U}$ et V à des ouverts, et T à un ouvert dense au-dessus duquel les fibres de $\mathcal{U}$ et de V sont denses (p. 26). Sur $W = p_{12}^{-1}(\mathcal{U}) \cap p_{23}^{-1}(\mathcal{U})$, la page définit $\psi : \pi^* X_1 \simeq \pi^* X_2$, $\pi = p_{13}$, en composant φ par un point médian (p. 27). Sa compatibilité avec π se lit sur une partie W' de T^5 par le cocycle ; elle demande que $W' \to W \times_{T \times_S T} W$ soit surjectif, et la page l'admet « sauf erreur » (p. 28). $W \to T \times_S T$ étant plat et surjectif, ψ descend en φ', dont le cocycle se vérifie sur une partie W''' de T^6 (pp. 28–29), et $\varphi' = \varphi$ sur $\mathcal{U}$ car $V \to \mathcal{U}$ est surjectif (p. 29). La lecture réordonne les restrictions.

◊ non vérifiée en Lean

Partie 10

Topos et sites

14 Cote 161-3 : le topos d'un produit d'espaces [15]

La cote 161-3, *Topos : notes manuscrites (s.d.)*, cinquante-quatre pages que l'inventaire date « [vers 1963-1973] », appartient au même groupe de dossiers que les cotes 161-1 et 161-2 (sections 28 et 5). C'est un dossier rassemblé : plusieurs chantiers sans lien entre eux y voisinent sous le seul mot « Topos ». Le premier, pages 3 à 14, porte sur les produits. Les pages 3 à 8 construisent le produit de deux topos (161-3, lot 1, p. 3). Les pages 9 à 14 le comparent au produit de deux espaces (161-3, lot 1, p. 9).

Pour deux espaces topologiques X et Y, le produit est le produit cartésien $X \times Y$, dont les rectangles $U \times V$ forment une base d'ouverts. Un topos se donne par ses faisceaux, et le produit des topos $\mathrm{Top}(X)$ et $\mathrm{Top}(Y)$ est l'endroit où vivent les données à deux variables qui sont locales séparément en chacune. Un faisceau sur $X \times Y$ est une telle donnée, d'où un foncteur $\mathrm{Top}(X \times Y) \to \mathrm{Top}(X) \times \mathrm{Top}(Y)$. La question des pages 9 à 14 est de savoir quand c'est une équivalence. Elle n'a rien d'évident : savoir une chose séparément en x et en y n'est pas la savoir en (x, y), de même qu'en algèbre linéaire les fonctions de deux variables ne sont pas toutes des combinaisons de produits $f(x)g(y)$.

Méthode (Grothendieck, pages 9 à 14, spatialité du locale produit ♦). Pour identifier $\mathrm{Top}(X \times Y)$ et $\mathrm{Top}(X) \times_{\mathrm{top}} \mathrm{Top}(Y)$, on les voit comme faisceaux sur le même site $O_X \times O_Y$ pour deux topologies : la topologie produit π, dont les faisceaux sont les bifaisceaux, et la topologie π' induite par $X \times Y$. On comble l'écart entre elles par trois passages à la borne supérieure dans le treillis des sous-objets, $X \times Y$ étant borne supérieure de rectangles ; la spatialité du locale produit en résulte.

Tout faisceau pour π' l'est pour π, et le foncteur est un plongement. C'est une équivalence exactement quand les deux topologies coïncident, c'est-à-dire quand tout recouvrement ensembliste $U \times V = \bigcup_i U_i \times V_i$ fait aussi de $U \times V$ la borne supérieure des $U_i \times V_i$ dans le produit des topos. Aux pages 9 et 10, la réponse habituelle : si tout point de X a un système fondamental de voisinages quasi-compacts, le lemme du tube referme l'écart. Aux pages 10 et 11 vient un énoncé plus fort, sous une hypothèse plus faible que la compacité locale.

Théorème 14.1 (Grothendieck, pages 10 et 11, topos d'un produit ♦). *Si toute partie localement fermée non vide de X a un point qui y possède un voisinage relativement quasi-compact,* $\mathrm{Top}(X \times Y) \to \mathrm{Top}(X) \times \mathrm{Top}(Y)$ *est une équivalence.*

Les feuillets en esquissent une démonstration : le lemme du tube, puis un plus grand ouvert U' et sa maximalité. L'inclusion $U'' \subset U' \cup \bigcup_i U_i$ qu'elle demande n'y est pas écrite, et l'édition la rétablit.

Le langage des cadres. Les ouverts d'un espace forment un *cadre* (*frame* en anglais) : un treillis complet où l'intersection se distribue sur les réunions quelconques. Un cadre qu'on regarde

15. Preuve vérifiée : `lean/Grothendieck/Folder161_3.lean`.

comme un espace sans points s'appelle un *locale*. En ces termes, le 2-produit $\mathrm{Top}(X) \times \mathrm{Top}(Y)$ est le topos des faisceaux sur le locale produit des ouverts de X et de Y, et la flèche de l'énoncé est une équivalence exactement quand ce locale est spatial, c'est-à-dire égal au locale des ouverts de $X \times Y$. La condition habituelle est la compacité locale d'un facteur.

La démonstration, sous la forme où la page la mène. Lean vérifie le cœur de l'argument, puis sa traduction en termes de locales. Appelons *famille de rectangles* un ensemble S de couples (U, V), formés d'un ouvert U de X et d'un ouvert V de Y, stable quand on rétrécit U ou V et stable par réunion quelconque en chaque variable séparément : c'est le « S » de la page, vu comme l'ensemble des rectangles situés sous la borne supérieure des $U_i \times V_i$ dans le produit des topos. Sous l'hypothèse de l'énoncé, et pour des espaces X et Y quelconques, Lean démontre qu'une telle famille contient tout rectangle $U \times V$ recouvert par ses propres rectangles (`covering`).

La preuve suit la page. Soit $U \times V$ recouvert par des rectangles $U_i \times V_i$ avec $(U_i, V_i) \in S$. On prend le plus grand ouvert U' de U avec $(U', V) \in S$; il existe, puisque S est stable par réunion en la première variable. Si $U' \neq U$, la partie $Z = U \setminus U'$ est localement fermée et non vide : elle a donc un point x muni d'un voisinage T dans Z qui est quasi-compact, et un ouvert U'' de U contenant x avec $U'' \cap Z \subset T$. Pour chaque $y \in V$, le lemme du tube au-dessus de T donne un nombre fini d'indices i avec $T \subset \bigcup_i U_i$, et l'intersection V_y des V_i correspondants est un voisinage ouvert de y. Comme $U'' \setminus U'$ est contenu dans T, on a $U'' \subset U' \cup \bigcup_i U_i$, et $(U' \cup U'', V_y)$ est dans S ; c'est l'inclusion que la page omet, et elle n'y coûte qu'une distinction de cas. La réunion en y donne $(U' \cup U'', V) \in S$, ce qui contredit la maximalité de U', puisque $x \in U'' \setminus U'$.

Lean en tire que ces familles correspondent exactement aux ouverts de $X \times Y$: à un ouvert W on associe les rectangles qu'il contient, et W en est la réunion (`iUnion_rect`, `eq_rect`).

Le coproduit des cadres. Sans aucune hypothèse sur X ni sur Y, ces familles sont les éléments du coproduit des treillis d'ouverts, et Lean le vérifie aussi. Elles forment un cadre : l'intersection de deux familles est leur intersection ensembliste, la réunion d'une collection est la plus petite famille qui les contient toutes, et la distributivité tient à un lemme sur la famille engendrée par un ensemble D de couples stable quand on rétrécit : elle rencontre un ensemble A de même nature à l'intérieur de la famille engendrée par $D \cap A$ (`CIdeal.instFrame`, `CIdeal.span_inter`). Un ouvert U de X donne la famille engendrée par (U, Y), un ouvert V de Y celle engendrée par (X, V) (`CIdeal.inl`, `CIdeal.inr`).

Pour deux morphismes de cadres f et g à valeurs dans un même cadre L, l'application $S \mapsto \bigvee_{(U,V)\in S} f(U) \wedge g(V)$ est l'unique morphisme de cadres qui prolonge f et g (`CIdeal.lift`, `CIdeal.existsUnique_lift`) : c'est la propriété universelle du coproduit. Pour l'existence, on vérifie que la borne supérieure ne change pas quand on remplace un ensemble de couples par la famille qu'il engendre ; c'est là que servent la compatibilité de f et g aux réunions et la distributivité de L. L'unicité vient du fait que chaque famille est la réunion de ses rectangles (`CIdeal.eq_iSup_rect`).

Quand f et g sont les images réciproques par les deux projections, ce morphisme envoie S sur l'ouvert $\bigcup_{(U,V)\in S} U \times V$ de $X \times Y$ (`toOpens`, `toOpens_comp_inl`, `toOpens_comp_inr`). Il est toujours surjectif (`toOpens_surjective`).

Les trois passages à la borne supérieure. La méthode des pages 9 à 14 se vérifie dans le même modèle, au niveau des cadres. Disons que X et Y ont la *propriété de recouvrement* (`Covers`) si toute famille de rectangles contient les rectangles recouverts par ses propres rectangles : c'est l'égalité des topologies π et π', lue sur les cadres. Si tout point de X a un système fondamental de voisinages quasi-compacts, la propriété tient (`covers_of_locallyCompact`), et la démonstration

est celle de la page. Soit $U \times V$ recouvert par des rectangles $U_i \times V_i$ d'une famille S. Pour $x \in U$, soit $K \subset U$ un voisinage compact de x ; pour $y \in V$, le lemme du tube donne un nombre fini de rectangles de S qui recouvrent $K \times \{y\}$, d'où $(\mathring{K}, V_{x,y}) \in S$ pour un voisinage ouvert $V_{x,y}$ de y (premier passage). La borne supérieure en y donne $(\mathring{K}, V)$ (deuxième), celle en x donne (U, V) (troisième). La seule égalité de la chaîne, $(\mathrm{Sup}_i\, U_i) \times V' = \mathrm{Sup}_i (U_i \times V')$, est la stabilité de S par réunions en une variable, qui fait partie de la définition du coproduit des cadres. Sous l'hypothèse plus faible du théorème 14.1, la propriété est le résultat `covering` (`covers_of_hypG`).

Elle rend injective la comparaison `toOpens` (`toOpens_injective_of_covers`), qui est donc un isomorphisme de cadres (`coversEquiv`) ; sous l'hypothèse de la page, c'est l'isomorphisme `frameEquiv` (`frameEquiv_apply`). Le cadre $\mathcal{O}(X \times Y)$, muni des images réciproques par les deux projections, est alors le coproduit de $\mathcal{O}(X)$ et $\mathcal{O}(Y)$: pour deux morphismes de cadres f et g à valeurs dans un cadre L, il existe un unique morphisme de cadres h de $\mathcal{O}(X \times Y)$ dans L avec $h(U \times Y) = f(U)$ et $h(X \times V) = g(V)$ (`existsUnique_opens_prod`). Le locale produit est spatial.

Remarque. Isbell démontre le même énoncé sous une hypothèse voisine : toute partie fermée non vide de X a un point qui y possède un voisinage quasi localement compact, c'est-à-dire dont les ouverts forment un treillis continu [59]. Il procède par récurrence transfinie, et la réciproque vaut pour X complètement régulier [74, th. 1 et 4]. Pour X sobre, son hypothèse entraîne celle de la page, et les deux coïncident pour X séparé (remarque de l'édition, qui s'appuie sur [67, cor. 4.6]). La page remplace la récurrence par un seul argument de maximalité. Plewe caractérise la spatialité des produits de locales par un jeu topologique [105].

Comparaison avec l'hypothèse d'Isbell. Pour X sobre, l'hypothèse de la page est strictement plus faible que celle d'Isbell, et Lean le vérifie sur le contre-exemple d'une réponse publiée sur MathOverflow [98].

On part de l'espace K formé d'un point $\perp$, d'un point p et de points isolés $d_{n,m}$ indexés par $\mathbf{N} \times \mathbf{N}$: le seul ouvert qui contient $\perp$ est K tout entier, et un ouvert contient p seulement s'il contient toutes les lignes $R_n = \{d_{n,m} : m \in \mathbf{N}\}$ à partir d'un certain rang. Toute partie non vide de K a un point isolé dans elle (`K.scattered`), et cela suffit à rendre K sobre, car un point isolé d'un fermé irréductible en est le point générique (`Scattered.quasiSober`, `Scattered.t0Space`). Pourtant K n'est pas quasi localement compact en p (`K.not_coreCompact`). Un ouvert W de $K \setminus \{\perp\}$ qui contient p contient en effet une ligne entière R_n. Si l'on retire de $K \setminus \{\perp\}$ les points $d_{n,m}$ avec $m \geq m_0$, on obtient des ouverts qui croissent avec m_0 et recouvrent $K \setminus \{\perp\}$, mais aucun ne contient W.

L'espace du contre-exemple est la puissance dénombrable $K^{\mathbf{N}}$.

— Il est sobre, parce qu'un produit quelconque d'espaces sobres l'est [59] : le point générique d'un fermé irréductible a pour coordonnées les points génériques des adhérences de ses projections (`quasiSober_pi`).

— Il vérifie l'hypothèse de la page, comme tout produit d'espaces compacts où chaque partie non vide a un point isolé (`hypG_pi`). Dans une partie localement fermée $Z = U \cap H$, avec U ouvert et H fermé, on fixe une à une les coordonnées, en nombre fini, d'un ouvert élémentaire contenu dans U, en prenant chaque fois une valeur isolée (`exists_isolated_pi`). La fibre au-dessus des valeurs choisies est compacte par le théorème de Tychonoff, et sa trace sur H est un voisinage compact dans Z.

— Il ne vérifie pas l'hypothèse d'Isbell (`not_hypI_pi`). Un ouvert de $K^{\mathbf{N}}$ laisse au moins une

coordonnée libre, le long de laquelle K est un rétracte de cet ouvert, et l'argument fait en p vaut pour tout espace dont K est un rétracte (`K.not_coreCompact_of_retract`).

Le théorème `hypG_not_hypI` rassemble ces faits : un espace sobre peut vérifier l'hypothèse de la page sans vérifier celle d'Isbell. Avec la remarque de l'édition selon laquelle, pour X sobre, l'hypothèse d'Isbell entraîne celle de la page, le théorème 14.1 est donc strictement plus général que le théorème 4 d'Isbell.

Portée de la vérification. Les noms cités sont ceux de `Folder161_3.lean`, sauf `quasiSober_pi`, `Scattered.quasiSober` et `Scattered.t0Space`, résultats généraux que la bibliothèque du projet démontre une fois pour toutes dans `Upstream/QuasiSoberPiCoreCompact.lean`. Lean démontre l'argument de la page dans le modèle des familles de rectangles, les trois passages à la borne supérieure des pages 9 et 10, la bijection avec les ouverts de $X \times Y$, la propriété universelle du coproduit des cadres, la spatialité du locale produit sous l'une ou l'autre hypothèse, puis le contre-exemple `hypG_not_hypI`. Reste le côté des topos : l'égalité $\pi = \pi'$ des topologies elles-mêmes, et l'identification des faisceaux sur le locale produit au 2-produit $\mathrm{Top}(X) \times \mathrm{Top}(Y)$. Mathlib n'a pas de 2-catégorie des topos, et l'équivalence de l'énoncé n'est démontrée qu'au niveau des cadres. Lean ne vérifie pas non plus la remarque de l'édition selon laquelle, pour X sobre, l'hypothèse d'Isbell entraîne celle de la page. Elle repose sur le théorème de Hofmann et Lawson : un espace sobre quasi localement compact est localement quasi-compact [67, cor. 4.6].

Ne sont pas démontrés ici : la construction du 2-produit de topos (pages 3 à 8) ; le cas d'un produit infini (pages 11 et 12) au-delà des cadres d'ouverts, démontré ci-dessous ; la question de la page 14, sur des facteurs discrets, que la page laisse sur un point d'interrogation.

Théorème (Grothendieck, pages 3 à 8, 2-produit de topos ♦). *Le 2-produit des topos $\tilde{C}$ et $\tilde{D}$ existe : c'est l'intersection, dans le topos des préfaisceaux sur $C \times D$, des images réciproques des sous-topos $\tilde{C} \subset \hat{C}$ et $\tilde{D} \subset \hat{D}$. Les familles quelconques de topos ont de même un 2-produit.*

◊ non vérifié en Lean

Démonstration de la page (pages 3 à 8). SGA 4 ne construit pas ce produit : la remarque IV 5.13 renvoie à un § 15 qui n'a pas paru, et VI § 8 ne traite que des limites projectives cofiltrantes [7]. SGA 4 énonce en revanche (IV 9.1.2 d) et 9.1.3) que l'intersection de sous-topos est le topos des faisceaux pour la borne supérieure des topologies, ce qu'utilise la page. La construction par intersection elle-même figure chez Pitts (*Cahiers* 26, 1985, preuve du théorème 2.3), qui la donne comme connue, et chez Caramello et Lafforgue (2025, lemme III.1.9 (ii), théorème III.1.10 (ii)) pour les produits finis. Dans $\widehat{C \times D}$, les préfaisceaux qui sont des faisceaux en la première variable, resp. la seconde, forment deux sous-topos, dont les bifaisceaux sont l'intersection (pp. 3–4). Ce sont les images réciproques de $\tilde{C} \subset \hat{C}$ et $\tilde{D} \subset \hat{D}$ par les projections, et $\widehat{C \times D}$ est le 2-produit de $\hat{C}$ et $\hat{D}$, les foncteurs exacts à gauche sur $C \times D$ correspondant aux couples de tels foncteurs sur C et sur D (pp. 5–6). Pour une famille, la page prend le produit restreint des C_i et l'intersection des images réciproques (pp. 7–8). L'existence de l'intersection de sous-topos n'est pas énoncée.

◊ non vérifiée en Lean

Les sous-topos sont ici les sous-catégories réflexives à réflecteur exact à gauche de la section 28.

Théorème (Grothendieck, pages 11 et 12, topos d'un produit infini ♦). *Pour une famille quelconque d'espaces (X_i), $\mathrm{Top}(\prod X_i) \to \prod \mathrm{Top}(X_i)$ est une équivalence quand tous les facteurs sauf un au plus ont des systèmes fondamentaux de voisinages quasi-compacts et que tous sauf un au plus sont quasi-compacts.*

◊ non vérifié en Lean

Démonstration de la page (pages 11 et 12). Le cas fini se tire du cas de deux facteurs (p. 11).

◊ non vérifiée en Lean

En général, I étant réunion filtrante de parties finies J_α, le 2-produit est le topos des faisceaux sur la catégorie $\mathcal{O}'_Z$ des ouverts de $Z = \prod X_i$ venus d'un $Z_\alpha = \prod_{i\in J_\alpha} X_i$, pour la topologie limite ; il reste à voir qu'elle est la topologie induite par Z. Pour $W = U \times Z'_\alpha$ recouvert par des V_λ, la quasi-compacité de $Z'_\alpha = \prod_{i\notin J_\alpha} X_i$ donne pour chaque $z \in U$ un voisinage U_z tel que $U_z \times Z'_\alpha$ soit majoré par la borne supérieure S des V_λ, d'où $S \geq W$ (p. 12). Cet argument suppose quasi-compacts tous les facteurs hors d'un nombre fini.

Le cas des cadres d'ouverts. Comme pour deux facteurs, la page raisonne sur le produit restreint $\prod' \mathcal{O}_{X_i}$, au niveau des cadres d'ouverts. C'est cette forme de l'énoncé que Lean démontre, sous une hypothèse un peu plus faible que celle de la page, celle que dégage la note de la lecture.

Énoncé (Grothendieck, pages 11 et 12, forme des cadres d'ouverts). [a] *Soit $(X_i)_{i\in I}$ une famille quelconque d'espaces topologiques. On appelle* pavé *une famille (U_i) d'ouverts avec $U_i = X_i$ sauf pour un nombre fini d'indices, et on note $\bigotimes_i \mathcal{O}(X_i)$ le cadre des ensembles de pavés stables par rétrécissement et par réunion quelconque en chaque coordonnée séparément.*

(a) Muni des injections $U \mapsto \mathrm{pr}_i^{-1}(U)$, $\bigotimes_i \mathcal{O}(X_i)$ est le coproduit des cadres $\mathcal{O}(X_i)$.

(b) Si tous les X_i sauf un au plus sont localement quasi-compacts, et si tous sauf un nombre fini sont quasi-compacts, l'application $S \mapsto \bigcup_{(U_i)\in S} \prod_i U_i$ est un isomorphisme de cadres de $\bigotimes_i \mathcal{O}(X_i)$ sur $\mathcal{O}(\prod_i X_i)$. Le cadre $\mathcal{O}(\prod_i X_i)$, muni des images réciproques par les projections, est alors le coproduit des $\mathcal{O}(X_i)$: le locale produit est spatial.

En particulier, l'hypothèse de la page (« tous sauf au plus un », deux fois) suffit.

a. Preuve vérifiée : `lean/Grothendieck/Folder161_3.lean`.

Démonstration. (a) Un élément S est la borne supérieure de ses pavés, et un pavé est la borne inférieure *finie* des $\mathrm{pr}_i^{-1}(U_i)$, $U_i \neq X_i$; un morphisme de cadres est donc déterminé par ses composées avec les injections, et $S \mapsto \bigvee_{(U_i)\in S} \bigwedge_i f_i(U_i)$ le fournit. La loi distributive se démontre comme pour deux facteurs.

(b) L'application est surjective sans hypothèse, car tout ouvert du produit est réunion des pavés qu'il contient. Pour l'injectivité, il faut voir qu'un S contient tout pavé u que ses pavés recouvrent ensemblistement. D'abord un lemme du tube, sans hypothèse : un produit de parties compactes $\prod_i K_i$ recouvert par les pavés de S est contenu dans un seul pavé de S. Par Tychonoff, un nombre fini de pavés suffisent, à supports dans une partie finie H, et l'on raisonne coordonnée par coordonnée sur H, par la récurrence des parties compactes, les autres coordonnées étant figées en un point. Soient ensuite e l'indice exceptionnel et G la partie finie des indices où $u_i \neq X_i$ ou bien X_i n'est pas quasi-compact. On passe à la borne supérieure sur chaque coordonnée de G autre que e, au moyen de voisinages compacts $K_i \subset u_i$. On passe enfin à la borne supérieure sur les points y de la coordonnée e : le compact $\prod_{i\in G\setminus\{e\}} K_i \times \{y\} \times \prod_{i\notin G\cup\{e\}} X_i$ est dans $\prod u_i$, donc dans un pavé de S, ce qui donne un voisinage de y. □

Lean : `PIdeal.existsUnique_lift` pour (a) ; `PIdeal.exists_box_of_isCompact` pour le lemme du tube, `piCovers` pour la spatialité, `piCoversEquiv` et `existsUnique_opens_pi` pour (b), `piFrameEquiv` pour l'hypothèse de la page.

Remarque. La démonstration de Lean ne suit pas le chemin de la page, qui passe par les produits finis $\prod_{i\in J_\alpha} X_i$ et la limite filtrante sur α : elle va directement au produit restreint, et les passages à la borne supérieure sont ceux des pages 9 et 10. Reste le côté des topos : l'identification des faisceaux sur le locale produit au 2-produit $\prod^{\mathrm{top}} \mathrm{Top}(X_i)$. Mathlib n'a pas de 2-catégorie des topos.

15 Cote 37 : le contre-exemple à EGA I 10.10.5 [16]

La cote 37, *Rééditions SGA, EGA [SGA 4 à SGA 7, EGA I et EGA II]*, quatre-vingt-dix-neuf pages de tapuscrits, de lettres et de notes, dont l'inventaire date les lettres « (1967-1971, s.d.) », est un dossier de travail éditorial : les rééditions de SGA 1, 4, 5, 6 et 7 et d'EGA I et II, avec les lettres échangées et quelques morceaux de mathématiques inédits. La page 92 est une lettre dactylographiée à Dieudonné, datée à la main du 27.8.1967. Dieudonné avait tiqué sur la généralisation proposée d'EGA I 10.10.5 hors du cas noethérien ; la lettre admet que les conditions a) et c) « ne son[t] pas impliquées par b) » et le montre sur $A = B[[T]]$, $A_n = B[T]/(T^{n+1})$, $M_n = A_n/J_n$ avec $J_n = (X_0, X_1T, \dots, X_nT^n)$ et $B = k[(X_i)_{i\geq 0}]$, pour lequel les générateurs écrits de J_n sont « en nombre minimal » (37, lot 5, p. 92). La lettre affirme pour cela que ces générateurs sont linéairement indépendants sur B dans J_n/TJ_n ; c'est faux : $X_0 \cdot X_1T = T \cdot X_1X_0 \in TJ_n$. Sa réduction modulo les X_j, $j \neq i$, montre seulement que chaque coefficient est dans l'idéal $(X_j)_{j\geq 0}$, et cela suffit. La lecture rédige ainsi la minimalité et ajoute l'étape de Schanuel, que la lettre laisse implicite.
Conventions. k est un corps, $B = k[X_0, X_1, \dots]$, $P = B[T]$, $A_n = P/(T^{n+1})$ et $J_n \subset A_n$ l'idéal engendré par les classes de X_lT^l, $0 \leq l \leq n$. Pour $f \in P$, on note $\lambda_i(f) \in k$ le coefficient du monôme X_iT^i et $\varepsilon(f) \in k$ le terme constant ; ε est un homomorphisme d'anneaux, λ_i est k-linéaire.

Lemme 15.1. *Pour $a \in P$ et $i, l \geq 0$, $\lambda_i(a \cdot X_lT^l)$ vaut $\varepsilon(a)$ si $l = i$ et 0 sinon. Pour $i \leq n$, $\lambda_i(a\,T^{n+1}) = 0$.*

Démonstration. Tout monôme de $a\,X_lT^l$ est divisible par X_lT^l. Le monôme X_iT^i ne l'est que si $l = i$, et le coefficient de X_iT^i dans $a\,X_iT^i$ est alors celui du monôme 1 dans a. Tout monôme de $a\,T^{n+1}$ a un degré en T au moins $n + 1 > i$. □

Théorème 15.2 (Grothendieck, page 92, minimalité des générateurs ♦)**.** *L'idéal J_n de A_n est engendré par $n + 1$ éléments et ne l'est par aucune famille de moins de $n + 1$ éléments.*

Démonstration. Soient $g_1, \dots, g_m$ des générateurs de J_n. On écrit chaque X_jT^j, $0 \leq j \leq n$, comme combinaison $\sum_r a_{jr}g_r$, et chaque g_r comme combinaison $\sum_l b_{rl}X_lT^l$, puis on relève tout dans P : les égalités y valent à un multiple de T^{n+1} près. Appliquons λ_i, $i \leq n$, à la première. Par le lemme 15.1, le membre de gauche donne δ_{ij}, le multiple de T^{n+1} ne contribue pas, et chaque $a_{jr}g_r$ donne $\sum_l \lambda_i(a_{jr}b_{rl}X_lT^l) = \varepsilon(a_{jr})\,\varepsilon(b_{ri})$. Les matrices $E = (\varepsilon(a_{jr}))$, de taille $(n + 1) \times m$, et $L = (\varepsilon(b_{ri}))$, de taille $m \times (n + 1)$, à coefficients dans k, vérifient donc $EL = 1$. Le rang de l'identité, $n + 1$, est au plus celui de E, lui-même au plus m. □

Énoncé (Page 92, compatibilité)**.** *Le A_n-module $M_n = A_n/J_n$ est de présentation finie, et la réduction $A_{n+1} \to A_n$ envoie J_{n+1} sur J_n : les M_n forment un système compatible.*

Démonstration. M_n est le quotient de A_n par un idéal de type fini. L'image de J_{n+1} est engendrée par les classes de X_lT^l, $l \leq n + 1$, et $X_{n+1}T^{n+1}$ est nul dans A_n. □

Lemme 15.3 (l'étape de Schanuel)**.** *Soient S un anneau commutatif, J un idéal de S, F un S-module projectif, $\varphi : F \to N$ surjective et $\gamma : K \to F$ d'image le noyau de φ, où K est engendré par p éléments. Si $N \simeq S/J$, alors J est engendré par $p + 1$ éléments.*

16. Preuve vérifiée : `lean/Grothendieck/Folder37.lean`.

Démonstration. Soit $\varphi' : F \to S/J$ le composé de φ et de l'isomorphisme. Comme F est projectif, φ' se relève en $\psi : F \to S$; comme φ' est surjective, il existe $x_0 \in F$ d'image la classe de 1, et l'on pose $\chi(s) = sx_0$. Alors $c = 1 - \psi(x_0)$ est dans J, et les $\psi(\gamma(v_r))$, pour des générateurs $v_1, \dots, v_p$ de K, aussi, puisque $\varphi \circ \gamma = 0$. Réciproquement, pour $x \in J$, $\varphi'(\chi(x))$ est la classe de x, nulle, donc $\chi(x) = \gamma(y)$ pour un $y \in K$, et $x = xc + x\,\psi(x_0) = xc + \psi(\gamma(y))$ est dans l'idéal engendré par c et les $\psi(\gamma(v_r))$. □

Théorème 15.4 (D'après la page 92, contre-exemple à EGA I 10.10.5, sous une forme plus générale ♦). *Soient A un anneau commutatif quelconque et, pour tout n, un homomorphisme d'anneaux quelconque $A \to A_n$. Il n'existe pas de A-module de présentation finie M tel que $A_n \otimes_A M \simeq M_n$ comme A_n-modules pour tout n. En particulier, pour $A = B[[T]]$ et ses réductions, le système compatible (M_n) de modules de présentation finie ne vient d'aucun A-module de présentation finie : la condition b) d'EGA I 10.10.5 n'entraîne pas a) et c) sans hypothèse noethérienne.*

Démonstration. Soit $A^p \xrightarrow{\gamma_0} A^q \xrightarrow{\varphi_0} M \to 0$ une présentation. Le produit tensoriel par A_n est exact à droite : $A_n \otimes_A A^p \to A_n \otimes_A A^q \to A_n \otimes_A M \to 0$ est exact, le module du milieu est libre, et celui de gauche est engendré par p éléments. Si $A_n \otimes_A M \simeq A_n/J_n$, le lemme 15.3 engendre J_n par $p+1$ éléments, et le théorème 15.2 donne $n+1 \leq p+1$ pour tout n, ce qui est absurde pour $n = p+1$. □

Remarque. Le contre-exemple tient tel que la lettre l'énonce, et plus généralement. Ni la complétude de A, ni la surjectivité des $A \to A_n$, ni la compatibilité des isomorphismes ne servent : une présentation de M par q générateurs et p relations borne uniformément, par $p+1$, le nombre de générateurs de chaque J_n. La borne de la lecture, $p+q$, est remplacée par $p+1$. La minimalité est démontrée comme la lecture la rédige, par l'indépendance des $n+1$ générateurs dans $J_n/(TJ_n + \mathfrak{m}J_n)$, $\mathfrak{m} = (X_j)_{j\geq 0}$, mise en équations : les formes λ_i sont nulles sur $TJ_n + \mathfrak{m}J_n$ et valent δ_{il} sur $X_l T^l$.

Ne sont pas démontrés ici : les schémas formels et les conditions a), b), c) d'EGA I 10.10.5 elles-mêmes, que la page ne rappelle pas ; l'implication a) ⇒ c) sans hypothèse noethérienne, que les deux correspondants laissent ouverte ; le « canular » d'EGA IV 17.1.6 (i) que signale la page 93. Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 86 à 88, finitude de la normalisation ♦). *Soit A un anneau noethérien intègre quotient d'un anneau régulier. La clôture intégrale de A est finie sur A si et seulement si les premiers $\mathfrak{p}$ de hauteur un tels que $A_\mathfrak{p}$ n'est pas régulier sont en nombre fini et que, pour chacun, la normalisée de $A_\mathfrak{p}$ est finie sur $A_\mathfrak{p}$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : ils construisent $C = i_* i^* \tilde{B}$ à travers un fermé de codimension ≥ 2 et la montrent (S_2) et (R_1) par le critère de Serre ; l'universelle caténarité de A vient de l'édition, et la cohérence de C repose sur une phrase dont le milieu est illisible.

Théorème (Grothendieck, page 22, quand $\mathrm{Ind}(C)$ est un topos ♦). *Pour une petite catégorie C d'enveloppe de Karoubi C', $\mathrm{Ind}(C)$ est un topos si et seulement si C' a les limites inductives finies et que son foncteur canonique vers les faisceaux pour la topologie finitaire les respecte ; ce topos est alors parfait exactement quand C' a les limites projectives finies.*

◊ non vérifié en Lean

Mathlib n'a pas les conditions de SGA 4 pour que $\mathrm{Ind}(C)$ soit un topos. On se reportera aux notes de Grothendieck (37, lot 2, p. 22).

Conjecture (Grothendieck, pages 1 à 4, Dold–Kan hors de Δ ♦). *Pour une petite catégorie A, la restriction aux préfaisceaux abéliens « lisses », ceux le long desquels la linéarisation ne varie pas, donne une correspondance de type Dold–Kan avec une catégorie dérivée de complexes localement constants. La page pose la question sous plusieurs formes et relève que L_b porte des coefficients tordus et non constants.*

Mathlib n'a pas les catégories dérivées de complexes localement constants. On se reportera aux notes de Grothendieck (112, lot 1, p. 1).

Théorème (Grothendieck, pages 6 et 7, recollement de topos de préfaisceaux ♦). *Un topos recollé d'un sous-topos ouvert X_0 et de son fermé complémentaire X_1 le long d'un foncteur exact à gauche φ est un topos de préfaisceaux exactement quand X_0 et X_1 sont de la forme $\mathrm{Top}(\mathcal{X}_0)$ et $\mathrm{Top}(\mathcal{X}_1)$ et que φ commute aux limites projectives quelconques ; la donnée de recollement est alors un bifoncteur $\mathcal{X}_0^{\mathrm{op}} \times \mathcal{X}_1 \to (\mathrm{Ens})$.*

◊ non vérifié en Lean

Mathlib n'a pas le recollement des topos. On se reportera aux notes de Grothendieck (116, lot 1, p. 6).

Partie 11

Variétés abéliennes et schémas de Picard

16 Cote 44 : l'intégralité des nombres de Cartan à partir des axiomes [17]

La cote 44, *Jacobiennes intermédiaires : notes manuscrites (s.d.), lettre (1964)*, compte huit pages. Trois feuillets d'un programme sur les jacobiennes intermédiaires y entourent la lettre à Serre du 12 août 1964. La page 4 est étrangère au programme : c'est un feuillet barré d'une longue diagonale, qui énumère deux structures axiomatiques, un système de racines réduit et ce qu'on appelle aujourd'hui une donnée radicielle. La première est un couple (P, Δ), P abélien libre de rang fini et $\Delta \subset P$ finie, soumis à trois conditions : a) Δ engendre P ; b) si $a \in \Delta$, alors $-a \in \Delta$, « mais $na \notin \Delta$ si $n \neq 1, -1$, $n \in \mathbb{Q}$ » ; c) pour tout $a \in \Delta$, il existe une « symétrie » S_a qui envoie a sur $-a$ et vérifie $S_a(\Delta) \subset \Delta$. Une note réalise toutes les symétries par la forme invariante $\sum_{a \in \Delta} \langle x, a\rangle \langle y, a\rangle$, écrit $S_\alpha x = x - \langle \gamma_\alpha, x\rangle\, \alpha$ avec $\gamma_\alpha \in P'^{\mathbb{Q}}$, puis, après un mot illisible, « que l'on a en fait $\gamma_\alpha \in P'$ », c'est-à-dire que les nombres de Cartan $c_{\alpha\beta} = \langle \gamma_\alpha, \beta\rangle$ sont entiers. Un crochet en donne la raison : chaque α serait indivisible dans P, parce qu'il peut faire partie d'un « système fondamental de racines » (44, lot 1, p. 4). Le mot qui gouverne l'assertion et une bonne part du crochet sont illisibles. La lecture modernisée tient l'intégralité pour une conséquence des axiomes ; la piste de l'onglet Findings objecte que les trois axiomes seuls ne la donnent pas.

Conventions. Soient V un espace vectoriel sur $\mathbb{Q}$ et P un sous-groupe de V. Un élément $\alpha \in P$ est *indivisible dans P* si, chaque fois que $\alpha = my$ avec $m \in \mathbb{Z}$ et $y \in P$, on a $m = \pm 1$. Dans l'exemple, $P = \mathbb{Z}^2$, de base (e_1, e_2), et les symétries sont calculées dans $\mathbb{Q}^2$.

Énoncé (Page 4, de l'indivisibilité à l'intégralité ♦). *Soient $\alpha \in P$ indivisible dans P et $f : V \to \mathbb{Q}$ une application telle que $x - f(x)\,\alpha \in P$ pour tout $x \in P$. Alors $f(x) \in \mathbb{Z}$ pour tout $x \in P$. En particulier, si la symétrie $S_\alpha x = x - \langle \gamma_\alpha, x\rangle\, \alpha$ envoie P dans P et si α est indivisible dans P, les nombres $\langle \gamma_\alpha, \beta\rangle$, $\beta \in P$, sont entiers.*

Démonstration. Soient $x \in P$ et $q = f(x)$; on a $q\alpha = x - (x - q\alpha) \in P$. On conclut par l'énoncé général : si $\alpha \in P$ est indivisible dans P et si $q\alpha \in P$ pour un rationnel q, alors $q \in \mathbb{Z}$. □

Résultat général, démontré en Lean dans
`Upstream/RatSmulMemIndivisible.lean` *; la démonstration n'est pas reprise ici.*

Remarque. L'argument n'utilise ni la liberté de P, ni la finitude de Δ, ni la forme invariante : il suffit que S_α préserve P et soit de la forme $x \mapsto x - f(x)\,\alpha$. C'est le pas que le crochet attribue à l'indivisibilité.

Contre-exemple 16.1 (Page 4, les trois axiomes seuls ♦). *Dans $P = \mathbb{Z}^2$, soit*

$$\Delta = \{\pm 3e_1, \pm 3e_2, \pm(e_1 + e_2), \pm(e_1 - e_2)\}.$$

1. *Δ engendre $\mathbb{Z}^2$ (axiome a).*

17. Preuve vérifiée : `lean/Grothendieck/Folder44.lean`.

2. *$\Delta = -\Delta$, et aucune racine n'est un multiple rationnel qa d'une racine a avec $q \neq \pm 1$ (axiome b, avec $n \in \mathbb{Q}$ comme sur la page).*
3. *Pour chaque $a \in \Delta$, il existe un automorphisme S de $\mathbb{Z}^2$ tel que $Sa = -a$ et $S(\Delta) \subset \Delta$ (axiome c).*
4. *Soit $f : \mathbb{Z}^2 \to \mathbb{Q}$ additive, avec $f(3e_1) = 2$, telle que $x \mapsto x - f(x) \cdot 3e_1$ envoie Δ dans Δ. Alors $f(e_1 + e_2) = 2/3$. Une telle f existe : $f(x_1, x_2) = 2x_1/3$.*

Le nombre de Cartan $\langle \gamma_{3e_1}, e_1 + e_2 \rangle$ vaut donc $2/3$, qui n'est pas entier, et $3e_1 = 3 \cdot e_1$ est divisible dans P.

Démonstration. On a $e_1 = 3e_1 - (e_1 + e_2) - (e_1 - e_2)$ et $e_2 = (e_1 + e_2) - e_1$, d'où l'axiome a). Pour b), deux racines proportionnelles sont sur une même droite par l'origine, et chacune des quatre droites $\mathbb{Q}e_1$, $\mathbb{Q}e_2$, $\mathbb{Q}(e_1 + e_2)$, $\mathbb{Q}(e_1 - e_2)$ ne contient que deux racines opposées ; on vérifie les soixante-quatre couples. Pour c), les quatre réflexions du groupe de Weyl de type B_2, $(x_1, x_2) \mapsto (-x_1, x_2)$, $(x_1, -x_2)$, $(-x_2, -x_1)$ et (x_2, x_1), permutent Δ et changent en leur opposé respectivement $\pm 3e_1$, $\pm 3e_2$, $\pm(e_1 + e_2)$ et $\pm(e_1 - e_2)$.

Pour 4), l'additivité donne $3f(2e_1) = 2f(3e_1) = 4$, donc $f(e_1 + e_2) + f(e_1 - e_2) = f(2e_1) = 4/3$. L'image de $e_1 + e_2$ est $(1 - 3f(e_1 + e_2),\ 1)$; c'est une racine de seconde coordonnée 1, donc $e_1 + e_2$ ou $-e_1 + e_2$, et $f(e_1 + e_2) \in \{0, 2/3\}$. De même l'image $(1 - 3f(e_1 - e_2),\ -1)$ de $e_1 - e_2$ donne $f(e_1 - e_2) \in \{0, 2/3\}$. La somme valant $4/3$, les deux valent $2/3$. Pour $f(x_1, x_2) = 2x_1/3$, l'application $x \mapsto x - f(x) \cdot 3e_1$ est la première réflexion. Enfin $3e_1 = 3 \cdot e_1$ avec $e_1 \in P$ et $3 \neq \pm 1$. □

Remarque. La réserve de la piste se confirme : les axiomes a) à c), même avec $n \in \mathbb{Q}$ dans b), ne donnent pas l'intégralité, et la symétrie de $3e_1$ y est unique, de sorte que le nombre $2/3$ ne dépend d'aucun choix. Les longueurs des racines sont dans le rapport $3/\sqrt{2}$ au lieu de $\sqrt{2}$: le groupe engendré par les symétries est celui de B_2, mais Δ n'est pas cristallographique. La fiche ajoutait que $3e_1$ appartient encore au système simple $\{3e_1, e_2 - e_1\}$; c'est vrai au sens des groupes de réflexions, à coefficients rationnels positifs, mais pas au sens entier, car $e_1 + e_2 = \frac{2}{3} \cdot 3e_1 + (e_2 - e_1)$ n'est pas combinaison entière de $3e_1$ et $e_2 - e_1$ (vérifié dans le fichier). Comme un élément d'un système fondamental au sens entier fait partie d'une base de P, il est indivisible, et le crochet de la page n'est pas réfuté : les trois axiomes ne garantissent pas l'existence d'un tel système. Reste à lire sur le fac-similé le mot qui gouverne l'assertion, pour savoir si la page affirme, se propose de démontrer ou demande.

Ne sont pas démontrés ici : l'unicité des symétries par la forme invariante $\sum_a \langle x, a\rangle\langle y, a\rangle$ dans le cas général ; l'énoncé qu'un élément d'un système fondamental au sens entier est indivisible ; les axiomes de la donnée radicielle $(P, P', \Delta, \Delta', \varphi)$ de la seconde moitié du feuillet.

17 Cote 50 : la formule des traces dans le cadre axiomatique [18]

La cote 50, *Sur bouquin Lang : notes manuscrites*, que l'inventaire date d'après 1965, compte dix pages. Les pages 6 à 10, à lire dans l'ordre 10, 9, 8, 7, puis le haut de 8 et enfin 6, posent pour les endomorphismes des variétés abéliennes un cadre sans points ni diviseurs : une catégorie additive à dualité D, un groupe $N(A)$ d'éléments antisymétriques de $\mathrm{Hom}(A, D(A))$, deux cônes N^+ et $N^>$, une forme d'intersection I r-linéaire à valeurs entières, strictement positive

18. Preuve vérifiée : `lean/Grothendieck/Folder50.lean`.

sur $N^>$, et un degré ν tel que $I(u^*\xi_1,\dots,u^*\xi_r)=\nu(u)\,I(\xi_1,\dots,\xi_r)$ (50, lot 1, p. 7). La page 8 en tire les coefficients $\sigma_i(\alpha)$ de $\nu(\alpha+n)$ et la formule des traces $\mathrm{tr}(\alpha)=r\,I(\xi^{r-1},D_\xi(\alpha))/I(\xi^r)$, où $D_\xi(\alpha)=(\alpha+1)^*\xi-\alpha^*\xi-\xi$; la page 6 l'écrit pour $\alpha\beta'$ et $\alpha\alpha'$, puis s'arrête sur le mot « Corollaire », que la lecture complète par la positivité de l'involution de Rosati, $\mathrm{tr}(\alpha\alpha')>0$ pour $\alpha\neq 0$ (50, lot 1, p. 6).

Pour une courbe elliptique E et un endomorphisme α, le degré de $\alpha+n$ est un polynôme en l'entier n, de la forme $n^2+\mathrm{tr}(\alpha)\,n+\deg\alpha$; pour $\alpha=m$ entier, on trouve $(n+m)^2$, d'où $\mathrm{tr}(m)=2m$. La page cherche à obtenir ce polynôme et sa trace à partir des seuls axiomes, sans géométrie ; la trace s'y lit comme un rapport de deux nombres d'intersection. Si la positivité de Rosati suivait des axiomes, elle donnerait la structure de l'algèbre $\mathrm{End}(A)\otimes\mathbf{Q}$. Vérification faite, la formule des traces suit des axiomes à condition que I soit symétrique, et la positivité n'en suit pas.

Conventions. On fixe un objet A et une classe ξ dont le morphisme φ_ξ est un $\mathbf{Q}$-isomorphisme, et l'on transporte tout dans $E=\mathrm{End}(A)$ par $\psi(\eta)=\varphi_\xi^{-1}\varphi_\eta$: l'involution de Rosati $\alpha'=\varphi_\xi^{-1}\,{}^t\alpha\,\varphi_\xi$ est une anti-involution de E, et $\varphi_{\alpha^*\eta}={}^t\alpha\,\varphi_\eta\,\alpha$ se lit $\psi(\alpha^*\eta)=\alpha'\psi(\eta)\alpha$, avec ψ injectif et $\psi(\xi)=1$. Les cônes, quand ils servent, sont stables par addition et par multiplication par $n>0$, $N^>\subset N^+$, $N^>$ engendre N, φ_x est un $\mathbf{Q}$-isomorphisme pour $x\in N^>$, $I>0$ sur $(N^>)^r$, $u^*N^+\subset N^+$ pour tout u et $u^*N^>\subset N^>$ si $\nu(u)\neq 0$.

Énoncé (Pages 8 et 9, le polynôme $\nu(\alpha+n)$)**.** *Les identités (1)–(3) de la page 9 valent :* $\psi(D_\xi(\alpha,\beta))=\alpha'\beta+\beta'\alpha$, $D_\xi(\alpha,\beta)=D_\xi(\alpha'\beta)=D_\xi(\beta'\alpha)$, $D_\xi(\alpha')=D_\xi(\alpha)$*; de plus* $(uv)^*=v^*u^*$ *et* $\nu(uv)=\nu(u)\nu(v)$*. Il existe un unique polynôme de* $\mathbf{Q}[X]$ *qui prend en tout entier* n *la valeur* $\nu(\alpha+n)$*; il est unitaire de degré* $2r$*, de terme constant* $\nu(\alpha)$*, et les* $\sigma_i(\alpha)$ *sont ses coefficients.*

L'énoncé tient. Les théorèmes `nu_mul`, `charPoly_unique` et `charPoly_monic` sont dans le fichier `Folder50.lean`.

Théorème 17.1 (D'après la page 8, avec I symétrique ♦)**.** *Si I est symétrique,* $\mathrm{tr}(\alpha)\,I(\xi^r)=r\,I(\xi^{r-1},D_\xi(\alpha))$ *pour tout* $\alpha\in E$*. En particulier* $\mathrm{tr}(\alpha'\alpha)\,I(\xi^r)=2r\,I(\xi^{r-1},\alpha^*\xi)$ *et* $\mathrm{tr}(\alpha\alpha')\,I(\xi^r)=2r\,I(\xi^{r-1},\alpha'^*\xi)$.

Démonstration. On a $\psi((\alpha+n)^*\xi)=(\alpha'+n)(\alpha+n)=n^2+n(\alpha+\alpha')+\alpha'\alpha$, donc $(\alpha+n)^*\xi=n^2\xi+n\,D_\xi(\alpha)+\alpha^*\xi$ par injectivité de ψ. Par l'axiome du degré, $\nu(\alpha+n)\,I(\xi^r)=I\big((n^2\xi+n\,D_\xi(\alpha)+\alpha^*\xi)^r\big)$, que la multilinéarité développe en une somme sur les $f:\{1,\dots,r\}\to\{\xi,D_\xi(\alpha),\alpha^*\xi\}$, de poids 2, 1, 0. Le poids total $2r$ n'est atteint que pour f constante en ξ ; le poids $2r-1$ l'est pour les r fonctions qui prennent une fois la valeur $D_\xi(\alpha)$, et la symétrie ramène chacun des r termes à $I(\xi^{r-1},D_\xi(\alpha))$. Enfin $\psi(D_\xi(\alpha'\alpha))=2\alpha'\alpha$, d'où $D_\xi(\alpha'\alpha)=2\alpha^*\xi$. □

Remarque. La page 6 écrit $\alpha^*\xi$ en regard de $\mathrm{tr}(\alpha\alpha')$; les axiomes donnent $\alpha^*\xi$ pour $\alpha'\alpha$ et $\alpha'^*\xi$ pour $\alpha\alpha'$. L'égalité des deux formes est $\mathrm{tr}(\alpha\alpha')=\mathrm{tr}(\alpha'\alpha)$, que le cadre ne donne pas sans autre argument.

Contre-exemple 17.2 (Contre-exemple de l'édition, I non symétrique)**.** *Soient* $E=N=\mathbf{Z}^2$*, d'involution triviale,* $\psi=\mathrm{id}$*,* $\alpha^*\eta=\alpha^2\eta$*,* $\xi=(1,1)$*,* $r=2$*,* $I(x,y)=x_1y_2$*,* $\nu(u)=u_1^2u_2^2$*,* $N^+=\mathbf{N}^2$*,* $N^>=(\mathbf{N}\setminus\{0\})^2$*. Tous les axiomes sont satisfaits, et pour* $\alpha=(1,0)$ *on a* $\mathrm{tr}(\alpha)\,I(\xi^2)=2$*, tandis que* $2\,I(D_\xi(\alpha),\xi)=4$ *et* $2\,I(\xi,D_\xi(\alpha))=0$.

Démonstration. $I(u^2x,u^2y)=u_1^2u_2^2\,x_1y_2$, I est >0 sur $(N^>)^2$, $(1,1)$ et $(1,2)$ engendrent $\mathbf{Z}^2$, $x\cdot(x_2,x_1)=x_1x_2(1,1)$, et u^* préserve les deux cônes. Ici $\nu(\alpha+n)=(1+n)^2n^2=n^4+2n^3+n^2$, donc $\mathrm{tr}(\alpha)=2$, et $D_\xi(\alpha)=(4,1)-(1,0)-(1,1)=(2,0)$. □

L'axiome (e) dit seulement I r-linéaire. Dans ce modèle, la formule échoue que $D_\xi(\alpha)$ soit placé en premier ou en second.

Contre-exemple 17.3 (Contre-exemple de l'édition, le Corollaire de la page 6)**.** *Soient $E = \mathbf{H}[\mathbf{Z}, 0, 0, 0]$, l'algèbre de quaternions où $i^2 = j^2 = 0$, munie de sa conjugaison, $N = \mathbf{Z}$, $\psi(x) = x$, $\alpha^* x = (\operatorname{re}\alpha)^2 x$, $\xi = 1$, $r = 1$, $I(x) = x$, $\nu(\alpha) = (\operatorname{re}\alpha)^2$, $N^+ = \mathbf{N}$, $N^> = \mathbf{N} \setminus \{0\}$. Tous les axiomes sont satisfaits, ainsi que $I(\xi^{r-1}, \eta) > 0$ pour tout $\eta \in N^+$ non nul, mais $i \neq 0$ et $\operatorname{tr}(i'i) = 0$.*

Démonstration. $\alpha' x \alpha = x\,\alpha'\alpha = (\operatorname{re}\alpha)^2 x$, car $\alpha'\alpha = (\operatorname{re}\alpha)^2$ quand $i^2 = j^2 = 0$. Comme $i'i = -i^2 = 0$, $\nu(i'i + n) = n^2$ et $\operatorname{tr}(i'i) = 0$. □

La lecture déduit le Corollaire de ce que $\alpha^*\xi$ est dans le cône positif ; ici $i^*\xi = 0$. La piste proposait d'ajouter la positivité de I sur N^+. Elle tient dans ce modèle, et le Corollaire y est faux.

Énoncé (Énoncé de l'édition, le Corollaire sous deux axiomes de plus)**.** *Si I est symétrique, si $I(\xi^{r-1}, \eta) > 0$ pour tout $\eta \in N^+$ non nul et si $\alpha^*\xi \neq 0$ pour tout $\alpha \neq 0$, alors $\operatorname{tr}(\alpha'\alpha) > 0$ pour tout $\alpha \neq 0$.*

Voir `tr_star_mul_self_pos` : $\alpha^*\xi \in N^+$ est non nul, et $I(\xi^r) > 0$.

Ne sont pas démontrés ici : la catégorie elle-même et la Propriété fondamentale 1 sur les produits, qui n'est « purement formelle » que si N contient tous les éléments antisymétriques ; la première moitié du dossier (pages 2 et 4).

18 Cote 63 : les quatre composantes de $j = 0$ ont quatre tangentes en $p = 2$ [19]

La cote 63, *Formulaire courbes elliptiques*, rassemble des textes d'autres auteurs (la lettre de Tate à Cassels, le formulaire de Deligne d'après Tate, des tapuscrits d'Atkin) et des notes de Grothendieck ; la carte la date de 1967. Aux pages 95 à 99, il étudie le schéma M_3 des courbes elliptiques munies d'une base de leurs points d'ordre 3, au-dessus de $\mathbf{Z}[\frac{1}{3}]$, et le lieu $j = 0$, c'est-à-dire $M_3' = M_3 \cap V(c_4)$. Ce lieu a quatre composantes irréductibles, qui se rencontrent toutes en un point a au-dessus de $\mathbf{F}_4$, en caractéristique 2. La page 97 pose la question : « À examiner si les 4 composantes de $(M_3')_2$ ont « tangentes distinctes » » (63, lot 5, p. 97). La page 99 commence par « … aux composantes irréductibles sont égales » et affirme que l'espace tangent de Zariski en a se scinde en $V_1 \times V_2$, stable sous le groupe $G' = \mathrm{SL}(2, \mathbf{F}_3)$ (63, lot 5, p. 99). La lecture en conclut, par un argument d'orbites, que les quatre branches ont la même tangente. Elles en ont quatre.

Le modèle. On travaille sur la famille de Hesse $x^3 + y^3 + z^3 = 3t\,xyz$, de paramètre t, qui est le niveau 3 au-dessus de $\mathbf{Z}[\frac{1}{3}, \zeta]$, ζ racine primitive cubique de l'unité. Pour cette famille, c_4 vaut $t(t^3 + 8)$ à une unité près (Artebani et Dolgachev) ; ce calcul et l'identification de la famille de Hesse à M_3 sont admis ici. Soient $R = \mathbf{Z}[\zeta]$, l'anneau $A = R[t]$, et l'idéal maximal $P = (2, t)$ du point a, de corps résiduel $A/P = R/2R = \mathbf{F}_4$. L'espace cotangent en a est P/P^2, un $\mathbf{F}_4$-espace vectoriel de base les classes de 2 et de t. La tangente d'une branche lisse $f = 0$ passant par a est la droite de P/P^2 engendrée par la classe de f.

19. Preuve vérifiée : `lean/Grothendieck/Folder63.lean`.

Contre-exemple 18.1 (Énoncé de l'édition, pages 97 à 99)**.** *Dans $R[t]$, $t^3+8=(t+2)(t+2\zeta)(t+2\zeta^2)$, de sorte que $V(c_4)$ est formé des quatre branches $t=0$, $t=-2$, $t=-2\zeta$, $t=-2\zeta^2$, toutes dans P. Pour deux branches distinctes f et g de cette liste et tous $a,b\in R[t]$, si $af+bg\in P^2$, alors $a\in P$ et $b\in P$: les quatre tangentes sont deux à deux distinctes. L'involution de Hesse $t\mapsto(t+2)/(t-1)$ fixe a et agit sur P/P^2 par $2\mapsto 2$, $t\mapsto t+2$: c'est une transvection, qui ne respecte pas le scindage de la page 99.*

Démonstration. La factorisation se vérifie en développant : le produit vaut $t^3+2(1+\zeta+\zeta^2)t^2+4(\zeta+\zeta^2+\zeta^3)t+8\zeta^3$, et $1+\zeta+\zeta^2=0$, $\zeta^3=1$.

Un polynôme $h=\sum h_i t^i$ de $R[t]$ est dans P si et seulement si 2 divise h_0 dans R ; s'il est dans P^2, alors 4 divise h_0 et 2 divise h_1, car c'est vrai des produits de deux éléments de P et ces conditions définissent un idéal. Soient $f=t+2\alpha$ et $g=t+2\beta$ deux branches, $\alpha\neq\beta$ dans $\{0,1,\zeta,\zeta^2\}$, et $af+bg\in P^2$. Les coefficients de degré 0 et 1 de $af+bg$ sont $2(\alpha a_0+\beta b_0)$ et $a_0+b_0+2(\alpha a_1+\beta b_1)$. Le premier est divisible par 4 ; comme R est un $\mathbf{Z}$-module libre de base $1,\zeta$, on peut simplifier par 2, et 2 divise $\alpha a_0+\beta b_0$. Le second est divisible par 2, donc $b_0=2w-a_0$ pour un $w\in R$, et $(\alpha-\beta)a_0=2(u-\beta w)$ si $\alpha a_0+\beta b_0=2u$. Or chaque différence $\alpha-\beta$ est inversible modulo 2 : $(-1)(-1)=1$, $(-\zeta)(-\zeta^2)=1$, $(1-\zeta)(1-\zeta^2)=3=1+2$, et $(\zeta-\zeta^2)\,\zeta^2(1-\zeta^2)=3$. Si $(\alpha-\beta)\varepsilon=1+2m$, on obtient $a_0=2\big(\varepsilon(u-\beta w)-ma_0\big)$, donc $a\in P$, puis $b_0=2w-a_0$ est pair et $b\in P$.

Pour l'involution, $t-1$ n'est pas dans P (son terme constant -1 n'est pas pair, en comparant les coordonnées sur la base $1,\zeta$), donc inversible dans l'anneau local en a, et $(t+2)-(t-1)(t+2)=4-t^2\in P^2$: modulo P^2, l'image $(t+2)/(t-1)$ de t est $t+2$. Le nombre 2 est fixe. □

Remarque. L'argument de la page 99 suppose que G' respecte le scindage $V_1\times V_2$ de l'espace tangent, V_1 vertical et V_2 horizontal, et qu'il agit trivialement sur V_2. L'involution de Hesse, qui provient du groupe $Q_8\subset G'$, envoie la direction horizontale t sur $t+2$: elle ne respecte pas le scindage, et les quatre droites non verticales de P/P^2 forment une seule orbite de quatre éléments au lieu d'être fixées. La multiplicité 4 du point et la non-régularité de M' en $p=2$ (page 95) ne sont pas en cause.

Ne sont pas démontrés ici : l'identification de la famille de Hesse au schéma M_3 et la formule de c_4, admises ; la structure de $M_3[\frac{1}{6}]\cap V(c_4)$ de la page 98 ; les notes des pages 65 à 76 sur les périodes et les deux décompositions de H^1_{dR}.

19 Cote 100 : un point de dimension un hors d'une famille dénombrable de diviseurs [20]

La cote 100, *Bonne réduction des variétés abéliennes via bonne réduction de Barsotti–Tate $T_p(A)$ (base quelconque)*, cinquante-deux pages que l'inventaire date « [à partir de 1967-1968] », mêle des notes manuscrites et la copie annotée d'un tapuscrit. Pour algébriser un schéma abélien formel, les pages 30 à 38 ont besoin d'un lemme d'algèbre commutative : dans le spectre d'un anneau local noethérien complet intègre, une famille dénombrable de fermés rares laisse échapper un point x avec $\dim\overline{\{x\}}=1$ (corollaire de la page 38, 100, lot 2, p. 38). La page le démontre en passant à $\Theta=V[[T_1,\dots,T_n]]$, V anneau de valuation discrète complet. Un V-homomorphisme $\varphi:\Theta\to V$ est déterminé par les images des T_i, qui sont des éléments

20. Preuve vérifiée : `lean/Grothendieck/Folder100.lean`.

arbitraires de l'idéal maximal $\mathfrak{m}$; son noyau est un point de dimension un. Chaque fermé rare, contenu dans un $V(f)$ avec $f \neq 0$, exclut les φ tels que $f(\varphi(T_1), \ldots, \varphi(T_n)) = 0$, partie fermée rare de l'espace métrique complet $\mathfrak{m}^n$, et le théorème de Baire conclut.

On démontre ici le cas $n = 1$, celui de $\Theta = V[[T]]$, anneau de dimension 2. Les homomorphismes $\Theta \to V$ sont alors les $\varphi_a : T \mapsto a$, $a \in \mathfrak{m}$, de noyau l'idéal $(T - a)$. Dans ce cas l'argument de Baire peut être remplacé par un dénombrement : chaque série $f \neq 0$ n'exclut qu'un nombre fini de valeurs de a, tandis que $\mathfrak{m}$ n'est pas dénombrable.
Conventions. V est un anneau de valuation discrète, complet pour la topologie $\mathfrak{m}$-adique, d'uniformisante ϖ ; $V[[T]]$ est l'anneau des séries formelles. Dire qu'un point de dimension un, le noyau de φ_a, est hors de $V(f)$ revient à dire que f n'appartient pas à l'idéal $(T - a)$.

Théorème 19.1 (énoncé de l'édition, cas $n = 1$ du corollaire de la page 38 ♦)**.** *Soit V un anneau de valuation discrète complet. Pour $a \in \mathfrak{m}$, l'anneau $V[[T]]/(T - a)$ est isomorphe à V. Pour toute famille dénombrable (f_i) de séries non nulles de $V[[T]]$, il existe $a \in \mathfrak{m}$ tel qu'aucune f_i n'appartienne à $(T - a)$.*

Démonstration. Le polynôme $T - a$ est unitaire et son terme constant $-a$ est dans $\mathfrak{m}$: il est distingué au sens de Weierstrass. La division de Weierstrass identifie alors $V[[T]]/(T - a)$ à $V[T]/(T - a)$, qui est V par $P \mapsto P(a)$, et un polynôme P est dans l'idéal $(T - a)$ de $V[[T]]$ si et seulement si $P(a) = 0$.

Soit $f \neq 0$. Le plus petit v tel que ϖ^{v+1} ne divise pas tous les coefficients de f existe, et $f = \varpi^v g$ où g a un coefficient inversible, c'est-à-dire que l'image de g dans $k[[T]]$, k le corps résiduel, n'est pas nulle. Le théorème de préparation de Weierstrass écrit $g = Pu$, avec P polynôme distingué et u inversible. Donc $f = Qu$, où $Q = \varpi^v P$ est un polynôme non nul, et $f \in (T - a)$ si et seulement si $Q(a) = 0$: seules les racines de Q, en nombre fini, sont exclues.

Il reste à voir que $\mathfrak{m}$ n'est pas dénombrable ; comme $a \mapsto \varpi a$ est une injection de V dans $\mathfrak{m}$, il suffit que V ne le soit pas. À toute suite $\varepsilon \in \{0, 1\}^{\mathbf{N}}$, la complétude associe une limite L_ε des sommes partielles $\sum_{i<n} \varepsilon_i \varpi^i$, congrue à la n-ième modulo ϖ^n. Si ε et ε' diffèrent pour la première fois en j, les sommes partielles d'indice $j + 1$ diffèrent de $\pm\varpi^j$, et $L_\varepsilon = L_{\varepsilon'}$ forcerait $\varpi^{j+1} \mid \varpi^j$, ce qui est impossible. L'ensemble des $a \in \mathfrak{m}$ exclus par l'une des f_i est une réunion dénombrable d'ensembles finis, donc dénombrable, et il ne peut pas contenir $\mathfrak{m}$. □

Le dénombrement ne remplace Baire qu'en une variable. Pour $n \geq 2$, une série non nulle exclut en général une infinité non dénombrable de points de $\mathfrak{m}^n$, par exemple tout l'hyperplan $T_1 = 0$ pour $f = T_1$, et il faut l'argument de la page : une série non nulle ne s'annule identiquement sur aucun ouvert de $\mathfrak{m}^n$. Le théorème ne suppose rien sur le corps résiduel, qui peut être fini, comme pour $V = \mathbf{Z}_p$: la non-dénombrabilité de V vient de la complétude seule. Vérifié tel quel (`quotEquiv`, `exists_poly_mul_unit`, `finite_bad`, `uncountable`, `exists_avoid`), avec le théorème de préparation de Weierstrass et l'isomorphisme $V[T]/(g) \simeq V[[T]]/(g)$ de mathlib pour un polynôme distingué g.

Théorème 19.2 (Pages 36 à 38, forme corrigée par l'édition, points de dimension un ♦)**.** *Soit R un anneau local noethérien complet, d'idéal maximal $\mathfrak{m}$.*

1. *(Proposition, page 36.) Dans $\operatorname{Spec} R$, une famille dénombrable de fermés dont la réunion contient tous les points x tels que $\dim \overline{\{x\}} \leq 1$ a une sous-famille finie qui recouvre le spectre.*
2. *(Corollaire, page 38.) Si R est intègre et n'est pas un corps, une famille dénombrable de*

fermés rares de $\operatorname{Spec} R$ *laisse échapper un point* x *tel que* $\dim \overline{\{x\}} = 1$.

La page barre « complet », que l'édition rétablit : sans cette hypothèse l'énoncé est faux. Les feuillets démontrent le cas de dimension ≤ 1 et le corollaire, par Cohen et une propriété de Baire sur les $\mathfrak{m}^n$; le cas général de la proposition s'interrompt page 36 sur des lignes illisibles et annulées, et le passage du corollaire à la proposition n'est pas écrit. Le cas d'une variable de l'argument de la page est le théorème 19.1.

Conventions. Un point x de $\operatorname{Spec} R$ est un idéal premier $\mathfrak{p}$, et $\overline{\{x\}} = V(\mathfrak{p}) \simeq \operatorname{Spec} R/\mathfrak{p}$: la dimension de $\overline{\{x\}}$ est la longueur maximale d'une chaîne de premiers commençant en $\mathfrak{p}$, que Lean appelle la cohauteur de x dans l'ensemble ordonné $\operatorname{Spec} R$. Elle est finie, R étant local noethérien. Dans $\operatorname{Spec} R$ intègre, irréductible, un fermé est rare si et seulement s'il est propre, et c'est sous cette forme, un peu plus générale, que Lean énonce le corollaire.

Lemme 19.3 (dimension de l'adhérence d'un point)**.** *Pour tout anneau commutatif* A *et tout point* x *de* $\operatorname{Spec} A$*, la dimension topologique de* $\overline{\{x\}}$*, longueur maximale d'une chaîne de fermés irréductibles de cet espace, est la cohauteur de* x *dans* $\operatorname{Spec} A$*, et vaut* $\dim A/\mathfrak{p}$.

Démonstration. On a $\overline{\{x\}} = V(\mathfrak{p})$, et l'application $\operatorname{Spec} A/\mathfrak{p} \to \operatorname{Spec} A$ induite par la surjection $A \to A/\mathfrak{p}$ est un plongement fermé d'image $V(\mathfrak{p})$: c'est un homéomorphisme sur $\overline{\{x\}}$, qui a donc la dimension de $\operatorname{Spec} A/\mathfrak{p}$, soit $\dim A/\mathfrak{p}$. Les premiers de $A/\mathfrak{p}$ sont, dans l'ordre, ceux de A qui contiennent $\mathfrak{p}$, et la dimension de l'ensemble ordonné des $y \geq x$ est la cohauteur de x. □

La démonstration ne passe ni par le théorème de structure de Cohen ni par Baire sur $\mathfrak{m}^n$. La complétude n'intervient qu'une fois, par le lemme suivant, connu sous le nom d'évitement dénombrable des idéaux premiers (on l'attribue à Burch ; voir aussi Sharp et Vámos, 1985).

Lemme 19.4 (évitement dénombrable)**.** *Si* R *est local noethérien complet,* $\mathfrak{m}$ *n'est pas contenu dans la réunion d'une famille dénombrable* $(\mathfrak{p}_j)_{j\in\mathbf{N}}$ *d'idéaux premiers distincts de* $\mathfrak{m}$.

Démonstration. On construit par récurrence des $x_k \in R$ et des entiers $N_0 < N_1 < \cdots$, avec $x_0 = 0$, $N_0 = 1$, tels que $x_k \notin \mathfrak{p}_j + \mathfrak{m}^{N_k}$ pour tout $j < k$ et $x_{k+1} - x_k \in \mathfrak{m}^{N_k}$. Si $x_k \notin \mathfrak{p}_k$, on garde $x' = x_k$; sinon, $\mathfrak{m}^{N_k} \not\subset \mathfrak{p}_k$ puisque $\mathfrak{p}_k$ est premier et ne contient pas $\mathfrak{m}$, et l'on pose $x' = x_k + y$ avec $y \in \mathfrak{m}^{N_k} \setminus \mathfrak{p}_k$. Dans les deux cas $x' \notin \mathfrak{p}_k$. Le théorème d'intersection de Krull dans l'anneau local noethérien $R/\mathfrak{p}_k$, où $\bigcap_N \mathfrak{m}^N = 0$, donne un M tel que $x' \notin \mathfrak{p}_k + \mathfrak{m}^M$: les premiers sont fermés pour la topologie $\mathfrak{m}$-adique. On pose $x_{k+1} = x'$ et $N_{k+1} = \max(N_k + 1, M)$; les conditions pour $j < k$ subsistent, puisque $x_{k+1} \equiv x_k \pmod{\mathfrak{m}^{N_k}}$.

La suite (x_k) est de Cauchy, avec $x_n - x_k \in \mathfrak{m}^{N_k}$ pour $n \geq k$; comme R est complet, elle a une limite L, et $L - x_k \in \mathfrak{m}^{N_k}$ pour tout k. En particulier $L \in x_0 + \mathfrak{m} = \mathfrak{m}$, et si L était dans $\mathfrak{p}_j$, alors $x_{j+1} = L - (L - x_{j+1})$ serait dans $\mathfrak{p}_j + \mathfrak{m}^{N_{j+1}}$, ce que la construction exclut. C'est l'argument de Baire, rendu explicite sur l'espace complet $\mathfrak{m}$. □

Démonstration du théorème. Écrivons $Z_i = V(I_i)$, avec I_i l'idéal des fonctions nulles sur Z_i : un point $\mathfrak{q}$ est dans Z_i si et seulement si $I_i \subset \mathfrak{q}$.

Montée. Soient $\mathfrak{p}$ un premier ne contenant aucun I_i, et une chaîne $\mathfrak{p} \subsetneq \mathfrak{a} \subsetneq \mathfrak{b}$ de premiers (c'est dire que $\dim \overline{\{\mathfrak{p}\}} \geq 2$). Alors il existe un premier $\mathfrak{q} \supsetneq \mathfrak{p}$ qui ne contient aucun I_i. Supposons le contraire, et soit S l'ensemble des premiers distincts de $\mathfrak{m}$ minimaux sur l'un des $\mathfrak{p} + I_i$: chaque $\mathfrak{p} + I_i$ n'a qu'un nombre fini de premiers minimaux, et S est dénombrable. Le lemme 19.4 donne $x \in \mathfrak{m}$ hors de tous les premiers de S. Si $x \in \mathfrak{p}$, comme $\mathfrak{a}$ contient un I_i, un premier minimal sur $\mathfrak{p} + I_i$ contenu dans $\mathfrak{a}$ est dans S et contient x. Si $x \notin \mathfrak{p}$, soit $\mathfrak{q}$ un premier minimal

sur $\mathfrak{p}+(x)$. Le théorème de l'idéal principal de Krull, appliqué dans $R/\mathfrak{p}$, dit qu'il n'y a pas de chaîne $\mathfrak{p} \subsetneq \mathfrak{c} \subsetneq \mathfrak{q}$; en particulier $\mathfrak{q} \neq \mathfrak{m}$, à cause de la chaîne $\mathfrak{p} \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}$. Par hypothèse $\mathfrak{q}$ contient un I_i, donc un premier $\mathfrak{q}'$ minimal sur $\mathfrak{p}+I_i$; $\mathfrak{q}' \neq \mathfrak{p}$ puisque $I_i \not\subset \mathfrak{p}$, et donc $\mathfrak{q}'=\mathfrak{q}$. Ainsi $\mathfrak{q} \in S$ et $x \in \mathfrak{q}$. Les deux cas contredisent le choix de x.

Proposition. Supposons qu'aucune sous-famille finie ne recouvre le spectre. Les premiers minimaux de R sont en nombre fini et tout point en spécialise un ; si chacun était dans un Z_i, ces Z_i, fermés, recouvriraient le spectre. Il existe donc un premier minimal $\mathfrak{p}$ hors de tous les Z_i. Tant que $\dim \overline{\{\mathfrak{p}\}} \geq 2$, la montée remplace $\mathfrak{p}$ par un $\mathfrak{q} \supsetneq \mathfrak{p}$ hors de tous les Z_i, et $\dim \overline{\{\mathfrak{q}\}} < \dim \overline{\{\mathfrak{p}\}}$. On aboutit à un point de dimension ≤ 1 hors de la réunion des Z_i, contre l'hypothèse.

Corollaire. On ajoute à la famille le fermé $\{\mathfrak{m}\}$. Le point générique (0) n'est dans aucun Z_i, puisqu'un fermé qui le contient est le spectre entier, ni égal à $\mathfrak{m}$, puisque R n'est pas un corps : aucune sous-famille finie ne recouvre le spectre. La proposition donne un point x de dimension ≤ 1 hors des Z_i et distinct de $\mathfrak{m}$, le seul point de dimension 0 : $\dim \overline{\{x\}} = 1$. □

La complétude n'est utilisée que par le lemme 19.4, et c'est là qu'elle est nécessaire : pour l'anneau local de $\mathbf{Q}[x,y]$ à l'origine, qui n'a qu'un ensemble dénombrable d'idéaux premiers, $\mathfrak{m}$ est la réunion des premiers de hauteur un. Le nombre de variables $\dim S$ ou $\dim S - 1$ que la page donne à $V[[T_1,\dots,T_n]]$ n'intervient plus.

Portée de la vérification. Lean démontre ces énoncés dans `Folder100.lean`, espace `Baire` : `exists_notMem_sup_pow` pour la fermeture des premiers, `exists_mem_maximalIdeal_forall_notMem` et `exists_mem_maximalIdeal_notMem_of_countable` pour le lemme 19.4, `not_chain_of_mem_minimalPrimes` pour le théorème de l'idéal principal au-dessus de $\mathfrak{p}$, `exists_isPrime_gt` pour la montée, `exists_coheight_le_one` pour la descente sur la dimension, `exists_finite_subcover` et `exists_finite_subcover_of_countable` pour la proposition, `exists_coheight_eq_one` pour le corollaire. La dimension de $\overline{\{x\}}$ y est la cohauteur de x dans $\operatorname{Spec} R$; le lemme 19.3, qui l'identifie à la dimension topologique de l'adhérence, est `topologicalKrullDim_closure_singleton` (par `PrimeSpectrum.closure_singleton`, `PrimeSpectrum.topologicalKrullDim_eq_ringKrullDim`, `ringKrullDim_quotient` et `Order.coheight_eq_krullDim_Ici`), et le corollaire sous sa forme littérale, avec $\dim \overline{\{x\}}$ dimension topologique, est `exists_topologicalKrullDim_closure_eq_one`. La voie de la page, par Cohen et Baire sur $\mathfrak{m}^n$, n'est pas formalisée au-delà d'une variable, et l'application à l'algébrisation des schémas abéliens formels reste hors de portée.

Ne sont pas démontrés ici, pour la voie de la page : le cas de plusieurs variables, où Baire est nécessaire ; la réduction d'un anneau local complet intègre à une extension finie de $V[[T_1,\dots,T_n]]$ (théorème de structure de Cohen) et la remontée des points de dimension un le long de cette extension. La proposition de la page 36 et le corollaire de la page 38 en toute dimension sont démontrés ci-dessus par une autre voie (théorème 19.2). Les autres pistes de la cote restent ouvertes :

Théorème (Grothendieck, pages 2, 3 et 20, pleine fidélité et composantes connexes ♦). *Soient S un schéma localement noethérien et $U \subset S$ un ouvert tel que toutes les caractéristiques résiduelles de $S-U$ soient égales à p. Le foncteur $A \mapsto (A_U, A[p^\infty], \mathrm{id})$ des schémas abéliens sur S vers les triplets est pleinement fidèle dès que U rencontre chaque composante connexe de S, sans hypothèse de normalité, de réduction ni de densité schématique.*

♢ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (page 3). Le lemme d'existence de S_v y renvoie à « Invariants 1.2 ». Mathlib n'a pas les schémas abéliens ni les groupes p-divisibles. On se

reportera aux notes de Grothendieck (100, lot 1, p. 2).

Théorème (Grothendieck, pages 22 à 24, descente des morphismes le long d'un épimorphisme propre ♦). *Soit $f : S' \to S$ un morphisme propre de schémas localement noethériens tel que $\mathcal{O}_S \to f_*\mathcal{O}_{S'}$ soit injectif, sans hypothèse de platitude, et soit $S'' = S' \times_S S'$. Pour tout S-schéma X formellement non ramifié, la suite $\mathrm{Hom}_S(S, X) \to \mathrm{Hom}_S(S', X) \rightrightarrows \mathrm{Hom}_S(S'', X)$ est exacte ; le changement de base le long de f est donc pleinement fidèle sur les schémas abéliens.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 22 et 24) : le lemme 1 se ramène, par l'algèbre $\mathrm{Ker}(f_*\mathcal{O}_{S'} \rightrightarrows h_*\mathcal{O}_{S''})$, au cas d'un épimorphisme fini et radiciel, le corollaire 1, dont la page 24 donne la réduction au cas local, l'image schématique et la finitude de $\mathcal{O}_{X,x}$ sur $\mathcal{O}_{S,s}$. La fin du corollaire 1 (non-ramification, Nakayama) et la radicialité de la réduction sont de l'édition, comme la représentabilité et la non-ramification du schéma des homomorphismes de schémas abéliens. Mathlib n'a pas la descente des morphismes le long d'un morphisme propre. On se reportera aux notes de Grothendieck (100, lot 2, p. 22).

Théorème (Grothendieck, pages 30 à 38, algébrisation par les courbes ♦). *Soit R un anneau local noethérien complet. Un schéma abélien formel sur $\mathrm{Spf}\, R$ est algébrisable si et seulement si son changement de base à $\mathrm{Spf}\, B'$ l'est pour tout quotient intègre B de dimension un de R, de normalisé B', ou encore s'il le devient après un morphisme propre surjectif $S' \to \mathrm{Spec}\, R$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 32 à 38). Mathlib n'a pas l'algébrisation des schémas formels. On se reportera aux notes de Grothendieck (100, lot 2, p. 30).

Théorème (Grothendieck, pages 47 à 52, prolongement vers un modèle de Néron ♦). *Sur un trait S, pour tout modèle de Néron G et tout groupe p-divisible M sur S, tout homomorphisme $M_K \to G_K$ des fibres génériques se prolonge de façon unique en $M \to G$, le théorème de pleine fidélité de Tate pour les groupes p-divisibles sur S étant admis.*

◊ non vérifié en Lean

La conclusion repose sur le théorème de Tate, et le cas où G_K est extension d'une variété abélienne par un tore est traité dans le tapuscrit des pages 47 à 50, dont l'auteur n'est pas établi ; la part des feuillets manuscrits est le lemme des pages 51 et 52. Les feuillets en esquissent une démonstration incomplète : ce lemme renvoie deux fois à « on sait », et la page 52 l'applique au modèle de Néron et conclut « On gagne ! ».

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 93 et 94, amplitude par la caractéristique d'Euler ♦). *Un faisceau inversible L sur un schéma projectif est ample dès que $\chi(\mathcal{O}_Z \otimes L^{\otimes n}) \to +\infty$ pour tout sous-schéma fermé intègre Z de dimension ≥ 1, et de même avec $\dim H^0$ à la place de χ. La page attribue l'énoncé à Mumford et Nakai.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (page 94). Ses deux lemmes y sont renvoyés à une « lettre de Mumford ». Mathlib n'a pas la caractéristique d'Euler des faisceaux cohérents ni l'amplitude. On se reportera aux notes de Grothendieck (14, lot 5, p. 93).

Théorème (D'après les pages 1 à 22, forme corrigée par l'édition, section canonique par le déterminant ♦). *Soient X/S propre et plat, avec $\mathrm{Pic}^0_{X/S} = B$ schéma abélien de dual A, et δ une section de $\mathrm{NS}_{X/S}$. Le déterminant de la cohomologie du faisceau de Poincaré donne une trivialisation canonique du A-torseur $\mathrm{Alb}^{\chi(\delta)}_{X/S} \times^A \mathrm{Pic}^{\varphi(\delta)}_{B/S} \times^A (\widetilde{\varphi(\delta)})_*\mathrm{Pic}^{\delta}_{X/S})^{(-1)}$, où*

◊ non vérifié en Lean

$\varphi : \mathrm{NS}_{X/S} \to \mathrm{NS}_{B/S}$ *est une application polynomiale de degré* $n-1$*, non additive.*

Les feuillets en esquissent une démonstration incomplète (pages 1 à 4 et 16 à 19). La descente y est marquée « détailler », la propriété universelle de Alb^1 annoncée page 22 sans preuve, et l'inverse sur le torseur poussé est de l'édition. Mathlib n'a pas le déterminant de la cohomologie ni le faisceau de Poincaré. On se reportera aux notes de Grothendieck (59, lot 1, p. 1).

Théorème (Grothendieck, pages 39 à 48, faisceau des quasi-fonctions ♦)**.** *Les fonctions de Weil forment un faisceau de Zariski* QF_X*, somme amalgamée du faisceau* Φ_X *des fonctions admissibles et de* $\mathcal{R}_X^*$ *au-dessus de* $\mathcal{O}_X^*$*, dans une suite exacte* $0 \to \Phi_X \to QF_X \to \mathrm{Div}_X \to 0$*. Pour* X *quasi-projectif, tout diviseur de Cartier est le diviseur d'une quasi-fonction globale.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 41 à 48). La page s'arrête avant le cas de $\mathbf{P}^r$. Mathlib n'a pas les fonctions de Weil ni les diviseurs de Cartier. On se reportera aux notes de Grothendieck (130, lot 2, p. 39).

Théorème (Grothendieck, pages 22 à 28, déterminants des parties étales ♦)**.** *Pour un schéma abélien* A *ordinaire localement polarisable sur une base connexe de caractéristique* p*,* $\alpha_A = \det T_p(\tilde{\varphi})_{ét}/\sqrt{\deg \tilde{\varphi}}$ *ne dépend pas de la polarisation* φ *et est un isomorphisme de réseaux* $\det T_p(A)_{ét} \simeq \det T_p(A^*)_{ét}$*, compatible au changement de base ; pour une isogénie* u*, on a seulement* $\det T_p(u)_{ét} \cdot \det T_p(u^*)_{ét} = \deg u$*.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : définitions, énoncés a) et b) et leurs arguments sont sur les pages, mais l'identité $\Delta(u)\Delta(u^*) = \deg u$ y est introduite par une justification illisible (la page 25, qui l'attribuait à un théorème p-adique, est annulée), les points c) et d) sont laissés « à vérifier », et les hypothèses de polarisabilité locale et de base connexe sont de l'édition.

Théorème (Grothendieck, pages 24 et 26, déterminant et racine du degré ♦)**.** *Pour une variété abélienne ordinaire polarisée* A *et* $u \in \mathrm{End}(A) \otimes \mathbf{Q}$ *symétrique et positif pour l'involution de Rosati, le déterminant de* u *sur la partie étale du module de Tate* p*-adique vaut* $+\sqrt{\deg u}$*.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : la page 24 ramène l'énoncé au signe, et la page 26 l'obtient par positivité, $u = v^2$ sur le cône positif ; l'identité $\Delta(u)\Delta(u^*) = \deg u$ y repose sur une justification illisible, et la restriction de l'argument de rationalité aux éléments symétriques est de l'édition.

Théorème (Grothendieck, pages 23 à 29 et 33, équivalence d'Albanese ♦)**.** *Sur les cycles de toute codimension, posons* $z \sim 0$ *quand* $z = Z_*(t)$ *pour un cycle* Z *sur* $X \times T$*,* T *projective lisse connexe, et un* 0*-cycle* t *de degré* 0 *sur* T *tel que* $\mathrm{alb}_T(t) = 0$*. Cette relation est comprise entre les équivalences rationnelle et algébrique, passe aux produits, aux images réciproques et aux images directes propres, coïncide avec l'équivalence rationnelle sur les diviseurs et avec le degré et la somme d'Albanese sur les* 0*-cycles ; dans l'anneau quotient, le produit de deux classes algébriquement triviales est nul.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : les théorèmes 1.4 et 1.6 sont démontrés (pages 28 et 29), mais la proposition 1.2 (iii) est laissée « à vérifier » (page 27), le (iv) est fait « par l'AQT », abréviation non reconstituée, et le corollaire 2.4 (page 33) est sans démonstration.

Théorème (Grothendieck, pages 9 et 10, Riemann–Roch et transformation de Fourier sur une base ♦)**.** *Sur une base* S*, Grothendieck–Riemann–Roch pour* m_A *et* pr_2 *donne* $\mathrm{ch}(x *$

◊ non vérifié en Lean

$y) = (\mathrm{ch}\, x * \mathrm{ch}\, y) \cdot \mathrm{Todd}(t_A)$ *sur un schéma abélien* A *et, pour* $\Psi_D = \mathrm{pr}_{2*}(\mathrm{pr}_1^*(-) \cdot \exp D)$, $\Psi_D(a * b) = \Psi_D(a)\, \Psi_D(b)$ *sans correction ; la formule qui échange cup-produit et produit de Pontrjagin prend un facteur venu de* S.

La page 9 affirme $(*)$ par Riemann–Roch (« On vérifie ») sans le calcul, et la page 10 dérive la seconde formule avec le seul facteur $\mathrm{Todd}(t_A)$. Comme la seconde application de $(*)$ se fait sur B, l'édition corrige ce facteur en $\mathrm{Todd}(t_A)\,\mathrm{Todd}(t_B)\,\mathrm{ch}(\omega_A)$: c'est le facteur venu de S de l'encadré. Le théorème de Riemann–Roch de Grothendieck, appliqué ici à m_A et à pr_2, n'est vérifié en Lean nulle part dans l'annexe ; la partie « K-théorie, classes de Chern et Riemann–Roch » (section 32) n'en contrôle que quelques calculs. Les pages 3 à 7 qui précèdent établissent l'inversion de Fourier relative, $\Phi_{s_L} \circ \Phi_L \simeq s_A^*(-) \otimes \tau_A[-n]$ sur les complexes parfaits, τ_A le déterminant de l'algèbre de Lie de A : c'est le théorème 1.1 de Mukai (1987) [102], pour un schéma abélien sur une base quelconque, avec la torsion par le dual du fibré canonique relatif. Deninger et Murre (1991) [42] étudient la transformation de Fourier sur l'anneau de Chow rationnel d'un schéma abélien ; la comparaison de leurs formules avec le facteur corrigé n'a pas été faite.

Théorème (Grothendieck, pages 16, 17 et 20, bonne réduction de l'Albanese ♦). *Si* X *est projectif et plat sur un anneau de valuation discrète* V*, à fibres lisses hors d'un fermé de codimension* ≥ 2*, de fibre générique géométriquement intègre et normale,* $\mathrm{Alb}(X_K)$ *et* $(\mathrm{Pic}^0_{X_K})_{\mathrm{red}}$ *ont bonne réduction.*

◊ non vérifié en Lean

L'hypothèse que la fibre générique est normale est de l'édition. Les feuillets en esquissent une démonstration incomplète : une courbe C lisse sur V qui engendre la variété abélienne, puis Koizumi–Shimura ; l'existence de C et le fait qu'elle engendre sont affirmés (« on sait ») sans démonstration.

Théorème (Grothendieck, pages 98 et 99, section hyperplane générique ♦). *Soient* $X \subset \mathbf{P}^r$ *normal intègre de dimension* ≥ 2 *sur un corps algébriquement clos et* $Y_{\bar{K}}$ *sa section hyperplane générique sur la clôture algébrique de* $k(t_1, \ldots, t_r)$*. Alors* $H^1(X, G) \to H^1(Y_{\bar{K}}, G)$ *est injectif pour* $G = \mathbf{G}_a$ *et pour* G *fini commutatif,* μ_p *et* α_p *compris ; le noyau de* $\mathrm{Pic}^\tau_{X_{\bar{K}}} \to \mathrm{Pic}^\tau_{Y_{\bar{K}}}$ *est un* p*-groupe unipotent fini.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : la page 98 ramène le théorème aux corollaires 1 à 4, et la page 99 plonge $H^1(X, \alpha_p)$ et $\mathrm{Pic}(X)[p]$ dans $H^0(X, \tilde{\Omega}^1)$ par Cartier ; l'injectivité de la restriction sur $H^0(\tilde{\Omega}^1)$, dite « presque triviale », n'est pas faite, et le corollaire 1 n'est pas achevé.

Théorème (Grothendieck, pages 226 à 228 et 247 à 271, Picard analytique et complété ♦). *Soient* $f : X \to Y$ *un morphisme propre d'espaces analytiques complexes et* $y \in Y$*. L'application* $(R^1 f_* \mathcal{O}_X^*)_y \to \varprojlim \mathrm{Pic}(X_n)$ *est un isomorphisme si et seulement si* $(R^1 f_* \mathcal{O}_X)_y$ *est de longueur finie ; le système* $(\mathrm{Pic}(X_n))$ *est de Mittag-Leffler ;* X *est projectif au voisinage de* y *si et seulement si tous les* X_n *sont projectifs.*

◊ non vérifié en Lean

Démonstration de la page (pages 226 à 228 et 247 à 261). La lettre à Hironaka du 6 juillet 1962 (pp. 226–228) énonce le théorème et en annonce la démonstration par les théorèmes de Grauert et la suite exponentielle ; le brouillon la donne. Par Grauert (lemme 1.3), $(H^i(X_n, \mathcal{O}_{X_n}))_n$ est de Mittag-Leffler, de limite $(R^i f_* \mathcal{O}_X)^\wedge_y$; la suite exponentielle, où $H^i(X_n, \mathbf{Z}) = H^i(X_0, \mathbf{Z})$ est de type fini, en tire la même condition pour $(H^i(X_n, \mathcal{O}_{X_n}^*))_n$ et une suite exacte (proposition 1.5). Le lemme des cinq, qui compare celle-ci à la suite des tiges, rend la flèche de $(R^i f_* \mathcal{O}_X^*)_y$ vers la limite injective, et bijective si et seulement si $(R^i f_* \mathcal{O}_X)_y$ est de longueur finie : c'est le théorème pour $i = 1$ (remarque 1.7, et corollaire 1.8 pour la projectivité).

◊ non vérifiée en Lean

Exemple (Grothendieck, pages 11 à 13, torseur de Picard en dimension 2 ♦). Pour un schéma abélien A/S de dimension relative 2 et une section δ de $\mathrm{NS}_{A/S}$ avec $\chi(\delta)$ pair, le torseur $\mathrm{Pic}^{\delta}_{A/S}$ sous le dual est trivial.

◊ non vérifié en Lean

La page le donne en exemple d'un calcul (« Exemple », page 13). Les feuillets en esquissent une démonstration incomplète : la page 13 déduit la trivialité des puissances $\chi^{n-2}(\chi-1)$ et $2\chi^{n-2}$ du torseur, et conclut pour $n=2$ sur un « si » de lecture incertaine ; les compatibilités des trivialisations que les marges demandent ne sont pas démontrées.

Conjecture (Grothendieck, pages 7 et 8, intégralité sur une variété abélienne ♦). *Sur une variété abélienne, pour un fibré en droites L de classe de Néron–Severi δ avec $\chi=\chi(\delta)\neq 0$ et δ' la classe déterminée par $\det\Phi_L(L)$, les classes $\binom{\chi}{k}\delta'^k/\chi^m$ sont entières, comme conséquences de $c(\Phi_L(\mathrm{cl}\,L))=(1-D'/\chi)^{\chi}$.*

La lecture prend $m=k$, que la ligne du caractère de Chern de la page impose, et en donne une démonstration sur un corps algébriquement clos par l'image réciproque le long de l'isogénie φ_L, injective sur l'anneau de Chow rationnel ; l'exposant $m=k-2$ de la page donne un énoncé plus faible, vrai si celui de la lecture l'est. Cette démonstration est de l'édition et n'est pas vérifiée en Lean ; l'argument surchargé de φ_L reste à relire sur le fac-similé. Mathlib n'a pas les classes de Chern sur les variétés abéliennes. On se reportera aux notes de Grothendieck (47, lot 1, p. 7).

Théorème (D'après la page 3, forme reconstituée par l'édition, critère de platitude ♦). *Soient S localement noethérien, $\varphi : X\to Y$ un morphisme de S-schémas de type fini, F quasi-cohérent sur X et plat sur S, G cohérent sur Y et $G\to\varphi_*F$. Si $G\to\varphi_*F$ est injectif sur la fibre en s aux points au-dessus de y, G est plat sur S en y.*

◊ non vérifié en Lean

L'édition retient la forme barrée de la clause c), la clause conservée étant coupée par un mot illisible. Mathlib n'a pas la platitude des faisceaux cohérents sur les schémas. On se reportera aux notes de Grothendieck (49, lot 1, p. 3).

Théorème (Grothendieck, pages 42 à 49, rigidité des sous-groupes ♦). *Soient S localement noethérien connexe et G un schéma en groupes de type fini sur S. Deux sous-schémas en groupes fermés « rigides » de G, c'est-à-dire commutatifs, plats, et dont chaque fibre géométrique est l'adhérence schématique de sa torsion d'ordre premier à la caractéristique résiduelle, qui coïncident sur une fibre, sont égaux.*

◊ non vérifié en Lean

Mathlib n'a pas les schémas en groupes sur une base noethérienne. On se reportera aux notes de Grothendieck (57, lot 3, p. 42).

Théorème (Grothendieck, pages 3 à 5, symbole local de Néron ♦). *Pour une variété abélienne A sur le corps des fractions K d'un anneau de valuation discrète, le symbole local de Néron $(X,a)_v$ est la somme d'un nombre d'intersection $i(\bar X,\bar a)$ sur le modèle de Néron et d'une correction $v(X,a)$ caractérisée par quatre axiomes (bilinéarité, invariance par translation, normalisation par la partie verticale de $\operatorname{div}\bar f$, bornitude), avec $m\,v(X,a)\in\mathbf{Z}$ pour m l'ordre du groupe des composantes ; d'où un accouplement $A^\vee(K)\times A(K)\to\mathbf{Z}/m\mathbf{Z}$.*

◊ non vérifié en Lean

Mathlib n'a pas les modèles de Néron ni les symboles locaux. On se reportera aux notes de Grothendieck (130, lot 1, p. 3).

Partie 12

Catégories tensorielles et dualité tannakienne

20 Cote 155 : le produit de Takeuchi comme quotient d'un idéalisateur [21]

La cote 155 porte sur les catégories tannakiennes dont le foncteur fibre n'existe que sur une extension k' du corps de base k. La page 1 traduit une telle catégorie en une algèbre A sur laquelle k' agit de deux façons, et demande que la comultiplication de A soit un morphisme d'anneaux (155, lot 1, p. 1). Elle l'écrit d'abord à valeurs dans $A \hat{\otimes}_{k'} A$, puis se corrige : les valeurs sont dans $\tilde{\mathcal{J}}/\mathcal{J}$, où $J = \mathrm{Ker}(k' \otimes_k k' \to k')$, $\mathcal{J} = J \cdot (A \hat{\otimes}_k A)$ et $\tilde{\mathcal{J}} = \{\lambda \mid \lambda\mathcal{J} \subset \mathcal{J}\}$.

La correction est nécessaire : quand k' n'est pas central dans A, le produit $(a \otimes b)(c \otimes d) = ac \otimes bd$ n'est pas bien défini sur $A \otimes_{k'} A$: on peut faire passer un scalaire d'un facteur à l'autre avant de multiplier, et le résultat change. Le quotient $(A \otimes_k A)/\mathcal{J}$ est seulement un groupe abélien. On garde les éléments λ qui préservent $\mathcal{J}$ par multiplication à gauche ; sur eux, le produit passe au quotient. La lecture reconnaît là le produit de Takeuchi $A \times_{k'} A$, formé des $\sum a_i \otimes b_i$ tels que $\sum a_i x \otimes b_i = \sum a_i \otimes b_i x$ pour tout $x \in k'$. La piste note que la littérature lue ne présente pas ce produit comme un quotient d'idéalisateur.

Conventions. On travaille sans complétion. k est un anneau commutatif, K une k-algèbre commutative (le k' de la page), A un anneau muni d'un morphisme de k-algèbres $\iota : K \to A$ dont l'image n'est pas supposée centrale, et A est un K-module par $x \cdot a = \iota(x)a$. Pour un sous-groupe L d'un anneau S, on note $\mathbb{I}(L) = \{\lambda \in S \mid \lambda L \subset L\}$ son idéalisateur.

Énoncé (Énoncé de l'édition, l'idéalisateur)**.** *Si L est un idéal à droite de S, $\mathbb{I}(L)$ est un sous-anneau de S qui contient L, L y est un idéal bilatère, et $\mathbb{I}(L)/L$ est un anneau. C'est le plus grand sous-anneau de S où L est un idéal bilatère.*

Voir `idealiser`, `ringCon` et `le_idealiser_of`. La seule vérification est $ac - bd = a(c-d) + (a-b)d \in L$ pour $a, b \in \mathbb{I}(L)$, $a - b$ et $c - d$ dans L.

Théorème 20.1 (D'après la page 1, sans complétion ♦)**.** *Soit $S = A \otimes_k A$ et $\mathcal{J}$ l'idéal à droite engendré par les $\iota(x) \otimes 1 - 1 \otimes \iota(x)$, $x \in K$; c'est $J \cdot S$, pour J le noyau de la multiplication $K \otimes_k K \to K$. L'application $a \otimes b \mapsto a \otimes b$ de S vers $A \otimes_K A$ est surjective, de noyau $\mathcal{J}$. Un élément λ de S est dans $\tilde{\mathcal{J}}$ si et seulement si son image $\sum a_i \otimes b_i$ vérifie $\sum a_i \iota(x) \otimes b_i = \sum a_i \otimes b_i \iota(x)$ dans $A \otimes_K A$ pour tout $x \in K$. Ainsi $\tilde{\mathcal{J}}/\mathcal{J}$ s'identifie au produit de Takeuchi $A \times_K A$.*

Démonstration. Comme J est engendré par les $x \otimes 1 - 1 \otimes x$ et que l'image de $K \otimes_k K$ dans S est commutative, $J \cdot S$ est l'idéal à droite engendré par les $g_x = \iota(x) \otimes 1 - 1 \otimes \iota(x)$. L'application $a \otimes b \mapsto [a \otimes b]$ de $A \otimes_K A$ vers $S/\mathcal{J}$ est bien définie, car $\iota(x)a \otimes b - a \otimes \iota(x)b = g_x(a \otimes b)$; elle est inverse de la projection, d'où le noyau. Enfin $\lambda \in \tilde{\mathcal{J}}$ équivaut à $\lambda g_x \in \mathcal{J}$ pour tout x, puisque $\mathcal{J}$ est engendré à droite par les g_x, et l'image de λg_x dans $A \otimes_K A$ est $\sum a_i \iota(x) \otimes b_i - \sum a_i \otimes b_i \iota(x)$. □

21. Preuve vérifiée : `lean/Grothendieck/Folder155.lean`.

La présentation de la page est donc juste dans ce cadre. La preuve n'utilise pas l'isomorphisme $\mathbb{I}(L)/L \simeq \mathrm{End}_S(S/L)$ que la piste invoquait. Lean ne vérifie ni le cas des produits tensoriels complétés de pro-objets, que mathlib n'a pas, ni la comultiplication elle-même.

21 IHÉS 2ILL5 : objets « sereins » et objets dualisables [22]

Comme les sections 24 et 33, cette section porte sur une pièce du fonds Grothendieck–Illusie de l'IHÉS, `2ILL5` (vue 2). C'est un manuscrit au crayon de dix pages, sans date, intitulé « Motifs » : le plan d'une théorie des systèmes de coefficients comme cadre des motifs, avec une liste de conjectures. Il n'a pas de pendant dans le fonds de Montpellier, et aucune lecture modernisée n'en a été faite : seul l'énoncé de la définition des pages 2 et 3 est repris ici.

L'idée. Dans une catégorie tensorielle, un objet F a un dual faible, le hom interne $F^\vee = \underline{\mathrm{Hom}}(F, \mathbf{1})$, et une flèche canonique $F^\vee \otimes F \to \underline{\mathrm{End}}(F)$. Pour les espaces vectoriels, c'est la flèche $V^* \otimes V \to \mathrm{End}(V)$, $\varphi \otimes v \mapsto (w \mapsto \varphi(w)\, v)$, qui est un isomorphisme exactement quand V est de dimension finie. Les pages 2–3 appellent « serein » un objet F tel que $F^\vee \otimes F \simeq \underline{\mathrm{End}}(F)$. C'est la caractérisation usuelle des objets *dualisables* : ceux qui ont un dual Y, avec une coévaluation $\eta : \mathbf{1} \to Y \otimes F$ et une évaluation $\varepsilon : F \otimes Y \to \mathbf{1}$ qui vérifient les deux identités triangulaires (Dold–Puppe [43], Lewis–May–Steinberger [89], III.1.3).

Énoncé (Manuscrit, pp. 2–3)**.** *Soient $\mathcal{C}$ une catégorie monoïdale et F un objet qui a un hom interne. Posons $F^\vee = \underline{\mathrm{Hom}}(F, \mathbf{1})$, notons $\mathrm{ev} : F \otimes F^\vee \to \mathbf{1}$ l'évaluation, et $\nu_X : F^\vee \otimes X \to \underline{\mathrm{Hom}}(F, X)$ la transposée de $\mathrm{ev} \otimes X$. Alors F a un dual si et seulement si $\nu_F : F^\vee \otimes F \to \underline{\mathrm{End}}(F)$ est un isomorphisme. Dans ce cas tous les ν_X sont des isomorphismes, et $F^\vee$ est lui-même le dual de F, d'évaluation* ev.

Démonstration. Si F a un dual Y, la flèche $Y \otimes X \to \underline{\mathrm{Hom}}(F, X)$ transposée de $\varepsilon \otimes X$ est inversible : son inverse est la transposée de $\underline{\mathrm{Hom}}(F, X) \to Y \otimes F \otimes \underline{\mathrm{Hom}}(F, X) \to Y \otimes X$, faite de η et de l'évaluation, et les identités triangulaires donnent les deux composées. Pour $X = \mathbf{1}$, elle identifie Y à $F^\vee$ en envoyant ε sur ev, et ν_X s'en déduit. Réciproquement, si ν_F est inversible, on pose $\eta : \mathbf{1} \to \underline{\mathrm{End}}(F) \xrightarrow{\nu_F^{-1}} F^\vee \otimes F$, l'identité suivie de ν_F^{-1}. La première identité triangulaire, pour F, est la définition même de ν_F. La seconde, pour $F^\vee$, est le seul point non formel : on la ramène à la première en comparant les transposées, par la propriété universelle de $F^\vee$. □

Aucune tresse n'est nécessaire. Dans une catégorie tressée, un dual à gauche est aussi un dual à droite, de sorte que « serein », dualisable à gauche et dualisable à droite y coïncident. L'énoncé lit le « $\simeq$ » de la page comme « la flèche canonique est un isomorphisme » : un isomorphisme abstrait $F^\vee \otimes F \simeq \underline{\mathrm{End}}(F)$ serait en général plus faible, et la page ne dit pas lequel est visé.
Vérification en Lean. La catégorie est monoïdale au sens de mathlib, et F est fermé (`Closed F`) ; `MonoidalClosed C` n'est pas supposé. Avec la convention de mathlib, `tensorLeft F ⊣ ihom F`, le dual interne $F^\vee$ est un dual *à gauche*, et un dual est un `ExactPairing Y F`. Les objets sont `dual`, `ev`, `canonicalMap` et `endMap`, pour $F^\vee$, ev, ν_X et ν_F. L'équivalence encadrée est `exists_exactPairing_iff_isIso_endMap`, et `nonempty_hasLeftDual_iff_isIso_endMap` sous la forme `HasLeftDual` ; `isIso_endMap_iff_forall` dit que tous les ν_X sont alors

22. Preuve vérifiée : `lean/Grothendieck/Ihes2ILL5.lean`.

inversibles, et `isIso_canonicalMap_of_exactPairing` donne le sens direct pour un dual quelconque, avec `whiskerLeft_comparison_ev` pour l'identification de Y à $F^\vee$. Le dual construit est `exactPairingOfIsIso`, à partir de `triangle_one` et `triangle_two`. Le cas tressé est `exists_exactPairing_right_iff_isIso_endMap`. Un exemple vérifie que tout espace vectoriel de dimension finie sur un corps (`FGModuleCat K`) est serein. Les noms sont ceux de `Ihes2ILL5.lean`.

Ne sont pas démontrés ici : que le « $\simeq$ » des pages 2–3 désigne la flèche canonique ; les modules libres de type fini sur un anneau commutatif quelconque, l'exemple ne portant que sur les espaces vectoriels ; et le reste du manuscrit.

Partie 13

Algèbre commutative

Ces cotes sont contemporaines de la rédaction d'EGA avec Dieudonné. Le 29 septembre 1965, il lui envoie le plan des paragraphes 20 à 27 du chapitre IV (25, lot 7, p. 134). Le 27 août 1967, il lui envoie un contre-exemple à EGA I 10.10.5 sans hypothèse noethérienne ; Dieudonné répond le 11 septembre qu'il n'est pas convaincu pour les modules de présentation finie (37, lot 5, p. 92, 37, lot 5, p. 95). La cote 22 est elle-même un tapuscrit de travail pour EGA IV.

22 Cote 21 : injectifs de I-torsion, critère ponctuel pour un champ [23]

La cote 21, *[Chapitre] 0 III : tapuscrit et copies de tapuscrit annotés (s.d.), notes manuscrites (s.d.)*, datée par l'inventaire « [vers 1960-1967] », s'ouvre sur un tapuscrit corrigé à la main. Pour un anneau noethérien A et un idéal I, il étudie les foncteurs contravariants sur la catégorie $\underline{C}$ des A-modules de type fini annulés par une puissance de I, et les représente par des modules H dont tout élément est annulé par une puissance de I (2.9 à 2.14). La proposition 2.15, énoncée page 11, caractérise ceux de ces modules qui sont injectifs. Sa démonstration, page 13, invoque le critère de Baer sous le nom de « Tohoku ». Pour l'étape décisive, elle écrit « En vertu de *Krull*, $I^n N$ contient une intersection $N \cap I^m N$ », avec N là où la ligne suivante et l'argument demandent M (21, lot 1, p. 13). Le corollaire 2.16 suit, puis une ligne biffée à la machine : « Si on rejette tout ce numéro (comme il me semble raisonnable) ».

On explicite deux notions que la lecture prend dans les numéros précédents.

Définition. Un A-module H est *de I-torsion* si tout élément de H est annulé par une puissance de I. Le foncteur $\mathrm{Hom}(-, H)$ est *exact à droite sur $\underline{C}$* si, pour tout $M \in \underline{C}$ et tout sous-module $N \subseteq M$, tout homomorphisme $N \to H$ se prolonge en un homomorphisme $M \to H$. Pour un A-module K, on note $H^0_I(K)$ le sous-module des éléments de K annulés par une puissance de I.

Énoncé (Proposition 2.15 ♦ 4)**.** *Soient A un anneau noethérien, I un idéal de A et H un A-module de I-torsion. Pour que H soit un A-module injectif, il faut et il suffit que le foncteur $T_H(M) = \mathrm{Hom}(M, H)$ sur la catégorie $\underline{C}$ des A-modules de type fini annulés par une puissance de I soit exact à droite, donc exact.*

Énoncé (Corollaire 2.16)**.** *Soit K un A-module. Si K est injectif, $H^0_I(K)$ l'est aussi.*

Résultat général, démontré en Lean dans `Upstream/PrimaryComponentInjective.lean` *; la démonstration n'est pas reprise ici.*

Lemme 22.1. *Soient H un module de I-torsion, M un module de type fini et $g : M \to H$ un homomorphisme. Il existe n tel que $a\, g(x) = 0$ pour tout $a \in I^n$ et tout $x \in M$.*

Démonstration. Soient $s_1, \dots, s_k$ des générateurs de M, et e_i tel que I^{e_i} annule $g(s_i)$. Posons $n = \max_i e_i$; comme $I^n \subseteq I^{e_i}$, I^n annule chaque $g(s_i)$. L'ensemble des $x \in M$ tels que I^n annule $g(x)$ est un sous-module (il contient 0, est stable par somme, et par multiplication par

23. Preuve vérifiée : `lean/Grothendieck/Folder21.lean`.

$c \in A$ puisque $a\,g(cx) = c\,(a\,g(x))$) ; il contient les générateurs, donc c'est M. C'est la phrase du feuillet : l'image de u est « un sous-module de type fini de H, donc annulé par une puissance de I ». □

Démonstration de la proposition 2.15. Nécessité. Si H est injectif, tout homomorphisme d'un sous-module N de M vers H se prolonge à M, pour tout M, a fortiori pour $M \in \underline{C}$.

Suffisance. Supposons $\mathrm{Hom}(-, H)$ exact à droite sur $\underline{C}$. Par le critère de Baer [10], il suffit de montrer que, pour tout idéal J de A, tout homomorphisme $g : J \to H$ se prolonge à A. L'idéal J est de type fini (A est noethérien) ; par le lemme 22.1, il existe n tel que I^n annule $g(J)$, et donc g est nul sur $I^n J$, qui est engendré par les produits ay avec $a \in I^n$, $y \in J$, sur lesquels $g(ay) = a\,g(y) = 0$.

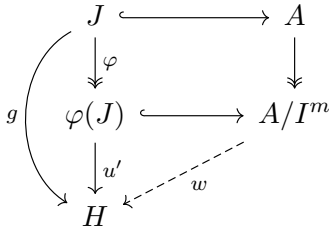
Appliquons le lemme d'Artin–Rees au module A, à son sous-module J et à l'idéal I (lemme établi indépendamment par E. Artin et par D. Rees, qui l'a publié en 1956 [110]) : il existe k tel que $J \cap I^p = I^{p-k}(J \cap I^k)$ pour tout $p \geqslant k$. Posons $m = n + k$; alors

$$J \cap I^m = I^n(J \cap I^k) \subseteq I^n J.$$

C'est l'inclusion $N \cap I^m M \subseteq I^n N$ de la lecture, pour $M = A$ et $N = J$.

Soit $\varphi : J \to A/I^m$ la composée de l'inclusion et de la projection. Son noyau est $J \cap I^m$, contenu dans $I^n J$, sur lequel g est nul. Donc g se factorise par l'image de φ : il existe $u' : \varphi(J) \to H$ avec $u'(\varphi(x)) = g(x)$ pour $x \in J$. Le module A/I^m est de type fini et annulé par I^m, donc dans $\underline{C}$, et $\varphi(J) \simeq J/(J \cap I^m)$ en est un sous-module. Par hypothèse, u' se prolonge en $w : A/I^m \to H$. La composée de la projection $A \to A/I^m$ et de w prolonge g : pour $x \in J$, elle envoie x sur $w(\varphi(x)) = u'(\varphi(x)) = g(x)$. □

Les flèches de la démonstration, où le prolongement cherché est w composé avec la projection :



$$\ker\varphi = J \cap I^m \subseteq I^n J, \quad g = u' \circ \varphi.$$

Remarque. La démonstration a besoin de l'inclusion d'Artin–Rees $N \cap I^m M \subseteq I^n N$, avec le module ambiant dans l'intersection, comme la lecture le rétablit. Celle de la page, $N \cap I^m N \subseteq I^n N$, est triviale pour $m \geqslant n$ et ne sert pas. L'inclusion utile résulte du lemme d'Artin–Rees ; le théorème d'intersection de Krull (1938) qu'invoque la page ne la donne pas.

Remarque. Dans 2.15, la finitude des objets de $\underline{C}$ n'intervient qu'à travers les modules monogènes A/I^m : pour l'injectivité, il suffit que les homomorphismes vers H se prolongent le long des inclusions $J/(J \cap I^m) \hookrightarrow A/I^m$.

Remarque. Le corollaire 2.16 se déduit de 2.15 : si K est injectif, le prolongement à K d'un homomorphisme vers $H^0_I(K)$ défini sur un sous-module d'un module annulé par I^n prend encore ses valeurs dans $H^0_I(K)$. Aucune finitude n'y sert, et la noethérianité n'intervient qu'à travers 2.15.

Remarque. L'énoncé selon lequel la composante I-primaire d'un module injectif sur un anneau noethérien est injective est le lemme 08XW de [116].

Catégories fibrées (pages 21 à 26). Soient Y un fermé de X et $\mathcal{F}$ une catégorie fibrée sur les ouverts de X. La définition 6 (page 21) dit que $\mathcal{F}$ satisfait (P_1), resp. (P_2), resp. (P_3), relativement à Y si, pour tout ouvert V, la restriction $\mathcal{F}(V) \to \mathcal{F}(V \smallsetminus Y)$ est fidèle, resp. pleinement fidèle, resp. une équivalence, et qu'elle les satisfait en x si le foncteur $\mathrm{Pseudolim}_W \mathcal{F}(W) \to \mathrm{Pseudolim}_W \mathcal{F}(W \smallsetminus \overline{\{x\}})$, W parcourant les voisinages ouverts de x, l'est. La proposition 7 (page 24) affirme l'équivalence des deux formes sur un espace noethérien spectral ; le recollement de la page 26 demande que $\mathcal{F}$ soit un champ, hypothèse que la lecture ajoute.

Théorème 22.2 (D'après les pages 21 à 26, forme complétée par l'édition ♦)**.** *Soient X un espace noethérien quasi-sobre (par exemple noethérien spectral), Y une partie fermée et $\mathcal{F}$ une catégorie fibrée scindée sur les ouverts de X qui est un champ pour les recouvrements par deux ouverts. Pour chacune des conditions (P_1), (P_2), (P_3), $\mathcal{F}$ la satisfait relativement à Y si et seulement si elle la satisfait en tout point de Y. Pour (P_1) et (P_2), il suffit que $\mathcal{F}$ soit un préchamp pour ces recouvrements.*

L'énoncé tient (`proposition7_P1`, `_P2`, `_P3` ; corollaire 8 : `corollaire8_P3`).

Esquisse. (i) $\Rightarrow$ (ii) est formel : le corollaire 8, qui vaut pour toute partie $Y' \subseteq Y$, appliqué à $\overline{\{x\}}$. Pour (ii) $\Rightarrow$ (i), récurrence noethérienne sur les fermés $Y' \subseteq Y$. Un fermé non vide Y' a un point x et un voisinage ouvert W_0 de x tels que $W_0 \cap Y' \subseteq \overline{\{x\}}$: le point générique d'une composante irréductible maximale, W_0 étant le complémentaire des autres composantes. Si $x \notin V$, alors $V \cap \overline{\{x\}} = \emptyset$ et l'hypothèse de récurrence pour $Y' \smallsetminus W_0$ conclut. Sinon, sur $W = V \cap W_0$, on a $W \smallsetminus \overline{\{x\}} = W \smallsetminus Y'$; la condition en x donne, sur un voisinage $W' \subseteq W$ de x, une flèche (resp. un objet) qui coïncide hors de $\overline{\{x\}}$ avec la donnée. On recolle sur $(V \smallsetminus Y') \cup W' = V \smallsetminus (Y' \smallsetminus W')$, et la récurrence pour $Y' \smallsetminus W'$ conclut. □

Remarque. Les pseudo-limites ne sont pas construites : la condition en x est écrite dépliée, en germes de flèches et d'objets. Une catégorie fibrée y est un foncteur $(\mathrm{Ouv}\, X)^{\mathrm{op}} \to \mathrm{Cat}$; le champ n'est demandé que pour deux ouverts, sans compatibilité de l'objet recollé à l'isomorphisme. Dans (ii) $\Rightarrow$ (i), les trois propriétés se démontrent séparément : la surjectivité essentielle en chaque point donne à elle seule la surjectivité essentielle, sans les conditions (P_1) et (P_2) que la page suppose acquises (« Reste le cas P_3, quand P_1, P_2 sont déjà vérifiés »).

Ne sont pas démontrés ici : la profondeur le long d'un fermé et le prolongement de type Hartogs ; les numéros 2.1 à 2.14 (Eilenberg–Watts, module représentant, premiers associés) ; la proposition 2.15 comme équivalence de catégories ; le numéro 2.17 ; les faisceaux des pages 15 à 20 ; l'identification de la page 23 à $\mathcal{F}_{(x)}$ sur le localisé $X_{(x)}$; le corollaire 10 et les torseurs des pages 27 et 28.

23 Cote 22 : produits de modules plats (lemme 3.3, corollaires 3.4 et 3.5), l'obstruction sur $k[[t]]$, un noyau de différentielles [24]

La cote 22, *[EGA IV]. [Chapitre] 0 IV. Cohen, différentielles, algèbres formellement simples (Compléments)*, datée par l'inventaire « 1963-[vers 1967] », réunit des tirés à part, un tapuscrit annoté et des notes manuscrites. Les pages 9 à 17 sont un tapuscrit paginé de sa main 24 à 32 et corrigé à l'encre : le numéro 3 d'un chapitre adressé à un correspondant qu'il tutoie. Avant le théorème central du numéro, la page 10 (sa page 25) place trois énoncés et en donne

24. Preuve vérifiée : `lean/Grothendieck/Folder22.lean`.

la fonction : « il nous sera commode d'avoir un critère permettant de déduire de la propriété P une propriété de platitude » (22, lot 1, p. 10). Dans la démonstration du lemme 3.3, les mots « de type fini », qui qualifient les modules libres de la présentation, sont une addition manuscrite. Dans l'énoncé du corollaire 3.5, un passage biffé portait « de A-modules projectifs de type fini ». Les pages manuscrites 22 et 24 prennent $k = \mathbf{Q}((x_i))$ et $A = k[[t]]$, écrivent $\Omega_k \otimes_k A \simeq A^{(I)} \subsetneq \prod_i A\,dx_i$ et cherchent une dérivation $D : A \to \Omega_k \otimes_k A$ qui prolonge d_k ; la page 22 présume que A « n'est jamais formellement lisse sur k pour la topologie discrète » (22, lot 2, p. 22). La page 23 énonce le cas général : si $\Omega_{K/k}$ est de dimension infinie sur K, $A = K[[t_1, \ldots, t_n]]$, muni de la topologie discrète, n'est pas formellement lisse sur K (22, lot 2, p. 23). La page 24 choisit des indices $i_0, i_1, \ldots$, commence la série $\sum_n a_n t^n$ et s'arrête.

Énoncé (Lemme 3.3)**.** *Soient A un anneau, $(P_i)_{i\in I}$ une famille de A-modules, $P = \prod_i P_i$ leur produit, et M un A-module de présentation finie. Alors l'homomorphisme canonique $M \otimes_A P \to \prod_i (M \otimes_A P_i)$ est un isomorphisme.*

Énoncé (Corollaire 3.4 ; cas noethérien du théorème de Chase)**.** *Supposons que tout A-module de type fini soit de présentation finie (par exemple A noethérien). Alors tout produit de A-modules plats est plat.*

Énoncé (Corollaire 3.5)**.** *Supposons A comme en 3.4, par exemple noethérien. Soit P un A-module isomorphe à la limite projective d'un système projectif strict, admettant un système cofinal dénombrable, de A-modules projectifs. Alors P est un A-module plat.*

Le corollaire 3.5 est démontré ici sous la forme à laquelle la lecture le ramène : un système $(P_n)_{n\in\mathbb{N}}$ dont les applications de transition $\pi_n : P_{n+1} \to P_n$ sont surjectives ; sa limite est le sous-module de $\prod_n P_n$ formé des suites (x_n) telles que $\pi_n(x_{n+1}) = x_n$ pour tout n.

Pour un homomorphisme $g : M \to N$, notons $c_M : M \otimes P \to \prod_i (M \otimes P_i)$ l'homomorphisme canonique, $m \otimes (p_i)_i \mapsto (m \otimes p_i)_i$. Il est naturel en M : $c_N \circ (g \otimes P) = \big(\prod_i (g \otimes P_i)\big) \circ c_M$, comme on le voit sur les tenseurs purs.

Lemme 23.1. *Pour tout entier n, c_{A^n} est bijectif.*

Résultat général, démontré en Lean dans `Upstream/FinitePresentationPiRightHomBijective.lean` *; la démonstration n'est pas reprise ici.*

Démonstration du lemme 3.3. C'est celle du feuillet. Le module M étant de présentation finie, il existe une suite exacte $A^m \xrightarrow{f} A^n \xrightarrow{g} M \to 0$ de modules libres *de type fini*. Comme le produit tensoriel est exact à droite, on obtient deux suites exactes

$$\begin{array}{ccccccc} A^m \otimes P & \longrightarrow & A^n \otimes P & \longrightarrow & M \otimes P & \longrightarrow & 0 \\ \downarrow{\scriptstyle c_{A^m}} & & \downarrow{\scriptstyle c_{A^n}} & & \downarrow{\scriptstyle c_M} & & \\ \prod_i (A^m \otimes P_i) & \longrightarrow & \prod_i (A^n \otimes P_i) & \longrightarrow & \prod_i (M \otimes P_i) & \longrightarrow & 0 \end{array}$$

la seconde parce qu'un produit de suites exactes est exact (on choisit un antécédent composante par composante). Les homomorphismes c_{A^m}, c_{A^n}, c_M forment un morphisme de la première suite dans la seconde, par naturalité de c. Les deux premiers sont bijectifs par le lemme 23.1. Le lemme des cinq, sous sa forme pour des suites exactes à droite (surjectivité à gauche, bijectivité au milieu), montre que c_M est bijectif. □

Démonstration du corollaire 3.4. On démontre en fait davantage : il suffit que tout idéal de type fini de A soit de présentation finie. Soient (P_i) des modules plats et $P = \prod_i P_i$. Par le critère classique de platitude par les idéaux, il suffit de voir que, pour tout idéal J de type fini de A, l'application $J \otimes P \to A \otimes P$ induite par l'inclusion $\iota : J \to A$ est injective. Par naturalité,

$$\Big(\prod_i (\iota \otimes P_i)\Big) \circ c_J = c_A \circ (\iota \otimes P).$$

Le membre de gauche est injectif : c_J l'est par le lemme 3.3, J étant de présentation finie, et chaque $\iota \otimes P_i$ l'est parce que P_i est plat. Donc $\iota \otimes P$ est injectif. Sous l'hypothèse de 3.4, tout idéal de type fini, module de type fini, est de présentation finie, et l'on conclut. □

Lemme 23.2. *Tout A-module de type fini est de présentation finie si et seulement si A est noethérien.*

Résultat général, démontré en Lean dans
`Upstream/IsNoetherianRingIffFinitePresentation.lean` *; la démonstration n'est pas reprise ici.*

Lemme 23.3. *Le produit de deux modules plats est plat.*

Résultat général, démontré en Lean dans
`Upstream/FlatProdPi.lean` *; la démonstration n'est pas reprise ici.*

Démonstration du corollaire 3.5, pour un système indexé par $\mathbb{N}$. Chaque $\pi_n : P_{n+1} \to P_n$ est surjective et P_n est projectif, donc π_n admet une section $s_n : P_n \to P_{n+1}$, $\pi_n \circ s_n = \mathrm{id}$. Le noyau K_n de π_n est un facteur direct de P_{n+1} (un projecteur sur K_n est $\mathrm{id} - s_n \circ \pi_n$), donc projectif, en particulier plat. Soit $\Phi : \varprojlim_n P_n \to P_0 \times \prod_n K_n$ l'application

$$(x_n)_n \longmapsto \big(x_0,\ (x_{n+1} - s_n(x_n))_n\big),$$

bien définie car $\pi_n(x_{n+1} - s_n(x_n)) = x_n - x_n = 0$, et linéaire. Elle est injective : si deux suites ont même image, elles ont même terme d'indice 0 et, comme $x_{n+1} = s_n(x_n) + k_n$ détermine x_{n+1} à partir de x_n, mêmes termes à tout indice par récurrence. Elle est surjective : étant donnés $y \in P_0$ et $(k_n) \in \prod_n K_n$, la suite définie par $x_0 = y$ et $x_{n+1} = s_n(x_n) + k_n$ vérifie $\pi_n(x_{n+1}) = x_n + 0$, est donc dans la limite, et a pour image $(y, (k_n))$. Ainsi $\varprojlim P_n \simeq P_0 \times \prod_n K_n$. Par le corollaire 3.4, $\prod_n K_n$ est plat ; par le lemme 23.3, $P_0 \times \prod_n K_n$ l'est, et la platitude passe à un module isomorphe. □

Remarque. Le lemme 3.3 vaut sur tout anneau commutatif. Sa réciproque, qu'un module pour lequel ces flèches sont bijectives pour toute famille (P_i) est de présentation finie, est due à Lenzing (1969) [88]. Avec l'addition manuscrite « de type fini », la démonstration du feuillet se ramène aux modules A^n.

Remarque. L'hypothèse de 3.4, que tout module de type fini soit de présentation finie, équivaut à la noethérianité (lemme 23.2). Le « par exemple A noethérien » de la page ne désigne donc pas une classe plus large.

Remarque. Le corollaire 3.4 est un cas du théorème de Chase, publié en 1960 [29], avant les dates que l'inventaire donne au dossier : sur un anneau cohérent, tout produit de modules plats est plat. La démonstration ci-dessus n'applique le lemme 3.3 qu'aux idéaux de type fini.

L'obstruction des pages 22 et 24. On note $A = k[[t]]$ et, pour un k-module M, $A \otimes_k M$ le A-module obtenu par extension des scalaires. Une dérivation est prise sur une base quelconque R (pour la page, $R = \mathbf{Q}$) ; seules servent l'additivité et la règle de Leibniz. « Formellement lisse pour la topologie discrète » est la lissité formelle de mathlib, `Algebra.FormallySmooth` : $\Omega_{A/k}$ projectif et $H_1(L_{A/k}) = 0$, condition équivalente au relèvement des morphismes à travers les idéaux de carré nul.

Lemme 23.4. *Soient k un anneau commutatif non nul, M un k-module libre de base $(b_i)_{i\in I}$, $(i_n)_{n\in\mathbb{N}}$ une suite injective d'indices et (a_n) une suite d'éléments de k. Il n'existe pas de dérivation $D : A \to A \otimes_k M$ telle que $D(a_n) = 1 \otimes b_{i_n}$ pour tout n.*

Démonstration. Pour $j \in I$, soit $p_j : A \otimes_k M \to A$ l'application A-linéaire $f \otimes m \mapsto b_j^*(m)\, f$, où b_j^* est la coordonnée d'indice j. Un élément de $A \otimes_k M$ est une somme finie de tenseurs purs, donc n'a qu'un nombre fini de coordonnées p_j non nulles. Soit $f = \sum_n a_n t^n$. Il existe donc n tel que $p_{i_n}(D(f)) = 0$ et $p_{i_n}(D(t)) = 0$. L'application $E = p_{i_n} \circ D : A \to A$ est une dérivation, puisque p_{i_n} est A-linéaire ; elle vérifie $E(t) = 0$, donc $E(t^m) = 0$ et $E(t^m g) = t^m E(g)$ pour tout m et tout $g \in A$, et $E(a_m) = b_{i_n}^*(b_{i_m}) = \delta_{mn}$, l'application $m \mapsto i_m$ étant injective. Écrivons $f = \sum_{m\le n} a_m t^m + t^{n+1} g$. Alors

$$E(f) = \sum_{m\le n} \delta_{mn}\, t^m + t^{n+1} E(g),$$

dont le coefficient de t^n est 1. Or $E(f) = 0$, et $1 \neq 0$ dans k. □

Théorème 23.5 (D'après les pages 22 et 24, obstruction différentielle sur $k[[t]]$, topologie discrète, forme complétée par l'édition ♦)**.** *Soient $k = \mathbf{Q}(x_i : i \in I)$, avec I infini, et $A = k[[t]]$. Les dx_i forment une base de $\Omega_{k/\mathbf{Q}}$, si bien que $A \otimes_k \Omega_{k/\mathbf{Q}} \simeq A^{(I)}$; aucune dérivation $D : A \to A \otimes_k \Omega_{k/\mathbf{Q}}$ ne vérifie $D(c) = 1 \otimes dc$ pour tout $c \in k$, et A n'est pas formellement lisse sur k pour la topologie discrète.*

Démonstration. Les dx_i forment une base de $\Omega_{P/\mathbf{Q}}$, pour $P = \mathbf{Q}[x_i : i \in I]$. Le corps k est un localisé de P, donc formellement étale sur P, et $k \otimes_P \Omega_{P/\mathbf{Q}} \to \Omega_{k/\mathbf{Q}}$ est un isomorphisme ; les dx_i forment donc une base de $\Omega_{k/\mathbf{Q}}$. Si D existait, on choisirait une suite injective (i_n) dans I et $a_n = x_{i_n}$: le lemme 23.4 interdit $D(x_{i_n}) = 1 \otimes dx_{i_n}$.

Supposons A formellement lisse sur k. La suite de Jacobi–Zariski

$$H_1(L_{A/k}) \xrightarrow{\delta} A \otimes_k \Omega_{k/\mathbf{Q}} \xrightarrow{\iota} \Omega_{A/\mathbf{Q}} \longrightarrow \Omega_{A/k} \longrightarrow 0$$

est exacte. Comme $H_1(L_{A/k}) = 0$ et que $\Omega_{A/k}$ est projectif, elle est scindée, et ι a une rétraction A-linéaire r : c'est l'énoncé général rappelé à la suite de la démonstration. Alors $D = r \circ d_A$ est une dérivation de A dans $A \otimes_k \Omega_{k/\mathbf{Q}}$, et $D(c) = r(\iota(1 \otimes dc)) = 1 \otimes dc$ pour $c \in k$: c'est le cas exclu au paragraphe précédent. □

Résultat général, démontré en Lean dans
`Upstream/FormallySmoothMapBaseChange.lean` *; la démonstration n'est pas reprise ici.*

La page 23 dit la même chose pour tout corps : sous l'hypothèse « de dimension infinie », elle conclut par la négative. C'est l'énoncé que l'édition avait démontré en partant de l'exemple.

Théorème 23.6 (Grothendieck, page 23, pour une seule variable)**.** *Soient k un anneau commutatif et K un corps qui est une k-algèbre, avec $\Omega_{K/k}$ de dimension infinie sur K. Aucune dérivation*

$D : K[[t]] \to K[[t]] \otimes_K \Omega_{K/k}$ ne vérifie $D(c) = 1 \otimes dc$ pour tout $c \in K$, et $K[[t]]$ n'est pas formellement lisse sur K pour la topologie discrète.

Démonstration. Les da, $a \in K$, engendrent $\Omega_{K/k}$; on en extrait une base, infinie par hypothèse, et une suite injective $da_0, da_1, \ldots$ de vecteurs de cette base. Le lemme 23.4 exclut alors D, et la seconde moitié de la démonstration précédente, où $\mathbf{Q}$ est remplacé par k, montre que la lissité formelle donnerait une telle D. □

Voir `no_derivation_of_field` et `not_formallySmooth_of_field` dans `Folder22.lean`. La page prend $n > 0$ variables $t_1, \ldots, t_n$; l'énoncé suivant ramène ce cas à une seule variable. Elle conclut que A « n'est pas f. lisse sur K relativement à k, et a fortiori n'est pas f. lisse sur k » : le « relativement à k » nomme vraisemblablement l'obstruction ci-dessus, et le « a fortiori » suppose une notion relative que le dossier ne définit pas ; il n'est pas démontré ici. Pour $k = \mathbf{Q}$ et $K = \mathbf{Q}(x_i : i \in I)$, c'est l'exemple des pages 22 et 24.

Théorème 23.7 (Grothendieck, page 23, en n variables ♦)**.** *Soient k un anneau commutatif, K un corps qui est une k-algèbre, avec $\Omega_{K/k}$ de dimension infinie sur K, et $A = K[[t_1, \ldots, t_n]]$, $n \geq 1$. Aucune dérivation $D : A \to A \otimes_K \Omega_{K/k}$ ne vérifie $D(c) = 1 \otimes dc$ pour tout $c \in K$, et A n'est pas formellement lisse sur K pour la topologie discrète.*

Démonstration. Soit $\iota : K[[t]] \to A$ le morphisme de K-algèbres $f(t) \mapsto f(t_1)$, et $\pi : A \to K[[t]]$ celui qui envoie t_1 sur t et les autres t_i sur 0 ; ce sont des substitutions de séries sans terme constant, et $\pi \circ \iota$ est l'identité. Soit $\varphi = \pi \otimes \mathrm{id} : A \otimes_K \Omega_{K/k} \to K[[t]] \otimes_K \Omega_{K/k}$; il vérifie $\varphi(a \cdot \tau) = \pi(a) \cdot \varphi(\tau)$, puisque c'est vrai des tenseurs purs $\tau = b \otimes \omega$. Si D existait, $D' = \varphi \circ D \circ \iota$ serait une dérivation de $K[[t]]$: $D'(fg) = \varphi\big(\iota(f)D(\iota g) + \iota(g)D(\iota f)\big) = f\,D'(g) + g\,D'(f)$, puisque $\pi(\iota f) = f$. Et $D'(c) = \varphi(1 \otimes dc) = 1 \otimes dc$ pour $c \in K$. Le théorème 23.6 l'exclut.

Supposons enfin A formellement lisse sur K. Comme pour une variable, la suite de Jacobi–Zariski, avec $H_1(L_{A/K}) = 0$ et $\Omega_{A/K}$ projectif, fournit une rétraction A-linéaire r de $\iota : A \otimes_K \Omega_{K/k} \to \Omega_{A/k}$, et $r \circ d_A$ est une dérivation de A dans $A \otimes_K \Omega_{K/k}$ qui envoie $c \in K$ sur $r(\iota(1 \otimes dc)) = 1 \otimes dc$: c'est ce que l'on vient d'exclure. □

Voir `incl`, `proj`, `no_derivation_mv` et `not_formallySmooth_mv` (qui applique `retraction_of_formallySmooth`) dans `Folder22.lean`, où les variables sont indexées par un ensemble fini non vide quelconque.

Remarque. La conclusion de l'exemple est de la lecture : la page 24 s'arrête sur la construction de la série. Les pages 22 et 23 se ramènent d'abord au cas $D(t) = 0$: $D(t)$ est une combinaison linéaire finie de dx_i, $i \in J$, et l'on remplace $\mathbf{Q}$ par le sous-corps k_0 engendré par les x_i, $i \in J$ (à la page 23, k par une extension de type fini K'). Ce pas n'est pas nécessaire : il suffit de prendre n assez grand pour que la coordonnée d'indice i_n de $D(t)$ soit déjà nulle. La page 24 choisit ensuite a_n tel que $d_{K/k}\, a_n \neq 0$, après avoir biffé $D_{i_n}(a_n) \neq 0$. La condition retenue ne suffit pas : si tous les a_n sont égaux et $D(t) = 0$, $D(\sum a_n t^n)$ n'a qu'une coordonnée non nulle. C'est la condition biffée, une coordonnée d'indice i_n non nulle, dont se sert le lemme 23.4. La caractéristique 0 ne sert pas : le théorème 23.6 vaut en caractéristique p, par exemple pour $\mathbb{F}_p(x_i : i \in I)$, I infini. La piste demande si l'exemple figure dans EGA 0_{IV} ou chez Matsumura ; le projet Stacks n'énonce la lissité formelle de $K[[x]]$ que pour la topologie (x)-adique [116, tags 07EL et 07EM].

Différentielles en caractéristique p (pages 25 à 28). La page 26 dessine le carré $k \subset K$, $k \cap K^p \subset K^p$, énonce que $\Omega^1_{k/k\cap K^p} \otimes_k K \to \Omega^1_K$ peut ne pas être injective, ou, ce qui revient au même, que le noyau $N_{K/k}$ de $\Omega^1_k \otimes_k K \to \Omega^1_K$ peut ne pas être engendré par les $dx \otimes 1$, $x \in k \cap K^p$, et annonce « Voici un contre-exemple » ; la page 28 établit par l'absurde la p-liberté de (x, y) sur $k \cap K^p$ et propose la spécialisation $a_i = 0$ pour $2 \le i \le p-1$ (22, lot 2, p. 26, 22, lot 2, p. 28).

Le carré de la page 26, où les traits sont des inclusions de corps :

$$\begin{array}{ccc} k' = k \cap K^p & \text{———} & K^p \\ | & & | \\ k & \text{———————} & K \end{array}$$

Contre-exemple 23.8 (Grothendieck, pages 26 et 28, noyau des différentielles, dans la spécialisation de la page 28 ♦). *Soient p un nombre premier, $K = \mathbb{F}_p(x, b_0, b_1)$ le corps des fractions rationnelles en trois indéterminées, $a_i = b_i^p$, $y = a_0 + a_1 x$, $k = \mathbb{F}_p(x, y) \subset K$ et $k' = k \cap K^p$. L'application $K \otimes_k \Omega_{k/k'} \to \Omega_{K/k'}$ n'est pas injective : $1 \otimes dy - a_1 \otimes dx$ est un élément non nul de son noyau.*

Démonstration. Toute dérivation de K tue les puissances p-ièmes, donc $dy = a_1\, dx$ dans $\Omega_{K/k'}$, et l'élément est dans le noyau. Pour voir qu'il n'est pas nul, il suffit d'une k'-dérivation $\delta : k \to K$ avec $\delta(x) = 0$ et $\delta(y) = 1$: elle donne une forme K-linéaire sur $K \otimes_k \Omega_{k/k'}$ qui vaut 1 sur l'élément. On prend $\delta = \partial/\partial y$, les dérivées partielles de $k = \mathbb{F}_p(x, y)$ venant de la base (dx, dy) de $\Omega_{k/\mathbb{F}_p}$, et il reste à voir que $\partial c/\partial y = 0$ pour $c \in k'$. Soit ∂_x la dérivée partielle de K par rapport à x, qui tue b_0, b_1 et K^p. Par la règle de dérivation des fonctions composées, $0 = \partial_x c = \partial c/\partial x + a_1\, \partial c/\partial y$. Si $\partial c/\partial y$ n'était pas nul, a_1 serait dans k. Or x, y, a_1 sont algébriquement indépendants sur $\mathbb{F}_p$: la substitution $(T_0, T_1, T_2) \mapsto (x, y, a_1)$ est l'automorphisme triangulaire $(T_0, T_1 + T_2 T_0, T_2)$ suivi de (T_0, T_1^p, T_2^p), que la substitution $T_0 \mapsto T_0^p$ rend égal au morphisme injectif $f \mapsto f(T^p)$. Une égalité $a_1 g(x, y) = f(x, y)$ donnerait $T_2\, g = f$ dans $\mathbb{F}_p[T_0, T_1, T_2]$, d'où $f = 0$ en faisant $T_2 = 0$, puis $g = 0$ (Lean : `contre_exemple_page26`, `a1_not_mem`, `triple_injective`). □

Remarque. La démonstration ne calcule pas k' : elle établit seulement que $\partial/\partial y$ le tue, c'est-à-dire la p-liberté de (x, y) sur k' que la page 28 démontre par l'absurde. Le but est $\Omega_{K/k'}$, qui est le Ω^1_K de la page puisque k' est formé de puissances p-ièmes (lemme 23.9 ci-dessous). Pour $p = 2$ la spécialisation est l'exemple entier ; le cas général est le contre-exemple 23.10.

Lemme 23.9 (identification $\Omega_{K/k'} = \Omega_K$). *Soient $R \to S \to B$ des homomorphismes d'anneaux commutatifs, B de caractéristique p, tels que l'image de S dans B soit formée de puissances p-ièmes. Alors $\Omega_{B/R} \to \Omega_{B/S}$ est bijective. En particulier $\Omega_K = \Omega_{K/\mathbb{F}_p} \to \Omega_{K/k'}$ est un isomorphisme pour tout $k' \subset K^p$.*

Démonstration. La suite $B \otimes_S \Omega_{S/R} \to \Omega_{B/R} \to \Omega_{B/S} \to 0$ est exacte, et sa première flèche envoie $b \otimes ds$ sur $b\, d(w^p) = p\, b\, w^{p-1}\, dw = 0$ si s a pour image w^p ; elle est donc nulle (Lean : `map_bijective_of_pow`, `omega_kPrimeOf_bijective`). □

Contre-exemple 23.10 (Grothendieck, pages 26 et 28, noyau des différentielles, l'exemple général ♦). *Soient p un nombre premier, $K = \mathbb{F}_p(x, b_0, \ldots, b_{p-1})$, $a_i = b_i^p$, $y = \sum_{i=0}^{p-1} a_i x^i$,*

$k = \mathbb{F}_p(x,y) \subset K$ et $k' = k \cap K^p$. Alors $\Omega_{k/k'} \otimes_k K \to \Omega_K$ n'est pas injective ; de façon équivalente, $dy - y'\,dx$, où $y' = \sum_i i\,a_i x^{i-1}$, est dans le noyau de $\Omega_k \otimes_k K \to \Omega_K$ sans être dans le sous-K-espace engendré par les $dc \otimes 1$, $c \in k'$.

Démonstration. C'est l'argument de la spécialisation, valable pour tout plongement $k = \mathbb{F}_p(x,y) \to K$ avec $dy = y'\,dx$ pour toute dérivation de K et $y' \notin k$: si $c = w^p \in k'$, la règle de dérivation des fonctions composées pour ∂_x donne $0 = \partial c/\partial x + y'\,\partial c/\partial y$, donc $\partial c/\partial y = 0$, et $\partial/\partial y$ fournit une forme linéaire qui tue les $dc \otimes 1$, $c \in k'$, et vaut 1 sur $dy - y'\,dx$. Ici $dy = y'\,dx$ car les a_i sont des puissances p-ièmes. Reste $y' \notin k$, conséquence de l'indépendance algébrique de x, y, y' : la spécialisation $b_0 \mapsto T_1$, $b_1 \mapsto T_2$, $b_i \mapsto 0$ pour $i \geq 2$ envoie (x, y, y') sur $(T_0, T_1^p + T_2^p T_0, T_2^p)$, le triplet de la spécialisation, dont l'indépendance est démontrée plus haut. On conclut comme pour a_1 (Lean : `contre_exemple_general`, `contre_exemple_general_span`, `not_injective_to_omega`, `ker_not_span`, `tripleG_injective`). □

Ne sont pas démontrés ici : la lissité, la non-ramification et l'étalitude formelles pour des topologies préadiques, et leurs critères de relèvement ; en particulier la moitié t-adique de l'obstruction ; dans le corollaire 3.5, la réduction à un système indexé par $\mathbb{N}$; les numéros 3.2 et 3.6 à 3.13 (algèbres de Cohen, homomorphismes réguliers) ; le « a fortiori … sur k » de la page 23 ; la seconde variante de la page 28, avec a_1 algébrique sur $\mathbb{F}$; les pages 1 à 8, 18 à 21, 25 et 27.

24 IHÉS SGA 6 1/5 : modules à n-présentation finie, extensions, noyaux et facteurs directs [25]

Cette section ne porte pas sur une cote du fonds de Montpellier, mais sur une pièce du fonds Grothendieck–Illusie de l'IHÉS, `FG_IL_5_SGA6_1_5`, que le site montre à l'onglet Illusie (vue 1). C'est un tapuscrit de treize feuillets, numérotés 22 à 34, écrit à la première personne ; des corrections à l'encre brune, noire et bleue y sont d'une main que les pages ne permettent pas d'identifier. Il contient les numéros 4 à 7 d'un texte plus long sur les n-présentations finies, et le catalogue de l'IHÉS le range parmi les pièces de SGA 6, avec la date « 1966 ? ». Aucune lecture modernisée n'en a été faite : les énoncés ci-dessous sont lus sur la transcription des vues 1 à 5.

L'idée. Un module M de type fini est un quotient d'un module libre de type fini : il y a une suite exacte $L_0 \to M \to 0$ avec $L_0 = A^k$. Il est de présentation finie si l'on peut, de plus, prolonger la suite en $L_1 \to L_0 \to M \to 0$ avec L_1 libre de type fini : un nombre fini de générateurs, et un nombre fini de relations entre eux. Rien n'empêche de continuer, avec un nombre fini de relations entre les relations, et ainsi de suite. Le tapuscrit appelle *n-présentation finie* de M une suite exacte

$$L_n \to L_{n-1} \to \cdots \to L_1 \to L_0 \to M \to 0$$

de modules libres de type fini (définition 4.1). Il note $\underline{C}_n$ la classe des modules qui en ont une, et convient que $\underline{C}_n$ contient tous les modules si $n < 0$. Ainsi $\underline{C}_0$ est la classe des modules de type fini, $\underline{C}_1$ celle des modules de présentation finie, et

$$\underline{C}_0 \supset \underline{C}_1 \supset \underline{C}_2 \supset \cdots .$$

25. Preuve vérifiée : `lean/Grothendieck/IhesSGA6_1_5.lean`.

Sur un anneau noethérien, la suite est constante à partir de $n = 0$, puisqu'un sous-module d'un module de type fini y est de type fini. Le tapuscrit en tire lui-même la remarque que ces classes ne servent que pour des anneaux non noethériens, qui interviennent en théorie de la descente même quand on part d'anneaux noethériens.

Le n° 4 se place dans une catégorie abélienne, avec une classe d'objets projectifs stable par sommes finies à la place des modules libres de type fini ; le n° 5 l'applique aux modules à gauche sur un anneau non nécessairement commutatif. On lit ici les énoncés du n° 4 dans le cas des modules.

Énoncé (Tapuscrit, vues 1 à 5, énoncés 4.2 à 4.7 bis et n° 5, pour les modules)**.** *Soient A un anneau et $n \geq 0$ un entier.*

(4.2) Si $0 \to M' \to M \to M'' \to 0$ est une suite exacte avec M' et M'' dans $\underline{C}_n$, alors M est dans $\underline{C}_n$.

(4.3) Une somme directe finie de modules de $\underline{C}_n$ est dans $\underline{C}_n$.

(4.4) Si $0 \to R \to M_0 \to X \to 0$ est une suite exacte avec M_0 dans $\underline{C}_n$, alors X est dans $\underline{C}_n$ si et seulement si R est dans $\underline{C}_{n-1}$.

(4.7 bis) Un facteur direct d'un module de $\underline{C}_n$ est dans $\underline{C}_n$.

(n° 5) Les classes $\underline{C}_n$ ne changent pas si l'on demande seulement aux L_i d'être projectifs de type fini.

Pourquoi le décalage d'indice dans 4.4. Si X est le quotient de M_0 par R, des générateurs de M_0 engendrent X, et les relations de X sont celles de M_0 augmentées des éléments de R. Pour présenter X jusqu'à l'étage n, il suffit donc de présenter R jusqu'à l'étage $n-1$: chaque étage de R fournit un étage de plus pour X. Dans le cas $n = 1$ avec $M_0 = A^k$, on retrouve un fait classique : X est de présentation finie si et seulement si le noyau d'une surjection $A^k \to X$ est de type fini, et alors le noyau de toute surjection de ce genre l'est.

La démonstration. Le tapuscrit démontre 4.2 par la construction « en fer à cheval » de Cartan et Eilenberg (chapitre V, 2.2, de [28]), qui résout une extension à partir des résolutions des deux termes extrêmes. Il démontre 4.4 par récurrence sur n, en modifiant une présentation de X jusqu'à ce qu'elle se relève en une surjection sur M_0 ; ce passage du feuillet 23 (vue 2) est encadré au crayon et barré, avec des mots biffés puis soulignés de tirets, et sa forme finale n'est pas sûre. La preuve vérifiée suit une autre route, qui tient en une seule construction.

Lemme 24.1. *Soient $p : N \to M$ une surjection et $u : F \to M$ une surjection depuis un module projectif F. Il existe une surjection $g : \ker p \times F \to N$ dont le noyau est isomorphe à $\ker u$.*

Démonstration. Comme F est projectif, u se relève en $h : F \to N$ avec $p \circ h = u$. On pose $g(a, b) = a + h(b)$. Pour $y \in N$, on choisit $b \in F$ tel que $u(b) = p(y)$; alors $a = y - h(b)$ est dans $\ker p$, et $g(a, b) = y$. Si $g(a, b) = 0$, on applique p et l'on trouve $u(b) = 0$; de plus $a = -h(b)$ est déterminé par b. Inversement, pour $b \in \ker u$, le couple $(-h(b), b)$ est dans $\ker g$. L'application $(a, b) \mapsto b$ est donc un isomorphisme de $\ker g$ sur $\ker u$. □

On démontre alors, par récurrence sur n, les énoncés dans l'ordre suivant.

Le sens « il suffit » de 4.4 au rang $n+1$, à partir de 4.2 au rang n. Soient $0 \to R \to M_0 \to X \to 0$ exacte, $M_0 \in \underline{C}_{n+1}$ et $R \in \underline{C}_n$. On choisit une surjection $u : L_0 \to M_0$, avec L_0 libre de type fini et $\ker u \in \underline{C}_n$. Le noyau S de la surjection composée $L_0 \to X$ est une extension de R

par $\ker u$: la suite $0 \to \ker u \to S \to R \to 0$ est exacte. Par 4.2 au rang n, S est dans $\underline{C}_n$, donc X est dans $\underline{C}_{n+1}$. C'est le raisonnement de la vue 3.

4.2 au rang n. Soit $0 \to M' \to M \to M'' \to 0$ exacte, avec M' et M'' dans $\underline{C}_n$. On choisit une surjection $u : L_0 \to M''$ dont le noyau est dans $\underline{C}_{n-1}$. Le lemme 24.1 donne une suite exacte $0 \to \ker u \to M' \times L_0 \to M \to 0$. Le produit $M' \times L_0$ est dans $\underline{C}_n$ (pour deux facteurs, on fait le produit des deux présentations, étage par étage). Le sens « il suffit » de 4.4 au rang n conclut. Pour $n = 0$, M est un quotient du module de type fini $M' \times L_0$.

4.7 bis. Si M est un facteur direct de $N \in \underline{C}_n$, la suite $0 \to M_1 \to N \to M \to 0$ est scindée, et le facteur complémentaire M_1 est lui aussi un facteur direct de N. Par récurrence, M_1 est dans $\underline{C}_{n-1}$, et le sens « il suffit » de 4.4 donne $M \in \underline{C}_n$. C'est l'argument de la vue 4, que le tapuscrit écrit en une ligne.

Le sens « il faut » de 4.4, sous une hypothèse plus faible. Soit $0 \to R \to M_0 \to X \to 0$ exacte, avec $M_0 \in \underline{C}_{n-1}$ et $X \in \underline{C}_n$. On choisit une surjection $u : L_0 \to X$ dont le noyau est dans $\underline{C}_{n-1}$. Le lemme donne $0 \to \ker u \to R \times L_0 \to M_0 \to 0$. Par 4.2 au rang $n-1$, $R \times L_0$ est dans $\underline{C}_{n-1}$, et R, qui en est un facteur direct, aussi, par 4.7 bis.

Le n° 5. Un module projectif de type fini P est un facteur direct d'un A^k, donc il est dans tous les $\underline{C}_n$ par 4.7 bis. Si $P \to M$ est une surjection de noyau dans $\underline{C}_n$, le sens « il suffit » de 4.4 donne $M \in \underline{C}_{n+1}$.

Remarque. Le sens « il faut » de 4.4 demande seulement $M_0 \in \underline{C}_{n-1}$, au lieu de $M_0 \in \underline{C}_n$. C'est la forme des trois énoncés « deux sur trois » pour une suite exacte courte $0 \to M' \to M \to M'' \to 0$ (Stacks, 064R [116]) : si M' et M'' sont dans $\underline{C}_n$, M aussi ; si $M \in \underline{C}_{n+1}$ et $M' \in \underline{C}_n$, alors $M'' \in \underline{C}_{n+1}$; si $M \in \underline{C}_n$ et $M'' \in \underline{C}_{n+1}$, alors $M' \in \underline{C}_n$. Les trois sont démontrés.

Vérification en Lean. La définition est faite par récurrence, ce qui est un choix de l'édition, le tapuscrit écrivant la suite exacte : `IsNPresented R n M` dit pour $n = 0$ que M est de type fini, et au rang $n+1$ qu'une surjection $R^k \to M$ a son noyau dans le rang n. L'anneau R est quelconque, non nécessairement commutatif, comme au n° 5, et les modules sont pris dans l'univers de R, pour que les noyaux y restent. Aux rangs 0 et 1, la notion est celle de mathlib : `isNPresented_zero_iff` (`Module.Finite`) et `isNPresented_one_iff` (`Module.FinitePresentation`). Le lemme 24.1 est `exists_coprod`. La proposition 4.2 est `IsNPresented.of_exact` ; le corollaire 4.3, pour deux facteurs, `IsNPresented.prod` ; la proposition 4.4, telle que la page l'énonce, `IsNPresented.iff_of_exact` ; les trois énoncés de la remarque, `IsNPresented.of_exact`, `IsNPresented.of_exact_right` et `IsNPresented.of_exact_left` ; le corollaire 4.7 bis, `IsNPresented.of_retract` ; le n° 5, `IsNPresented.of_projective` et `IsNPresented.succ_of_projective`. Avec M_0 libre de type fini, `isNPresented_succ_iff_forall` et `isNPresented_succ_iff_exists` disent qu'un module est dans $\underline{C}_{n+1}$ si et seulement s'il est de type fini et que le noyau d'une, ou de toute, surjection depuis un module libre de type fini est dans $\underline{C}_n$ (Stacks 064U et 064X). Les noms sont ceux de `IhesSGA6_1_5.lean`.

Ne sont pas démontrés ici : le cadre d'une catégorie abélienne du n° 4 ; les ∞-présentations et le corollaire 4.7 ; les corollaires 4.5 et 4.6, sur des suites exactes plus longues ; la proposition 4.8 et le corollaire 4.9, sur les foncteurs exacts et les foncteurs dérivés ; la suite du n° 5 (changement de base plat, localisation, résolutions finies, immersions régulières) et les n^{os} 6 et 7 (présentation relative sur une algèbre, préschémas).

25 Cote 67 : modules à involution et triples (P, Q, m) [26]

La cote 67, *Chirurgie des surfaces conformes : notes manuscrites (s.d., 1983-1984), lettres (1984)*, compte cent pages. Elle s'achève sur des notes consacrées aux courbes elliptiques réelles (pages 90 à 100). Une courbe elliptique réelle y revient à un réseau Π de rang 2 muni d'une involution qui renverse l'orientation (page 92). Pour classer ces involutions, la page 90, datée « Déc 83 », fait un détour d'algèbre linéaire sur un anneau quelconque, « par exemple » commutatif (mot lu avec doute, 67, lot 5, p. 90). Elle considère les k-modules M munis d'un automorphisme σ tel que $\sigma^2 = \mathrm{id}$ et sur lesquels la multiplication par 2 est injective, et leur associe les triples (P, Q, m). Elle établit $M_+ \cap M_- = 0$, $2M \subset M_+ \oplus M_-$, $M' \cap P = 2P$ et $M' \cap Q = 2Q$ pour $M' = 2M$, reconstitue (M, σ) à partir du triple par l'isomorphisme $2\,\mathrm{id}_M : M \to M'$, et énonce la proposition. La page 91 en est le brouillon ; la page 99 en tire le cas du rang 2 sur un anneau principal (67, lot 5, p. 99).

Conventions. Soit k un anneau, non nécessairement commutatif. Un k-module M est *2-régulier* si $2x = 0$ entraîne $x = 0$ dans M ; on note $2M$ l'image de la multiplication par 2, qui est un sous-module puisque 2 est central. La catégorie $\mathcal{I}$ a pour objets les couples (M, σ) d'un k-module 2-régulier et d'un endomorphisme k-linéaire σ tel que $\sigma^2 = \mathrm{id}$, et pour morphismes $(M, \sigma) \to (M', \sigma')$ les applications k-linéaires f telles que $f\sigma = \sigma' f$. On pose $M_+ = \mathrm{Ker}(1 - \sigma)$ et $M_- = \mathrm{Ker}(1 + \sigma)$. La catégorie $\mathcal{T}$ a pour objets les triples (P, Q, m) de deux k-modules 2-réguliers et d'un sous-module m de $P/2P \times Q/2Q$ tel que $(p, 0) \in m$ entraîne $p = 0$ et $(0, q) \in m$ entraîne $q = 0$; ses morphismes $(P, Q, m) \to (P', Q', m')$ sont les couples (f, g) d'applications linéaires $P \to P'$, $Q \to Q'$ telles que $(\bar{f} \times \bar{g})(m) \subset m'$, où $\bar{f}$, $\bar{g}$ sont les applications induites, qui existent puisque $f(2P) \subset 2P'$. Un sous-k-module de $P/2P \times Q/2Q$ est la même chose qu'un sous-$k/2k$-module, puisque 2 annule ce produit. Pour un triple $T = (P, Q, m)$, on note $N_T \subset P \times Q$ l'image réciproque de m : $(p, q) \in N_T$ si et seulement si $(\bar{p}, \bar{q}) \in m$.

Théorème 25.1 (Grothendieck, page 90, *proposition* ♦). *Soit (M, σ) un objet de $\mathcal{I}$, et $P = M_+$, $Q = M_-$.*

1. *$P \cap Q = 0$; $x + \sigma x \in P$ et $x - \sigma x \in Q$ pour tout $x \in M$; $P \cap 2M = 2P$ et $Q \cap 2M = 2Q$.*
2. *Soit m l'image dans $P/2P \times Q/2Q$ de $\{(p, q) \in P \times Q \mid p + q \in 2M\}$. Pour $p \in P$, $q \in Q$, on a $(\bar{p}, \bar{q}) \in m$ si et seulement si $p + q \in 2M$, et (P, Q, m) est un objet de $\mathcal{T}$.*
3. *Le foncteur $B : \mathcal{T} \to \mathcal{I}$, $(P, Q, m) \mapsto (N_T, \mathrm{id}_P \times (-\mathrm{id}_Q))$, est une équivalence de catégories. L'application $x \mapsto (x + \sigma x, x - \sigma x)$ est un isomorphisme de (M, σ) sur $B(P, Q, m)$; un quasi-inverse de B envoie donc (M, σ) sur un triple isomorphe à (M_+, M_-, m), et le foncteur $(M, \sigma) \mapsto (P, Q, m)$ de la page est une équivalence.*

Aucune hypothèse de finitude ni de projectivité n'est faite sur M, P ou Q.

Démonstration de (1). Si $x \in P \cap Q$, on a $\sigma x = x$ et $\sigma x = -x$, donc $2x = x + x = x - x = 0$, et $x = 0$ par 2-régularité. Comme $\sigma^2 = \mathrm{id}$, $\sigma(x + \sigma x) = \sigma x + x$ et $\sigma(x - \sigma x) = -(x - \sigma x)$. Soit $p \in P$ avec $p = 2y$, $y \in M$: alors $2\sigma y = \sigma(2y) = \sigma p = p = 2y$, donc $\sigma y = y$ par 2-régularité, et $y \in P$, d'où $p \in 2P$. De même, si $q \in Q$ et $q = 2y$, alors $2\sigma y = -q = 2(-y)$, donc $\sigma y = -y$ et $y \in Q$. Les inclusions inverses $2P \subset P \cap 2M$, $2Q \subset Q \cap 2M$ sont claires. □

Démonstration de (2). Si $(\bar{p}, \bar{q}) \in m$, il existe (p', q') avec $p' + q' \in 2M$, $p' - p \in 2P$ et $q' - q \in 2Q$; comme $2P$ et $2Q$ sont contenus dans $2M$, $p + q = (p' + q') - (p' - p) - (q' - q)$ est dans $2M$.

26. Preuve vérifiée : `lean/Grothendieck/Folder67.lean`.

La réciproque est la définition de m. Les modules P et Q sont 2-réguliers comme sous-modules de M. Si $(\bar{p},0)\in m$, alors $(\bar{p},\bar{0})\in m$, donc $p=p+0\in 2M$, donc $p\in 2P$ par (1), c'est-à-dire $\bar{p}=0$; de même pour Q. □

Démonstration de (3). Le foncteur. Pour $T=(P,Q,m)$, l'application $\tau=\mathrm{id}_P\times(-\mathrm{id}_Q)$ conserve N_T, car $-\bar{q}=\bar{q}$ dans $Q/2Q$ (puisque $-q-q=2(-q)$) ; on a $\tau^2=\mathrm{id}$, et N_T est 2-régulier comme sous-module de $P\times Q$. Un morphisme (f,g) envoie N_T dans $N_{T'}$ par la condition $(\bar{f}\times\bar{g})(m)\subset m'$, et $f\times g$ commute à τ ; c'est le foncteur B. Pour $p\in P$ et $q\in Q$, $(2p,0)$ et $(0,2q)$ sont dans N_T, car leurs classes sont nulles.

Fidélité. Si $B(f,g)=B(f',g')$, on évalue en $(2p,0)$: $2f(p)=2f'(p)$, donc $f(p)=f'(p)$ par 2-régularité de P' ; de même $g=g'$ en évaluant en $(0,2q)$.

Plénitude. Soit $h:B(T)\to B(T')$ un morphisme de $\mathcal{I}$, $T'=(P',Q',m')$. Pour $p\in P$, posons $h(2p,0)=(a,b)$. Comme $(2p,0)$ est fixe par τ, $(a,-b)=\tau h(2p,0)=h(2p,0)=(a,b)$, donc $2b=b+b=b-b=0$ et $b=0$. Comme $(a,0)\in N_{T'}$, $(\bar{a},0)\in m'$, donc $\bar{a}=0$ et $a\in 2P'$. La multiplication par 2 étant un isomorphisme linéaire de P' sur $2P'$, on pose $f(p)=a/2$; f est linéaire, comme composé de $p\mapsto h(2p,0)$, de la première projection et de cet inverse. De même, $(0,2q)$ étant changé de signe par τ, $h(0,2q)=(0,c)$ avec $c\in 2Q'$, et l'on pose $g(q)=c/2$. Pour $(p,q)\in N_T$, on a $2(p,q)=(2p,0)+(0,2q)$ dans N_T, donc

$$2\,h(p,q)=h(2p,0)+h(0,2q)=(2f(p),0)+(0,2g(q))=2\,(f(p),g(q)),$$

et $h(p,q)=(f(p),g(q))$ par 2-régularité de $P'\times Q'$. En particulier, si $(\bar{p},\bar{q})\in m$, alors $(p,q)\in N_T$ et $(f(p),g(q))=h(p,q)\in N_{T'}$, c'est-à-dire $(\overline{f(p)},\overline{g(q)})\in m'$: (f,g) est un morphisme de $\mathcal{T}$, et $B(f,g)=h$.

Essentielle surjectivité. Soit (M,σ) un objet de $\mathcal{I}$ et $T=(M_+,M_-,m)$ le triple de (2). L'application $\varphi(x)=(x+\sigma x,x-\sigma x)$ est linéaire de M dans $M_+\times M_-$ par (1), à valeurs dans N_T par (2), puisque $(x+\sigma x)+(x-\sigma x)=2x$. Elle commute aux involutions : $\varphi(\sigma x)=(\sigma x+x,\sigma x-x)=\tau\varphi(x)$. Elle est injective : si $\varphi(x)=\varphi(y)$, alors $2x=(x+\sigma x)+(x-\sigma x)=2y$, et $x=y$. Elle est surjective : si $(p,q)\in N_T$, alors $p+q\in 2M$ par (2), soit $p+q=2x$; on a $2\sigma x=\sigma p+\sigma q=p-q$, donc $2(x+\sigma x)=2p$ et $2(x-\sigma x)=2q$, d'où $\varphi(x)=(p,q)$. Un morphisme de $\mathcal{I}$ dont l'application sous-jacente est bijective est un isomorphisme, car son inverse commute encore aux involutions ; donc $(M,\sigma)\simeq B(T)$.

Un foncteur fidèle, plein et essentiellement surjectif est une équivalence. Si C en est un quasi-inverse, $B(C(M,\sigma))\simeq(M,\sigma)\simeq B(M_+,M_-,m)$, et, comme B est pleinement fidèle, $C(M,\sigma)\simeq(M_+,M_-,m)$. □

Remarque. L'énoncé tient tel que la piste le formule, pour un anneau quelconque, commutatif ou non, sans hypothèse de finitude ni de projectivité. Seule la 2-régularité sert, à trois endroits : pour $P\cap Q=0$; pour $P\cap 2M=2P$ et $Q\cap 2M=2Q$, qui font que m rencontre trivialement chaque facteur ; et pour la plénitude, où un morphisme h est déterminé par sa restriction à $2P\times 2Q$, parce que $2N_T\subset 2P\times 2Q$ et que le but est 2-régulier. La démonstration suit la page. La reconstruction de (M,σ) y est l'isomorphisme φ, multiplication par 2 de M sur $M'=2M$ lue dans $P\oplus Q$.

Remarque. La vérification énonce l'équivalence dans le sens $B:\mathcal{T}\to\mathcal{I}$ de la reconstruction. Elle en déduit le foncteur de la page, $(M,\sigma)\mapsto(P,Q,m)$, comme quasi-inverse, à isomorphisme près sur chaque objet. La page ne définit pas les morphismes de triples. On a pris les couples (f,g) tels que $(\bar{f}\times\bar{g})(m)\subset m'$, c'est-à-dire ceux pour lesquels $f\times g$ envoie M' dans M'. La

condition sur m, que la page écrit $m \cap P/2P = 0$, $m \cap Q/2Q = 0$, est prise telle quelle ; sa traduction en graphe d'un isomorphisme entre un sous-module de $P/2P$ et un sous-module de $Q/2Q$ n'est pas formalisée.

Ne sont pas démontrés ici : la description de m comme graphe d'un isomorphisme $p' \simeq q'$; le corollaire de la page 90 (M projectif de rang 2, k connexe), en partie illisible ; le corollaire de la page 99 (deux classes d'involutions $\neq \pm 1$ dans $\mathrm{GL}_2(k)$, pour k principal et $k/2k$ un corps) et les deux types de réseaux de la page 92 ; le reste du dossier (chirurgie et métriques canoniques des surfaces conformes).

Partie 14

Catégories et foncteurs

Les lettres du fonds sur les catégories monoïdales sont postérieures à la datation de la cote 19. Le 27 août 1974, il transpose pour Deligne les Gr-catégories de Hoàng Xuân Sính dans le langage des champs (103, lot 1, p. 8). Le 5 février 1975, il écrit à Lawrence Breen sur les 2-catégories de Picard strictes, les gerbes et les liens (134-2, lot 3, p. 38).

26 Cote 19 : le théorème de comonadicité 1.12, la comonade sur une base produit, le théorème de Gabriel–Popescu et les chaînes d'adjoints [27]

La cote 19, *Topos : notes manuscrites (s.d.)*, quatre-vingt-quinze pages que l'inventaire date « [à partir de 1958-1973] », est un dossier de travail en neuf liasses. La première, « Tapis cartésiens » (pages 3 à 11), étudie la comonade d'une adjonction et ses coalgèbres. La page 4 énonce le « Théorème 1.12 », suivi d'un nom propre que la transcription lit « Beck » avec doute. Elle écrit « il faut et il suffit » pour b), et porte en marge la restriction « il suffit de regarder les doubles flèches u, v de A telles que $\mathrm{Ker}(f(u), f(v))$ existe (condition C) » (19, lot 1, p. 4). La deuxième liasse, « Cohomologie relative », s'ouvre pages 14 et 15 sur la représentabilité. Pour une catégorie à générateur U, elle affirme une équivalence avec les modules sur $\mathrm{End}(U)$, « [détails laissés au lecteur] » (19, lot 1, p. 15).

Conventions. On note, comme la lecture, $f : A \to B$ l'adjoint à gauche de $g : B \to A$, $\eta : \mathrm{id}_A \to gf$ l'unité, $\varepsilon : fg \to \mathrm{id}_B$ la coünité, et $\varphi = fg$ la comonade, de comultiplication $\delta_X = f(\eta_{gX})$. Une φ-coalgèbre est un couple (X, a), $a : X \to \varphi X$, tel que $\varepsilon_X \circ a = 1_X$ et $\delta_X \circ a = \varphi(a) \circ a$; un morphisme $(X, a) \to (X', a')$ est une flèche $t : X \to X'$ telle que $a' \circ t = \varphi(t) \circ a$. Le foncteur de comparaison $h : A \to \varphi\text{-}\mathbf{Coalg}$ envoie Y sur $(fY, f(\eta_Y))$ et ψ sur $f(\psi)$. Le *noyau* $\mathrm{Ker}(u, v)$ d'une double flèche est son égalisateur, et *f y commute* s'il envoie un noyau de (u, v) sur un noyau de (fu, fv). On utilise les identités triangulaires $\varepsilon_{fY} \circ f(\eta_Y) = 1$ et $g(\varepsilon_X) \circ \eta_{gX} = 1$, et la bijection d'adjonction $t \mapsto t^\flat = g(t) \circ \eta_Y$, de $\mathrm{Hom}_B(fY, X)$ sur $\mathrm{Hom}_A(Y, gX)$, d'inverse $s \mapsto \varepsilon_X \circ f(s)$.

Définition. Le foncteur f vérifie la *condition C* si, pour toute double flèche (u, v) de A telle que $\mathrm{Ker}(fu, fv)$ existe, $\mathrm{Ker}(u, v)$ existe et f y commute. Un triplet (e, s, t) formé de $e : E \to Y$, $s : Y \to E$ et $t : Z \to Y$ est un *noyau scindé* de $u, v : Y \rightrightarrows Z$ si $ue = ve$, $se = 1_E$, $tu = 1_Y$ et $tv = es$. Une double flèche (u, v) de A est *f-scindée* si (fu, fv) admet un noyau scindé.

Énoncé (Théorème 1.12, page 4)**.** *Soit $f \dashv g$ une adjonction, $\varphi = fg$, et h le foncteur de comparaison.*

a) Si les noyaux de doubles flèches existent dans A et si f y commute, alors h est essentiellement surjectif.

b) h est une équivalence si et seulement si f est conservatif et si, pour toute double flèche (u, v) de A telle que $\mathrm{Ker}(fu, fv)$ existe, $\mathrm{Ker}(u, v)$ existe et f y commute.

27. Preuve vérifiée : `lean/Grothendieck/Folder19.lean`.

La restriction portée en marge (il suffit de considérer les doubles flèches (u, v) dont l'image par f a un noyau) est la condition C.

Lemme 26.1. *Si (e, s, t) est un noyau scindé de (u, v), alors e est un noyau de (u, v), et l'image de (e, s, t) par tout foncteur est un noyau scindé de l'image de (u, v).*

Démonstration. Soit $z : T \to Y$ avec $uz = vz$. Alors $z = tuz = tvz = e(sz)$, donc z se factorise par e, et de façon unique, puisque $ez' = ez''$ entraîne $z' = sez' = sez'' = z''$. Les quatre conditions sont des égalités entre composés, qu'un foncteur conserve. □

Un noyau scindé se dessine ainsi, les flèches s et t allant en sens inverse :

$$E \underset{s}{\overset{e}{\rightleftarrows}} Y \underset{t}{\overset{u}{\underset{v}{\rightrightarrows}}} Z \qquad ue = ve, \quad se = 1_E, \quad tu = 1_Y, \quad tv = es.$$

Lemme 26.2. *Pour toute coalgèbre (X, a), la double flèche $(\eta_{gX}, g(a)) : gX \rightrightarrows gfgX$ est f-scindée : $(a, \varepsilon_X, \varepsilon_{fgX})$ est un noyau scindé de $(f(\eta_{gX}), fg(a))$. Elle est de plus coréflexive : $g(\varepsilon_X)$ est une rétraction commune de η_{gX} et de $g(a)$.*

Démonstration. On a $f(\eta_{gX}) \circ a = \delta_X \circ a = \varphi(a) \circ a = fg(a) \circ a$ par coassociativité ; $\varepsilon_X \circ a = 1_X$ par l'axiome de coünité ; $\varepsilon_{fgX} \circ f(\eta_{gX}) = 1$ par l'identité triangulaire en gX ; et $\varepsilon_{fgX} \circ fg(a) = a \circ \varepsilon_X$ par naturalité de ε. Enfin $g(\varepsilon_X) \circ g(a) = g(\varepsilon_X \circ a) = 1$ et $g(\varepsilon_X) \circ \eta_{gX} = 1$. □

Lemme 26.3. *Supposons que, pour toute coalgèbre (X, a), la double flèche $(\eta_{gX}, g(a))$ ait un noyau $e_X : R(X, a) \to gX$ et que f y commute.*

1. *Pour tout $Y \in A$, $t \mapsto t^\flat$ induit une bijection entre les morphismes de coalgèbres $hY \to (X, a)$ et les flèches $k : Y \to R(X, a)$, par $t^\flat = e_X \circ k$.*
2. *Pour toute coalgèbre (X, a), la flèche $\theta = \varepsilon_X \circ f(e_X)$ est un isomorphisme de coalgèbres de $h(R(X, a))$ sur (X, a) ; en particulier h est essentiellement surjectif.*
3. *Si de plus f est conservatif, h est une équivalence.*

Démonstration. (1) Soit $t : fY \to X$. Les transposées des deux membres de $a \circ t = \varphi(t) \circ f(\eta_Y)$ sont $g(a) \circ t^\flat$ et, puisque $\varphi(t) \circ f(\eta_Y) = f(t^\flat)$, $gf(t^\flat) \circ \eta_Y = \eta_{gX} \circ t^\flat$ par naturalité de η. La transposition étant bijective, t est un morphisme de coalgèbres si et seulement si $t^\flat$ égalise $(\eta_{gX}, g(a))$, c'est-à-dire se factorise, de façon unique, par e_X.

(2) Posons $E = R(X, a)$. Par (1) appliqué à $k = 1_E$, la flèche θ, de transposée e_X, est un morphisme de coalgèbres $hE \to (X, a)$, et $a \circ \theta = \varphi(\theta) \circ f(\eta_E) = f(\theta^\flat) = f(e_X)$. Or a est un noyau de $(f(\eta_{gX}), fg(a))$ par les lemmes 26.1 et 26.2, et $f(e_X)$ en est un par hypothèse ; donc θ est un isomorphisme. Son inverse est un morphisme de coalgèbres :

$$\varphi(\theta^{-1}) \circ a = \varphi(\theta^{-1}) \circ a \circ \theta \circ \theta^{-1} = \varphi(\theta^{-1}) \circ \varphi(\theta) \circ f(\eta_E) \circ \theta^{-1} = f(\eta_E) \circ \theta^{-1}.$$

(3) Soit $Y' \in A$. La flèche $\eta_{Y'}$ égalise $(\eta_{gfY'}, gf(\eta_{Y'}))$, par naturalité de η ; c'est la double flèche attachée à la coalgèbre $hY' = (fY', f(\eta_{Y'}))$, et l'on a donc $\eta_{Y'} = e_{hY'} \circ k_{Y'}$ pour une flèche $k_{Y'} : Y' \to R(hY')$. Appliquons f : $f(\eta_{Y'})$ est un noyau de l'image de cette double flèche (lemmes 26.1 et 26.2, avec $a = f(\eta_{Y'})$), $f(e_{hY'})$ aussi par hypothèse, et $f(e_{hY'}) \circ f(k_{Y'}) = f(\eta_{Y'})$; donc $f(k_{Y'})$ est un isomorphisme, et $k_{Y'}$ aussi, f étant conservatif. Pour $\psi : Y \to Y'$, la transposée de $h(\psi) = f(\psi)$ est $gf(\psi) \circ \eta_Y = \eta_{Y'} \circ \psi = e_{hY'} \circ (k_{Y'} \circ \psi)$: dans la bijection (1),

$h(\psi)$ correspond à $k_{Y'} \circ \psi$. Comme $\psi \mapsto k_{Y'} \circ \psi$ est bijective, h est pleinement fidèle ; il est essentiellement surjectif par (2), c'est donc une équivalence. □

Démonstration de a) et de la suffisance de b). Si f vérifie la condition C, chaque double flèche $(\eta_{gX}, g(a))$ a un noyau auquel f commute, puisque son image a un noyau (lemmes 26.2 et 26.1). Le lemme 26.3 (2) donne alors a) sous la forme de la marge, et la forme du texte s'en déduit, car si tous les noyaux existent dans A et que f y commute, la condition C est vérifiée. Si de plus f est conservatif, h est une équivalence par le lemme 26.3 (3). □

La nécessité de b) est fausse. Soit B la catégorie des couples d'ensembles (X, Y), et A la sous-catégorie pleine des couples tels que $Y \neq \varnothing$ entraîne $X \neq \varnothing$; f est l'inclusion. Posons $g(X, Y) = (X, Y)$ si $X \neq \varnothing$ et $g(X, Y) = (\varnothing, \varnothing)$ sinon ; $g(X, Y)$ est dans A. Pour $(X', Y') \in A$, une flèche $(p, q) : (X', Y') \to (X, Y)$ de B se factorise de façon unique par $g(X, Y) \to (X, Y)$: si $Y' \neq \varnothing$, alors $X' \neq \varnothing$, donc $X \neq \varnothing$; si $Y' = \varnothing$, q est l'application vide. Ainsi $f \dashv g$, et f est une inclusion coréflexive. Une telle inclusion est pleinement fidèle, donc conservative, et elle est comonadique, résultat classique : la comonade est idempotente, et ses coalgèbres sont, à isomorphisme près, les objets de A. Le foncteur h est donc une équivalence.

Mais f ne vérifie pas la condition C. Soient $u, v : (*, *) \rightrightarrows (\{0, 1\}, *)$ les flèches de A qui envoient le point de la première composante sur 0 et sur 1 et sont l'identité sur la seconde. Leur noyau dans B existe, c'est $(\varnothing, *)$. Si $K \to (*, *)$ était un noyau de (u, v) dans A auquel f commute, K serait isomorphe à $(\varnothing, *)$, de seconde composante non vide ; étant dans A, il aurait un point x dans sa première composante, et u et v l'enverraient sur le même élément, c'est-à-dire $0 = 1$: c'est absurde. Le noyau de (u, v) dans A est $(\varnothing, \varnothing)$, et f n'y commute pas. □

Énoncé (Théorème de Beck, forme exacte)**.** *Le foncteur h est une équivalence si et seulement si f est conservatif et si, pour toute double flèche f-scindée (u, v) de A, $\mathrm{Ker}(u, v)$ existe et f y commute.*

L'équivalence est démontrée dans le fichier de la section (`beck_iff`), à partir des deux implications que mathlib contient séparément.

Une base produit. Les pages 7 à 11 reprennent la comonade d'une adjonction quand la base est un produit $B = \prod_{i \in I} B_i$: f est une famille $f_i : A \to B_i$, g envoie (X_i) sur $\prod_i g_i(X_i)$, et la page pose $\varphi_{ji} = f_j g_i$ en supposant « que les f_j commutent aux produits de type I (p. ex. f_j exacts ; ou I fini) » (19, lot 1, p. 7). Les données de la comonade y deviennent (3.9) $\bar{\alpha}_k = \alpha_k(X_k) \circ \mathrm{pr}_k$ et $\bar{\lambda}_{kji} = \lambda_{kji}(X_i) \circ \mathrm{pr}_i$, avec $\lambda_{kji} : \varphi_{ki} \to \varphi_{kj}\varphi_{ji}$ venu de l'unité $\mathrm{id} \to g_j f_j$; la marge note que λ_{iii} est λ_i, et le cas de deux facteurs, g', g'' pleinement fidèles, ne laisse que φ', φ'', λ', λ'' (19, lot 1, p. 9). On se donne ici des adjonctions $f_i \dashv g_i$, $f_i : A \to B_i$, et l'on suppose que A a les produits indexés par I ; on note η_i, ε_i leurs unités et coünités, pr_i les projections de $\prod_i g_i(X_i)$, et $\lambda_{kji}(X) = f_k(\eta_{j, g_i X}) : f_k g_i X \to f_k g_j f_j g_i X$.

Énoncé (Pages 7 et 8, la matrice de la comonade ♦)**.**

1. *Le foncteur $f = (f_i) : A \to \prod_i B_i$ est adjoint à gauche de g, $g((X_i)) = \prod_i g_i(X_i)$; l'unité a pour composantes les η_i, et la coünité en (X_i) a pour composante j la flèche $\varepsilon_{j, X_j} \circ f_j(\mathrm{pr}_j)$.*
2. *Si f_j commute aux produits indexés par I, la composante j de $\varphi((X_i))$ est un produit des $\varphi_{ji}(X_i)$, de projections les $f_j(\mathrm{pr}_i)$.*
3. *Sans autre hypothèse, la coünité de φ a pour composante k la flèche $\varepsilon_{k, X_k} \circ f_k(\mathrm{pr}_k)$, et la composante k de la comultiplication δ vérifie, pour tous j et i,*

$$f_k g_j f_j(\mathrm{pr}_i) \circ f_k(\mathrm{pr}_j) \circ \delta_k = \lambda_{kji}(X_i) \circ f_k(\mathrm{pr}_i) :$$

c'est (3.9). Si tous les f_j commutent aux produits indexés par I, ces égalités caractérisent δ_k.

4. *Pour $i=j=k$, λ_{iii} est la comultiplication de la comonade $\varphi_i = f_i g_i$.*

L'adjonction du point 1, et la comonade vue comme une matrice de foncteurs $\varphi_{ji} = f_j g_i : B_i \to B_j$ (ici pour $I=\{1,2\}$) :

$$A \underset{g=\prod_i g_i}{\overset{f=(f_i)}{\rightleftarrows}} \prod_i B_i \qquad \varphi \leftrightarrow \begin{pmatrix} f_1g_1 & f_1g_2 \\ f_2g_1 & f_2g_2 \end{pmatrix}.$$

Démonstration. (1) La bijection $\mathrm{Hom}(fY,(X_i)) = \prod_i \mathrm{Hom}(f_iY,X_i) \simeq \prod_i \mathrm{Hom}(Y,g_iX_i) \simeq \mathrm{Hom}(Y,\prod_i g_iX_i)$ est naturelle en Y et en (X_i), composante par composante ; l'unité est l'image de l'identité, c'est-à-dire la flèche de composantes $\eta_{i,Y}$, et la coünité l'image réciproque de l'identité, de composante j la transposée de pr_j, soit $\varepsilon_{j,X_j} \circ f_j(\mathrm{pr}_j)$.

(2) Le cône (pr_i) est un produit dans A, et f_j envoie un produit sur un produit : le cône $(f_j(\mathrm{pr}_i))$ de sommet $f_j(\prod_i g_iX_i)$ est un produit de la famille $f_jg_i(X_i)$.

(3) La coünité de φ est celle de l'adjonction, calculée en (1). La composante k de δ est $f_k(\eta_{gX})$, où η est l'unité de (1), dont la composante j est η_j. Donc δ_k suivie de $f_k(\mathrm{pr}_j)$ puis de $f_kg_jf_j(\mathrm{pr}_i)$ vaut $f_k\big(g_jf_j(\mathrm{pr}_i)\circ\eta_{j,gX}\big) = f_k\big(\eta_{j,g_iX_i}\circ\mathrm{pr}_i\big)$, par naturalité de η_j, c'est-à-dire $\lambda_{kji}(X_i)\circ f_k(\mathrm{pr}_i)$. Si les f_j commutent aux produits indexés par I, $f_k(\prod_j g_jf_jgX)$ est un produit de projections $f_k(\mathrm{pr}_j)$; g_j, adjoint à droite, commute aux produits, si bien que $f_kg_jf_j(\prod_i g_iX_i)$ est un produit de projections $f_kg_jf_j(\mathrm{pr}_i)$. Deux flèches qui ont les mêmes composées avec toutes ces projections sont égales.

(4) $\lambda_{iii}(X) = f_i(\eta_{i,g_iX})$ est, par définition, la comultiplication de f_ig_i. □

Énoncé (Pages 7 à 9, les cas dégénérés et les deux facteurs ♦). *Supposons les g_i pleinement fidèles.*

1. *$\varepsilon_i : \varphi_{ii} \to \mathrm{id}_{B_i}$ est un isomorphisme ; λ_{kki} et λ_{kjj} sont des isomorphismes pour tous i,j,k.*
2. *Pour $i \neq j$, $\lambda_{iji} = \lambda' \circ \varepsilon_i$, où $\lambda' = \lambda_{iji}\circ\varepsilon_i^{-1} : \mathrm{id}_{B_i} \to \varphi_{ij}\varphi_{ji}$.*
3. *Pour deux facteurs, $B = B'\times B''$, $\varphi' = f'g''$, $\varphi'' = f''g'$: si f' commute aux produits binaires, la composante B' de $\varphi(X',X'')$ est un produit de X' et de $\varphi'(X'')$, de projections $\varepsilon'_{X'}\circ f'(\mathrm{pr}')$ et $f'(\mathrm{pr}'')$; de même, si f'' y commute, la composante B'' est un produit de $\varphi''(X')$ et de X''.*

Démonstration. (1) Un adjoint à droite pleinement fidèle a une coünité inversible. L'identité triangulaire $\varepsilon_{k,f_kY}\circ f_k(\eta_{k,Y}) = 1$ montre alors que $f_k(\eta_{k,Y})$ est l'inverse de ε_{k,f_kY} ; avec $Y = g_iX$, c'est $\lambda_{kki}(X)$. L'autre identité, $g_j(\varepsilon_{j,X})\circ\eta_{j,g_jX} = 1$, montre que η_{j,g_jX} est l'inverse de $g_j(\varepsilon_{j,X})$, et $\lambda_{kjj}(X) = f_k(\eta_{j,g_jX})$ est inversible.

(2) C'est la définition de λ'.

(3) Par (2) de l'énoncé précédent, la composante B' de $\varphi(X',X'')$ est un produit de $f'g'(X')$ et de $f'g''(X'')$; remplacer la première projection par sa composée avec l'isomorphisme $\varepsilon'_{X'}$ donne encore un produit, de facteurs X' et $\varphi'(X'')$. De même pour B''. □

Contre-exemple 26.4 (Page 7, « ou I fini » ♦). *Il existe des adjonctions $f_i \dashv g_i$, avec I à deux éléments, pour lesquelles la composante j de $\varphi((X_i))$ n'est isomorphe au produit des $\varphi_{ji}(X_i)$ pour aucun choix d'isomorphisme.*

Démonstration. Prenons $I = \{0,1\}$, $A = B_0 = B_1$ la catégorie des ensembles, $f_i(Y) = \{0,1\} \times Y$ et $g_i(X) = X^{\{0,1\}}$, l'adjonction étant la curryfication, et $X_0 = X_1 = *$. Alors $g_i(*) = *$, $\prod_i g_i(X_i) = *$ et la composante j de $\varphi(X)$ est $\{0,1\} \times *$, à deux éléments, tandis que $\prod_i \varphi_{ji}(X_i) = (\{0,1\} \times *)^2$ en a quatre. □

Remarque. La page suppose que les f_j commutent aux produits indexés par I : c'est l'hypothèse qui sert, et elle suffit. Elle en donne deux exemples. Le premier est juste : un foncteur exact à gauche commute aux produits finis. Le second est faux : un adjoint à gauche ne commute pas en général aux produits finis, et l'exemple ci-dessus est un cas où la formule $\mathrm{pr}_j \varphi((X_i)) = \prod_i \varphi_{ji}(X_i)$ est fausse avec I fini. La lecture reprend la parenthèse de la page (« ce qui est automatique si I est fini, ou si les f_j sont exacts »). Il faut l'exactitude, ou directement la commutation aux produits.

Remarque. Les formules (3.9) ne demandent aucune hypothèse : elles décrivent les composées de la coünité et de la comultiplication avec les projections. La commutation des f_j aux produits sert seulement à en déduire que ces données forment une matrice, c'est-à-dire qu'elles déterminent φ et δ. Les cas « dégénérés » de la page 8, $i = j$ ou $j = k$, sont, pour des g_i pleinement fidèles, ceux où λ_{kji} est un isomorphisme ; il ne reste donc, pour deux facteurs, que λ' et λ''. La formule $\varphi(X', X'') = (X' \times \varphi'(X''), \varphi''(X') \times X'')$ demande encore que f' et f'' commutent aux produits binaires, condition que la page tire de son hypothèse générale.

Énoncé (Pages 14 et 15 ; théorème de Gabriel–Popescu ♦ 4)**.** *Soient C une catégorie de Grothendieck, U un générateur de C et $R = \mathrm{End}_C(U)$. Le foncteur $\mathrm{Hom}_C(U, -) : C \to \mathbf{Mod}_R$, à valeurs dans les R-modules à droite, est pleinement fidèle, et son adjoint à gauche $- \otimes_R U$ est exact.*

Démonstration. La fidélité de $\mathrm{Hom}_C(U, -)$ est la définition d'un générateur. La pleine fidélité et l'exactitude à gauche de $- \otimes_R U$ sont le théorème de Gabriel–Popescu, publié par Popescu et Gabriel en 1964 [108], que la preuve vérifiée invoque ; l'exactitude à droite vient de ce que $- \otimes_R U$ est un adjoint à gauche. □

Remarque. Sous la forme de la marge, a) n'utilise que la condition C, et non la conservativité ; la suffisance de b) est le théorème de comonadicité de Beck, dual du théorème de monadicité (Mac Lane 1998, § VI.7, théorème 1 [93]).

Remarque. L'erreur est sur la page : elle affirme la nécessité de b) par « il faut et il suffit », alors que l'exemple ci-dessus est une adjonction comonadique dont l'adjoint à gauche ne vérifie pas la condition C. La condition b) ne coïncide donc pas avec le théorème de Beck sous sa forme exacte, qui caractérise les adjonctions comonadiques par une condition nécessaire et suffisante.

Remarque. Toute double flèche f-scindée est une double flèche dont l'image a un noyau (lemme 26.1), et la réciproque est fausse. La condition C est donc plus forte que celle de Beck : suffisante, elle n'est pas nécessaire.

Remarque. Pour un générateur seul, la page affirme une équivalence $C \simeq \mathbf{Mod}_R$. Seul le plongement pleinement fidèle est acquis, et la lecture retient cette forme.

Remarque. Le théorème sert en théorie des topos sous sa forme comonadique. Pour un morphisme de topos $u : E \to F$ dont l'image inverse u^* est conservative (un morphisme surjectif), u^* est adjoint à gauche de u_*, conservatif et exact à gauche, donc commute à tous les noyaux ; le théorème 1.12, sous la forme de la marge, et le lemme 5.1 identifient alors F à la catégorie des coalgèbres de la comonade $u^* u_*$ sur E. C'est la descente le long d'un morphisme surjectif, dont la page 34 de la cote 161-2 note un critère (section 5). Cette application est de l'édition ; elle n'est pas formalisée, mathlib n'ayant pas les morphismes de topos.

Chaînes d'adjoints (pages 79 et 80). La page 80 prolonge une chaîne d'adjoints vers le bas par les foncteurs $f_!, f^*, f_*, f^!, \ldots$, énonce une Proposition, puis pose une Question : « Peut-on trouver une suite infinie dans les deux directions ? » La phrase s'achève page 81 sur une ébauche illisible (19, lot 4, p. 80). La clause « dont aucun n'est pl. fid. » est une insertion interlinéaire. Pour un foncteur u entre petites catégories, u^* désigne la restriction des préfaisceaux d'ensembles le long de u.

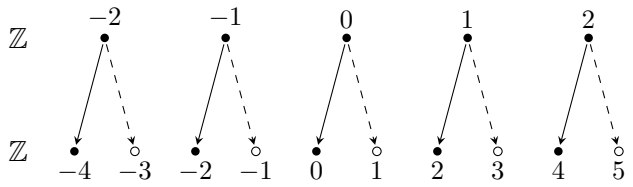
Théorème 26.5 (Grothendieck, page 80, Proposition ♦). *Pour tout n, il existe une petite catégorie C et n foncteurs $\widehat{C} \to \widehat{C}$, chacun adjoint à droite du précédent, dont aucun n'est pleinement fidèle.*

Théorème 26.6 (Page 80, la Question, énoncé de l'édition ♦). *Soit $C = \mathbb{Z} \sqcup \mathbb{Z}$, réunion disjointe de deux copies de l'ensemble ordonné $\mathbb{Z}$. Il existe des foncteurs $F_k : \widehat{C} \to \widehat{C}$, $k \in \mathbb{Z}$, avec $F_k \dashv F_{k+1}$ pour tout k, dont aucun n'est fidèle, donc aucun pleinement fidèle. La Question de la page a donc une réponse positive, pour des topos de préfaisceaux sur une petite catégorie.*

Démonstration. Sur $\mathbb{Z}$, posons $e_m(x) = 2x + m$ et $r_m(x) = \lfloor (x-m)/2 \rfloor$. On a $2x + m \leqslant y \iff x \leqslant \lfloor (y-m)/2 \rfloor$ et $\lfloor (x-m)/2 \rfloor \leqslant y \iff x \leqslant 2y + m + 1$, d'où la chaîne de correspondances de Galois $e_m \dashv r_m \dashv e_{m+1}$, infinie dans les deux sens. Sur C, soient $B_{2m} = e_m \sqcup r_m$ et $B_{2m+1} = r_m \sqcup e_{m+1}$; alors $B_k \dashv B_{k+1}$ pour tout k. Une adjonction $u \dashv v$ entre petites catégories donne $u^* \dashv v^*$ sur les préfaisceaux, et l'on pose $F_k = B_k^*$.

Chaque B_k agit sur l'une des deux copies par un e_m, dont l'image évite une classe de parité. Soit q un point de cette copie hors de l'image, et $p = q - 1$: tout $B_k(c) \leqslant q$ vérifie $B_k(c) \leqslant p$, et $q \not\leqslant p$. Soient h_q le préfaisceau représenté par q et G le préfaisceau $x \mapsto \{b \in \{0,1\} : x \leqslant p \Rightarrow b = 0\}$, dont les restrictions remplacent b par 0 au-dessous de p. Les deux morphismes $h_q \to G$ de valeurs 0 et 1 en q sont distincts, et leurs restrictions par B_k coïncident, puisque ces restrictions ne voient que des points au-dessous de p. Donc F_k n'est pas fidèle. La Proposition s'obtient en prenant $F_0, \ldots, F_{n-1}$ (Lean : `proposition_page80`, `chain_adj`, `chain_not_fullyFaithful`). □

Sur une copie de $\mathbb{Z}$, la chaîne $\cdots \dashv r_{-1} \dashv e_0 \dashv r_0 \dashv e_1 \dashv r_1 \dashv \cdots$ se lit sur la figure suivante : e_0 (en trait plein) envoie x sur $2x$, e_1 (en tirets) sur $2x+1$, et r_0 renvoie $2x$ et $2x+1$ sur x. L'image de e_0 évite les impairs (cercles blancs) : c'est le point q de la démonstration.



Sur $C = \mathbb{Z} \sqcup \mathbb{Z}$, les deux copies sont décalées d'un cran : $B_{2m} = e_m \sqcup r_m$ et $B_{2m+1} = r_m \sqcup e_{m+1}$, de sorte que chaque B_k agit sur l'une des copies par un e.

Remarque. La réunion disjointe est nécessaire : sur une seule copie de $\mathbb{Z}$, un e_m^* sur deux est pleinement fidèle, puisque $r_m e_m = \mathrm{id}$. Les deux copies décalées d'un cran font qu'aucun F_k ne l'est. Une note de la lecture, à la page 81, tient une chaîne infinie dans les deux sens pour impossible « dans des situations très générales » ; l'exemple montre qu'elle existe entre topos de préfaisceaux. La suggestion de la page, un g à la fois adjoint à gauche et à droite de f, n'est pas celle suivie ici.

Ne sont pas démontrés ici : l'énoncé de Morita (équivalence si et seulement si U est petit et projectif) ; la Conclusion des pages 4 à 6 (adjonctions et comonades) ; la reconstruction de l'adjonction ; les topos de coalgèbres (page 6) ; dans le cas dégénéré des pages 10 et 11, l'équivalence de l'intersection des images essentielles de g' et g'' avec la sous-catégorie pleine de B' où λ' est inversible, et les trois conditions équivalentes pour qu'elle soit ponctuelle ; les pages 7 à 95 (résolutions standard, cohomologie relative, SGA 4, localisation, recollement, catégories fibrées).

Théorème 26.7 (Grothendieck, pages 7 à 11, comonade sur une base produit ♦). *On reprend les adjonctions $f_i \dashv g_i$, $f_i : A \to B_i$, A ayant les produits indexés par I.*

1. *Sans autre hypothèse, la matrice $(\varphi_{ji}, \varepsilon_i, \lambda_{kji})$ vérifie les relations de coünité et de coassociativité :*

$$\varphi_{ki}(\varepsilon_i) \circ \lambda_{kii} = 1, \qquad \varepsilon_k \varphi_{ki} \circ \lambda_{kki} = 1, \qquad \varphi_{lk}(\lambda_{kji}) \circ \lambda_{lki} = \lambda_{lkj} \varphi_{ji} \circ \lambda_{lji}.$$

2. *Si les f_j commutent aux produits indexés par I, une flèche $a : X \to \varphi X$, d'entrées $u_{ki} = f_k(\mathrm{pr}_i) \circ a_k : X_k \to \varphi_{ki}(X_i)$, est une coalgèbre si et seulement si $\varepsilon_k \circ u_{kk} = 1$ et $\lambda_{kji}(X_i) \circ u_{ki} = \varphi_{kj}(u_{ji}) \circ u_{kj}$ pour tous k, j, i ; une flèche $t : X \to Y$ vers une coalgèbre (Y, b) d'entrées v_{ki} est un morphisme de coalgèbres si et seulement si $v_{ki} \circ t_k = \varphi_{ki}(t_i) \circ u_{ki}$ pour tous k, i.*
3. *Deux facteurs, $B = B' \times B''$, g' et g'' pleinement fidèles, f' et f'' commutant aux produits binaires : la catégorie des φ-coalgèbres est équivalente à celle des quadruplets (X', X'', u', u''), $u' : X' \to \varphi'(X'')$, $u'' : X'' \to \varphi''(X')$, tels que*

$$\lambda'(X') = \varphi'(u'') \circ u', \qquad \lambda''(X'') = \varphi''(u') \circ u'',$$

un morphisme de quadruplets étant un couple (t', t'') qui commute à u' et à u''. Si de plus $f = (f', f'')$ est comonadique, A est équivalente à la catégorie des quadruplets, par $Y \mapsto (f'Y, f''Y, f'(\eta''_Y), f''(\eta'_Y))$.

Démonstration. (1) Avec $\lambda_{kji}(X) = f_k(\eta_{j,g_iX})$, la première relation est f_k appliqué à l'identité triangulaire $g_i(\varepsilon_{i,X}) \circ \eta_{i,g_iX} = 1$, la deuxième est l'identité triangulaire $\varepsilon_{k,f_kY} \circ f_k(\eta_{k,Y}) = 1$ en $Y = g_iX$. Les deux membres de la troisième sont f_l appliqué à $g_k f_k(\eta_{j,g_iX}) \circ \eta_{k,g_iX}$ et à $\eta_{k,g_jf_jg_iX} \circ \eta_{j,g_iX}$, égaux par naturalité de η_k (Lean : `lam_counit_right`, `lam_counit_left`, `lam_coassoc`).

(2) La coünité de φ a pour composante k la flèche $\varepsilon_k \circ f_k(\mathrm{pr}_k)$ (énoncé des pages 7 et 8, point 3) : la condition de coünité, composante par composante, est $\varepsilon_k \circ u_{kk} = 1$, et ceci sans hypothèse. Pour la coassociativité, on compose les deux membres de $\delta \circ a = \varphi(a) \circ a$, en la composante k, avec les flèches $f_k g_j f_j(\mathrm{pr}_i) \circ f_k(\mathrm{pr}_j)$. Le membre de gauche donne $\lambda_{kji}(X_i) \circ u_{ki}$ par (3.9). Celui de droite donne $\varphi_{kj}(u_{ji}) \circ u_{kj}$, puisque $\varphi(a)$ suivi de $f_k(\mathrm{pr}_j)$ vaut $f_k g_j(a_j) \circ f_k(\mathrm{pr}_j)$. Ces flèches séparent les morphismes à valeurs dans $(\varphi^2 X)_k$ quand les f_j commutent aux produits (même argument que pour (3.9)). Les morphismes se traitent de même avec les seules projections $f_k(\mathrm{pr}_i)$ (Lean : `counit_iff`, `coassoc_iff`, `hom_iff`).

(3) Les g_i étant pleinement fidèles, ε_i est inversible et la coünité impose $u_{kk} = \varepsilon_k^{-1}$: c'est en ce sens que « l'axiome de coünité est automatiquement satisfait ». Il reste les deux entrées croisées $u' = u_{12}$ et $u'' = u_{21}$. Des huit relations de coassociativité, celles où $j = i$ se réduisent à $\lambda_{kii} = \varphi_{ki}(\varepsilon_i^{-1})$, conséquence de (1) ; celles où $k = j \neq i$ à $\lambda_{kki} = \varepsilon_k^{-1} \varphi_{ki}$ et à la naturalité de

ε_k^{-1} ; les deux qui restent, $k = i \neq j$, sont exactement les deux triangles, puisque $\lambda' = \lambda_{iji} \circ \varepsilon_i^{-1}$. Dans l'autre sens, un quadruplet donne une flèche a dont la composante k a pour entrées $u_{kk} = \varepsilon_k^{-1}$, u', u'', ce qui la définit puisque $(\varphi X)_k$ est un produit des $\varphi_{ki}(X_i)$, et (2) montre que c'est une coalgèbre. Le foncteur des coalgèbres vers les quadruplets, qui retient les entrées croisées, est donc fidèle, plein (les conditions diagonales sur un morphisme sont la naturalité de ε_k^{-1}) et essentiellement surjectif. Si f est comonadique, on le compose avec le foncteur de comparaison h ; l'entrée u' de $h(Y)$ est $f'(\mathrm{pr}'') \circ f'(\eta_Y) = f'(\eta''_Y)$ (Lean : `versQuadruplets_isEquivalence`, `quadruplets`, `quadruplet_u'`, `quadruplet_u''`). □

Remarque. Le manuscrit écrit « il semble qu'on trouve » et biffe le calcul : il est juste, à condition d'ajouter l'hypothèse que la page tient de son cadre général, la commutation de f' et f'' aux produits binaires, et, pour décrire A elle-même et non les coalgèbres, la comonadicité de f, qui est le propos du théorème 1.12. Le cas dégénéré qui suit (pages 10 et 11) fait l'objet du théorème 26.8.

Théorème 26.8 (Grothendieck, pages 10 et 11, le cas dégénéré ♦). *On se place dans la situation du point (3) du théorème 26.7, $f = (f', f'')$ comonadique, et l'on note $\Phi : A \to \mathrm{Quad}$, $Y \mapsto (f'Y, f''Y, f'(\eta''_Y), f''(\eta'_Y))$, l'équivalence qu'il fournit.*

1. *Si $\varphi'\varphi''$ et $\varphi''\varphi'$ sont à valeurs finales, tout (X', X'', u', u'') est un quadruplet : les deux triangles sont sans contenu.*
2. *Sans hypothèse de dégénérescence, un quadruplet Q est dans l'image essentielle de $\Phi g'$ si et seulement si u'' est inversible, et dans celle de $\Phi g''$ si et seulement si u' l'est ; de façon équivalente, $Y \in A$ est dans l'image essentielle de g' si et seulement si $f''(\eta'_Y)$ est inversible. Plus généralement, pour I quelconque, g_i pleinement fidèle et $f = (f_j)$ conservatif, Y est dans l'image essentielle de g_i si et seulement si $f_j(\eta_{i,Y})$ est inversible pour tout $j \neq i$.*
3. *L'intersection des deux images essentielles est formée des quadruplets où u' et u'' sont inversibles ; dans le cas dégénéré, X' et X'' y sont finals.*

Démonstration. (1) Les deux membres de chaque triangle sont des flèches vers un objet final (Lean : `Quadruplet.degenere`).

(2) Pour g_i pleinement fidèle, Y est dans l'image essentielle de g_i si et seulement si $\eta_{i,Y}$ est inversible (mathlib : `isIso_unit_app_iff_mem_essImage`). Or $f_i(\eta_{i,Y})$ l'est toujours, par l'identité triangulaire $\varepsilon_{i,f_iY} \circ f_i(\eta_{i,Y}) = 1$ et l'inversibilité de ε_i ; un f conservatif, ce qu'est tout foncteur comonadique, rend donc $\eta_{i,Y}$ inversible dès que les $f_j(\eta_{i,Y})$, $j \neq i$, le sont (Lean : `essImage_iff`, `reflectsIso_of_comonadic`). Pour deux facteurs, $f''(\eta'_Y)$ est l'entrée u'' de $\Phi(Y)$ (`essImage_g'_iff`, `essImage_g''_iff`). Enfin Φ est pleinement fidèle et essentiellement surjective, et un isomorphisme de quadruplets $(t', t'') : P \to Q$ donne $u''_Q \circ t'' = \varphi''(t') \circ u''_P$, avec t' et t'' inversibles, ce qui transporte l'inversibilité (Lean : `Quadruplet.isIso_u''_of_iso`, `essImage_g'_quadruplets`, `essImage_g''_quadruplets`).

(3) La première assertion est la conjonction des deux précédentes (`essImage_inter`). Si u' et u'' sont inversibles, $\varphi'(u'') \circ u' : X' \to \varphi'\varphi''(X')$ l'est, et le but est final ; de même pour X'' (`final_of_inter`). □

Remarque. Le critère de la page, « image essentielle de g' : u'' est un isomorphisme », ne dépend pas de la dégénérescence : il vaut dès que g', g'' sont pleinement fidèles et f comonadique.

Restent non formalisées l'équivalence de l'intersection avec la sous-catégorie pleine de B' où λ' est inversible et les trois conditions équivalentes pour que cette intersection soit ponctuelle.

27 Cote 133 : le centre et le groupe dérivé vus par deux modules croisés [28]

La cote 133, *[Groupes de Witt et formes quadratiques, groupes formels] : notes manuscrites (s.d.), tirés à part (1974)*, que l'inventaire date « 1974-[à partir de 1975] », réunit sept suites distinctes. La dernière, sous une chemise titrée « Fourbis auxiliaires cohomologiques pour groupes formels » (page 44), occupe les pages 45 à 53, qu'il pagine de 1 à 7 ; les pages 47 et 49 ne sont pas de sa main. Elle traite en général le problème que la « Solution » des pages 35 et 36 pose pour un groupe formel : décrire un groupe G par son centre et son groupe dérivé. La page 45 se donne deux modules croisés $\mathcal{C} = (N \to M)$ et $\mathcal{C}' = (N' \to M')$ de mêmes invariants π_0, π_1, et note $K = G/\pi_1$ (133, lot 3, p. 45). La page 46 définit $\mathfrak{Z} = [\mathrm{Cent}(K)/(N'/\pi_1)] \cap \mathrm{Ker}\,\Theta$, construit φ_G puis Ψ_G, et encadre « Ψ_G injectif » comme équivalent à $N' = \mathrm{Cent}(G)$ (133, lot 3, p. 46). La page 48 définit l'accouplement c_E d'une extension centrale E de π_0 par π_1 et écrit « On doit trouver, au signe près » $\Psi_{G_1} = \Psi_G + \tilde{c}_E\,\alpha$ (133, lot 3, p. 48). Les pages 51 et 52 définissent $\mathcal{D} = (N_{\mathrm{ab}})_M$ et λ_G, et écrivent $N/DG \simeq \mathcal{D}/\lambda_G(\pi_0 \otimes \pi_0)$ et $\lambda_{G_1} = \lambda_G + \beta c_E$ (133, lot 3, p. 51, 133, lot 3, p. 52). Malgré le titre, rien n'y est propre aux groupes formels, et les énoncés sont démontrés ici pour des groupes abstraits.

Conventions. Le commutateur est $[x, y] = xyx^{-1}y^{-1}$. Dans tout ce qui suit, G est un groupe, N et N' deux sous-groupes distingués, avec $N' \subset \mathrm{Cent}(G)$; alors $[N, N'] = 1$, $\pi_1 = N \cap N'$ est central, $\pi_0 = G/NN'$, $K = G/\pi_1$, $M = G/N'$ agit sur N par conjugaison, et $\Theta : M \to \mathrm{Aut}(N)$ est cette action. Le groupe $\mathfrak{Z}$ est pris par son image inverse $\overline{N'}$ dans G : les $z \in G$ dont l'image dans K est centrale et qui commutent à tout élément de N, c'est-à-dire tels que $[g, z] \in \pi_1$ pour tout $g \in G$ et $nz = zn$ pour tout $n \in N$. On a $N' \subset \overline{N'}$ et $\mathfrak{Z} = \overline{N'}/N'$.

Lemme 27.1. *Si c est central dans un groupe, $[g, zc] = [g, z]$ et $[gc, z] = [g, z]$.*

Démonstration. $[g, zc] = gzcg^{-1}c^{-1}z^{-1} = gzg^{-1}cc^{-1}z^{-1} = [g, z]$, en faisant passer c devant g^{-1}. La seconde s'en déduit par $[x, y]^{-1} = [y, x]$. □

Théorème 27.2 (Grothendieck, page 46, l'injectivité de Ψ_G ♦). *Pour $z \in \overline{N'}$, l'application $g \mapsto [g, z]$ définit un homomorphisme $\varphi_G(z) : \pi_0 \to \pi_1$, qui ne dépend que de la classe de z dans $\mathfrak{Z}$; l'application $\Psi_G : \mathfrak{Z} \to \mathrm{Hom}(\pi_0, \pi_1)$ ainsi définie est un homomorphisme, et*

$$N' = \mathrm{Cent}(G) \iff \Psi_G \text{ est injectif.}$$

Démonstration. Soit $z \in \overline{N'}$. Par définition $[g, z] \in \pi_1$, donc $[g, z]$ est central. On a $[gh, z] = g\,[h, z]\,zg^{-1}z^{-1}$; comme $[h, z]$ est central, c'est $[h, z]\,[g, z] = [g, z]\,[h, z]$, et $g \mapsto [g, z]$ est un homomorphisme $G \to \pi_1$. Il est trivial sur N, puisque z commute à N, et sur N', qui est central ; il se factorise donc par $\pi_0 = G/NN'$, ce qui définit $\varphi_G(z)$. Si z et w ont même classe modulo N', $w = zc$ avec $c \in N'$ central, et $[g, w] = [g, z]$ par le lemme 27.1 : d'où Ψ_G sur $\mathfrak{Z}$. Il est multiplicatif : $[g, zw] = gzg^{-1}\,[g, w]\,z^{-1} = [g, z]\,[g, w]$, puisque $[g, w]$ est central.

Supposons Ψ_G injectif et soit $c \in \mathrm{Cent}(G)$. Alors $c \in \overline{N'}$, et $\Psi_G(\bar{c})$ est trivial, comme $\Psi_G(1)$: donc $\bar{c} = 1$ dans $\mathfrak{Z}$, c'est-à-dire $c \in N'$. Ainsi $\mathrm{Cent}(G) \subset N'$, et l'égalité vient de $N' \subset \mathrm{Cent}(G)$.

28. Preuve vérifiée : `lean/Grothendieck/Folder133.lean`.

Réciproquement, supposons $N' = \mathrm{Cent}(G)$, et soient $z, w \in \overline{N'}$ avec $\Psi_G(\bar{z}) = \Psi_G(\bar{w})$, c'est-à-dire $[g,z] = [g,w]$ pour tout g. Appliquée à g^{-1}, l'égalité donne $zgz^{-1} = wgw^{-1}$, d'où $g\,z^{-1}w = z^{-1}(zgz^{-1})w = z^{-1}(wgw^{-1})w = z^{-1}w\,g$: $z^{-1}w$ est central, donc dans N', et $\bar{z} = \bar{w}$. □

Remarque. Seule l'hypothèse $N' \subset \mathrm{Cent}(G)$ sert. L'hypothèse $[N, N'] = 1$ que la lecture ajoute en découle, et $N \supset D(G)$ n'intervient pas ici. La vérification confirme les contrôles d'additivité et de nullité que donne la lecture et que la page résume par « triviale sur N' et sur $\mathfrak{Z}$ ». En chemin, elle établit que $\mathrm{Cent}(G)$ est l'image inverse de $\mathrm{Ker}\,\Psi_G$, point que la page dit « clair ».

On suppose maintenant de plus $D(G) \subset N$. Soit $\mathcal{D} = (N_{\mathrm{ab}})_M$; c'est le quotient $N/[G,N]$, le sous-groupe $[G,N]$ engendré par les $[g,n]$ contenant les $[n,n']$. On note $\bar{n}$ la classe dans $\mathcal{D}$ d'un $n \in N$.

Lemme 27.3. *Le groupe $\mathcal{D}$ est commutatif, G y agit trivialement, et π_0 est commutatif.*

Démonstration. Pour $a, b \in N$, $(ab)^{-1}(ba) = [b^{-1}, a^{-1}] \in [G,N]$, donc $\bar{a}\bar{b} = \bar{b}\bar{a}$. Pour $c \in N$ et $x \in G$, $(xcx^{-1})^{-1}c = [x, c^{-1}] \in [G,N]$, donc $\overline{xcx^{-1}} = \bar{c}$. Pour $x, y \in G$, $(xy)^{-1}(yx) = [y^{-1}, x^{-1}] \in D(G) \subset N \subset NN'$, donc xy et yx ont même image dans π_0. □

Énoncé (Pages 51 et 52, la surjectivité de λ_G ♦). *Supposons $D(G) \subset N$ et $N' \subset \mathrm{Cent}(G)$. L'application $(x,y) \mapsto \overline{[x,y]}$ définit une forme $\lambda_G : \pi_0 \times \pi_0 \to \mathcal{D}$, multiplicative en chaque variable et alternée, et*

$$N = D(G) \iff \lambda_G \text{ est surjectif,}$$

c'est-à-dire si et seulement si les valeurs de λ_G engendrent $\mathcal{D}$.

Démonstration. Pour y fixé, $x \mapsto \overline{[x,y]}$ est un homomorphisme $G \to \mathcal{D}$: $[xx', y] = (x[x',y]x^{-1})[x,y]$, et le lemme 27.3 donne $\overline{[xx',y]} = \overline{[x',y]}\;\overline{[x,y]} = \overline{[x,y]}\;\overline{[x',y]}$. Il est trivial sur N, car $[n,y] = [y,n]^{-1} \in [G,N]$, et sur N', car $[n',y] = 1$ pour n' central ; il se factorise donc par π_0. Comme $\overline{[x,y]} = \overline{[y,x]}^{-1}$, la même chose vaut pour la seconde variable, et λ_G est bien défini sur $\pi_0 \times \pi_0$, multiplicatif en chaque variable ; $[x,x] = 1$ le rend alterné.

Si $N = D(G)$, tout $n \in N$ est produit de commutateurs et de leurs inverses ; sa classe $\bar{n}$ est le produit correspondant de valeurs de λ_G et de leurs inverses, et ces valeurs engendrent $\mathcal{D}$. Réciproquement, les valeurs de λ_G sont des classes d'éléments de $D(G)$, donc le sous-groupe qu'elles engendrent est contenu dans l'image de $D(G)$ dans $\mathcal{D}$. S'il est égal à $\mathcal{D}$, tout $n \in N$ s'écrit $n = m\,(m^{-1}n)$ avec $m \in D(G)$ et $m^{-1}n \in [G,N] \subset D(G)$; donc $N \subset D(G)$, et $N = D(G)$. □

Remarque. Comme $\mathcal{D}$ est commutatif et λ_G bimultiplicatif, λ_G définit une application linéaire $\pi_0 \otimes \pi_0 \to \mathcal{D}$, dont l'image est le sous-groupe engendré par les valeurs de λ_G ; c'est la surjectivité de la page. L'hypothèse $N' \subset \mathrm{Cent}(G)$ est nécessaire à la définition même de λ_G sur π_0, et la lecture la cite (« puisque N' est central »). L'hypothèse plus faible $[N,N'] = 1$ ne suffit pas à l'équivalence. Dans le groupe des quaternions Q_8, avec $N = D(Q_8) = \mathrm{Cent}(Q_8)$, d'ordre 2, et $N' = Q_8$, on a $[N,N'] = 1$ et $\pi_0 = 1$, donc toute forme sur π_0 est nulle, alors que $\mathcal{D} = N/[G,N] = N$ n'est pas trivial (exemple non vérifié en Lean). La commutativité de π_0 découle de $D(G) \subset N$ (lemme 27.3) et n'est pas une hypothèse de plus. L'isomorphisme $N/D(G) \simeq \mathcal{D}/\lambda_G(\pi_0 \otimes \pi_0)$ de la page n'est démontré ici que sous la forme de l'équivalence.

Soient enfin E un groupe, $\iota : \pi_1 \to E$ un homomorphisme injectif d'image centrale, et $q : E \to \pi_0$ un homomorphisme de noyau $\iota(\pi_1)$: une extension centrale de π_0 par π_1, si q est surjectif, ce dont on ne se sert pas. Soit $G \times_{\pi_0} E$ le produit fibré et G_1 son quotient par

l'image antidiagonale $\{(a, \iota(a)^{-1})\}$ de π_1, centrale, prise en Lean par son sous-groupe distingué engendré.

Énoncé (Pages 48 et 52, le changement de G en G_1 ♦). *Supposons $D(G) \subset N$ et $N' \subset \mathrm{Cent}(G)$.*

1. *Pour $e, f \in E$, $[e, f] = \iota(c_E(e, f))$ pour un unique $c_E(e, f) \in \pi_1$, qui ne dépend que des images de e et f dans π_0.*
2. *Dans G_1, le commutateur des classes de (g, e) et (z, f) est la classe de $([g, z]\, c_E(e, f), 1)$.*
3. *En particulier, si $z \in \overline{N'}$, ce commutateur est l'image de $\Psi_G(\bar{z})(\bar{g})\, c_E(e, f) \in \pi_1$; et la classe dans $\mathcal{D}$ de $[x, y]\, c$, pour $c \in \pi_1$, est $\lambda_G(\bar{x}, \bar{y})\, \beta(c)$, où $\beta : \pi_1 \to \mathcal{D}$ est le passage au quotient.*

Démonstration. (1) L'image de $[e, f]$ dans π_0 est le commutateur des images, trivial puisque π_0 est commutatif ; $[e, f]$ est donc dans $\mathrm{Ker}\, q = \iota(\pi_1)$, et ι est injectif. Si e et e' ont même image, $e' = e\, \iota(a)$, et de même $f' = f\, \iota(b)$; comme $\iota(a)$ et $\iota(b)$ sont centraux, le lemme 27.1 donne $[e', f'] = [e, f]$.

(2) Le commutateur de (g, e) et (z, f) dans le produit fibré est $([g, z], [e, f]) = ([g, z], \iota(c))$, $c = c_E(e, f)$, et

$$([g, z], \iota(c))^{-1}\, ([g, z]\, c, 1) = (c, \iota(c)^{-1})$$

est dans l'image antidiagonale de π_1 ; les deux éléments ont donc même classe dans G_1. L'élément $([g, z]\, c, 1)$ est bien dans le produit fibré, $[g, z]\, c$ étant dans N.

(3) Si $z \in \overline{N'}$, $[g, z] = \Psi_G(\bar{z})(\bar{g})$ par définition. La seconde assertion est $\overline{[x, y]\, c} = \overline{[x, y]}\, \bar{c}$. □

Remarque. Ce calcul donne les deux formules de la page, $\Psi_{G_1} = \Psi_G + \tilde{c}_E\, \alpha$ et $\lambda_{G_1} = \lambda_G + \beta c_E$, écrites additivement : dans G_1, un commutateur est le produit du commutateur dans G et de la valeur de c_E. L'ordre des facteurs fixe le signe que la page laisse ouvert (« au signe près »). Avec $[x, y] = xyx^{-1}y^{-1}$ et $\Psi_G(\bar{z})(\bar{g}) = [g, z]$, le terme correctif est $c_E(\bar{g}, \bar{z})$, c'est-à-dire $\tilde{c}_E(\alpha(\bar{z}))$ évalué en $\bar{g}$, au signe près selon le côté où l'on curryfie. L'identification des deux modules croisés de G_1 avec ceux de G n'est pas formalisée ; elle ferait de cette égalité d'éléments une égalité d'applications $\Psi_{G_1} = \Psi_G \cdot \tilde{c}_E\, \alpha$ sur un même $\mathfrak{Z}$.

Ne sont pas démontrés ici : l'identification des modules croisés de G_1 avec ceux de G ; l'isomorphisme $N/D(G) \simeq \mathcal{D}/\lambda_G(\pi_0 \otimes \pi_0)$ au-delà de l'équivalence ; l'obstruction dans H^3 et l'indétermination dans H^2 (page 45) ; les conditions b) et c) des pages 50 à 53 ; la réduction aux formes alternées ; les suites de Witt, les λ-anneaux et les groupes formels (pages 34 à 39), les pages 41 à 43 sur Chevalley.

Exemple 27.4 (Grothendieck, pages 42 et 43, quotient affine non constructible ♦). Sur une base de caractéristique mixte, soit G une extension d'un schéma abélien A par $\mathbb{G}_a$, non triviale en un point y de caractéristique 0 et triviale en une spécialisation s de caractéristique p. Alors $(G_y)_{\mathrm{aff}} = 1$ et $(G_s)_{\mathrm{aff}} \simeq \mathbb{G}_a$: le plus grand quotient affine des fibres d'un schéma en groupes lisse à fibres connexes ne varie pas de façon constructible.

◊ non vérifié en Lean

28 Cote 161-1 : la partie fixe d'une adjonction, les adjonctions idempotentes, les objets locaux [29]

La cote 161-1, *Catégories : notes manuscrites (s.d.)*, dix-neuf pages sans date, appartient au groupe des dossiers rassemblés par Grothendieck sur différentes thématiques, que l'inventaire

29. Preuve vérifiée : `lean/Grothendieck/Folder161_1.lean`.

date « [après 1961-vers 1977] ». Les pages 3 à 7 étudient un couple de foncteurs adjoints $E \rightleftarrows F$ et les équivalences qu'il induit entre des sous-catégories des deux côtés. La page 3 s'ouvre sur « Foncteurs adjoints [demander Schanuel] » et écrit le critère (1) de pleine fidélité sur une sous-catégorie pleine. Elle porte en marge « donner un exemple montrant que cette condition n'est pas surabondante, avec E' réduit à un élément » (161-1, lot 1, p. 3). La page 5 dresse la liste des conditions équivalentes qui définissent aujourd'hui une adjonction idempotente (161-1, lot 1, p. 5). La page 7 se demande si une sous-catégorie réflexive est le lieu des objets locaux pour les flèches que le réflecteur inverse, et conclut « Or c'est vrai sauf erreur… » (161-1, lot 1, p. 7). On note, comme la lecture, u l'adjoint à gauche de v, $\eta : \mathrm{id}_E \to vu$ l'unité et $\varepsilon : uv \to \mathrm{id}_F$ la coünité (le manuscrit écrit i et j).

Énoncé ((1), page 3). *Soient $E' \subset E$ une sous-catégorie pleine et $\overline{E}'$ sa clôture par isomorphie. Alors*

$$u|E' \text{ est pleinement fidèle et } vu(E') \subset \overline{E}'$$
$$\iff \text{pour tout } Y \in E',\ \eta_Y : Y \to vu(Y) \text{ est un isomorphisme.}$$

La seconde condition du membre de gauche n'est pas surabondante : la pleine fidélité de $u|E'$ ne force pas vu à ramener E' dans $\overline{E}'$.

Énoncé (Adjonctions idempotentes, page 5). *Les conditions « $\eta v : v \to vuv$ est un isomorphisme » et « $\varepsilon u : uvu \to u$ est un isomorphisme » de la condition 2 du manuscrit sont redondantes : chacune des quatre conditions (ηv, $v\varepsilon$, εu, $u\eta$ inversible) implique les trois autres.*

Résultat général, démontré en Lean dans
`Upstream/AdjunctionIdempotent.lean` *; la démonstration n'est pas reprise ici.*

Les identités triangulaires disent que les deux composés suivants sont des identités ; dans chaque ligne, une flèche est donc inversible si et seulement si l'autre l'est. L'énoncé ajoute le passage d'une ligne à l'autre.



Énoncé (Objets locaux, pages 6 et 7). *Soient $\alpha : E_1 \to E$ un foncteur pleinement fidèle admettant un adjoint à gauche α', et Σ la classe des flèches de E que α' rend inversibles. Une flèche $f : X \to Y$ est dans Σ si et seulement si $\mathrm{Hom}_E(Y, \alpha Z_1) \to \mathrm{Hom}_E(X, \alpha Z_1)$ est bijective pour tout $Z_1 \in E_1$; et un objet ξ de E tel que $\mathrm{Hom}_E(-, \xi)$ transforme les flèches de Σ en bijections (un objet Σ-local) est dans l'image essentielle de α.*

On rappelle que la bijection d'adjonction $\mathrm{Hom}_F(uX, P) \simeq \mathrm{Hom}_E(X, vP)$ envoie g sur $\eta_X \circ v(g)$ (on compose de gauche à droite : η_X, puis $v(g)$), et qu'on a les identités triangulaires $\eta_{vP} ; v(\varepsilon_P) = \mathrm{id}_{vP}$ et $u(\eta_X) ; \varepsilon_{uX} = \mathrm{id}_{uX}$. Dans les démonstrations qui suivent, on écrit $f ; g$ pour « f puis g ».

Lemme 28.1. *Pour $X, Y \in E$, l'application $\mathrm{Hom}_E(X, Y) \to \mathrm{Hom}_F(uX, uY)$, $f \mapsto u(f)$, est bijective si et seulement si l'application $f \mapsto f ; \eta_Y$, de $\mathrm{Hom}_E(X, Y)$ dans $\mathrm{Hom}_E(X, vuY)$, l'est.*

Démonstration. La seconde application est la composée de la première et de la bijection d'adjonction : celle-ci envoie $u(f)$ sur $\eta_X ; vu(f)$, qui vaut $f ; \eta_Y$ par naturalité de η. C'est la phrase de la page 3 : l'application « se déduit de l'application $i(Y) : Y \to vu(Y)$ au moyen de $\mathrm{Hom}(X, i(Y))$ ». □

Démonstration de (1). Supposons que η_Y soit un isomorphisme pour tout $Y \in E'$. Pour $X, Y \in E'$, la composition avec η_Y est alors bijective, et $u|E'$ est pleinement fidèle par le lemme 28.1 ; et $vu(Y)$, isomorphe à Y, est dans $\overline{E}'$.

Réciproquement, soit $Y \in E'$; par hypothèse il existe $Z \in E'$ et un isomorphisme $e : vu(Y) \to Z$. Le lemme 28.1, appliqué aux couples (Z, Y) et (Y, Y) d'objets de E', dit que $f \mapsto f\,;\eta_Y$ est bijective de $\mathrm{Hom}(Z, Y)$ sur $\mathrm{Hom}(Z, vuY)$ et de $\mathrm{Hom}(Y, Y)$ sur $\mathrm{Hom}(Y, vuY)$. Par la surjectivité de la première, il existe $g : Z \to Y$ avec $g\,;\eta_Y = e^{-1}$. Posons $s = e\,;g : vu(Y) \to Y$. D'une part $s\,;\eta_Y = e\,;e^{-1} = \mathrm{id}_{vuY}$. D'autre part $(\eta_Y\,;s)\,;\eta_Y = \eta_Y\,;(s\,;\eta_Y) = \eta_Y = \mathrm{id}_Y\,;\eta_Y$, et l'injectivité de la seconde bijection donne $\eta_Y\,;s = \mathrm{id}_Y$. Donc η_Y est un isomorphisme, d'inverse s. □

L'exemple demandé en marge. Prenons pour E la catégorie des ensembles, pour F la catégorie ponctuelle, pour u l'unique foncteur $E \to F$ et pour v le foncteur qui pointe un ensemble à un élément $\{*\}$; on a $u \dashv v$ parce que $\{*\}$ est final. Soit $E' = \{\varnothing\}$, réduite à un objet. Alors $u|E'$ est pleinement fidèle, puisque $\mathrm{Hom}(\varnothing, \varnothing)$ et $\mathrm{Hom}(u\varnothing, u\varnothing)$ ont chacun un seul élément ; mais $vu(\varnothing) = \{*\}$ n'est pas isomorphe à $\varnothing$, et $\eta_\varnothing : \varnothing \to \{*\}$ n'est pas un isomorphisme. La condition $vu(E') \subset \overline{E}'$ est donc nécessaire à l'équivalence (1). □

Démonstration de l'énoncé sur les objets locaux. Caractérisation de Σ. Par l'adjonction $\alpha' \dashv \alpha$, $\mathrm{Hom}_E(Y, \alpha Z_1) \simeq \mathrm{Hom}_{E_1}(\alpha' Y, Z_1)$ naturellement en Y, de sorte que la composition avec f à la source correspond à la composition avec $\alpha'(f)$. Par le lemme de Yoneda, $\alpha'(f)$ est un isomorphisme si et seulement si $\mathrm{Hom}_{E_1}(\alpha' Y, Z_1) \to \mathrm{Hom}_{E_1}(\alpha' X, Z_1)$ est bijective pour tout Z_1. En particulier tout objet αZ_1, et tout objet qui lui est isomorphe, est Σ-local.

Un objet local est dans l'image essentielle. Soit ξ un objet Σ-local et $\eta = \eta_\xi : \xi \to \alpha\alpha'\xi$ l'unité. Pour tout Z_1, la composition avec η, de $\mathrm{Hom}_E(\alpha\alpha'\xi, \alpha Z_1)$ dans $\mathrm{Hom}_E(\xi, \alpha Z_1)$, est bijective : c'est la bijection d'adjonction $\mathrm{Hom}_{E_1}(\alpha'\xi, Z_1) \simeq \mathrm{Hom}_E(\xi, \alpha Z_1)$ lue à travers la pleine fidélité de α. Par la caractérisation qui précède, $\eta \in \Sigma$. Comme ξ est local, la composition avec η, de $\mathrm{Hom}(\alpha\alpha'\xi, \xi)$ dans $\mathrm{Hom}(\xi, \xi)$, est bijective ; il existe donc $r : \alpha\alpha'\xi \to \xi$ avec $\eta\,;r = \mathrm{id}_\xi$. Alors $\eta\,;(r\,;\eta) = \eta = \eta\,;\mathrm{id}$, et comme la composition avec η est injective sur les flèches à valeurs dans l'objet local $\alpha\alpha'\xi$, $r\,;\eta = \mathrm{id}$. Ainsi $\xi \simeq \alpha(\alpha'\xi)$. Avec la dernière phrase du paragraphe précédent, on obtient que les objets Σ-locaux sont exactement ceux de l'image essentielle de α. □

Énoncé ((2), page 3)**.** *Soient $F' \subset F$ une sous-catégorie pleine et $\overline{F}'$ sa clôture par isomorphie. Alors*

$$v|F' \text{ est pleinement fidèle et } uv(F') \subset \overline{F}'$$
$$\iff \text{pour tout } P \in F',\ \varepsilon_P : uv(P) \to P \text{ est un isomorphisme.}$$

Démonstration. C'est la démonstration de (1) retournée. Pour $P, Q \in F$, l'application $g \mapsto v(g)$, de $\mathrm{Hom}_F(P, Q)$ dans $\mathrm{Hom}_E(vP, vQ)$, suivie de la bijection d'adjonction réciproque $h \mapsto u(h)\,;\varepsilon_Q$, donne $g \mapsto uv(g)\,;\varepsilon_Q = \varepsilon_P\,;g$ par naturalité de ε : c'est le « $\mathrm{Hom}(j(P), Q)$ » de la page, et v est bijective sur $\mathrm{Hom}(P, Q)$ si et seulement si $g \mapsto \varepsilon_P\,;g$ l'est. Si ε_P est inversible pour tout $P \in F'$, la composition avec ε_P est bijective, et $uv(P) \simeq P$. Réciproquement, soient $P \in F'$, $Z \in F'$ et $e : uv(P) \to Z$ un isomorphisme ; la surjectivité de $g \mapsto \varepsilon_P\,;g$ sur $\mathrm{Hom}(P, Z)$ donne g avec $\varepsilon_P\,;g = e$. Posons $s = g\,;e^{-1}$. Alors $\varepsilon_P\,;s = \mathrm{id}$, et $\varepsilon_P\,;(s\,;\varepsilon_P) = \varepsilon_P = \varepsilon_P\,;\mathrm{id}$; l'injectivité sur $\mathrm{Hom}(P, P)$ donne $s\,;\varepsilon_P = \mathrm{id}$. □

Énoncé (Les cinq conditions, page 3)**.** *Soient $E' \subset E$ et $F' \subset F$ des sous-catégories strictement pleines ; on note $u' : E' \to F'$ et $v' : F' \to E'$ les foncteurs induits quand $u(E') \subset F'$ et $v(F') \subset E'$. Les conditions suivantes sont équivalentes :*

1. *E' vérifie (1), F' vérifie (2), et $F' = \overline{u(E')}$, $E' = \overline{v(F')}$;*
2. *$u(E') \subset F'$, $v(F') \subset E'$, et u', v' sont pleinement fidèles ;*
3. *$u(E') \subset F'$, $v(F') \subset E'$, et u' est une équivalence ;*
4. *$u(E') \subset F'$, $v(F') \subset E'$, et v' est une équivalence.*

De plus, si E' strictement pleine vérifie (1), $\alpha(E') = \overline{u(E')}$ vérifie (2) et $\beta(\alpha(E')) = E'$; dualement pour F'.

Démonstration. On lit « u' est une équivalence » comme « u' est pleinement fidèle et tout objet de F' est isomorphe à un $u(Y)$, $Y \in E'$ ». On utilise deux faits : si η_Y est inversible, ε_{uY} l'est, puisque $u(\eta_Y)\,;\varepsilon_{uY} = \mathrm{id}$; et si ε_P l'est, η_{vP} l'est, par l'autre identité triangulaire. Les objets où η (resp. ε) est inversible forment une sous-catégorie strictement pleine, par naturalité.

Si $u(E') \subset F'$, $v(F') \subset E'$, η est inversible sur E' et ε sur F', alors 1. vaut : un $P \in F'$ est isomorphe, par ε_P, à $u(vP)$ avec $vP \in E'$, et tout objet isomorphe à un $u(Y)$, $Y \in E'$, est dans F', strictement pleine ; de même pour E', par η_Y^{-1}. Réciproquement 1. donne $u(E') \subset F'$, $v(F') \subset E'$, et, par (1) et (2), la pleine fidélité de u' et v' et l'essentielle surjectivité de u' et de v' ; donc 1. entraîne 2., 3. et 4.

Sous 2., $vu(E') \subset v(F') \subset E'$, et (1) donne η inversible sur E' ; de même (2) donne ε inversible sur F' ; d'où 1. Sous 3., (1) donne de même η inversible sur E' ; un $P \in F'$ est isomorphe à un $u(Y)$, $Y \in E'$, où ε est inversible par le premier fait ; donc ε_P l'est, d'où 1. Le cas 4. est symétrique.

Pour la bijection : si $Y \in E'$, $Y \simeq vu(Y)$ par η_Y et $uY \in \alpha(E')$; si $Y \simeq v(P)$ avec $P \simeq u(Y')$, $Y' \in E'$, alors $Y \simeq vu(Y') \simeq Y'$ et $Y \in E'$. Et ε est inversible sur $\alpha(E')$ par le premier fait. □

Énoncé (Les points fixes, page 4)**.** *Soient $E_0 \subset E$ la sous-catégorie pleine des Y où η_Y est inversible et $F_0 \subset F$ celle des P où ε_P l'est. Ce sont les plus grandes sous-catégories vérifiant (1) et (2) ; on a $F_0 = \overline{u(E_0)}$, $E_0 = \overline{v(F_0)}$, et u, v induisent des équivalences quasi-inverses $E_0 \simeq F_0$.*

Démonstration. La maximalité est la forme de (1) et (2) démontrée plus haut : E' vérifie (1) si et seulement si $E' \subset E_0$. Par les deux faits de la démonstration précédente, $u(E_0) \subset F_0$ et $v(F_0) \subset E_0$; les égalités $F_0 = \overline{u(E_0)}$ et $E_0 = \overline{v(F_0)}$ en résultent comme dans le cas 1. ci-dessus. Les foncteurs induits $u_0 : E_0 \to F_0$ et $v_0 : F_0 \to E_0$ sont quasi-inverses, par les isomorphismes naturels $\eta_Y : Y \to v_0u_0(Y)$ et $\varepsilon_P : u_0v_0(P) \to P$. □

Énoncé (Conditions 1), 3) et 4), page 5 ; la préservation des colimites)**.** *La condition 1), $\mathrm{Im}\, v \subset E_0$ et $\mathrm{Im}\, u \subset F_0$, est l'idempotence, et chacune de ses moitiés suffit. Si $\mathrm{Im}\, u \subset F_0$, l'inclusion $E_0 \subset E$ admet pour adjoint à gauche $v_0 \circ u'$, $X \mapsto vu(X)$; si $\mathrm{Im}\, v \subset E_0$, l'inclusion $F_0 \subset F$ admet pour adjoint à droite $u_0 \circ v'$, $P \mapsto uv(P)$. Ce réflecteur $E \to E_0$ commute aux limites inductives et l'inclusion $E_0 \subset E$ aux limites projectives ; E_0 a les limites inductives qu'a E ; dualement, le coréflecteur $F \to F_0$ commute aux limites projectives, l'inclusion $F_0 \subset F$ aux limites inductives, et F_0 a les limites projectives qu'a F. Enfin, pour une adjonction idempotente, $u \simeq \beta\, u_0\, \alpha'$ et $v \simeq \alpha\, v_0\, \beta'$, avec α' le réflecteur, qui est un passage à la catégorie des fractions, β' le coréflecteur, et α, β les inclusions ; $\beta\, u_0 : E_0 \to F$ est pleinement fidèle (condition 4)).*

Démonstration. Condition 1). $Y = vP$ est dans E_0 si et seulement si η_{vP} est inversible, et $uX \in F_0$ si et seulement si ε_{uX} l'est : c'est l'énoncé sur les adjonctions idempotentes.

Le réflecteur. Si $\mathrm{Im}\, u \subset F_0$, le foncteur $X \mapsto vu(X)$ arrive dans E_0, et il est adjoint à gauche de l'inclusion $E_0 \subset E$, d'unité $\eta_X : X \to vu(X)$ et de coünité η_Y^{-1} en $Y \in E_0$; c'est

le calcul de Hom de la page 5. Dualement, si $\operatorname{Im} v \subset E_0$, le foncteur $P \mapsto uv(P)$ est adjoint à droite de l'inclusion $F_0 \subset F$, de coünité ε_P ; c'est le calcul entre crochets de la page 4. Ces deux adjonctions sont démontrées en Lean dans le même fichier général que l'énoncé sur les adjonctions idempotentes.

Limites. Un adjoint à gauche commute aux limites inductives, un adjoint à droite aux limites projectives. Une sous-catégorie réflexive a les limites inductives de la catégorie ambiante : on réfléchit la limite inductive calculée dans E.

Condition 4). Pour $X \in E$, $u_0(vu(X)) = uvu(X)$, et $\varepsilon_{uX} : uvu(X) \to u(X)$ est inversible et naturel en X : d'où $\beta\, u_0\, \alpha' \simeq u$. De même $\eta_{vP}^{-1} : vuv(P) \to v(P)$ donne $\alpha\, v_0\, \beta' \simeq v$. Le foncteur $\beta\, u_0$ est pleinement fidèle comme composé d'une équivalence et d'une inclusion pleine. Enfin, un adjoint à gauche dont l'adjoint à droite est pleinement fidèle est une localisation en les flèches qu'il inverse ; c'est le cas de α'. □

Énoncé (La descente d'adjoints, page 6)**.** *Soient $\alpha : E_1 \to E$ pleinement fidèle d'adjoint à gauche α', et $\psi : E_1^\circ \to \mathrm{Ens}$ tel que $\psi \circ \alpha'$ soit représentable. Alors ψ est représentable. Par suite, si $\beta : E_1 \to F$ est un foncteur tel que $u = \beta\alpha'$ admette un adjoint à droite, β admet un adjoint à droite.*

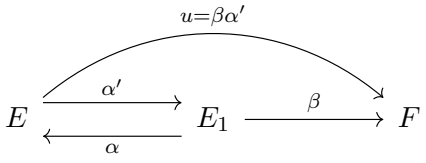
Démonstration. Soit $\xi \in E$ représentant $\psi \circ \alpha' : \mathrm{Hom}_E(X, \xi) \simeq \psi(\alpha' X)$, naturellement en X. Si $f : X \to Y$ est dans Σ, la composition avec f, de $\mathrm{Hom}(Y, \xi)$ dans $\mathrm{Hom}(X, \xi)$, correspond à $\psi(\alpha' f)$, qui est bijective puisque $\alpha'(f)$ est inversible ; ξ est donc Σ-local, et, par l'énoncé sur les objets locaux, il existe $\xi_1 \in E_1$ et un isomorphisme $\alpha\xi_1 \simeq \xi$. Pour $Z \in E_1$, on compose alors les bijections

$$\mathrm{Hom}_{E_1}(Z, \xi_1) \simeq \mathrm{Hom}_E(\alpha Z, \alpha\xi_1) \simeq \mathrm{Hom}_E(\alpha Z, \xi) \simeq \psi(\alpha'\alpha Z) \simeq \psi(Z),$$

la première par la pleine fidélité de α, la dernière par ψ appliqué à la coünité $\alpha'\alpha Z \to Z$, inversible puisque α est pleinement fidèle. La naturalité en Z résulte de celle de la coünité. Donc ψ est représenté par ξ_1.

Pour la seconde assertion, β admet un adjoint à droite si et seulement si, pour tout $P \in F$, le préfaisceau $Z \mapsto \mathrm{Hom}_F(\beta Z, P)$ sur E_1 est représentable. Composé avec α', c'est $X \mapsto \mathrm{Hom}_F(\beta\alpha' X, P)$, représentable puisque $\beta\alpha'$ a un adjoint à droite. La première assertion conclut. □

La situation de la descente d'adjoints, avec $\alpha' \dashv \alpha$ et α pleinement fidèle : si $u = \beta\alpha'$ a un adjoint à droite, β en a un.



Remarque. L'exemple ci-dessus répond à la question de la marge de la page 3, avec E' réduit à un objet ; la réponse de la lecture, « Elle l'est », est juste.

Remarque. L'énoncé des pages 6 et 7 vaut pour toute sous-catégorie réflexive. La caractérisation de Σ est classique : Gabriel et Zisman établissent, au chapitre I de leur livre de 1967 [57], que l'adjoint à gauche d'un foncteur pleinement fidèle est la localisation par les flèches qu'il rend

inversibles. L'identification des objets Σ-locaux à l'image essentielle, le « Or c'est vrai » de la page 7, est un lemme de base de la théorie des localisations.

Remarque. La cinquième condition de la page 3, « —— et u' et v' pl. fid. », répète mot pour mot la deuxième ; l'énoncé ci-dessus en retient quatre.

Remarque. La descente de la page 6 tient sans l'hypothèse que β soit pleinement fidèle, dont la démonstration ne se sert pas. Pour une catégorie F quelconque, la réduction de la page au cas $\mathrm{Ob}\, F = \mathrm{Ob}\, E_1 \cup \{a\}$ revient à traiter un objet P de F à la fois, comme on l'a fait. La vérification suppose que les ensembles de flèches de E, E_1 et F vivent dans le même univers, comme le demande la notion de foncteur représentable.

Remarque. La page 5 construit le réflecteur de E_0 sous la seule hypothèse $\mathrm{Im}\, u \subset F_0$, et le coréflecteur de F_0 sous $\mathrm{Im}\, v \subset E_0$. Ces deux hypothèses sont équivalentes par l'énoncé sur les adjonctions idempotentes, et l'identité triangulaire du réflecteur passe par cette équivalence.

Remarque. Les conditions équivalentes qui définissent une adjonction idempotente et l'équivalence entre les parties fixes sont exposées par Borceux (1994, §§ 3.4 et 4.2) [18].

Remarque. La théorie des topos se sert de ces énoncés. Un sous-topos d'un topos E est une sous-catégorie pleine réflexive dont le réflecteur est exact à gauche, et le faisceau associé est ce réflecteur ; les objets locaux des pages 6 et 7 sont alors les faisceaux, et Σ la classe des flèches bicouvrantes. La page 15 du dossier, que l'onglet Findings range parmi les pistes déjà publiées, en tire en une demi-page le critère de reconnaissance de Giraud sous sa forme de localisation exacte à gauche d'un topos de préfaisceaux (SGA 4, exposé IV [7]). Les sous-topos classifiants de la cote 161-2 (section 5) et le 2-produit de topos de la cote 161-3 (section 14) s'écrivent dans ce langage ; l'adjonction $\mathcal{O} \dashv \mathrm{Spec}$ de la section 11 en est un exemple.

Ne sont pas démontrés ici : la reconstruction d'une adjonction idempotente à partir de $(E_0, F_0, E_0 \simeq F_0)$ (page 5) ; les pages 9 à 19, sauf la relation de la page 12 entre les deux trivialisations de $L' \otimes L$, démontrée ci-dessous. Le calcul des contractions des pages 11 et 12 est une notation et non un énoncé ; l'édition retient comme énoncé la question que la page 12 pose et résout par ses ficelles.

Définition (Grothendieck, pages 11 et 12, contractions ♦)**.** La catégorie monoïdale symétrique libre $\Phi(A)$ sur A est étendue par des contractions, accouplements $L'_j \otimes L''_j \to \mathbf{1}$ qui évaluent chaque facteur apparié contre son partenaire. On obtient un calcul diagrammatique pour les catégories monoïdales à duaux ; les ficelles dessinées en marge de la page 12 notent quel facteur est apparié à quel autre.

Théorème (Grothendieck, page 12, « Relations entre $\varphi_{L',L}$ et $\psi_{L',L}$? »)**.** [30] *Soient C une catégorie monoïdale symétrique, de symétrie s, et L un objet inversible, d'inverse L' donné par un isomorphisme $\varphi_{L,L'} : L \otimes L' \xrightarrow{\sim} \mathbf{1}$. Posons $\varphi_{L',L} = \varphi_{L,L'} \circ s_{L',L} : L' \otimes L \xrightarrow{\sim} \mathbf{1}$. Il existe un unique morphisme $\psi_{L',L} : L' \otimes L \to \mathbf{1}$ tel que*

$$\varphi_{L,L'} \otimes \mathrm{id}_L = \mathrm{id}_L \otimes \psi_{L',L} \ : \ L \otimes L' \otimes L \longrightarrow L$$

(aux contraintes d'associativité et d'unité près), et c'est un isomorphisme. Pour un scalaire $e \in \mathrm{End}(\mathbf{1})$, on a $\varphi_{L',L} = e \cdot \psi_{L',L}$ si et seulement si la symétrie $s_{L,L}$ agit sur $L \otimes L$ par e. En particulier

$$\varphi_{L',L} = \varepsilon(L) \cdot \psi_{L',L},$$

30. Preuve vérifiée : `lean/Grothendieck/Folder161_1.lean`.

où $\varepsilon(L) \in \mathrm{Aut}(\mathbf{1})$ est le scalaire par lequel $s_{L,L}$ agit sur $L \otimes L$; il ne dépend que de L, non de l'inverse $(L', \varphi_{L,L'})$ choisi, et $\varepsilon(L)^2 = 1$.

Un scalaire $e : \mathbf{1} \to \mathbf{1}$ agit sur tout objet X par $e \cdot \mathrm{id}_X = e \otimes \mathrm{id}_X$, lu à travers $\mathbf{1} \otimes X \simeq X$; cette action commute à toutes les flèches, et $e \cdot \mathrm{id}_{X \otimes Y} = (e \cdot \mathrm{id}_X) \otimes \mathrm{id}_Y$. Sur $\mathbf{1}$, elle redonne e. Comme précédemment, on écrit $f\,;g$ pour « f puis g ».

Démonstration. Existence et unicité de ψ. Comme $L' \otimes L \simeq \mathbf{1}$ (par $\varphi_{L',L}$) et $L \otimes L' \simeq \mathbf{1}$, le foncteur $L \otimes -$ est une équivalence de C, de quasi-inverse $L' \otimes -$; il est donc pleinement fidèle, et $\psi_{L',L}$ est l'unique antécédent de l'isomorphisme $\varphi_{L,L'} \otimes \mathrm{id}_L$, lu de $L \otimes (L' \otimes L)$ vers $L \otimes \mathbf{1}$. De même $L' \otimes -$ est pleinement fidèle, et, la symétrie échangeant $f \otimes \mathrm{id}_Z$ et $\mathrm{id}_Z \otimes f$, on peut simplifier par $- \otimes L$ ou $- \otimes L'$.

Le carré de naturalité de la page. Posons $\varepsilon = \psi^{-1}_{L',L}\,;\varphi_{L',L}$, de sorte que $\varphi_{L',L} = \psi_{L',L}\,;\varepsilon$; comme $s_{L,L'}\,;s_{L',L} = \mathrm{id}$, on a $\varphi_{L,L'} = \chi\,;\varepsilon$ avec $\chi = s_{L,L'}\,;\psi_{L',L}$. La naturalité de la symétrie $s_{L,-}$ appliquée à $\varphi_{L,L'} : L \otimes L' \to \mathbf{1}$ donne, à l'identification $L \otimes \mathbf{1} \simeq L \simeq \mathbf{1} \otimes L$ près,

$$\mathrm{id}_L \otimes \varphi_{L,L'} = s_{L,\,L\otimes L'}\,;(\varphi_{L,L'} \otimes \mathrm{id}_L).$$

L'hexagone décompose $s_{L,\,L\otimes L'} = (s_{L,L} \otimes \mathrm{id}_{L'})\,;(\mathrm{id}_L \otimes s_{L,L'})$, et l'identité triangulaire remplace $\varphi_{L,L'} \otimes \mathrm{id}_L$ par $\mathrm{id}_L \otimes \psi_{L',L}$: le membre de droite devient $(s_{L,L} \otimes \mathrm{id}_{L'})\,;(\mathrm{id}_L \otimes \chi)$. Celui de gauche vaut $(\mathrm{id}_L \otimes \chi)\,;(\mathrm{id}_L \otimes \varepsilon)$, et $\mathrm{id}_L \otimes \varepsilon$ est l'action de ε sur L (encore par la symétrie, $s_{L,\mathbf{1}}$ échangeant $\mathrm{id}_L \otimes \varepsilon$ et $\varepsilon \otimes \mathrm{id}_L$). Comme les scalaires commutent aux flèches, il vient

$$(\varepsilon \cdot \mathrm{id}_{L\otimes L\otimes L'})\,;(\mathrm{id}_L \otimes \chi) = (s_{L,L} \otimes \mathrm{id}_{L'})\,;(\mathrm{id}_L \otimes \chi),$$

et l'isomorphisme $\mathrm{id}_L \otimes \chi$ se simplifie : $s_{L,L} \otimes \mathrm{id}_{L'} = (\varepsilon \cdot \mathrm{id}_{L\otimes L}) \otimes \mathrm{id}_{L'}$, puis $s_{L,L} = \varepsilon \cdot \mathrm{id}_{L\otimes L}$ en simplifiant par $- \otimes L'$.

Unicité du scalaire. Si $e \cdot \mathrm{id}_{L\otimes L} = e' \cdot \mathrm{id}_{L\otimes L}$, on simplifie deux fois par $- \otimes L$ et l'on trouve $e = e'$. Ainsi ε est le seul scalaire qui agisse comme $s_{L,L}$, ce qui donne l'équivalence de l'énoncé, l'indépendance de $\varepsilon(L)$ vis-à-vis de $(L', \varphi_{L,L'})$, et $\varepsilon(L)^2 = 1$ puisque $s_{L,L}\,;s_{L,L} = \mathrm{id}$. Enfin, $\psi_{L',L}\,;\varepsilon$ s'écrit $(\varepsilon \cdot \mathrm{id}_{L'\otimes L})\,;\psi_{L',L}$, la forme $\varepsilon(L) \cdot \psi_{L',L}$ de l'énoncé. □

L'énoncé tient tel que la lecture le donne, dans toute catégorie monoïdale symétrique, sans supposer que tous les objets soient inversibles (Lean : `psi_triangle`, `psi_unique`, `braiding_self_eq_scalar`, `phiSwap_eq_iff`, `phiSwap_eq_scalar_comp`, `epsilon_eq_of_inverse`, `epsilon_mul_self`). La symétrie ne sert qu'à deux endroits : la naturalité de $s_{L,-}$ et l'hexagone, qui sont le carré et les trois colonnes de ficelles sur lesquels la page s'interrompt. Ne sont pas vérifiés en Lean : le calcul diagrammatique des contractions lui-même et la catégorie $\Phi(A)$; l'exemple des super-espaces vectoriels, où $\varepsilon(L) = -1$ pour une droite impaire et où les deux trivialisations diffèrent donc d'un signe. Autres pistes de l'onglet Findings pour ce thème,

dans des cotes qui n'ont pas de section ici :

Théorème (Quillen, d'après les pages 43 à 45, universalité des correspondances de bordisme ♦). *Sur les variétés fermées et les classes d'homotopie d'applications, la catégorie $\mathbf{B}$ dont les morphismes $X \to Y$ sont les classes de bordisme non orienté de variétés au-dessus de $X \times Y$ est universelle parmi les catégories munies d'un foncteur covariant et d'un foncteur contravariant qui coïncident sur les objets et vérifient le changement de base pour les carrés cartésiens transverses. Tout tel couple $(F'_\bullet, F'^\bullet)$ identifie les correspondances bordantes, une*

◊ non vérifié en Lean

correspondance $Z \to X \times Y$ de composantes p, q allant sur $F'_\bullet(q) \circ F'^\bullet(p)$. La page attribue l'énoncé à Quillen.

Les feuillets en esquissent une démonstration incomplète (pages 43 à 45). L'esquisse finit par « Le reste est sans doute l'AQT », sans rien sur la composition ni sur l'unicité, et le mot « fermées » est de l'édition. Mathlib n'a pas le bordisme des variétés. On se reportera aux notes de Grothendieck (162-5, lot 3, p. 43).

Théorème (Grothendieck, pages 27 à 30, de Rham et Hochschild pour une catégorie formelle ♦). *Soient X_0 un schéma de caractéristique nulle et $\mathcal{C}$ une catégorie formelle sur X_0 de conormal Ω plat. Les données de descente sur un $\mathcal{O}$-module M relativement à $\mathcal{C}$ correspondent aux Ω-connexions intégrables sur M, et le complexe de de Rham $\Lambda^\bullet\Omega \otimes M$ est canoniquement quasi-isomorphe, dans la catégorie dérivée, au complexe de Hochschild $C^\bullet(\mathcal{C}, M)$.*

◊ non vérifié en Lean

La page 30 l'énonce sans démonstration, « sous les conditions du th. de Quillen » ; le mot « intégrables » et la définition de $C^\bullet(\mathcal{C}, M)$ sont de la lecture. Deux cas particuliers sont classiques, et la lecture les identifie : pour $\mathcal{C}$ le complété formel de la diagonale d'un X_0 lisse sur $\mathbf{Q}$, les données de descente sont les stratifications, c'est-à-dire les connexions intégrables, et l'énoncé est la comparaison des cohomologies de de Rham et infinitésimale ; pour X_0 un point, c'est la comparaison de la cohomologie d'un groupe formel et de celle de son algèbre de Lie. Le cas d'une catégorie formelle quelconque, sans inverse supposé, de conormal plat non nécessairement de type fini, reste ouvert. C'est le pendant formel de la connexion de Gauss–Manin et des connexions projectives de la section 49 ; la monodromie modérée correspondante, en caractéristique résiduelle p, est l'objet des énoncés de la cote 34 (partie « Groupes fondamentaux et théorie de Galois »). Mathlib n'a pas les catégories formelles ni les complexes de de Rham sur un schéma. On se reportera aux notes de Grothendieck (162-5, lot 2, p. 27).

Théorème (Quillen, d'après les pages 21 à 26, catégories formelles à conormal plat ♦). *Sur un schéma X_0 de caractéristique nulle, le foncteur qui envoie une catégorie formelle I-adique sur X_0 (un pro-anneau complet augmenté muni d'un Δ coassociatif et counitaire, sans inverse supposé) sur l'algèbre différentielle graduée $(\Lambda^\bullet\Omega, \delta)$ de son conormal $\Omega = I/I^2$ est une équivalence entre les catégories formelles de Ω plat et les complexes de de Rham sur $\Lambda^\bullet\Omega$ de Ω plat, sans hypothèse de finitude sur Ω ni de lissité sur X_0.*

◊ non vérifié en Lean

La page 26 l'énonce comme « Th. de Quillen », sans démonstration ni référence, et dit qu'il contient le théorème de Cartan sur les groupes formels en caractéristique nulle. Quand Ω est localement libre de type fini, la lecture identifie la catégorie formelle à un algébroïde de Lie, de complexe de Chevalley–Eilenberg $(\Lambda^\bullet\Omega, \delta)$; la Remarque 1 de la page (que $\delta^2 = 0$ suit des axiomes) est fausse, et l'énoncé encadré suppose $\delta^2 = 0$ dans la définition d'un complexe de de Rham. Mathlib n'a pas les catégories formelles I-adiques. On se reportera aux notes de Grothendieck (162-5, lot 2, p. 21).

Partie 15

Géométrie formelle, modules et représentabilité

Le 11 septembre 1967, une lettre dactylographiée systématise l'étape principale de la preuve de Matsumura de la représentabilité du schéma des automorphismes d'un schéma propre (91, lot 2, p. 30). Le 21 octobre 1968, Deligne lui écrit qu'un espace analytique compact est un schéma si et seulement si sa réduction l'est (37, lot 4, p. 74). Le 30 avril 1969, il envoie à Jacob Murre les notes préliminaires sur les revêtements formels modérément ramifiés (29, lot 4, p. 78).

29 Cote 39 : le théorème de préparation « formel » ; fonctions implicites dans une classe de séries [31]

La cote 39, *Fonctions et structures « élémentaires » [Schémas formels, théorème de préparation] : notes manuscrites (s.d.)*, datée par l'inventaire « [vers 1960-1970] », compte dix-neuf pages en trois ensembles séparés par des intercalaires vierges. Les deux premiers sont deux rédactions successives d'une axiomatique des classes de séries formelles (pages 2 à 7, puis 9 à 16). Le troisième, pages 18 et 19, énonce et démontre un théorème sous un titre souligné de sa main, « Th. de préparation “formel” » (39, lot 1, p. 18). La démonstration commence par une réduction, « Comme A est séparé et complet pour sa top. linéaire, on est ramené au cas où A est discret », puis précise que (i) « **signifie** que les a_i ($0 \leq i \leq N-1$) sont nilpotents ». Un premier argument, par Nakayama et le gradué associé, est encadré et barré. Le second considère l'application $\varphi : ((b_i), Q) \mapsto \sum b_i Z^i + QF$ et conclut, par le gradué de la filtration $\mathfrak{m}$-adique, « finie », que φ est bijective (39, lot 1, p. 19).

Énoncé (Théorème de préparation « formel »)**.** *Soient A un anneau linéairement topologisé, séparé et complet, Z une indéterminée, $F = \sum_{i \geqslant 0} a_i Z^i \in A[[Z]]$, et $N \in \mathbb{N}$ tel que*

(i) a_i est topologiquement nilpotent pour $0 \leqslant i \leqslant N-1$;

(ii) a_N est inversible.

Alors F est un élément régulier de $A[[Z]]$, et $A[[Z]]/FA[[Z]]$ est un A-module libre de base les images des Z^i, $0 \leqslant i \leqslant N-1$: tout $G \in A[[Z]]$ s'écrit de façon unique $G = QF + \sum_{0 \leqslant i \leqslant N-1} b_i Z^i$, avec $Q \in A[[Z]]$ et $b_i \in A$.

On ne démontre ici que deux cas particuliers de cet énoncé : le cas d'un anneau complet pour une topologie I-adique, avec $a_i \in I$ pour $i < N$; et le cas discret auquel la démonstration du feuillet se ramène, avec $a_0, \dots, a_{N-1}$ nilpotents. Dans les deux cas, on écrit le reste $\sum_{i<N} b_i Z^i$ comme un polynôme $r \in A[Z]$ de degré $< N$.

On s'appuie sur le théorème classique de division de Weierstrass, sous la forme suivante : *soient A un anneau séparé et complet pour la topologie I-adique et $F \in A[[Z]]$; si l'image $\bar{F}$ de F dans $(A/I)[[Z]]$ est d'ordre N et si le coefficient a_N de F est inversible dans A, alors pour tout $G \in A[[Z]]$ il existe un unique couple (Q, r), $Q \in A[[Z]]$, $r \in A[Z]$ de degré $< N$, tel que $G = QF + r$; et si $QF = r$ avec $\deg r < N$, alors $Q = 0$ et $r = 0$.*

31. Preuve vérifiée : `lean/Grothendieck/Folder39.lean`.

Lemme 29.1. *Soient I un idéal de A, A séparé et complet pour la topologie I-adique, et $F = \sum a_i Z^i$ avec $a_i \in I$ pour $i < N$ et a_N inversible. Alors F est régulier dans $A[[Z]]$, et tout $G \in A[[Z]]$ s'écrit de façon unique $G = QF + r$ avec $Q \in A[[Z]]$ et $r \in A[Z]$ de degré $< N$.*

Démonstration. Si $I = A$, l'anneau A, séparé pour la topologie A-adique, est nul, et tout est trivial. Supposons $I \neq A$, de sorte que A/I n'est pas nul. Les coefficients de $\bar{F}$ d'indice $< N$ sont nuls, puisque $a_i \in I$; celui d'indice N est l'image de l'inversible a_N, donc est inversible dans l'anneau non nul A/I, et en particulier non nul. Ainsi $\bar{F}$ est d'ordre exactement N, et, a_N étant inversible, le théorème de division s'applique. Il donne l'existence et l'unicité de l'écriture $G = QF + r$. Si $FH = 0$, on a $HF = 0$ avec le reste $r = 0$ de degré $< N$, donc $H = 0$: F est régulier. □

Lemme 29.2. *Soit $\mathfrak{m}$ un idéal nilpotent de A. Alors A est séparé et complet pour la topologie $\mathfrak{m}$-adique. Si $a_0, \ldots, a_{N-1}$ sont nilpotents, l'idéal qu'ils engendrent est nilpotent.*

Démonstration. La première assertion est l'énoncé général rappelé à la suite de la démonstration, pour le module A : la suite des $\mathfrak{m}^n$ est nulle à partir d'un rang k, et une suite de Cauchy pour la topologie $\mathfrak{m}$-adique est stationnaire à partir de ce rang. Pour la seconde assertion : l'idéal $\mathfrak{m} = (a_0, \ldots, a_{N-1})$ est contenu dans le nilradical et engendré par un nombre fini d'éléments ; c'est un fait classique qu'un tel idéal est nilpotent (si $a_i^e = 0$ pour tout i, un produit de $N(e-1)+1$ éléments de $\mathfrak{m}$ est combinaison de monômes en les a_i dont l'un au moins des exposants atteint e). C'est la phrase de la lecture : « il est de type fini et engendré par des nilpotents, donc nilpotent ». □

Résultat général, démontré en Lean dans
`Upstream/IsAdicCompleteOfIsNilpotent.lean` *; la démonstration n'est pas reprise ici.*

Démonstration du cas discret. Soit A un anneau commutatif quelconque. Supposons que les coefficients a_i d'indice $i < N$ soient nilpotents et que a_N soit inversible. Soit $\mathfrak{m}$ l'idéal engendré par $a_0, \ldots, a_{N-1}$. Par le lemme 29.2, $\mathfrak{m}$ est nilpotent et A est séparé et complet pour la topologie $\mathfrak{m}$-adique. Comme $a_i \in \mathfrak{m}$ pour $i < N$, le lemme 29.1, appliqué à $I = \mathfrak{m}$, donne la régularité de F et l'écriture unique. □

Remarque. Dans le cas adique, l'idéal n'a pas à être de type fini. La lecture n'emploie cette hypothèse que pour obtenir $\mathfrak{m}^j A[[Z]] = \mathfrak{m}^j[[Z]]$ dans sa démonstration par le gradué associé.

Remarque. La démonstration ci-dessus admet la division de Weierstrass comme théorème classique, là où la page passe par le gradué associé ; le nom renvoie au théorème de préparation de Weierstrass pour les fonctions analytiques, dont l'énoncé est l'analogue formel.

Remarque. Pour la topologie I-adique, « topologiquement nilpotent » signifie $a_i \in \sqrt{I}$, condition plus faible que l'hypothèse $a_i \in I$ du lemme 29.1.

Ne sont pas démontrés ici : la préparation (unité × polynôme distingué) ; les séries algébriques ; le cas d'une topologie linéaire quelconque ; le cas I-adique sous l'hypothèse $a_i \in \sqrt{I}$.

L'axiomatique des pages 9 à 14. Sur un anneau commutatif k quelconque, pour une famille $A_n \subset S_n = k[[t_1, \ldots, t_n]]$, la seconde rédaction pose (I) $t_i \in A_n$; (S) si $\varphi \in A_n$ et si $f_1, \ldots, f_n \in A_m$ ont des termes constants nilpotents, $\varphi(f_1, \ldots, f_n) \in A_m$; (R) les A_n sont des sous-anneaux unitaires ; (H) l'inverse d'un A-morphisme $X_n \to X_n$ qui est un isomorphisme formel est un A-morphisme ; (D) les coefficients de $f \in A_{n+m}$ en ses m dernières variables sont dans A_n.

La page tire de (H) le corollaire 1 (si $f \in A_n$ et si $f(0)$ est inversible dans k, $f^{-1} \in A_n$), le corollaire 2 (le couple $(A_n, A_n \cap \mathfrak{m}_n)$ est zariskien et hensélien) et le corollaire 3 (les fonctions implicites), puis de (D) l'inclusion $A_n \subset k_0[[t]]$, $k_0 = A_0$ (39, lot 1, p. 11, 39, lot 1, p. 12, 39, lot 1, p. 14). La démonstration du corollaire 1 substitue $t_{n+1} = 1$, substitution que (S) interdit ; la lecture le démontre avec (D) et ne tient le couple pour hensélien que sous (D). On lit ici « isomorphisme formel » comme « admet un inverse pour la substitution », et $\mathfrak{m}_n$ comme l'idéal des séries sans terme constant.

Théorème 29.3 (Grothendieck, page 12, corollaires 2 et 3 ♦). *Supposons (I), (S), (R), (H). Si $P \in A_{n+1}$, vu comme série en $(Z, t_1, \ldots, t_n)$, vérifie $P(0) = 0$ et si $\partial P/\partial Z\,(0)$ est inversible dans k, l'unique $F \in S_n$ tel que $F(0) = 0$ et $P(F(t), t) = 0$ est dans A_n. Le couple $(A_n, A_n \cap \mathfrak{m}_n)$ est hensélien, en particulier zariskien.*

Démonstration. Existence et unicité de F. Vu dans $S_n[[Z]]$, P a son terme constant g_0 dans l'idéal I des variables, pour lequel S_n est séparé et complet, et son coefficient g_1 de Z inversible. La division de Weierstrass de Z par P donne $Z = qP + r$, $r \in S_n$. Le coefficient de Z donne $1 = g_0 q_1 + g_1 q_0$, et $g_0 \in I$ est dans le radical, donc q_0 et q sont inversibles ; ainsi $P = q^{-1}(Z - r)$ avec $r = -g_0 q_0 \in I$. La substitution $Z \mapsto G$, $G(0) = 0$, est un morphisme d'anneaux $S_{n+1} \to S_n$ qui envoie q^{-1} sur un inversible : $P(G, t) = 0$ si et seulement si $G = r$.

Appartenance. Appliquée à $P(W, t) - Z$, l'existence donne $\varphi(Z, t)$ avec $P(\varphi(Z, t), t) = Z$; appliquée à $P(W, t) - P(Z, t)$, dont $W = Z$ et $W = \varphi(P(Z, t), t)$ sont deux solutions, l'unicité donne $\varphi(P(Z, t), t) = Z$. Ainsi $(Z, t) \mapsto (\varphi, t)$ est l'inverse de l'A-morphisme $(Z, t) \mapsto (P, t)$; par (H), $\varphi \in A_{n+1}$, et par (S), $\varphi(0, t) \in A_n$. Comme $P(\varphi(0, t), t) = 0$, c'est F. C'est l'argument de la page.

Le couple. Soient f unitaire à coefficients dans A_n et $a_0 \in A_n$ tels que $f(a_0)(0) = 0$ et que $f'(a_0)$ soit inversible modulo $A_n \cap \mathfrak{m}_n$, donc $f'(a_0)(0)$ inversible dans k. La série $P(Z, t) = f(a_0 + Z)$ est dans A_{n+1} par (S), avec $P(0) = 0$ et $\partial P/\partial Z\,(0) = f'(a_0)(0)$; la racine $a_0 + F$ est dans A_n et congrue à a_0 modulo $\mathfrak{m}_n$. Si $g \in A_n \cap \mathfrak{m}_n$ et $y \in A_n$, le polynôme $(1 + gy)Z - 1$ et $a_0 = 1$ donnent un inverse de $1 + gy$ dans A_n. □

Le couple est donc hensélien sous (H) seul, sans la condition (D) que la lecture ajoute : le corollaire 3 ne passe pas par le corollaire 1, et seule la forme forte du corollaire 1 demande davantage. Voir `implicit_function`, `implicit_mem`, `hensel_mem` et `henselianRing` dans `Folder39.lean`.

Contre-exemple 29.4 (énoncé de l'édition). *Sur $k = \mathbb{Q}$, les séries à terme constant entier, $A_n = \{f \in S_n : f(0) \in \mathbb{Z}\}$, vérifient (I), (S), (R), (H), et $2 \in A_0$, inversible dans $\mathbb{Q}$, n'a pas d'inverse dans A_0. Le corollaire 1 de la page 11 ne découle pas de (I), (S), (R), (H).*

Démonstration. Un nilpotent de $\mathbb{Q}$ est nul ; une substitution par des séries sans terme constant conserve le terme constant, et un inverse pour la substitution est sans terme constant. □

Théorème 29.5 (D'après les pages 11 et 14, avec (D)). *Supposons (I), (S), (R), (H), (D). Si $f \in A_n$ et si $f(0)$ est inversible dans k, alors $f^{-1} \in A_n$. Sous (D) seule, $A_n \subset k_0[[t_1, \ldots, t_n]]$.*

L'énoncé tient, et (D) ne sert au corollaire 1 que pour $n = 0$: l'inverse de $s \mapsto f(0)s$ est dans A_1 par (H), son coefficient $f(0)^{-1}$ dans A_0 par (D), et le théorème 29.3 appliqué à $fZ - 1$ en $a_0 = f(0)^{-1}$ donne f^{-1}. Voir `inv_mem`, `coeff_mem`, `intConst_isFormalClass` et `intConst_not_inv_mem`. Ne sont pas démontrés : la forme jacobienne de (H) pour un morphisme quelconque, les produits fibrés transversaux, les sous-schémas formels, les parties principales, la question de fidèle platitude de la page 12, et la première rédaction (pages 2 à 7).

30 Cote 41 : continuité de la section générique et ouverture (proposition 1) [32]

La cote 41, *Construction de morphismes étales (Chap. V) : notes manuscrites (s.d.)*, datée par l'inventaire « [années 1960-1970] », est une seule section de rédaction en treize pages. Page 3, elle pose la notion de section *monogène*, qui choisit continûment le point générique d'une composante géométriquement irréductible de chaque fibre, et la question de la représentabilité du foncteur qu'elles forment. Elle construit ensuite, sous des conditions de spécialisation, un revêtement étale séparé qui la représente (pages 4 à 10). Page 11, elle revient au cas où les fibres elles-mêmes sont irréductibles, et écrit une « Prop. 1° » en trois conditions, à laquelle s'ajoute, encadrée, une condition « (iii bis) ». L'hypothèse de finitude porte sur la condition (ii), « f soit ouvert [...] si Y est loc. noeth., f de type fini », et la seule formule lisible de la démonstration est $\varphi^{-1}(U) = f(U)$ (41, lot 1, p. 11).

Énoncé (Proposition 1)**.** *Soit $f : X \to Y$ un morphisme de type fini dont les fibres sont irréductibles et non vides, et soit $\varphi(y)$ le point générique de X_y. On considère les conditions :*

(i) $\varphi : Y \to X$ *est continue ;*

(ii) f *est ouvert ;*

(iii) $y \in \overline{\{y'\}} \Rightarrow \varphi(y) \in \overline{\{\varphi(y')\}}$ *;*

(iii bis) pour tous $y \in \overline{\{y'\}}$ et x au-dessus de y, il existe x' au-dessus de y' tel que $x \in \overline{\{x'\}}$.

Alors (i) $\Leftrightarrow$ (ii) sans autre hypothèse, et (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (iii bis) ; si f est localement de présentation finie (par exemple Y localement noethérien), les quatre conditions sont équivalentes.

Sur les espaces sous-jacents, dire que $\varphi(y)$ est le point générique de la fibre se formule ainsi.

Définition. Soient X, Y des espaces topologiques et $f : X \to Y$ une application quelconque. On dit que $\varphi : Y \to X$ est une *section générique* de f si, pour tout $y \in Y$, on a $f(\varphi(y)) = y$ et $x \in \overline{\{\varphi(y)\}}$ pour tout $x \in f^{-1}(y)$.

Cela revient à dire que $\varphi(y)$ est un point générique de la fibre $f^{-1}(y)$ munie de la topologie induite, puisque l'adhérence de $\{\varphi(y)\}$ dans $f^{-1}(y)$ est la trace sur $f^{-1}(y)$ de son adhérence dans X ; une fibre qui a un point générique est irréductible et non vide. Pour un morphisme de schémas, la fibre schématique X_y est homéomorphe au sous-espace $f^{-1}(y)$; ce fait classique n'est pas démontré ici. Dans les lemmes qui suivent, f est une application quelconque entre espaces topologiques, qu'on ne suppose même pas continue, et φ une section générique de f.

Lemme 30.1. *Pour tout ouvert U de X, $\varphi^{-1}(U) = f(U)$.*

Démonstration. Si $\varphi(y) \in U$, alors $y = f(\varphi(y)) \in f(U)$. Inversement, soient $x \in U$ et $y = f(x)$; alors $x \in \overline{\{\varphi(y)\}}$, et l'ouvert U, qui contient un point de l'adhérence de $\{\varphi(y)\}$, contient $\varphi(y)$: $y \in \varphi^{-1}(U)$. □

Lemme 30.2. *On a (i) $\Leftrightarrow$ (ii), (i) $\Rightarrow$ (iii), et (iii) $\Leftrightarrow$ (iii bis).*

Démonstration. (i) $\Leftrightarrow$ (ii). Par le lemme 30.1, pour tout ouvert U de X, l'ensemble $\varphi^{-1}(U)$ est ouvert si et seulement si $f(U)$ l'est ; or φ est continue si et seulement si le premier l'est pour tout U, et f est ouverte si et seulement si le second l'est pour tout U.

32. Preuve vérifiée : `lean/Grothendieck/Folder41.lean`.

(i) $\Rightarrow$ (iii). Une application continue φ envoie l'adhérence de $\{y'\}$ dans l'adhérence de $\{\varphi(y')\}$.

(iii) $\Rightarrow$ (iii bis). Soient $y \in \overline{\{y'\}}$ et x au-dessus de y. Alors $x \in \overline{\{\varphi(y)\}}$ par définition de φ, et $\varphi(y) \in \overline{\{\varphi(y')\}}$ par (iii), donc $x \in \overline{\{\varphi(y')\}}$; et $x' = \varphi(y')$ est au-dessus de y'.

(iii bis) $\Rightarrow$ (iii). Soit $y \in \overline{\{y'\}}$. Appliquons (iii bis) à $x = \varphi(y)$, qui est au-dessus de y : il existe x' au-dessus de y' avec $\varphi(y) \in \overline{\{x'\}}$. Comme x' est dans la fibre de y', $x' \in \overline{\{\varphi(y')\}}$, et donc $\varphi(y) \in \overline{\{\varphi(y')\}}$. □

Démonstration de la proposition 1. Les implications (i) $\Leftrightarrow$ (ii), (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (iii bis) sont celles du lemme 30.2, (ii) $\Rightarrow$ (iii) passant par (i). Il reste, pour f un morphisme de schémas localement de présentation finie, à déduire (ii) de (iii bis). Or (iii bis) dit exactement que les générisations se relèvent le long de f, et un morphisme localement de présentation finie qui relève les générisations est ouvert : c'est un théorème de Grothendieck et Dieudonné (EGA IV, 1.10.4 [61]), qui repose sur le théorème de Chevalley sur les parties constructibles. Les quatre conditions sont donc équivalentes. □

Remarque. L'implication (iii bis) $\Rightarrow$ (ii) ne s'obtient pas par la seule topologie. Soient $X = \mathbb{N}$ muni de la topologie discrète, $Y = \mathbb{N}$ muni de la topologie cofinie, et $f : X \to Y$ l'identité, qui est continue. Les fibres sont des points, et $\varphi = f^{-1}$ est une section générique. Les deux espaces étant séparés au sens T_1, $y \in \overline{\{y'\}}$ entraîne $y = y'$, et (iii bis) est triviale. Mais f n'est pas ouverte : $f(\{0\}) = \{0\}$ n'est pas ouvert dans Y, puisque son complémentaire est infini. L'application f n'est pas un morphisme de schémas, et l'exemple montre seulement qu'une hypothèse, de finitude ou autre, est indispensable à cette implication, et à elle seule.

Remarque. Les implications (i) $\Leftrightarrow$ (ii) et (i) $\Rightarrow$ (iii) $\Leftrightarrow$ (iii bis) valent pour toute application entre espaces topologiques munie d'une section générique, sans que f soit de type fini, ni même continue.

Remarque. Seule l'implication (iii bis) $\Rightarrow$ (ii) emploie l'hypothèse de finitude, sous la forme de la présentation finie locale, par le critère d'ouverture par relèvement des générisations (EGA IV, 1.10.4), admis ici comme théorème classique.

Ne sont pas démontrés ici : la constructibilité ; l'ouverture universelle ; l'irréductibilité géométrique des fibres ; le cas « Y localement noethérien » ; la fibre schématique comme $f^{-1}(y)$; les définitions 2 et 3 ; la représentabilité des sections monogènes ; le théorème des pages 8 et 9.

Théorème (D'après les pages 3 et 8 à 10, composantes irréductibles des fibres, forme reconstituée par l'édition ♦). *Soit $f : X \to Y$ de type fini qui, en chaque point générique d'une composante d'une fibre, est localement universellement ouvert et quasi-fini sur un espace affine $Y[t_1, \ldots, t_{n-1}]$, sans platitude ni réduction géométrique des fibres. Un Y-schéma étale séparé M dont les points géométriques au-dessus de y indexent les composantes géométriquement irréductibles de $X_{\bar{y}}$ existe si et seulement si, au-dessus de tout trait, aucune composante de la fibre générique ne se spécialise en deux composantes distinctes de la fibre spéciale et deux composantes distinctes ne se rencontrent pas dans une spécialisation ; M est fini si et seulement si toute composante générique se spécialise en une composante spéciale.*

◊ non vérifié en Lean

La page énonce le théorème sans démonstration ; le sens de la seconde condition et le complément de finitude sont de la lecture.

31 Cote 42 : familles cohérentes de germes, le lemme 1 et le lemme 2[33]

La cote 42, *Réseaux d'anneaux locaux : notes manuscrites (s.d.)*, six pages que l'inventaire date « [années 1960-1970] », demande si une application entre préschémas localement noethériens est déterminée, et peut être construite, point par point, à partir des anneaux locaux reliés par les générisations. La page 3 ramène la question à une proposition sur les faisceaux : sous une condition (H) d'injectivité des flèches de générisation entre fibres, les sections globales sont les familles cohérentes de germes. Le lemme 1 en porte le contenu, et la page le démontre en une ligne. Le lieu considéré est stable par générisation, et « il suffit de montrer qu'il est *constructible*, donc que s'il contient x, il contient les pts d'un ouvert non vide de $\bar{x}$ » (42, lot 1, p. 3). Pour le faisceau structural, la page 4 enchaîne : « Il reste à vérifier que les conditions de la prop. sont vérifiées ». Elle isole un fait d'algèbre commutative, le lemme 2, dont la démonstration occupe le bas de la page 4 et le haut de la page 5 (42, lot 1, p. 4). La page glose le noyau de $A \to A_{\mathfrak{p}}$ comme « l'annulateur de $A - p$ », le premier mot étant lu avec doute. Elle traite la seconde assertion en se ramenant au cas $f = 1$, « car $A_p = (A_f)_{pA_f}$ » (42, lot 1, p. 5).

Énoncé (Proposition et lemme 1, page 3). *Soient X un espace topologique noethérien et sobre, et F un faisceau d'ensembles sur X vérifiant*

(H) pour tout $x \in X$, il existe un ouvert $W \ni x$ tel que $\rho_{yx} : F_y \to F_x$ soit injective pour tout $y \in W \cap \overline{\{x\}}$.

1. *(Lemme 1) Pour toute famille cohérente (ξ_x) et toute section $s \in F(U)$ sur un ouvert U, l'ensemble $E = \{x \in U : s_x = \xi_x\}$ est ouvert.*
2. *(Proposition) L'application $\Gamma(X, F) \to \varprojlim_x F_x$, qui envoie une section sur la famille de ses germes, est bijective.*

Énoncé (Lemme 2, pages 4 et 5). *Soient A un anneau noethérien et $\mathfrak{p}$ un idéal premier de A.*

1. *Il existe $f \in A \setminus \mathfrak{p}$ tel que $A_f \to A_{\mathfrak{p}}$ soit injectif.*
2. *Si de plus $A \to A_{\mathfrak{p}}$ est injectif, alors $A_{\mathfrak{q}} \to A_{\mathfrak{p}}$ est injectif pour tout idéal premier $\mathfrak{q} \supseteq \mathfrak{p}$.*
3. *(Forme de la page) Il existe $f \in A \setminus \mathfrak{p}$ tel que, pour tout idéal premier $\mathfrak{Q}$ de A_f dont la trace sur A contient $\mathfrak{p}$, $(A_f)_{\mathfrak{Q}} \to A_{\mathfrak{p}}$ soit injectif.*

Énoncé (Lemme 1 et corollaire 1, pages 3 et 4, cas affine). *Soit A un anneau noethérien. Appelons famille cohérente une famille $(\xi_{\mathfrak{p}})$, $\xi_{\mathfrak{p}} \in A_{\mathfrak{p}}$, indexée par les idéaux premiers, telle que $\xi_{\mathfrak{q}} \mapsto \xi_{\mathfrak{p}}$ par $A_{\mathfrak{q}} \to A_{\mathfrak{p}}$ chaque fois que $\mathfrak{p} \subseteq \mathfrak{q}$.*

1. *(Lemme 1) Pour toute famille cohérente $(\xi_{\mathfrak{p}})$ et tous $a, s \in A$, l'ensemble des $\mathfrak{p}$ tels que $s \notin \mathfrak{p}$ et $\xi_{\mathfrak{p}} = a/s$ est ouvert dans $\operatorname{Spec} A$.*
2. *(Corollaire 1) L'application $a \mapsto (a/1)_{\mathfrak{p}}$ est une bijection de $A = \Gamma(\operatorname{Spec} A, \mathcal{O})$ sur l'ensemble des familles cohérentes.*

Conventions. Pour $x, y \in X$, on écrit $x \rightsquigarrow y$ lorsque $y \in \overline{\{x\}}$: y est une spécialisation de x, x une générisation de y. Tout ouvert contenant y contient alors x, d'où une application $\rho_{yx} : F_y \to F_x$, compatible aux germes : $\rho_{yx}(s_y) = s_x$ pour toute section s définie au voisinage de y. Une famille (ξ_x), $\xi_x \in F_x$, est cohérente si $\rho_{yx}(\xi_y) = \xi_x$ chaque fois que $x \rightsquigarrow y$. Dans $\operatorname{Spec} A$, $\mathfrak{p} \rightsquigarrow \mathfrak{q}$

33. Preuve vérifiée : `lean/Grothendieck/Folder42.lean`.

équivaut à $\mathfrak{p} \subseteq \mathfrak{q}$. Un ouvert non vide de l'irréductible $\overline{\{x\}}$ contient son point générique x ; la condition (H) dit donc la même chose que la page, « un ouvert non vide » de $\overline{\{x\}}$ sur lequel les $F_y \to F_x$ sont injectives. Pour une partie multiplicative S de A, on note $a \mapsto a/1$ le morphisme $A \to S^{-1}A$; on rappelle que $a/1 = 0$ si et seulement s'il existe $s \in S$ avec $sa = 0$, que tout $z \in S^{-1}A$ vérifie $z \cdot (s/1) = a/1$ pour un $a \in A$ et un $s \in S$, et que si $g : A \to B$ envoie S dans les inversibles de B, il existe un unique $\bar{g} : S^{-1}A \to B$ avec $\bar{g}(a/1) = g(a)$. Les flèches $A_f \to A_{\mathfrak{p}}$ et $A_{\mathfrak{q}} \to A_{\mathfrak{p}}$ sont de cette forme, g étant le morphisme canonique $A \to A_{\mathfrak{p}}$.

Lemme 31.1. *Soient X un espace noethérien et sobre et $E \subseteq X$ une partie stable par générisation telle que, pour tout $x \in E$, il existe un ouvert $W \ni x$ avec $W \cap \overline{\{x\}} \subseteq E$. Alors E est ouvert.*

Résultat général, démontré en Lean dans `Upstream/NoetherianIsOpenOfStableUnderGeneralization.lean` *; la démonstration n'est pas reprise ici.*

Démonstration du lemme 1 de la page 3. E est stable par générisation. Soient $x \in E$ et $y \rightsquigarrow x$. Comme U est ouvert et contient x, il contient y, et $s_y = \rho_{xy}(s_x) = \rho_{xy}(\xi_x) = \xi_y$ par cohérence ; donc $y \in E$.

Condition locale. Soit $x \in E$, et soit W l'ouvert que fournit (H) en x. L'ouvert $W \cap U$ contient x. Pour $y \in W \cap U \cap \overline{\{x\}}$, on a $x \rightsquigarrow y$, et $\rho_{yx}(s_y) = s_x = \xi_x = \rho_{yx}(\xi_y)$; l'injectivité de ρ_{yx} donne $s_y = \xi_y$, donc $y \in E$. Le lemme 31.1 conclut. □

Démonstration de la proposition. L'injectivité est l'axiome de séparation des faisceaux : deux sections globales qui ont les mêmes germes en tout point sont égales. Soit (ξ_x) une famille cohérente. Pour chaque x, le germe ξ_x provient d'une section s^x sur un ouvert $U_x \ni x$; par le lemme 1, $V_x = \{y \in U_x : s^x_y = \xi_y\}$ est un ouvert, qui contient x. Les restrictions $s^x|_{V_x}$ ont, sur $V_x \cap V_{x'}$, les mêmes germes ξ_y en tout point ; elles y coïncident donc, et se recollent, les V_x recouvrant X, en une section globale s. Pour tout x, $s_x = (s^x|_{V_x})_x = \xi_x$. □

Lemme 31.2. *Soient $S \subseteq A$ une partie multiplicative et $g : A \to B$ un morphisme d'anneaux envoyant S dans les inversibles de B. Si, pour tout $a \in A$, $g(a) = 0$ entraîne $a/1 = 0$ dans $S^{-1}A$, alors $\bar{g} : S^{-1}A \to B$ est injectif.*

Démonstration. Comme $\bar{g}$ est additif, il suffit de montrer que son noyau est nul. Soit $z \in S^{-1}A$ avec $\bar{g}(z) = 0$, et écrivons $z \cdot (s/1) = a/1$ avec $a \in A$ et $s \in S$. En appliquant $\bar{g}$, on obtient $g(a) = \bar{g}(z)\, g(s) = 0$, donc $a/1 = 0$ par hypothèse, c'est-à-dire $z \cdot (s/1) = 0$. Comme $s/1$ est inversible dans $S^{-1}A$, $z = 0$. □

Lemme 31.3. *Soient A un anneau noethérien et $\mathfrak{p}$ un idéal premier. Il existe $f \notin \mathfrak{p}$ tel que $fy = 0$ pour tout y du noyau J de $A \to A_{\mathfrak{p}}$.*

Démonstration. Le noyau J est l'ensemble des $a \in A$ tels que $sa = 0$ pour *au moins un* $s \notin \mathfrak{p}$. L'anneau A étant noethérien, l'idéal J est engendré par un nombre fini d'éléments $x_1, \ldots, x_n$. Pour chaque i, l'appartenance $x_i \in J$ donne un $s_i \notin \mathfrak{p}$ tel que $s_i x_i = 0$. Posons $f = s_1 \cdots s_n$; comme $\mathfrak{p}$ est premier, son complémentaire est stable par produit, et $f \notin \mathfrak{p}$. L'ensemble des $y \in A$ tels que $fy = 0$ est un idéal de A ; il contient chaque x_i, car $f = s_i c_i$ avec $c_i = \prod_{j \neq i} s_j$, donc $fx_i = c_i(s_i x_i) = 0$; il contient donc l'idéal engendré par les x_i, qui est J. □

Démonstration du lemme 2. (1) Soit f donné par le lemme 31.3. Appliquons le lemme 31.2 à $S = \{f^n\}$ et au morphisme canonique $g : A \to A_\mathfrak{p}$. Si $g(a) = 0$, alors $a \in J$, donc $fa = 0$; comme $f \in S$, cela signifie $a/1 = 0$ dans A_f. Le morphisme $A_f \to A_\mathfrak{p}$ est donc injectif.

(2) Appliquons le lemme 31.2 à $S = A \setminus \mathfrak{q}$ et au morphisme canonique $g : A \to A_\mathfrak{p}$, qui inverse S puisque $\mathfrak{p} \subseteq \mathfrak{q}$. Si $g(a) = 0$, alors $a = 0$ par l'injectivité supposée de g, et a fortiori $a/1 = 0$ dans $A_\mathfrak{q}$.

(3) Prenons f comme en (1), et soit $\mathfrak{Q}$ un idéal premier de A_f dont la trace $\mathfrak{q}$ sur A contient $\mathfrak{p}$. Le morphisme $h : A_f \to A_\mathfrak{p}$ envoie $A_f \setminus \mathfrak{Q}$ dans les inversibles : écrivons $y \in A_f \setminus \mathfrak{Q}$ sous la forme $y \cdot (f^n/1) = a/1$; si a était dans $\mathfrak{p}$, donc dans $\mathfrak{q}$, $a/1 = y \cdot (f^n/1)$ serait dans $\mathfrak{Q}$, ce qui est exclu puisque $y \notin \mathfrak{Q}$ et que $f^n/1$, inversible, n'est pas dans $\mathfrak{Q}$. Donc $a \notin \mathfrak{p}$, $h(y)\, h(f^n/1) = a/1$ est inversible dans $A_\mathfrak{p}$, et $h(y)$ l'est aussi. Le morphisme $(A_f)_\mathfrak{Q} \to A_\mathfrak{p}$ est donc défini, et il est injectif par le lemme 31.2 appliqué à h, qui est injectif par (1) : c'est l'argument de (2) pour l'anneau A_f. □

Démonstration du lemme 1 et du corollaire 1, cas affine. Pour le lemme 1, soit E l'ensemble des $\mathfrak{p}$ tels que $s \notin \mathfrak{p}$ et $\xi_\mathfrak{p} \cdot (s/1) = a/1$. Il est stable par générisation : si $\mathfrak{q} \in E$ et $\mathfrak{p} \subseteq \mathfrak{q}$, alors $s \notin \mathfrak{p}$, et l'image par $A_\mathfrak{q} \to A_\mathfrak{p}$ de l'égalité $\xi_\mathfrak{q} \cdot (s/1) = a/1$ est $\xi_\mathfrak{p} \cdot (s/1) = a/1$. Soit $\mathfrak{p} \in E$, et f donné par le lemme 31.3. L'ouvert $D(f) \cap D(s)$ contient $\mathfrak{p}$. Soit $\mathfrak{q}$ un premier de cet ouvert qui contient $\mathfrak{p}$; le lemme 31.2, appliqué à $S = A \setminus \mathfrak{q}$, montre que $A_\mathfrak{q} \to A_\mathfrak{p}$ est injectif : si $a'/1 = 0$ dans $A_\mathfrak{p}$, alors $fa' = 0$ avec $f \notin \mathfrak{q}$, donc $a'/1 = 0$ dans $A_\mathfrak{q}$. Or $\xi_\mathfrak{q} \cdot (s/1) - a/1$ a pour image $\xi_\mathfrak{p} \cdot (s/1) - a/1 = 0$; il est donc nul, et $\mathfrak{q} \in E$. Le lemme 31.1 s'applique, $\operatorname{Spec} A$ étant noethérien et sobre.

Pour le corollaire 1, on utilise la description du faisceau structural comme faisceau des familles $(\sigma_\mathfrak{p}) \in \prod_{\mathfrak{p} \in U} A_\mathfrak{p}$ qui sont localement des fractions (pour tout $\mathfrak{p} \in U$, il existe un voisinage V de $\mathfrak{p}$ et $a, s \in A$ avec $s \notin \mathfrak{q}$ et $\sigma_\mathfrak{q} = a/s$ pour tout $\mathfrak{q} \in V$), et le fait que $a \mapsto (a/1)_\mathfrak{p}$ est une bijection de A sur les sections globales de ce faisceau. L'injectivité de l'application du corollaire en découle. Soit $(\xi_\mathfrak{p})$ une famille cohérente. Pour chaque $\mathfrak{p}$, écrivons $\xi_\mathfrak{p} \cdot (s/1) = a/1$ avec $s \notin \mathfrak{p}$; l'ensemble E du lemme 1 pour ces a et s est un voisinage ouvert de $\mathfrak{p}$, sur lequel $\xi_\mathfrak{q} = a/s$. La famille $(\xi_\mathfrak{p})$ est donc localement une fraction, c'est une section globale du faisceau structural, et elle provient d'un $a \in A$. □

Remarque. Le corollaire 1, dans le cas affine, est un cas d'un énoncé de D. Ferrand sur les modules qui sont limite projective de leurs localisés, annoncé sans démonstration en 1966 [50] et démontré dans une note de février 2004 (proposition 3).

Remarque. Le lemme 31.1 est le « donc » de la page 3. De la constructibilité, la page passe aussitôt à la propriété « s'il contient x, il contient les points d'un ouvert non vide de $\bar{x}$ ». Le lemme prend pour hypothèse cette propriété, jointe à la stabilité par générisation, et la constructibilité n'intervient pas dans la démonstration.

Remarque. Les énoncés sont démontrés pour un espace noethérien, et le corollaire 1 pour $X = \operatorname{Spec} A$ affine. C'est le cas auquel la page se ramène (« La question est locale. On peut donc supposer X noethérien »). La page 3 écrit « un voisinage U de $\bar{x}$ tel que pour tt $y \in \bar{x} \cap U$ ». Un ouvert contenant tout $\overline{\{x\}}$ donnerait une condition plus forte que (H), qui l'entraîne. La démonstration de la page, comme celle-ci, n'emploie que la forme faible, « un ouvert non vide U de $\bar{x}$ ». L'injectivité de $\Gamma(X, F) \to \varprojlim F_x$ ne demande ni (H) ni l'hypothèse noethérienne, et celle de $A \to \varprojlim A_\mathfrak{p}$ vaut pour tout anneau commutatif.

Remarque. L'hypothèse noethérienne n'intervient pas dans (2) du lemme 2, qui vaut pour tout anneau commutatif. Dans (1), elle sert seulement à rendre de type fini le noyau J de $A \to A_\mathfrak{p}$. Ce noyau est formé des éléments annulés par *un* élément de $A \setminus \mathfrak{p}$. L'annulateur de $A \setminus \mathfrak{p}$, que glose la page, est en général plus petit et ne convient pas. La démonstration de la page prend un annulateur par générateur, et suit donc la bonne description.

Remarque. Mathlib contient l'énoncé « constructible et stable par générisation, donc ouvert » pour les spectres d'anneaux, mais pas le critère de constructibilité des espaces noethériens par lequel la page y arrive ; le lemme 31.1 fait les deux pas à la fois.

Remarque. Dans la forme (3) du lemme 2, l'hypothèse que la trace de $\mathfrak{Q}$ contienne $\mathfrak{p}$ est celle de la page, « provenant d'un idéal $q' \supset p$ ne rencontrant pas f » ; elle rend la flèche $(A_f)_\mathfrak{Q} \to A_\mathfrak{p}$ définie. La démonstration n'a pas besoin de l'identification $A_\mathfrak{p} = (A_f)_{\mathfrak{p}A_f}$ par laquelle la page se ramène au cas $f = 1$. Le corollaire 1 n'utilise du lemme 2 que le lemme 31.3. Un même f tue le noyau de $A \to A_\mathfrak{p}$ et rend injectives toutes les flèches $A_\mathfrak{q} \to A_\mathfrak{p}$ pour $\mathfrak{q} \in D(f) \cap V(\mathfrak{p})$: c'est (H) pour le faisceau structural. Dans la démonstration du lemme 1, l'argument donne l'égalité $s_y = \xi_y$, là où la page écrit « d'où $s_x = \xi_y$ ».

Ne sont pas démontrés ici : le corollaire 1 pour un préschéma localement noethérien non affine ; les deux contre-exemples. Les corollaires 2 et 3 (pleine fidélité) sont démontrés dans l'encadré suivant, et le lemme 3 sous la forme de la page, « F vérifie (H) », dans le dernier encadré de la section.

Théorème (D'après les pages 1 à 6, réseaux d'anneaux locaux, forme corrigée par l'édition ♦)**.** *Soient S un préschéma localement noethérien, X et Y des S-préschémas localement de type fini, Y séparé sur S. Les S-morphismes $X \to Y$ correspondent bijectivement aux homomorphismes de réseaux d'anneaux locaux $p(X) \to p(Y)$ au-dessus de $p(S)$: applications croissantes des ensembles ordonnés de spécialisation, munies d'homomorphismes locaux compatibles $\mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$. L'hypothèse « Y séparé » est celle de l'édition.*

Conventions. Un homomorphisme de réseaux $\Phi : p(X) \to p(Y)$ au-dessus de $p(S)$ est la donnée d'une application $\varphi : X \to Y$ telle que $x \rightsquigarrow x'$ entraîne $\varphi(x) \rightsquigarrow \varphi(x')$ et que $s_Y(\varphi(x)) = s_X(x)$, et, pour chaque x, d'un homomorphisme local $\alpha_x : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$. On demande deux compatibilités : pour $x \rightsquigarrow x'$, le carré formé de $\alpha_{x'}$, α_x et des flèches de générisation $\mathcal{O}_{Y,\varphi(x')} \to \mathcal{O}_{Y,\varphi(x)}$, $\mathcal{O}_{X,x'} \to \mathcal{O}_{X,x}$ commute ; et le composé $\mathcal{O}_{S,s_X(x)} \to \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$ est la flèche de s_X. La condition de localisation de la page 1 porte sur $p(X)$ et $p(Y)$, qui viennent de préschémas ; elle n'a pas à figurer dans les homomorphismes. Un S-morphisme f donne $p(f) = (f, (f^\sharp_x)_x)$. On appelle *germe* de Φ en x le morphisme $g_x = \operatorname{Spec}(\alpha_x)$ suivi de $\operatorname{Spec}\mathcal{O}_{Y,\varphi(x)} \to Y$; c'est un S-morphisme $\operatorname{Spec}\mathcal{O}_{X,x} \to Y$, et pour $x \rightsquigarrow x'$ le germe g_x est $g_{x'}$ précédé de $\operatorname{Spec}\mathcal{O}_{X,x} \to \operatorname{Spec}\mathcal{O}_{X,x'}$. Le germe de $p(f)$ en x est $\operatorname{Spec}\mathcal{O}_{X,x} \to X \xrightarrow{f} Y$.

Démonstration. Φ est déterminé par ses germes. Le point fermé de $\operatorname{Spec}\mathcal{O}_{X,x}$ va sur $\varphi(x)$; et $\operatorname{Spec}\mathcal{O}_{Y,y} \to Y$ est un monomorphisme, de sorte que g_x détermine $\operatorname{Spec}(\alpha_x)$, donc α_x.

Injectivité (corollaire 2). Si $p(f) = p(f')$, les composés de f et f' avec $\operatorname{Spec}\mathcal{O}_{X,x} \to X$ coïncident pour tout x. Comme X est localement noethérien, il existe un ouvert affine $U \ni x$ tel que $\Gamma(U, \mathcal{O}_X) \to \mathcal{O}_{X,x}$ soit injectif (lemme 2, (1)) ; f et f' coïncident alors sur un voisinage de x, et, ces voisinages recouvrant X, $f = f'$. Ni la séparation ni la finitude de Y ne servent ici.

Le pas local du lemme 3. Soient $x \rightsquigarrow x''$ tels que $\mathcal{O}_{X,x''} \to \mathcal{O}_{X,x}$ soit injectif, et a, b : $\operatorname{Spec}\mathcal{O}_{X,x''} \to Y$ deux S-morphismes qui coïncident après $\operatorname{Spec}\mathcal{O}_{X,x} \to \operatorname{Spec}\mathcal{O}_{X,x''}$. L'égalisateur de a et b est un sous-schéma fermé parce que Y est séparé sur S, et $\operatorname{Spec}\mathcal{O}_{X,x} \to \operatorname{Spec}\mathcal{O}_{X,x''}$

se factorise par lui. Le noyau de cette flèche est nul, l'anneau étant injecté ; celui de l'égalisateur, plus petit, l'est aussi, et une immersion fermée de noyau nul est un isomorphisme : $a = b$. L'injectivité demandée a lieu pour x'' dans un ouvert affine $U \ni x$ où $\Gamma(U, \mathcal{O}_X) \to \mathcal{O}_{X,x}$ est injectif, puisque $\mathcal{O}_{X,x''}$ est alors un localisé de $\Gamma(U, \mathcal{O}_X)$.

Le lieu d'accord est ouvert (lemme 1). Soient W un préschéma localement noethérien, $\iota : W \to X$ et $h : W \to Y$ avec $s_Y h = s_X \iota$. Disons que h s'accorde à Φ en w si le composé $\operatorname{Spec} \mathcal{O}_{W,w} \to W \xrightarrow{h} Y$ est le germe $g_{\iota(w)}$ précédé de $\operatorname{Spec}(\iota^\sharp_w)$. Ce lieu E est stable par générisation, par la compatibilité des germes. Si $w \in E$, prenons l'ouvert affine $U \ni w$ du pas précédent : pour $w'' \in U \cap \overline{\{w\}}$, les deux morphismes $\operatorname{Spec} \mathcal{O}_{W,w''} \to Y$ à comparer coïncident après $\operatorname{Spec} \mathcal{O}_{W,w} \to \operatorname{Spec} \mathcal{O}_{W,w''}$, puisque $w \in E$, et le pas local donne $w'' \in E$. Le lemme 31.1, appliqué dans chaque ouvert affine de W, qui est un espace noethérien, montre que E est ouvert.

Surjectivité (corollaire 3). Soit Φ. Comme Y est localement de type fini sur S et que $\Gamma(U, \mathcal{O}_X) \to \mathcal{O}_{X,x}$ est injectif pour un ouvert affine $U \ni x$, le germe g_x se prolonge en un S-morphisme $f_x : U_x \to Y$ sur un ouvert $U_x \ni x$: c'est le théorème de passage à la limite d'EGA IV qu'invoque la lecture. Par le pas précédent, le lieu $V_x \subseteq U_x$ où f_x s'accorde à Φ est un ouvert, qui contient x. Sur $V_x \cap V_{x'}$, les restrictions de f_x et $f_{x'}$ s'accordent toutes deux à Φ en tout point, donc ont les mêmes germes, et coïncident par l'argument de l'injectivité. Elles se recollent en un S-morphisme $f : X \to Y$ dont les germes sont ceux de Φ, donc $p(f) = \Phi$. □

Remarque. Lean démontre l'énoncé dans `Folder42.lean`, espace `Reseau`, sous des hypothèses un peu plus larges : X localement noethérien, Y localement de type fini et séparé sur un S quelconque (`toReseau_bijective`) ; la forme de la page, S localement noethérien et X localement de type fini, s'en déduit (`corollaire3`). Les homomorphismes de réseaux sont la structure `ReseauHom`, et $p(f)$ est `toReseau`. L'injectivité, `toReseau_injective`, ne demande que X localement noethérien. La séparation de Y n'intervient qu'au pas local du lemme 3, `ext_of_injective_of_isSeparated` ; le lieu d'accord ouvert est `isOpen_matches`, qui s'appuie sur `isOpen_of_stableUnderGeneralization_of_locally`, version localement noethérienne du lemme 31.1 ; la surjectivité est `toReseau_surjective`. Le prolongement d'un germe en un morphisme sur un voisinage est pris dans mathlib (`spread_out_of_isGermInjective'`), avec l'unicité correspondante (`spread_out_unique_of_isGermInjective'`). La démonstration ne passe pas par le faisceau $U \mapsto \operatorname{Hom}_S(U, Y)$ ni par la proposition de la page 3 ; elle en reprend les deux pas, le lemme 1 et le lemme 3, sur les germes eux-mêmes. Le lemme 3 sous la forme de la page fait l'objet de l'encadré suivant. La question marginale de la page 6 sur la nécessité de l'hypothèse noethérienne et le cas non séparé ne sont pas formalisés.

Théorème (Lemme 3, page 5, forme de la page ♦). *Soient X un S-préschéma localement noethérien et Y un S-préschéma séparé sur S. Le préfaisceau $F : U \mapsto \operatorname{Hom}_S(U, Y)$ est un faisceau sur X, et il vérifie (H). Plus précisément, si $x \rightsquigarrow y$ et si $\mathcal{O}_{X,y} \to \mathcal{O}_{X,x}$ est injectif, alors $\rho_{yx} : F_y \to F_x$ est injective. Si de plus X est noethérien, $\operatorname{Hom}_S(X, Y) \to \varprojlim_x F_x$ est bijective (corollaire 2, par la proposition de la page 3). L'hypothèse « Y séparé » est celle de l'édition.*

Démonstration. F est un faisceau. Si $V = \bigcup_i U_i$ et si des S-morphismes $f_i : U_i \to Y$ coïncident deux à deux sur $U_i \cap U_j$, qui est le produit fibré de $U_i \to V \leftarrow U_j$, ils se recollent en un unique $f : V \to Y$, qui est un S-morphisme parce qu'il l'est sur chaque U_i.

Les germes. Pour $x \in U$, notons $\operatorname{Spec} \mathcal{O}_{X,x} \to U$ la flèche canonique. Deux sections $a \in F(U)$, $b \in F(V)$ ont le même germe en x si et seulement si leurs composés avec $\operatorname{Spec} \mathcal{O}_{X,x} \to U$ et

$\operatorname{Spec}\mathcal{O}_{X,x} \to V$ coïncident. Dans un sens, ces flèches se factorisent par un voisinage de x où a et b coïncident. Dans l'autre, $U \cap V$ est localement noethérien, et deux morphismes qui coïncident sur $\operatorname{Spec}\mathcal{O}_{X,x}$ coïncident au voisinage de x (le prolongement unique de mathlib, déjà employé pour l'injectivité du corollaire 2).

L'injectivité. Soient $x \rightsquigarrow y$ avec $\mathcal{O}_{X,y} \to \mathcal{O}_{X,x}$ injectif, et a, b deux sections au voisinage de y dont les germes ont même image dans F_x, c'est-à-dire, l'ouvert contenant aussi x, mêmes germes en x. Leurs composés avec $\operatorname{Spec}\mathcal{O}_{X,y} \to Y$ sont deux S-morphismes qui coïncident après $\operatorname{Spec}\mathcal{O}_{X,x} \to \operatorname{Spec}\mathcal{O}_{X,y}$. Le pas local du lemme 3 de l'encadré précédent les rend égaux, et les germes en y sont égaux.

La condition (H). Soit $W \ni x$ un ouvert affine où $\Gamma(W, \mathcal{O}_X) \to \mathcal{O}_{X,x}$ est injectif. Pour $y \in W \cap \overline{\{x\}}$, $\mathcal{O}_{X,y}$ est un localisé de $\Gamma(W, \mathcal{O}_X)$, donc $\mathcal{O}_{X,y} \to \mathcal{O}_{X,x}$ est injectif, et l'étape précédente s'applique. Pour $X = \operatorname{Spec} A$ avec $A \to A_{\mathfrak{p}}$ injectif, c'est le lemme 2, (2), qui donne l'injectivité de $A_{\mathfrak{q}} \to A_{\mathfrak{p}}$ pour $\mathfrak{q} \supseteq \mathfrak{p}$, comme le veut la page. Le corollaire 2 est la proposition de la page 3 appliquée à F, l'espace sous-jacent d'un préschéma noethérien étant noethérien et sobre. □

Remarque. Lean démontre l'énoncé dans `Folder42.lean`, espace `Reseau`, pour un S quelconque : le faisceau est `homSheaf` (`isSheaf_homPresheaf`), la description des germes `germ_homSheaf_eq_iff`, l'injectivité `stalkSpecializes_homSheaf_injective`, la condition (H) `lemme3`, et le corollaire 2 sous forme faisceautique `corollaire2`, qui applique `proposition` à `homSheaf`. La séparation ne sert, là encore, qu'à `ext_of_injective_of_isSeparated`. La forme affine de la page, avec $A_{\mathfrak{q}} \to A_{\mathfrak{p}}$, n'est pas énoncée en Lean : l'énoncé formalisé porte sur l'injectivité de $\mathcal{O}_{X,y} \to \mathcal{O}_{X,x}$, et l'identification de ces anneaux locaux aux localisés de A n'y est pas écrite.

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, page 12, critère d'immersion ouverte ♦). *Sur une base localement noethérienne S, un monomorphisme formellement étale $u : G \to F$ de foncteurs sur les S-schémas est une immersion ouverte dès que F et G sont des faisceaux fpqc qui commutent aux limites inductives filtrantes d'anneaux et aux limites adiques d'anneaux artiniens.*

◊ non vérifié en Lean

Démonstration donnée par l'édition, non vérifiée en Lean.

La page dit « infinitésimalement étale », et le mot « adiques » y est incertain. Mathlib n'a pas la descente fpqc des foncteurs sur les schémas. On se reportera aux notes de Grothendieck (102, lot 1, p. 12).

Théorème (Grothendieck, pages 2 à 4, 15 et 19, critère valuatif de platitude d'une adhérence ♦). *Soient $X \to Y$ localement noethérien, F cohérent sur X, U un ouvert rétrocompact et G_U un quotient cohérent de $F|_U$, plat sur Y. Si les anneaux locaux de X aux points de $X - U$ ont des fibres formelles géométriquement normales, alors $G = \operatorname{Im}(F \to i_* G_U)$ est plat sur Y, avec U universellement G-dense relativement à Y, si et seulement s'il en est ainsi après tout changement de base $Y' \to Y$ où Y' est artinien ou un trait.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 3 et 4). La page 4 est en grande partie illisible, et le « vrai théorème » de la page 15, qui porte « artinien ou trait », est sans démonstration ; le mot « artinien » n'est incertain que dans la remarque 1.4.2 qui le précède. Mathlib n'a pas la densité schématique universelle ni les fibres formelles. On se reportera aux notes de Grothendieck (127, lot 1, p. 2).

Théorème (Grothendieck, pages 7, 9, 10 et 12, ouverture de Hironaka sur une base réduite ; voir aussi Kollár 2011 ♦). *Soient $f : X \to Y$ de type fini, Y noethérien, et $\mathcal{O}_{Y,y}$ réduit à fibres formelles géométriquement normales. Supposons f universellement ouvert en x, à fibres équidimensionnelles de même dimension près de x, X_y réduit aux générisations maximales de x et $(X_y)_{\mathrm{red}}$ géométriquement normal. Alors x a un voisinage ouvert U tel que $U_{\mathrm{red}} \to Y$ soit plat à fibres géométriquement normales.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 9 à 12), avec un « lemme à dégager » jamais écrit. D'après le résumé de l'article de Kollár, Hironaka traite le cas d'une base régulière. Mathlib n'a pas les fibres formelles ni les morphismes universellement ouverts. On se reportera aux notes de Grothendieck (127, lot 1, p. 7).

Théorème (Grothendieck, pages 2 et 3, descente non plate sur une base artinienne ♦). *Sur une base artinienne Y, le problème d'un quotient plat G de F qui prolonge G_U, avec $G \to i_* G_U$ universellement injectif relativement à Y, descend le long de tout épimorphisme de schémas $Y' \to Y$, plat ou non, pourvu que $Y' \to Y$ soit fini, ou que f et la solution soient de présentation finie. La solution, si elle existe, est unique.*

◊ non vérifié en Lean

Le lemme 1.3 n'est pas démontré, et l'alternative « fini ou de présentation finie » vient d'une note au crayon. Mathlib n'a pas la descente le long des épimorphismes de schémas. On se reportera aux notes de Grothendieck (127, lot 1, p. 2).

Théorème (Grothendieck, pages 1 à 5, 13 et 15, représentabilité par un schéma localement quasi-fini ; voir aussi Murre 1965 ♦). *Un foncteur F sur les schémas au-dessus d'un S localement noethérien est représentable par un S-schéma séparé localement quasi-fini si et seulement s'il vérifie la descente fpqc, testée sur $B \to \hat{B}$, la présentation finie locale, l'effectivité sur $\hat{B} = \varprojlim B_n$, la pro-représentabilité sur les anneaux artiniens par des anneaux finis sur eux, le critère valuatif de séparation, et deux conditions de « modularité », l'une locale sur les bases locales complètes, l'autre générique.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 1 à 5) : la dernière étape s'arrête à la condition de constructibilité, et deux propositions formelles ne sont pas démontrées. Murre traite le cas non ramifié et dit seulement que le cas localement quasi-fini est possible. Mathlib n'a pas les critères de représentabilité de type Artin. On se reportera aux notes de Grothendieck (131, lot 1, p. 1).

Théorème (Grothendieck, pages 8, 9 et 19, Tor génériques et suites régulières : l'énoncé en un point ♦). *Soient A un anneau commutatif, J un idéal nilpotent de A ($J^n = 0$), $A_0 = A/J$, et R un A-module quelconque. On suppose que les gradués $\mathrm{gr}^k_J(A) = J^k A / J^{k+1} A$ sont des A_0-modules libres et que les gradués $\mathrm{gr}^k_J(R) = J^k R / J^{k+1} R$ sont des A_0-modules plats. Alors toute suite A-régulière $t = (t_1, \ldots, t_r)$ est R-régulière, et son image dans A_0 est A_0-régulière. Si A est local noethérien, il suffit que les $\mathrm{gr}^k_J(A)$ soient plats sur A_0 ; si de plus R est de type fini non nul et les t_i dans l'idéal maximal, t est une suite R-régulière au sens strict. C'est la situation de $A_{\mathfrak{p}}$, $\mathfrak{p} \in U$, dans les lemmes 6 et 16 ; le complexe de Koszul de t résolvant $A/(t)$, on en tire $\mathrm{Tor}_i^A(R, A/(t)) = 0$ pour $i > 0$.*

Démonstration. Trois outils. (1) Deux sur trois : pour une suite exacte $0 \to M' \to M \to M'' \to 0$ et t faiblement régulière sur M'', t est faiblement régulière sur M' si et seulement si elle l'est sur M, et $M'/(t)M' \to M/(t)M$ reste injective (c'est l'annulation de $\mathrm{Tor}_1(M'', A/(t))$ que demande la page) ; on le voit élément par élément, par le lemme du serpent. (2) Dévissage : si t est faiblement régulière sur les gradués $\mathrm{gr}^k_J(M)$ pour $k < j$, elle l'est sur $M/J^j M$, par la suite exacte $0 \to \mathrm{gr}^j_J(M) \to M/J^{j+1}M \to$

$M/J^jM \to 0$ et (1) ; avec $J^nM = 0$, elle l'est sur M. (3) Platitude : si $\bar{t}$ est A_0-régulière, elle l'est sur tout A_0-module plat $N = N \otimes_{A_0} A_0$. Le pas de récurrence du lemme 6 se fait alors ainsi. Supposons $\bar{t}_1, \dots, \bar{t}_k$ déjà A_0-régulière, et soit J^m le dernier gradué non nul de A ($J^{m+1} = 0$), libre et non nul sur A_0. Par (3) et (2), $(t_1, \dots, t_k)$ est faiblement régulière sur A/J^m, donc, par (1), $J^m/(t)J^m$ s'injecte dans $A/(t)A$, où t_{k+1} est régulier ; il l'est donc sur $J^m/(t)J^m \simeq (A_0/(\bar{t}))^{(I)}$, $I \neq \emptyset$, et, en restreignant à un facteur, sur $A_0/(\bar{t}_1, \dots, \bar{t}_k)$. Une fois $\bar{t}$ régulière dans A_0, (3) la rend régulière sur chaque $\mathrm{gr}^k_J(R)$ et (2) sur R. Comme le dit la note de la page 19, la liberté ne sert, côté module, qu'à travers la platitude, et aucune finitude n'est demandée à R. Dans le cas local noethérien, les $\mathrm{gr}^k_J(A)$ sont de type fini sur l'anneau local A_0, et plats, donc libres. Lean (`Folder94.lean`) démontre (1) (`isWeaklyRegular_iff_of_exact`, `injective_mapQ_of_exact`), (2) (`isWeaklyRegular_quotient_filt`, `isWeaklyRegular_of_layers`), (3) (`isWeaklyRegular_of_flat`), le pas de récurrence (`isWeaklyRegular_quotient_of_layers_free`), l'énoncé (`isWeaklyRegular_of_gr`) et sa forme locale (`isWeaklyRegular_of_gr_flat_of_isLocalRing`, `isRegular_of_gr_flat_of_isLocalRing`).

Ne sont pas démontrés en Lean : le passage de la régularité de t sur R à l'annulation des Tor_i par le complexe de Koszul (Mathlib n'a ni les complexes de Koszul ni la suite exacte longue des Tor ; seul l'analogue de Tor_1 ci-dessus l'est), et l'ouvert dense de l'énoncé global ci-dessous. On se reportera aux notes de Grothendieck (94, lot 1, p. 8).

Théorème (Grothendieck, pages 8 et 9, l'ouvert dense pour $X = S$ ♦). *Soient A un anneau noethérien, J un idéal nilpotent de A tel que $A_0 = A/J$ soit réduit (par exemple le nilradical), et R un A-module de type fini. Il existe un ouvert dense $U \subset \mathrm{Spec}\, A$ tel que, pour tout $\mathfrak{p} \in U$, toute suite $A_\mathfrak{p}$-faiblement régulière d'éléments de $A_\mathfrak{p}$ soit $R_\mathfrak{p}$-faiblement régulière. On peut prendre pour U le lieu, dans $\mathrm{Spec}\, A = \mathrm{Spec}\, A_0$, où les gradués non nuls, en nombre fini, $\mathrm{gr}^k_J(A)$ et $\mathrm{gr}^k_J(R)$ sont libres sur A_0.*

Démonstration. Les gradués sont des A_0-modules de type fini, donc de présentation finie, et leur lieu de liberté est ouvert ; l'intersection U de ces lieux contient les idéaux premiers minimaux, où l'anneau réduit A_0 se localise en un corps, et un ensemble qui contient les premiers minimaux est dense. Les gradués commutent à la localisation : $\mathrm{gr}^k_J(S^{-1}M) = S^{-1}\mathrm{gr}^k_J(M)$, car $J^k(S^{-1}M)$ est le localisé de J^kM ; si $\mathfrak{p}$ est au-dessus de $\mathfrak{q} \in \mathrm{Spec}\, A_0$, on a donc $\mathrm{gr}^k_J(M_\mathfrak{p}) = (A_0)_\mathfrak{q} \otimes_{A_0} \mathrm{gr}^k_J(M)$, libre sur $(A_0)_\mathfrak{q}$ pour $\mathfrak{p} \in U$. Le pas de récurrence de l'énoncé en un point vaut avec n'importe quelle A-algèbre B au lieu de A_0 et n'importe quel module non nul T au lieu de A, par la même démonstration ; avec $B = (A_0)_\mathfrak{q}$ et $T = A_\mathfrak{p}$, toute suite d'éléments de A faiblement régulière sur $A_\mathfrak{p}$ l'est sur $R_\mathfrak{p}$. Enfin tout élément de $A_\mathfrak{p}$ est le produit d'une unité par l'image d'un élément de A, et la régularité faible ne dépend de la suite qu'à des unités près. Lean (`Folder94.lean`) démontre la commutation à la localisation (`isLocalizedModule_layerMap`, `layerEquiv`), le pas de récurrence généralisé (`isWeaklyRegular_of_gr'`) et l'énoncé (`exists_isOpen_dense_isWeaklyRegular'`).

Théorème (Grothendieck, pages 8, 9 et 19, Tor génériques et suites régulières : l'ouvert dense ♦). *Soient $S = \mathrm{Spec}\, A$ noethérien, non nécessairement réduit, et R un faisceau cohérent sur un S-schéma X de type fini. Il existe un ouvert dense $U \subset S$ tel que $\mathrm{Tor}^A_i(R, A_\mathfrak{p}/(t)) = 0$ pour tout $i > 0$, tout $\mathfrak{p} \in U$ et toute suite $A_\mathfrak{p}$-régulière t. C'est un substitut de la platitude générique, qui tombe en défaut sur une base non réduite.*

◊ non vérifié en Lean

Le pas de récurrence du lemme 6, que la page dit « bien standard », est de l'édition, et la page écrit $\mathrm{gr}_J(\mathcal{O}_X)$ là où l'argument demande $\mathrm{gr}_J(R)$. L'énoncé en un point et le cas $X = S$ ci-dessus, pour la régularité des suites, sont vérifiés en Lean ; restent le passage aux Tor par le complexe de Koszul, et, pour X de type fini, la platitude générique, que Mathlib n'a pas. On se reportera aux notes de Grothendieck (94, lot 1, p. 8).

Théorème (Grothendieck, pages 15 et 16, critère de représentabilité sur $\mathrm{Mod}(A)$; voir aussi Hall 2013 ♦). *Soit A un anneau noethérien quotient d'un anneau régulier. Un foncteur $F : \mathrm{Mod}(A) \to \mathrm{Ens}$ est de la forme $\mathrm{Hom}_A(P, -)$ avec P fini si et seulement s'il est exact à gauche, commute aux limites inductives filtrantes, vérifie une condition de complétion $\mathfrak{m}_\mathfrak{p}$-adique et une g-adique sur les modules finis, envoie les modules finis sur des modules finis, a une fonction $\mathfrak{p} \mapsto \dim F(k(\mathfrak{p}))$ constructible et, pour tout quotient B et tout B-module fini Ω, commute génériquement à la réduction de Ω modulo les systèmes de paramètres. La conservation des produits n'en fait pas partie.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 15 et 16) : plusieurs liens sont de l'édition, et la démonstration telle qu'elle est écrite n'est sûre que pour A excellent. Hall énonce un autre critère, par la conservation des produits. Mathlib n'a pas ces conditions de complétion sur les foncteurs de modules. On se reportera aux notes de Grothendieck (94, lot 1, p. 15).

Piste dont l'énoncé dépend d'une lecture à vérifier :

— Cote 94 : pour A noethérien dont tout quotient intègre est génériquement normal, et F exact à gauche, commutant aux limites inductives filtrantes et vérifiant la condition de complétion locale et la finitude locale, la représentabilité de F par un module fini sur un ouvert non vide de chaque $V(\mathfrak{p})$ équivaut à la constructibilité de $\mathfrak{p} \mapsto \dim_{k(\mathfrak{p})} F(k(\mathfrak{p}))$. La réciproque repose sur le milieu de la page 7, en grande partie illisible, et l'hypothèse de normalité sur une lecture incertaine, à vérifier sur le fac-similé. Mathlib n'a pas la constructibilité de ces fonctions de rang. On se reportera aux notes de Grothendieck (94, lot 1, p. 7). ♦

Contre-exemple 31.4 (Page 7, la réciproque de la remarque 5 bis sous la finitude locale). [a] *Sur $A = k[x, y]$, k un corps infini, soient $a_2, a_3, \ldots$ des éléments distincts de k et $h_j = x - a_j$. Le foncteur $F(M) = \varinjlim (M \xrightarrow{h_2} M \xrightarrow{h_3} M \to \cdots)$ est l'identité sur chaque $A_\mathfrak{p}$, vérifie la condition de complétion et la finitude locale, et $\dim_{k(\mathfrak{p})} F(k(\mathfrak{p})) = 1$ pour tout $\mathfrak{p}$; pourtant $F(A_g)$ n'est de type fini sur A_g pour aucun $g \neq 0$, et F n'est représentable sur aucun ouvert non vide de $\mathrm{Spec}\, A$.*

a. Preuve vérifiée : `lean/Grothendieck/Folder94.lean`.

Démonstration. Un idéal premier contient au plus un h_j, donc presque tous les h_j sont inversibles dans $A_\mathfrak{p}$ et F y est l'identité à partir d'un rang (`tele_atPrime_bijective`) ; d'où les conditions locales et la dimension 1 des fibres (`finrank_tele_field`). Un $g \neq 0$ n'est divisible que par un nombre fini de h_j, et $F(A_g)$ est la réunion strictement croissante des $(h_2 \cdots h_i)^{-1} A_g$ (`not_finite_tele_away`, `not_representable_away`). L'exactitude à gauche et la commutation aux limites inductives filtrantes sont classiques et ne sont pas formalisées. Sous la finitude globale, $F(M)$ de type fini pour tout M de type fini, que l'esquisse de la page utilise, la réciproque tient, et sans l'hypothèse sur le lieu normal : sur un ouvert de $V(\mathfrak{p})$ où le rang vaut n, les modules locaux de la proposition 4 sont libres de rang n, $F(B)$ est projectif de type fini et $F(B) \otimes M \to F(M)$ est un isomorphisme en chaque point. Les deux étapes d'algèbre commutative de cet argument sont démontrées en Lean ci-dessous ; la proposition 4 et le passage du foncteur F à ces énoncés ne le sont pas. Quelle finitude la page écrit au juste reste à lire sur le fac-similé.

Théorème (Page 7, rang constant sur un anneau réduit ♦). *Soient B un anneau local réduit, de corps résiduel k, et P un B-module de type fini tel que $\dim_{B_\mathfrak{q}}(B_\mathfrak{q} \otimes_B P) = \dim_k(k \otimes_B P)$ pour tout idéal premier minimal $\mathfrak{q}$ ($B_\mathfrak{q}$ est alors un corps). Alors P est libre. Par suite, si P est de présentation finie sur un anneau B, à localisés libres aux idéaux maximaux, et si $\varphi\colon P \otimes_B M \to N$ est bijectif après localisation en chaque idéal maximal, P est projectif et $N \simeq \mathrm{Hom}_B(P^\vee, M)$.*

Démonstration. Une base de $k \otimes P$ se relève, par Nakayama, en une surjection $B^n \to P$. En un premier minimal $\mathfrak{q}$, elle devient une surjection entre deux $B_\mathfrak{q}$-espaces de même dimension n, donc une bijection ; les coordonnées d'un élément du noyau ont donc une image nulle dans chaque $B_\mathfrak{q}$, sont dans chaque premier minimal, donc nilpotentes, donc nulles. Aucune hypothèse noethérienne n'est utile. Pour le second point, la projectivité se lit sur les localisés en les idéaux maximaux, de même que la bijectivité de φ, et $P \otimes M \simeq P^{\vee\vee} \otimes M \simeq \mathrm{Hom}(P^\vee, M)$ pour P projectif de type fini. C'est ce qu'on applique à $P = F(B)$ et $\varphi\colon F(B) \otimes M \to F(M)$ dans la réciproque sous la finitude globale. Lean (`Folder94.lean`) : `free_of_finrank_eq_of_isReduced`, `nonempty_equiv_hom_dual`.

Partie 16

K-théorie, classes de Chern et Riemann–Roch

Le 3 novembre 1970, il demande à Daniel Ferrand s'il peut compter sur l'exposé XI de SGA 6 avant la fin de décembre, ou si le volume doit paraître sans lui (37, lot 4, p. 73). La cote 153, datée « [à partir de 1982] », reprend les λ-anneaux plus de dix ans après.

32 Cote 2 : une classe non nulle de classe de Chern totale triviale [34]

Cette partie suit le groupe de Grothendieck $K(X)$ d'une variété X. On y range les faisceaux cohérents sous une seule règle : une suite exacte $0 \to E' \to E \to E'' \to 0$ donne $[E] = [E'] + [E'']$; le produit tensoriel en fait un anneau. Les classes de Chern traduisent une classe de $K(X)$ en classes de cycles : la classe de Chern totale $c(x) = 1 + c_1(x) + c_2(x) + \cdots$, dans l'anneau de Chow $A(X)$, vérifie $c(x+y) = c(x)\,c(y)$ et vaut $1 + c_1(L)$ pour un fibré en droites L. Le théorème de Riemann–Roch de Grothendieck dit comment se comporte par image directe le caractère de Chern, version additive de c qui demande des coefficients rationnels. La cote 2 garde les classes de Chern entières, et le prix se lit dans le facteur $(r-1)!$ des énoncés ci-dessous. La cote 47 (partie « Variétés abéliennes et schémas de Picard ») applique le théorème à l'addition m_A et à la projection pr_2 d'un schéma abélien, à côté de l'inversion de Fourier relative, qui est le théorème 1.1 de Mukai (1987) [102]. La cote 153 (section 34) revient aux λ-anneaux, le cadre algébrique de $K(X)$ et de ses opérations, par les polynômes à valeurs entières. Le théorème de Riemann–Roch lui-même n'est vérifié en Lean nulle part dans cette annexe : mathlib n'a ni $K(X)$ ni les classes de Chern, et les sections 32 et 34 démontrent l'algèbre de quelques calculs, dans des modèles explicites.

La cote 2, *Théorème de Riemann-Roch*, notes que l'inventaire dit antérieures à 1958, calcule aux pages 9 à 13 la classe de Chern de l'image directe par l'immersion $i : X \to X \times \mathbf{P}^r$ d'une section constante (2, lot 1, p. 9). Dans $K(\mathbf{P}^r) = \mathbf{Z}[\xi]/(\xi^{r+1})$, $\xi = 1 - L^{-1}$, la classe d'un point est $\xi^r = \sum_i (-1)^i \binom{r}{i} L^{-i}$, et $c(L^{-i}) = 1 - i\eta$, où η est la classe d'un hyperplan. Lean démontre l'algèbre des deux pages, dans le modèle du principe de scindage que suit la lecture : $i_!(\mathcal{O}_Y) = \sum_i (-1)^i \binom{r}{i} \big([L^{-i}] - [L^{-i} \otimes \mathcal{O}(-Y)]\big)$ et $c(L^{-i} \otimes \mathcal{O}(-Y)) = 1 - y - i\eta$, avec $y = x'$. Une congruence modulo η^{r+1} dans $A[[\eta]]$ est une égalité dans $A[\eta]/(\eta^{r+1})$.

Le premier énoncé calcule la classe de Chern totale du faisceau d'un point de $\mathbf{P}^r$. Pour $r = 1$ on trouve $1 + \eta$, pour $r = 2$, $1 - \eta^2$, et pour $r = 3$, $1 + 2\eta^3$: le coefficient $(r-1)!$ grandit avec la dimension. Le second en tire une conséquence : si la classe y du diviseur Y est tuée par $(r-1)!$, le terme correctif disparaît, et l'image directe $i_!(\mathcal{O}_Y)$ a pour classe de Chern totale 1. Si cette classe est non nulle dans K, elle échappe entièrement aux classes de Chern entières ; c'est l'énoncé encadré plus bas, dont la non-nullité n'est pas vérifiée. Pour $r \le 2$, le coefficient vaut ± 1, l'hypothèse force $y = 0$, et le phénomène ne se produit pas.

Théorème 32.1 (Grothendieck, page 9, la classe de Chern d'un point ♦). *Soient $r \ge 1$ et A un*

34. Preuve vérifiée : `lean/Grothendieck/Folder2.lean`.

anneau commutatif. Dans $A[\eta]/(\eta^{r+1})$*,*

$$\prod_{i=0}^{r}(1-i\eta)^{(-1)^i\binom{r}{i}} \;=\; 1+(-1)^{r-1}(r-1)!\,\eta^r.$$

Théorème 32.2 (D'après la page 13, la classe de Chern de $i_!(\mathcal{O}_Y)$)**.** *Soient* $r\geq 1$*,* A *un anneau commutatif et* $y\in A$ *tel que* $1-y$ *soit inversible (par exemple* y *nilpotent) et* $(r-1)!\,y=0$*. Dans* $A[\eta]/(\eta^{r+1})$*,*

$$\prod_{i=0}^{r}\Big(\frac{1-i\eta}{1-y-i\eta}\Big)^{(-1)^i\binom{r}{i}} \;=\; 1,$$

c'est-à-dire $c(i_!(\mathcal{O}_Y))=1$ *dans ce modèle.*

Les deux énoncés tiennent tels que la lecture les donne (`chernPoint`, `chernImmersion`, dans `Folder2.lean`). Le premier est démontré sur $\mathbf{Z}$ par la dérivée logarithmique, au lieu du logarithme de la lecture, puis transporté à tout anneau ; le second en découle, le produit des dénominateurs étant celui des numérateurs où η est remplacé par $\eta/(1-y)$. La page 13 suppose y dans $A^1(X)$; seules servent l'inversibilité de $1-y$ et l'hypothèse $(r-1)!\,y=0$.

Au bas de la page 13, un *N.B.* donne lui-même l'exemple : X une courbe elliptique d'origine 0, $a\neq 0$ un point tel que $a+a=0$, $x=(a)-(0)$ la classe d'un diviseur de degré zéro, et $r=3$. La page affirme que $y=i_!(x)$ n'est pas nul, et que pourtant « les coefficients de la classe de Chern sont nuls ». Dans le même modèle, $x=[\mathcal{O}_a]-[\mathcal{O}_0]=[\mathcal{O}(-0)]-[\mathcal{O}(-a)]$, et l'on note p, q les classes des points 0 et a dans $A^1(X)$. Sur une courbe, $p^2=q^2=0$, et $a+a=0$ donne $2(p-q)=0$.

Théorème 32.3 (Grothendieck, page 13, le *N.B.* : la classe de Chern de $i_!(x)$)**.** *Soient* $r\geq 1$*,* A *un anneau commutatif et* $p,q\in A$ *tels que* $p^2=q^2=0$ *et* $r!\,(p-q)=0$*. Dans* $A[\eta]/(\eta^{r+1})$*,*

$$\prod_{i=0}^{r}\Big(\frac{1-p-i\eta}{1-q-i\eta}\Big)^{(-1)^i\binom{r}{i}} \;=\; 1.$$

Pour $r=3$*, l'hypothèse* $2(p-q)=0$ *suffit.*

Démonstration. C'est encore le même calcul. Si u est un élément inversible de A, le produit des $(u-i\eta)^{(-1)^i\binom{r}{i}}$ est celui du théorème 32.1 où η est remplacé par η/u, les exposants étant de somme nulle ; il vaut donc $1+(-1)^{r-1}(r-1)!\,u^{-r}\eta^r$. Le quotient des deux produits, pour $u=1-p$ et $v=1-q$, vaut 1 dès que $(r-1)!\,(u^{-r}-v^{-r})=0$. Comme $p^2=0$, $(1-p)^{-1}=1+p$ et $(1+p)^r=1+rp$, de sorte que $(r-1)!\,(u^{-r}-v^{-r})=r!\,(p-q)$. Pour $r=3$, $r!=6=3\cdot 2$. □

Voir `chernRatio`, `chernCurve` et `chernEllipticNB` dans `Folder2.lean`.

Théorème (Grothendieck, page 13, une classe non nulle de classe de Chern totale 1)**.** *Soient* X *une courbe elliptique d'origine* 0*,* $a\neq 0$ *un point tel que* $a+a=0$*, et* $x=(a)-(0)\in K(X)$*. La classe* $y=i_!(x)$ *est non nulle dans* $K(X\times\mathbf{P}^3)$*, et sa classe de Chern totale vaut* 1*. Plus généralement, si* $Y\subset X$ *est un diviseur dont la classe* $x'\in A^1(X)$ *est non nulle mais tuée par* $(r-1)!$*, la classe* $i_!(\mathcal{O}_Y)$ *est non nulle et de classe de Chern totale* 1*. (L'hypothèse « tuée par* $(r-1)!$ *» ne s'énonce utilement que pour* $r\geq 3$*, mais elle n'est pas nécessaire : le calcul de* `computations/chern-trivial-2` *donne* $c(i_!x)=1+(-1)^{r-1}r!\,(p-q)\,\eta^r$*, si bien que pour* a *d'ordre* 2 *la classe est déjà triviale pour* $r=2$*.)*

◊ non vérifié en Lean

La partie qui porte sur les classes de Chern est démontrée plus haut, dans le modèle du principe de scindage. La non-nullité des classes et la restriction $r \geq 3$ relèvent de la géométrie : y n'est pas nul parce que $c^1(x) = q - p$ ne l'est pas et que $i_!$ est injectif, ce que la page affirme sans le démontrer. Le second énoncé est celui de la « Conséquence » qui ouvre la page ; ce bloc est encadré et barré d'une longue oblique, alors que le *N.B.* ne l'est pas. Le dernier membre de la formule de la « Conséquence » est écrit 0 là où la classe totale vaut 1 ; le *N.B.* dit la même chose en parlant des coefficients. La page nomme aussi la classe $[\mathcal{O}_{Y \times \mathbf{P}^r}]$ là où le calcul porte sur $Y \times \{\text{point}\}$. Mathlib n'a pas le groupe K des faisceaux cohérents ni les classes de Chern. On se reportera aux notes de Grothendieck (2, lot 1, p. 9).

La page 21 pose une question sur deux anneaux attachés à un λ-anneau K muni d'éléments « géométriques » (2, lot 2, p. 21). L'anneau de Chern CK est engendré par des symboles $c^i(x)$, soumis aux règles que vérifient les classes de Chern : formule de Whitney, produit, et $c^i(E) = 0$ au-delà du rang pour un élément géométrique E. L'anneau GK est le gradué de K pour la filtration γ. Une flèche $\varphi_K : CK \to GK$ envoie $c^i(x)$ sur la classe de $\gamma^i(x - \varepsilon(x))$. La page énonce que φ_K est toujours surjective et que son noyau est un groupe de torsion, de sorte qu'elle devient bijective après tensorisation par $\mathbf{Q}$. Elle demande ensuite si φ_K est toujours bijective, répond « Non », et donne l'exemple de $K = K(\mathbf{P}^{n-1}) = \mathbf{Z}[L]/(L-1)^n$, avec L pour seul élément géométrique : la relation $(L-1)^n = 0$ n'impose à CK que $(n-1)!\,\zeta^n = 0$ en degré n, de sorte que « si $n - 1 > 1$, i.e. $n \geq 3$, CK a de la torsion », alors que GK est sans torsion.

Dans cet exemple, CK est engendré par $\zeta = c^1(L)$. On pose $\xi = 1 - L^{-1}$; comme L est inversible, $\xi^n = 0$ équivaut à $(L-1)^n = 0$. Avec $c(L^{-i}) = 1 - i\zeta$, la seule relation est $c(\xi^n) = 1$, c'est-à-dire l'annulation des composantes de degré ≥ 1 de

$$c(\xi^n) = \prod_{i=0}^{n} (1 - i\zeta)^{(-1)^i \binom{n}{i}} = 1 + (-1)^{n-1}(n-1)!\,\zeta^n + \cdots,$$

le produit de la page 9 calculé plus haut. On prend donc $CK = \mathbf{Z}[\zeta]/I$, où I est engendré par les $a_m \zeta^m$, a_m le coefficient de ζ^m dans ce produit, et $GK = \mathbf{Z}[\zeta]/(\zeta^n)$. Les a_m sont nuls pour $1 \leq m < n$, de sorte que $I \subset (\zeta^n)$ et que φ_K est bien définie.

Pour $n = 3$, la relation de degré 3 est $2\zeta^3 = 0$. Pour que CK ait de la torsion, il faut encore que ζ^3 ne soit pas nul dans CK ; la page l'affirme sans le montrer.

Théorème 32.4 (Grothendieck, page 21, cas $n \geq 3$ ♦). *Pour $n \geq 3$, ζ^n est non nul dans CK et $(n-1)!\,\zeta^n = 0$; GK est sans torsion, et φ_K est surjective sans être injective. Pour $n \leq 2$, φ_K est bijective.*

Démonstration. L'idéal I est engendré par des monômes $a_m \zeta^m$ avec $m \geq n$, et $a_n = \pm(n-1)!$, d'où $(n-1)!\,\zeta^n = 0$. Pour voir que $\zeta^n \neq 0$, on envoie ζ sur h dans $T = (\mathbf{Z}/(n-1)!)[h]/(h^{n+1})$. Les relations y sont satisfaites : $a_m h^m = 0$ pour $m > n$ parce que $h^{n+1} = 0$, et $a_n h^n = 0$ parce que $(n-1)! = 0$ dans T. Or $h^n \neq 0$ dans T dès que $(n-1)! > 1$, c'est-à-dire $n \geq 3$. Dans GK, si kf est divisible par ζ^n avec $k \neq 0$, les coefficients de f de degré $< n$ sont nuls. Pour $n \leq 2$, $a_n = \pm 1$, donc $\zeta^n \in I$ et $I = (\zeta^n)$. □

Voir `φ_not_injective`, `ζ_pow_ne_zero`, `factorial_mul_ζ_pow`, `GK_torsionFree`, `φ_bijective_of_le_two` et `exists_chern` dans `Folder2.lean`. L'anneau T répond à la question que laissait la piste : il porte un homomorphisme de Chern avec $c(L) = 1 + h$, $c(\xi^n) = 1$, $h^n \neq 0$ et $(n-1)!\,h^n = 0$. Le cas $n \leq 2$ est de l'édition ; la page n'énonce que $n \geq 3$. L'exemple dépend aussi de la famille géométrique : si l'on déclare géométrique la classe $n - L^{-1}$, de rang

$n-1$, sa classe de Chern $(1-\zeta)^{-1}$ force $\zeta^n = 0$, et $CK = GK$. La note en diagonale, où se lisent l'idéal, $P(n-1)$ et l'anneau $\mathbf{Z}[\xi]/\xi^n$, dit sans doute cela ; ce point n'est pas formalisé.

Lean ne vérifie pas que la présentation de CK par ζ et la seule relation $c(\xi^n) = 1$ découle des relations générales de la page 28 : c'est la réduction que fait la page, reprise par l'édition. Les λ-anneaux et la filtration γ ne sont pas construits. L'image directe $i_!$ et la formule de la page 11 qui donne $c(i_!x)$ ne sont pas formalisées non plus : Lean part du modèle de scindage que suit la lecture.

Pour la question de la page 21, la fiche de la piste relève un travail publié. Mackall (2020) [92] construit un anneau gradué universel pour les théories de classes de Chern dont la première classe est additive, et le relie au gradué de K pour la filtration γ par un théorème de type Grothendieck–Riemann–Roch. Dans sa remarque 4.3 (numérotation arXiv), il donne un exemple de non-injectivité en degré 3, pour une approximation finie du classifiant $BO^+(2n+1)$, en s'appuyant sur un théorème de Karpenko et Merkurjev. L'exemple de $K(\mathbf{P}^{n-1})$ avec L pour seul élément géométrique n'y figure pas. L'énoncé encadré de la page 13 n'a pas encore été confronté à la littérature : sa fiche ne relève aucune source, et l'édition n'en cite pas.

33 IHÉS SGA 6 2/3 : le groupe K d'une catégorie triangulée, et la formule d'Euler[35]

Comme la section 24, cette section porte sur une pièce du fonds Grothendieck–Illusie de l'IHÉS, `FG_IL_5_SGA6_2_3` (vue 1). Ce sont des notes manuscrites de quinze vues, intitulées « Groupes K », qui portent en haut de la première « (Pour Illusie) » ; le catalogue de l'IHÉS les date « 1965 ? ». Elles esquissent un exposé sur les groupes K : le groupe d'une catégorie triangulée, sa comparaison avec celui d'une catégorie abélienne, puis une généralisation. Aucune lecture modernisée n'en a été faite : les énoncés ci-dessous sont lus sur la transcription des vues 1 à 3.

L'idée. On cherche à mesurer les objets d'une catégorie par des nombres, ou des éléments d'un groupe abélien, de façon additive. Pour les espaces vectoriels de dimension finie, la dimension vérifie $\dim V = \dim V' + \dim V''$ pour toute suite exacte $0 \to V' \to V \to V'' \to 0$. Une *fonction additive* sur une catégorie abélienne est une fonction χ des objets qui vérifie la même règle, et le groupe K est le réceptacle universel de ces fonctions : le groupe abélien libre sur les objets, divisé par les relations $[V] = [V'] + [V'']$. Dans une catégorie triangulée, comme la catégorie dérivée, les *triangles distingués* $X \to Y \to Z \to X[1]$ jouent le rôle des suites exactes courtes ; une suite exacte courte de complexes donne un tel triangle. Les notes posent donc : $K(\mathcal{C})$ est le quotient du groupe abélien libre sur les objets de $\mathcal{C}$ par le sous-groupe engendré par les $[Y] - [X] - [Z]$, un pour chaque triangle distingué, et $\mathrm{cl}(X)$ est l'image de X (vue 1).

Il faut rappeler ce qu'on demande aux triangles. Une catégorie *prétriangulée* est une catégorie additive munie d'un foncteur de translation $X \mapsto X[1]$, inversible, et d'une classe de triangles $X \to Y \to Z \to X[1]$, dits distingués, telle que : un triangle isomorphe à un triangle distingué est distingué ; pour tout X, le triangle $X \xrightarrow{\mathrm{id}} X \to 0 \to X[1]$ est distingué ; tout morphisme $X \to Y$ se complète en un triangle distingué ; $X \to Y \to Z \to X[1]$ est distingué si et seulement si sa rotation $Y \to Z \to X[1] \to Y[1]$ l'est (au signe près) ; enfin un carré commutatif entre deux triangles distingués se complète en un morphisme de triangles. Une catégorie triangulée vérifie de plus l'axiome de l'octaèdre, qui ne sert pas ici.

35. Preuve vérifiée : `lean/Grothendieck/IhesSGA6_2_3.lean`.

Énoncé (Notes, vues 1 et 2). *Soit $\mathcal{C}$ une catégorie triangulée. Dans $K(\mathcal{C})$:*

— $\mathrm{cl}(0) = 0$*, et* $\mathrm{cl}(X) = \mathrm{cl}(X')$ *si* $X \simeq X'$*;*

— $\mathrm{cl}(X[n]) = (-1)^n \mathrm{cl}(X)$ *pour tout* $n \in \mathbf{Z}$*, en particulier* $\mathrm{cl}(X[1]) = -\mathrm{cl}(X)$*;*

— $\mathrm{cl}(X \oplus Y) = \mathrm{cl}(X) + \mathrm{cl}(Y)$*;*

— *(proposition de la vue 2) tout élément de $K(\mathcal{C})$ s'écrit $\mathrm{cl}(X)$ pour un objet X ;*

— *(fonctorialité) un foncteur exact $\varphi : \mathcal{C} \to \mathcal{C}'$ induit un homomorphisme $K(\varphi)$ tel que $K(\varphi)(\mathrm{cl}\, X) = \mathrm{cl}\, \varphi(X)$, et deux foncteurs isomorphes induisent le même.*

Les notes écrivent ces propriétés pour une fonction additive χ quelconque, en partie dans une accolade ajoutée d'une encre plus foncée en marge de la vue 1 ; la propriété universelle de $K(\mathcal{C})$ les transporte à cl, et réciproquement.

Démonstration. Chaque égalité vient d'un triangle bien choisi. Le triangle $0 \to 0 \to 0 \to 0$ donne $\mathrm{cl}(0) = \mathrm{cl}(0) + \mathrm{cl}(0)$, d'où $\mathrm{cl}(0) = 0$. Pour un isomorphisme $e : X \to Y$, le triangle $X \xrightarrow{e} Y \to 0 \to X[1]$ est isomorphe à $X \xrightarrow{\mathrm{id}} X \to 0 \to X[1]$, donc distingué, et donne $\mathrm{cl}(Y) = \mathrm{cl}(X) + \mathrm{cl}(0)$. La rotation de $X \to X \to 0 \to X[1]$ est le triangle $X \to 0 \to X[1] \to X[1]$, qui donne $\mathrm{cl}(0) = \mathrm{cl}(X) + \mathrm{cl}(X[1])$, soit $\mathrm{cl}(X[1]) = -\mathrm{cl}(X)$. Comme $X[n+1] \simeq X[n][1]$, une récurrence sur n, vers le haut et vers le bas, donne $\mathrm{cl}(X[n]) = (-1)^n \mathrm{cl}(X)$. Le triangle scindé $X \to X \oplus Y \to Y \xrightarrow{0} X[1]$ est distingué, et donne la somme directe.

Pour la surjectivité, un élément de $K(\mathcal{C})$ est une combinaison $\sum_i \mathrm{cl}(X_i) - \sum_j \mathrm{cl}(Y_j)$. Puisque $-\mathrm{cl}(Y) = \mathrm{cl}(Y[1])$, c'est une somme de classes, donc la classe d'une somme directe :

$$\sum_i \mathrm{cl}(X_i) - \sum_j \mathrm{cl}(Y_j) = \mathrm{cl}\Big(\bigoplus_i X_i \oplus \bigoplus_j Y_j[1]\Big).$$

En particulier $\mathrm{cl}(X) - \mathrm{cl}(Y) = \mathrm{cl}(X \oplus Y[1])$. Enfin, un foncteur exact envoie triangles distingués sur triangles distingués, donc $X \mapsto \mathrm{cl}\, \varphi(X)$ est additive et passe au quotient ; si $\varphi \simeq \varphi'$, les objets $\varphi(X)$ et $\varphi'(X)$ sont isomorphes et ont la même classe. □

Remarque. La translation fait la différence avec les catégories abéliennes. À la vue 4, les notes doutent que tout élément du K d'une catégorie abélienne soit une classe $\mathrm{cl}(X)$, et n'affirment que la forme $\mathrm{cl}(X) - \mathrm{cl}(Y)$. Dans une catégorie triangulée, l'objet $Y[1]$ joue le rôle de $-Y$. Pour les espaces vectoriels gradués de dimension finie, où $X[1]$ décale les degrés, la caractéristique d'Euler $\sum_i (-1)^i \dim X^i$ change de signe par translation, ce qui est l'égalité $\chi(X[1]) = -\chi(X)$.

Le critère des deux triangles. Un corollaire de la vue 2 dit que $\mathrm{cl}(X) = \mathrm{cl}(X')$ si et seulement s'il existe deux triangles distingués $A \to B \to C \to A[1]$ et $A' \to B' \to C' \to A'[1]$ tels que

$$X \oplus B \oplus A[1] \oplus C[1] \;\simeq\; X' \oplus B' \oplus A'[1] \oplus C'[1].$$

Le sens « si » est un calcul : la classe de $B \oplus A[1] \oplus C[1]$ est $\mathrm{cl}(B) - \mathrm{cl}(A) - \mathrm{cl}(C) = 0$. Il est démontré. Le sens « seulement si » est le lemme 2.4 de Thomason [118]. Les notes le déduisent d'une description de $K(\mathcal{C})$ comme quotient du monoïde des classes d'isomorphie d'objets par le sous-monoïde des $B \oplus A[1] \oplus C[1]$; ce sens n'est pas formalisé.

La formule d'Euler. À la vue 3, pour une fonction additive χ sur une catégorie abélienne, la

cinquième propriété d'une liste est

$$\sum_i (-1)^i \chi(X^i) = \sum_i (-1)^i \chi\big(H^i(X^\bullet)\big)$$

pour un complexe $X^\bullet$ fini. La même égalité est en marge de la vue 2 de la pièce voisine `FG_IL_5_SGA6_2_1`, pour la somme alternée des classes. Elle dit que la caractéristique d'Euler d'un complexe ne dépend que de sa cohomologie. En particulier, un complexe exact a une somme alternée nulle : pour $0 \to K \to K^2 \to K \to 0$ exacte, $1 - 2 + 1 = 0$. On la démontre ici pour la dimension.

Énoncé (Notes, vue 3, propriété 5, pour $\chi = \dim$)**.** *Soit $V^0 \xrightarrow{d^0} V^1 \xrightarrow{d^1} \cdots \xrightarrow{d^{n-1}} V^n \to 0$ un complexe d'espaces vectoriels de dimension finie sur un corps, éventuellement gauche ($d^{i+1} \circ d^i = 0$). Avec $H^i = \ker d^i / \operatorname{im} d^{i-1}$,*

$$\sum_{i=0}^{n} (-1)^i \dim V^i = \sum_{i=0}^{n} (-1)^i \dim H^i.$$

Démonstration. Notons $z_i = \dim \ker d^i$ et $b_i = \dim \operatorname{im} d^{i-1}$, avec $b_0 = 0$, et $b_{n+1} = 0$ puisque $d^n = 0$. Le théorème du rang donne $\dim V^i = z_i + b_{i+1}$, et $\operatorname{im} d^{i-1} \subset \ker d^i$ donne $\dim H^i = z_i - b_i$. La différence des deux membres est donc $\sum_{i=0}^{n} (-1)^i (b_{i+1} + b_i)$, une somme télescopique : les termes $b_1, \ldots, b_n$ s'y annulent deux à deux, et il reste $b_0 + (-1)^n b_{n+1} = 0$. □

Le quotient de Verdier. La vue 3 énonce encore, avec la mention « à vérifier », que pour une sous-catégorie triangulée *épaisse* $\mathcal{D}$ d'une catégorie triangulée $\mathcal{C}$ la suite $K(\mathcal{D}) \to K(\mathcal{C}) \to K(\mathcal{C}/\mathcal{D}) \to 0$ est exacte. Le quotient $\mathcal{C}/\mathcal{D}$ est la localisation de Verdier : on inverse les morphismes dont le cône est dans $\mathcal{D}$; épaisse veut dire ici stable par facteurs directs.

Énoncé (Notes, vue 3)**.** *Soient $\mathcal{C}$ une catégorie triangulée, $\mathcal{D}$ une sous-catégorie triangulée stable par facteurs directs, et $L : \mathcal{C} \to \mathcal{C}/\mathcal{D}$ le foncteur de localisation. Alors $K(L)$ est surjectif, $K(\mathcal{D}) \to K(\mathcal{C}) \to K(\mathcal{C}/\mathcal{D})$ est nul, et le noyau de $K(L)$ est exactement l'image de $K(\mathcal{D})$.*

Démonstration. La surjectivité vient de ce que tout objet de $\mathcal{C}/\mathcal{D}$ est un $L(X)$, et de la proposition de la vue 2. La composée est nulle parce que L annule les objets de $\mathcal{D}$. Pour le milieu, on construit l'inverse : un homomorphisme $K(\mathcal{C}/\mathcal{D}) \to K(\mathcal{C})/\operatorname{im} K(\mathcal{D})$ qui envoie $\mathrm{cl}(LX)$ sur la classe de X. Il faut voir qu'il est bien défini. D'abord, $LX \simeq 0$ si et seulement si $X \in \mathcal{D}$: le morphisme nul $X \to 0$ a pour cône $X[1]$, et c'est là que sert l'épaisseur, car un morphisme nul inversé par L a un cône $Y \oplus X[1]$ dans $\mathcal{D}$, dont $X[1]$ est un facteur direct. Ensuite, un isomorphisme de $\mathcal{C}/\mathcal{D}$ est un toit $X \to Y' \leftarrow Y$ de deux morphismes à cône dans $\mathcal{D}$, et chacun ne change la classe que d'un élément de l'image de $K(\mathcal{D})$. Enfin, les triangles distingués de $\mathcal{C}/\mathcal{D}$ sont, à isomorphisme près, les images de triangles de $\mathcal{C}$. L'inverse existe donc, et le noyau de $K(L)$ est l'image de $K(\mathcal{D})$. □

L'épaisseur ne sert pas seulement à nommer le quotient : sans elle, l'exactitude au milieu est fausse. Dans $D^b(k)$, les complexes de caractéristique d'Euler paire forment une sous-catégorie triangulée $\mathcal{D}$, non épaisse puisque $k \oplus k$ y est et pas k ; son épaissie est $D^b(k)$ tout entière, de sorte que $\mathcal{C}/\mathcal{D} = 0$, alors que l'image de $K(\mathcal{D})$ dans $K(D^b(k)) = \mathbf{Z}$ est $2\mathbf{Z}$ (Thomason [118], théorème 2.1, qui classe les sous-catégories triangulées denses par les sous-groupes de K). La surjectivité et la nullité de la composée valent pour toute sous-catégorie triangulée.

Vérification en Lean. La catégorie est prétriangulée au sens de mathlib (`Pretriangulated C`), qui n'a pas de groupe K_0 de catégorie triangulée ; l'axiome de l'octaèdre n'est pas supposé. Le groupe est `K₀ C`, quotient de `FreeAbelianGroup C` par le sous-groupe `relations C` qu'engendrent les relations des triangles distingués : c'est la forme que l'édition donne au $\mathbf{Z}^{(\mathrm{Ob}\,\mathcal{C})}$ des notes. La relation d'un triangle est `cl_obj₂`, la propriété universelle `lift`, `lift_cl` et `hom_ext`. Les énoncés encadrés sont `cl_zero`, `cl_eq_of_iso`, `cl_shift_one`, `cl_shift`, `cl_biprod`, `cl_sub`, `cl_surjective`, et, pour la fonctorialité, `map`, `map_cl` et `map_eq_of_iso`. Le sens « si » du critère des deux triangles est `cl_eq_of_iso_biprod`. La formule d'Euler est `sum_finrank_eq_sum_finrank_cohomology` : le complexe est une famille $(V^i)_{i\in\mathbf{N}}$ d'espaces de dimension finie sur un anneau à division, avec $d^n = 0$, et la cohomologie `cohomology d i` est le quotient de $\ker d^i$ par l'image de d^{i-1}, vue dans $\ker d^i$. La somme télescopique est `sum_alternating_telescope`. Les noms sont ceux de `IhesSGA6_2_3.lean`. Le quotient de Verdier est dans `IhesSGA6_2_3Verdier.lean`, qui suppose $\mathcal{C}$ triangulée (l'octaèdre sert, à travers le calcul de fractions de mathlib pour les morphismes à cône dans $\mathcal{D}$) et vaut pour tout foncteur de localisation triangulé, le quotient `P.trW.Localization` de mathlib compris : la surjectivité est `map_surjective`, la nullité de la composée `map_comp_map_ι`, et l'exactitude au milieu `ker_map_eq_range`, `exact` et `exact_localization`, à partir de l'inverse `descQuotient`, de `isZero_map_iff` et de `cl_sub_cl_mem_range_of_iso`.

Ne sont pas démontrés ici : le sens « seulement si » du critère des deux triangles, et la description de $K(\mathcal{C})$ par le monoïde des classes d'isomorphie ; le fait qu'une équivalence induise un isomorphisme ; le contre-exemple de Thomason sans l'hypothèse d'épaisseur ; la comparaison $K(\mathcal{C}) \simeq K(D^b(\mathcal{C}))$ pour une catégorie abélienne, au n° 2 ; la formule d'Euler pour une fonction additive quelconque, ou pour les longueurs de modules.

34 Cote 153 : polynômes à valeurs entières, co-opérations, analyseurs [36]

La cote 153, *Analyseurs : notes manuscrites (s.d.)*, dix pages que l'inventaire date « [à partir de 1982] », cherche la structure abstraite d'un anneau d'opérations muni d'une composition, aujourd'hui appelée pléthorie, notion étudiée par Tall et Wraith en 1970 [117] et nommée ainsi par Borger et Wieland en 2005 [20]. Elle y arrive par les polynômes à valeurs entières. La page 3 fixe une inclusion d'anneaux commutatifs $k_0 \subset K_0$ et l'anneau $\Omega = \{F \in K_0[T] \mid F(\lambda) \in k_0\ \forall \lambda \in k_0\}$. Les co-opérations $F(x+y) = \sum_i G_i(x)H_i(y)$ et $F(xy) = \sum_\alpha J_\alpha(x)K_\alpha(y)$ doivent être des éléments « bien déterminés » de $\Omega \otimes_{k_0} \Omega$. Pour cela, la page énonce un lemme, le mot « Lemme » étant lu sans certitude : le sous-ensemble des $F \in K_0[T] \otimes_{k_0} M$ tels que $F(x) \in M$ pour tout $x \in k_0$ « s'identifie à $\Omega \otimes_{k_0} M$ » (153, lot 1, p. 3). La lecture précise : coordonnée par coordonnée dans une base de M.

La page 2 écrit les polynômes binomiaux $F_n = \binom{T}{n} \in \mathbf{Q}[T]$, affirme que $\bigoplus_n \mathbf{Z}F_n$ est une $\mathbf{Z}$-algèbre, et écrit la co-addition sous la forme générale $F_m(P+Q) = \sum \gamma_{ij}^m F_i(P)F_j(Q)$; la co-multiplication reste inachevée (153, lot 1, p. 2). La page 5 définit l'analyseur, puis les constantes, et écrit sans justification $\Omega = \Omega_0 \oplus \Omega^0$ (153, lot 1, p. 5). Les exemples $\mathrm{Appl}(A, A)$, $k[T]$ et $k[[T]]^+$ sont à la page 7, avec l'application $\Omega \to \mathrm{Appl}(\Omega_0, \Omega_0) = \Omega_{\Omega_0}$, avec le souhait « que $\Omega \to \Omega_{\Omega_0}$ soit injectif ! » (153, lot 1, p. 7). La page 9 donne l'exemple relatif et l'analyseur binomial de $\mathbf{Z} \subset \mathbf{Q}$ (153, lot 1, p. 9).

36. Preuve vérifiée : `lean/Grothendieck/Folder153.lean`.

Définition. Soit K_0 une k_0-algèbre commutative ; on note $\iota : k_0 \to K_0$ le morphisme structural. On pose $\Omega = \{F \in K_0[T] \mid F(\iota(\lambda)) \in \iota(k_0)\ \forall \lambda \in k_0\}$; c'est une sous-k_0-algèbre de $K_0[T]$, les valeurs d'une somme et d'un produit étant la somme et le produit des valeurs, et un polynôme constant $\iota(c)$ y appartenant. Pour un k_0-module M, $x \in k_0$ et $F \in K_0[T] \otimes_{k_0} M$, on note $F(x) \in K_0 \otimes_{k_0} M$ l'image de F par $\mathrm{ev}_x \otimes \mathrm{id}_M$, où $\mathrm{ev}_x : K_0[T] \to K_0$ est l'évaluation en $\iota(x)$, et l'on dit que $F(x) \in M$ lorsque $F(x)$ est dans l'image de $M \to K_0 \otimes_{k_0} M$, $m \mapsto 1 \otimes m$. On note Ω_M l'ensemble des F tels que $F(x) \in M$ pour tout $x \in k_0$. Enfin « Ω_M s'identifie à $\Omega \otimes_{k_0} M$ » est lu : l'application canonique $\Omega \otimes_{k_0} M \to K_0[T] \otimes_{k_0} M$ est injective, et son image est Ω_M.

Énoncé (Lemme, page 3)**.** *Soit M un k_0-module libre, de base $(e_i)_{i\in I}$, et écrivons tout $F \in K_0[T] \otimes_{k_0} M$ sous la forme $\sum_i F_i \otimes e_i$, les $F_i \in K_0[T]$ étant presque tous nuls.*

1. *$F \in \Omega_M$ si et seulement si $F_i \in \Omega$ pour tout i.*
2. *L'application canonique $\Omega \otimes_{k_0} M \to K_0[T] \otimes_{k_0} M$ est injective.*
3. *Son image est exactement Ω_M.*

Dans la suite, N et P désignent des k_0-modules et $f : N \to P$ une application k_0-linéaire. La base (e_i) donne, pour tout N, un isomorphisme $c_N : N \otimes_{k_0} M \to N^{(I)}$ sur les familles presque nulles d'éléments de N, qui envoie $n \otimes m$ sur $(m_i\, n)_i$, où les m_i sont les coordonnées de m ; c'est l'isomorphisme $N \otimes_{k_0} k_0^{(I)} \simeq N^{(I)}$. On appelle $c_N(t)_i$ la i-ième coordonnée de t.

Lemme 34.1. *Les coordonnées sont naturelles : pour $t \in N \otimes_{k_0} M$, la i-ième coordonnée de $(f \otimes \mathrm{id}_M)(t)$ est $f(c_N(t)_i)$.*

Démonstration. Les deux membres sont additifs en t, et il suffit de le vérifier sur un tenseur pur $n \otimes m$: la i-ième coordonnée de $f(n) \otimes m$ est $m_i f(n) = f(m_i n)$. □

Lemme 34.2. *Un élément t de $P \otimes_{k_0} M$ est dans l'image de $f \otimes \mathrm{id}_M$ si et seulement si chacune de ses coordonnées est dans l'image de f.*

Résultat général, démontré en Lean dans
`Upstream/TensorProductMemRangeRTensorBasis.lean` *; la démonstration n'est pas reprise ici.*

Lemme 34.3. *L'image de $M \to K_0 \otimes_{k_0} M$, $m \mapsto 1 \otimes m$, est l'image de $\iota \otimes \mathrm{id}_M : k_0 \otimes_{k_0} M \to K_0 \otimes_{k_0} M$.*

Démonstration. La première application est la composée de l'isomorphisme $M \simeq k_0 \otimes_{k_0} M$, $m \mapsto 1 \otimes m$, et de $\iota \otimes \mathrm{id}_M$. □

Démonstration du lemme de la page 3. (1) Soit $x \in k_0$. Par le lemme 34.3, $F(x) \in M$ signifie que $(\mathrm{ev}_x \otimes \mathrm{id})(F)$ est dans l'image de $\iota \otimes \mathrm{id}$, c'est-à-dire, par le lemme 34.2, que chacune de ses coordonnées est dans $\iota(k_0)$. Par le lemme 34.1, sa i-ième coordonnée est $\mathrm{ev}_x(F_i) = F_i(\iota(x))$. Ainsi $F \in \Omega_M$ si et seulement si $F_i(\iota(x)) \in \iota(k_0)$ pour tout x et tout i, c'est-à-dire si et seulement si $F_i \in \Omega$ pour tout i.

(2) Un module libre est plat, fait classique ; le produit tensoriel par M conserve donc l'injectivité de l'inclusion $\Omega \hookrightarrow K_0[T]$.

(3) Par le lemme 34.2 appliqué à l'inclusion $\Omega \hookrightarrow K_0[T]$, F est dans l'image de $\Omega \otimes_{k_0} M$ si et seulement si chaque F_i est dans Ω, c'est-à-dire, par (1), si et seulement si $F \in \Omega_M$. □

Remarque. L'hypothèse de la page que $k_0 \to K_0$ soit une inclusion ne sert pas. Le lemme vaut pour toute k_0-algèbre commutative K_0, Ω étant l'ensemble des polynômes qui envoient k_0 dans l'image de k_0.

Stabilité par composition et co-opérations (page 3). On garde les notations de la définition ; on écrit $K_0[X,Y]$ pour l'anneau des polynômes en deux variables sur K_0, et, pour $F \in K_0[T]$, $\Delta_a F = F(X+Y)$ et $\Delta_m F = F(XY)$. On note $\Phi : \Omega \otimes_{k_0} \Omega \to K_0[X,Y]$ l'application k_0-linéaire qui envoie $G \otimes H$ sur $G(X)H(Y)$.

Énoncé (Page 3, stabilité)**.** *Si $F, G \in \Omega$, alors $F \circ G \in \Omega$.*

Démonstration. Pour $x \in k_0$, $G(\iota(x)) = \iota(y)$ pour un $y \in k_0$, et $(F \circ G)(\iota(x)) = F(\iota(y)) \in \iota(k_0)$. □

Énoncé (Page 3, les co-opérations)**.** *Supposons que K_0 soit un localisé $S^{-1}k_0$ de k_0, et que Ω soit un k_0-module libre.*

1. *L'application Φ est injective.*
2. *Son image est l'ensemble des $P \in K_0[X,Y]$ tels que $P(\iota(x), \iota(y)) \in \iota(k_0)$ pour tous $x, y \in k_0$.*
3. *Pour $F \in \Omega$, il existe un unique $t \in \Omega \otimes_{k_0} \Omega$ tel que $\Phi(t) = F(X+Y)$, et un unique t' tel que $\Phi(t') = F(XY)$.*
4. *Si $\Phi\big(\sum_i G_i \otimes H_i\big) = F(X+Y)$, alors $F \circ (P+Q) = \sum_i (G_i \circ P)(H_i \circ Q)$ pour tous $P, Q \in K_0[T]$; si $\Phi\big(\sum_\alpha J_\alpha \otimes K_\alpha\big) = F(XY)$, alors $F \circ (PQ) = \sum_\alpha (J_\alpha \circ P)(K_\alpha \circ Q)$.*

Soit $(e_j)_{j \in I}$ une base du k_0-module Ω. Deux lemmes traduisent l'hypothèse sur K_0 : toute famille finie d'éléments de K_0 admet un dénominateur commun $s \in S$, c'est-à-dire que les $\iota(s)a$ sont dans $\iota(k_0)$, et $\iota(s)$ est inversible dans K_0.

Lemme 34.4. *Les e_j, vus dans $K_0[T]$, sont linéairement indépendants sur K_0.*

Démonstration. Soit $\sum_j a_j e_j = 0$, les $a_j \in K_0$ presque tous nuls, et $s \in S$ un dénominateur commun : $\iota(s)a_j = \iota(d_j)$, $d_j \in k_0$. Alors $\sum_j d_j e_j = \iota(s) \sum_j a_j e_j = 0$ dans Ω, donc les d_j sont nuls, puis $\iota(s)a_j = 0$ et $a_j = 0$, $\iota(s)$ étant inversible. □

Lemme 34.5. *Les e_j engendrent $K_0[T]$ comme K_0-module.*

Démonstration. Soit $p \in K_0[T]$. On chasse les dénominateurs des coefficients : il existe $s \in S$ et $q \in k_0[T]$ tels que $\iota(s)p$ soit l'image de q. Cette image envoie $\iota(x)$ sur $\iota(q(x))$, elle est donc dans Ω, combinaison k_0-linéaire des e_j, et $p = \iota(s)^{-1} \cdot \iota(s)p$ est combinaison K_0-linéaire des e_j. □

Démonstration des co-opérations. (1) Tout $t \in \Omega \otimes_{k_0} \Omega$ s'écrit $\sum_j G_j \otimes e_j$, les $G_j \in \Omega$ étant les coordonnées de t dans la base (e_j) du second facteur, et $\Phi(t) = \sum_j G_j(X) e_j(Y)$. Le coefficient de X^m dans $\Phi(t)$ est $\sum_j c_m(G_j)\, e_j(Y)$, où $c_m(G_j) \in K_0$ est le coefficient de T^m dans G_j. Si $\Phi(t) = \Phi(t')$, le lemme 34.4 donne $c_m(G_j) = c_m(G'_j)$ pour tous j et m, donc $G_j = G'_j$ et $t = t'$.

(2) Les valeurs de $G(X)H(Y)$ en $(\iota(x), \iota(y))$ sont les produits $G(\iota(x))H(\iota(y)) \in \iota(k_0)$, et la condition passe aux sommes. Réciproquement, soit P à valeurs dans $\iota(k_0)$. Le lemme 34.5, appliqué aux coefficients de chaque monôme X^n, écrit $P = \sum_j G_j(X)\, e_j(Y)$ avec des $G_j \in K_0[T]$. Pour $x \in k_0$, le polynôme $P(\iota(x), T) = \sum_j G_j(\iota(x))\, e_j$ est dans Ω, donc égal à $\sum_j \iota(\beta_j) e_j$ pour des $\beta_j \in k_0$; le lemme 34.4 donne $G_j(\iota(x)) = \iota(\beta_j)$. Ainsi chaque G_j est dans Ω, et $P = \Phi\big(\sum_j G_j \otimes e_j\big)$.

(3) Pour $F \in \Omega$, $(\Delta_a F)(\iota(x), \iota(y)) = F(\iota(x+y))$ et $(\Delta_m F)(\iota(x), \iota(y)) = F(\iota(xy))$ sont dans $\iota(k_0)$: l'existence vient de (2), l'unicité de (1).

(4) Soit $\mathrm{ev}_{P,Q} : K_0[X,Y] \to K_0[T]$ le morphisme d'anneaux qui fixe K_0 et envoie X sur P, Y sur Q. Il envoie $G(X)H(Y)$ sur $(G \circ P)(H \circ Q)$, $F(X+Y)$ sur $F \circ (P+Q)$ et $F(XY)$ sur $F \circ (PQ)$; on l'applique à l'égalité supposée. □

Remarque. L'hypothèse employée est que K_0 soit un localisé de k_0 ; la lecture le donne comme exemple de son hypothèse $K_0 \otimes_{k_0} K_0 = K_0$. La démonstration ne passe pas par l'identification $K_0[X] \otimes_{k_0} K_0[Y] = K_0[X,Y]$, l'application Φ arrivant directement dans $K_0[X,Y]$. La liberté de Ω, que demande la marge de la page, sert aux deux lemmes et à l'écriture $t = \sum_j G_j \otimes e_j$. L'inclusion $k_0 \subset K_0$ n'est pas supposée. Elle découle de la liberté de Ω dès que $K_0 \neq 0$, un $c \in k_0$ tel que $\iota(c) = 0$ annulant tous les e_j. Les règles de (4) valent pour n'importe quel représentant et ne demandent pas l'unicité ; l'unicité fait des co-opérations des éléments « bien déterminés » de $\Omega \otimes_{k_0} \Omega$. La formule $F \circ \lambda T = \sum_\alpha J_\alpha(\lambda) K_\alpha$ de la page en est le cas $P = \lambda$, $Q = T$.

L'hypothèse de localisation ne sert qu'aux deux lemmes, et le second n'en a pas besoin. On le voit sur l'application K_0-linéaire $\beta : K_0 \otimes_{k_0} \Omega \to K_0[T]$, $a \otimes F \mapsto aF$.

Énoncé (Page 3, les co-opérations sans localisation ♦). *Soit K_0 une k_0-algèbre commutative quelconque.*

1. *L'application β est surjective.*
2. *Si β est injective et que Ω est un k_0-module libre, les conclusions (1) à (3) de l'énoncé précédent valent : Φ est injective, son image est l'ensemble des P à valeurs dans $\iota(k_0)$ sur $k_0 \times k_0$, et $F(X+Y)$, $F(XY)$ sont, pour $F \in \Omega$, les images d'éléments uniques de $\Omega \otimes_{k_0} \Omega$.*
3. *L'application β est injective lorsque K_0 est un localisé de k_0 et que Ω est libre, et lorsque K_0 est plat sur k_0 et que la multiplication $K_0 \otimes_{k_0} K_0 \to K_0$ est injective, c'est-à-dire $K_0 \otimes_{k_0} K_0 = K_0$.*

Démonstration. (1) Les monômes T^n sont dans Ω, puisqu'ils envoient $\iota(x)$ sur $\iota(x^n)$, et $\beta(a \otimes T^n) = aT^n$; ces polynômes engendrent $K_0[T]$.

(2) Soit (e_j) une base de Ω. Les $1 \otimes e_j$ forment une base du K_0-module $K_0 \otimes_{k_0} \Omega$, et $\beta\big(\sum_j a_j \otimes e_j\big) = \sum_j a_j e_j$. La surjectivité de β donne donc la conclusion du lemme 34.5, son injectivité celle du lemme 34.4, et la démonstration des co-opérations n'utilise rien d'autre de l'hypothèse sur K_0.

(3) Pour un localisé, l'injectivité est le lemme 34.4, lu dans la base $(1 \otimes e_j)$. Dans le cas plat, β est la composée de $\mathrm{id}_{K_0} \otimes (\Omega \hookrightarrow K_0[T])$, injective par platitude, et de $\mu : K_0 \otimes_{k_0} K_0[T] \to K_0[T]$, $a \otimes p \mapsto ap$. Comme k_0-module, $K_0[T]$ est isomorphe à $K_0^{(\mathbf{N})}$ par les coefficients, donc $K_0 \otimes_{k_0} K_0[T]$ à $(K_0 \otimes_{k_0} K_0)^{(\mathbf{N})}$, et μ devient la multiplication $K_0 \otimes_{k_0} K_0 \to K_0$ coefficient par coefficient, injective par hypothèse. □

Remarque. L'hypothèse de la lecture, $K_0[X] \otimes_{k_0} K_0[Y] = K_0[X,Y]$, revient à $K_0 \otimes_{k_0} K_0 = K_0$, le premier membre étant $(K_0 \otimes_{k_0} K_0)[X,Y]$. Elle suffit ici avec la platitude de K_0, qui couvre les localisés. Sans platitude, la démonstration demande l'injectivité de β, et l'on ne sait pas ici si $K_0 \otimes_{k_0} K_0 = K_0$ et la liberté de Ω la donnent. Ni l'inclusion $k_0 \subset K_0$ ni le passage par $K_0[X] \otimes_{k_0} K_0[Y]$ ne servent.

Pólya et Vandermonde (page 2). Pour $k_0 = \mathbf{Z} \subset K_0 = \mathbf{Q}$, $\Omega = \mathrm{Int}(\mathbf{Z})$; on pose $F_n = \binom{T}{n} = T(T-1)\cdots(T-n+1)/n!$, et l'on note $\Delta f(x) = f(x+1) - f(x)$ la différence finie.

Énoncé (Page 2, théorème de Pólya). *Les F_n sont dans $\mathrm{Int}(\mathbf{Z})$ et linéairement indépendants sur $\mathbf{Z}$. Tout $P \in \mathrm{Int}(\mathbf{Z})$ de degré d s'écrit $P = \sum_{k \leq d} c_k F_k$ avec $c_k = (\Delta^k P)(0) \in \mathbf{Z}$. Ainsi $(F_n)_{n \in \mathbf{N}}$ est une base du $\mathbf{Z}$-module $\mathrm{Int}(\mathbf{Z})$.*

Résultat général, démontré en Lean dans
`Upstream/PolynomialIntegerValued.lean` *; la démonstration n'est pas reprise ici.*

Énoncé (Page 2, Vandermonde, et les co-opérations de $\mathrm{Int}(\mathbf{Z})$)**.** *Dans* $\mathbf{Q}[X,Y]$, $F_m(X+Y) = \sum_{i+j=m} F_i(X)F_j(Y)$. *Par suite l'unique élément de* $\mathrm{Int}(\mathbf{Z}) \otimes_{\mathbf{Z}} \mathrm{Int}(\mathbf{Z})$ *qui représente* $F_m(X+Y)$ *est* $\sum_{i+j=m} F_i \otimes F_j$ *: les* γ_{ij}^m *de la page valent* 1 *si* $i+j=m$ *et* 0 *sinon. De même* $F_m(XY) = \sum_{i,j} \delta_{ij}^m F_i(X)F_j(Y)$ *pour des entiers* δ_{ij}^m *uniquement déterminés.*

Démonstration. L'identité est la formule de Chu–Vandermonde (Zhu Shijie, 1303 ; Vandermonde, 1772) dans un anneau binomial, $\binom{r+s}{m} = \sum_{i+j=m} \binom{r}{i}\binom{s}{j}$, que mathlib démontre (`Ring.add_choose_eq`) et qu'on applique dans $\mathbf{Q}[X,Y]$ à $r = X$, $s = Y$; les morphismes d'anneaux commutent aux coefficients binomiaux généralisés, d'où l'identification de $\binom{X}{i}$ à $F_i(X)$. Par le théorème de Pólya, $\mathrm{Int}(\mathbf{Z})$ est libre, $\mathbf{Q}$ est le localisé de $\mathbf{Z}$ en les entiers non nuls, et l'énoncé des co-opérations s'applique : il donne l'unicité, et, pour $F_m(XY)$, l'existence ; les coefficients dans la base $(F_i \otimes F_j)$ sont les δ_{ij}^m. □

Remarque. Les entiers $c_{m,n}^p$ et $d_{m,n}^p$ de la page s'en déduisent : F_mF_n et $F_m \circ F_n$ sont dans $\mathrm{Int}(\mathbf{Z})$, sous-anneau stable par composition, donc sont des combinaisons entières des F_p, de degré au plus $m+n$ et mn ; cette conséquence n'a pas d'énoncé Lean séparé. La lecture attribue le théorème à G. Pólya, dont l'article de 1919 étudie les bases de ce type pour les polynômes à valeurs entières sur l'anneau des entiers d'un corps de nombres [106] (voir aussi [27]) ; la démonstration suivie ici est celle des différences finies. La structure de biring de $\mathrm{Int}(\mathbf{Z})$ que définissent ces co-opérations, et sa structure de pléthorie, sont étudiées par Elliott [48].

Constantes et décomposition (page 5). Soit Ω un pseudo-anneau commutatif muni d'une loi $\circ$ associative, d'unité T, telle que $F \mapsto F \circ G$ soit un morphisme de pseudo-anneaux pour tout G : ce sont les conditions 1) et 2). On note $\Omega_0 = \{\lambda \mid \lambda \circ F = \lambda \ \forall F\}$ et $\Omega^0 = \{F \mid F \circ 0 = 0\}$.

Énoncé (Page 5, $\Omega = \Omega_0 \oplus \Omega^0$)**.** Ω_0 *est un sous-pseudo-anneau de* Ω*; pour* $F \in \Omega$ *et* $\lambda \in \Omega_0$*,* $F \circ \lambda \in \Omega_0$*, et en particulier* $F \circ 0 \in \Omega_0$*;* Ω^0 *est un sous-groupe et un idéal ; et* Ω *est somme directe des sous-groupes* Ω_0 *et* Ω^0*, par* $F = F \circ 0 + (F - F \circ 0)$*. L'application* $F \mapsto (\lambda \mapsto F \circ \lambda)$ *de* Ω *dans* $\mathrm{Appl}(\Omega_0, \Omega_0)$ *respecte la somme, le produit et la composition, envoie* T *sur l'identité, et envoie une constante* λ *sur l'application constante de valeur* λ*.*

Démonstration. Comme $F \mapsto F \circ G$ est additif, $0 \circ G = 0$ et $(-F) \circ G = -(F \circ G)$; additivité et multiplicativité montrent que Ω_0 est stable par somme, opposé et produit. Si $\lambda \in \Omega_0$, $(F \circ \lambda) \circ G = F \circ (\lambda \circ G) = F \circ \lambda$, et $0 \in \Omega_0$. Si $F \in \Omega^0$, $(GF) \circ 0 = (G \circ 0)(F \circ 0) = 0$. Une constante λ de Ω^0 vérifie $\lambda = \lambda \circ 0 = 0$: l'intersection est nulle. Enfin $(F - F \circ 0) \circ 0 = F \circ 0 - (F \circ 0) \circ 0 = 0$, $F \circ 0$ étant une constante, ce qui donne la somme. Les propriétés de $F \mapsto (\lambda \mapsto F \circ \lambda)$ sont les conditions 2), l'associativité, $T \circ \lambda = \lambda$ et la définition des constantes. □

Remarque. Les conditions 3) n'interviennent pas, ni l'unité T sauf pour l'image de T. La décomposition n'utilise que l'associativité et l'additivité de $F \mapsto F \circ G$. La multiplicativité sert seulement à faire de Ω_0 un sous-pseudo-anneau et de Ω^0 un idéal. La somme directe est une somme de groupes abéliens, Ω_0 n'étant pas un idéal en général.

Exemples et contre-exemples (page 7).

Énoncé (Page 7, l'exemple $\mathrm{Appl}(A,A)$)**.** *Soit* A *un pseudo-anneau commutatif et* $\Omega_A = \mathrm{Appl}(A,A)$*, avec les lois ponctuelles et la composition des applications. Il vérifie 1) et 2) ; ses constantes sont les applications constantes, et* $(\Omega_A)_0 \simeq A$ *comme pseudo-anneaux. Si* A *est un anneau commutatif unitaire non nul et infini,* Ω_A *ne vérifie pas 3a) : l'indicatrice* δ *de* 0 *n'admet aucune famille finie* $(F_i', F_i'')_{i<n}$ *telle que* $\delta \circ (G' + G'') = \sum_i (F_i' \circ G')(F_i'' \circ G'')$ *pour tous* G'*,* G''*.*

Démonstration. Une constante λ vérifie $\lambda = \lambda \circ c_0$, où c_0 est l'application constante de valeur 0, donc $\lambda(x) = \lambda(0)$ pour tout x ; l'isomorphisme est $\lambda \mapsto \lambda(0)$. Pour 3a), prenons G' et G'' constantes de valeurs x et y : on obtiendrait $\delta(x+y) = \sum_{i<n} F'_i(x)F''_i(y)$ pour tous $x, y \in A$. Choisissons $n+1$ éléments distincts $a_0, \ldots, a_n$ de A et posons $U_{ji} = F'_i(a_j)$, $V_{ik} = F''_i(-a_k)$. Alors $(UV)_{jk} = \delta(a_j - a_k)$ est la matrice identité d'ordre $n+1$, de rang $n+1$ sur l'anneau commutatif non nul A, alors que le rang de UV est au plus celui de U, qui a n colonnes. □

Énoncé (Page 7, l'analyseur des polynômes et l'application $\Omega \to \Omega_{\Omega_0}$)**.** *Soit k un anneau commutatif et $\Omega = k[T]$ avec la composition des polynômes. Il vérifie 1) et 2), et ses constantes sont les polynômes constants. Si k est un corps fini à q éléments, $T^q - T$ est non nul et $(T^q - T) \circ \lambda = 0$ pour toute constante λ : l'application $\Omega \to \mathrm{Appl}(\Omega_0, \Omega_0)$ n'est pas injective. Si k est un anneau intègre infini, elle l'est. Pour $\mathrm{Int}(\mathbf{Z})$, deux polynômes $F, G \in \mathbf{Q}[T]$ tels que $F \circ n = G \circ n$ pour tout $n \in \mathbf{Z}$ sont égaux.*

Démonstration. Pour une constante λ, $\lambda = \lambda \circ 0$ est le polynôme constant $\lambda(0)$; réciproquement un polynôme constant est une constante. Sur un corps fini, $a^q = a$ pour tout a, d'où $(T^q - T) \circ a = a^q - a = 0$, et $T^q - T$ est de degré $q \geq 2$. Sur un anneau intègre infini, comme sur $\mathbf{Q}$ avec la partie infinie $\mathbf{Z}$, un polynôme est déterminé par ses valeurs, et $F \circ a$ est le polynôme constant $F(a)$. □

Énoncé (Page 7, $k[[T]]^+$ ne vérifie pas 3a))**.** *Soit k un anneau commutatif non nul et $F = \sum_{m \geq 1} T^m$. Les coefficients de $X^p Y^q$ dans $F(X+Y) = \sum_{m \geq 1} (X+Y)^m$, qui valent $\binom{p+q}{p}$ hors de $(p,q) = (0,0)$ et 0 en $(0,0)$, ne sont ceux d'aucune somme finie $\sum_{i<n} a_i(X) b_i(Y)$ de séries formelles : il n'existe pas de suites $(a_{i,p})$, $(b_{i,q})$ telles que ce coefficient soit $\sum_{i<n} a_{i,p} b_{i,q}$ pour tous p, q.*

Démonstration. La matrice de Pascal $P_N = \left(\binom{p+q}{p}\right)_{p,q<N}$ est de déterminant 1, énoncé général rappelé à la suite de la démonstration. Si les coefficients étaient $\sum_{i<n} a_{i,p} b_{i,q}$, ceux de P_{n+2} seraient $\sum_{i<n} a_{i,p} b_{i,q} + [p=0][q=0]$, et P_{n+2} serait le produit d'une matrice à $n+1$ colonnes par une matrice à $n+1$ lignes, de rang au plus $n+1$, alors qu'elle est inversible, de rang $n+2$. □

Résultat général, démontré en Lean dans
`Upstream/DetPascalMatrix.lean` *; la démonstration n'est pas reprise ici.*

Remarque. Le contre-exemple de 3a) pour $\mathrm{Appl}(A, A)$ est établi pour A unitaire, commutatif, non nul et infini. La page ne parle pas de 3), et la lecture dit « pour A infini ». Pour $k[[T]]^+$, la matrice des coefficients de $F(X+Y)$ diffère de la matrice de Pascal, que nomme la note de la lecture, par le coefficient $(0,0)$, nul puisque F n'a pas de terme constant ; l'argument coûte donc un rang de plus. Le déterminant de la matrice de Pascal valant 1 sur $\mathbf{Z}$, le contre-exemple vaut en toute caractéristique. L'énoncé Lean porte sur les coefficients. Le passage aux séries, où le coefficient de $X^p Y^q$ d'un produit $a(X)b(Y)$ est $a_p b_q$, est celui de la note.

Ne sont pas démontrés ici : l'isomorphisme $(\Omega_A)_0 \simeq \Gamma A$ pour un anneau d'un topos et l'exemple $\mathrm{End}(W_k(A))$; les constantes de $k[[T]]^+$ et les séries à terme constant nilpotent ; les co-opérations sous la seule hypothèse $K_0 \otimes_{k_0} K_0 = K_0$, sans platitude ; le contre-exemple de 3a) pour $\mathrm{Appl}(A, A)$, A pseudo-anneau infini quelconque ; les analyseurs des puissances divisées et des λ-anneaux.

Théorème 34.6 (Pages 3 et 9, co-opérations de Int relatif, forme corrigée par l'édition ♦). *Soit K_0 une k_0-algèbre commutative telle que $K_0 \otimes_{k_0} K_0 = K_0$, et soit $\Omega = \{F \in K_0[T] \mid F(k_0) \subset k_0\}$, supposé libre comme k_0-module. Alors $F(X+Y)$ et $F(XY)$ sont, pour tout $F \in \Omega$, les images d'éléments uniques de $\Omega \otimes_{k_0} \Omega$, et Ω porte ainsi une co-addition et une co-multiplication, lois de composition d'un analyseur.*

◊ non vérifié en Lean

Partie 17

Cohomologie cristalline et de de Rham

35 Cote 5 : l'algèbre artinienne universelle à puissances divisées [37]

La cote 5, *Cristaux et cohomologie de De Rham : généralités, correspondances Deligne et Berthelot*, que l'inventaire date de 1965–1969, porte sur les puissances divisées et les sites cristallins. À la page 4, l'algèbre locale artinienne universelle sur $W(k)$ dont l'idéal maximal porte des puissances divisées nulles en degrés $\geq p^{\nu+1}$ est présentée comme $W[\Lambda_0,\dots,\Lambda_\nu]/(\Lambda_i^p - q_i\Lambda_{i+1}, \Lambda_\nu^p, \Lambda_0 - p)$, où $\Lambda_i = \gamma_{p^i}(p)$ et $q_i = (p^{i+1})!/((p^i)!)^p$ (5, lot 1, p. 4) ; la relation est $\gamma_{p^i}(x)^p = q_i\,\gamma_{p^{i+1}}(x)$. Une note de la lecture s'appuie sur $v_p(q_\nu) = 1$.

Théorème 35.1 (Énoncé de l'édition, d'après la page 4 ♦). *Pour tout entier p et tout i, $((p^i)!)^p\, q_i = (p^{i+1})!$: q_i est un entier, le coefficient multinomial de p blocs de taille p^i. Si p est premier, $(p-1)\,v_p((p^i)!) = p^i - 1$ et $v_p(q_i) = 1$.*

L'énoncé tient. La valuation vient de la formule de Legendre sous la forme $v_p((pm)!) = v_p(m!) + m$; voir les théorèmes `factorial_eq_mul_q`, `q_eq_multinomial` et `padicValNat_q` de `Folder5.lean`.

L'universalité (page 4). La page place l'énoncé d'universalité entre crochets, sans démonstration ; la lecture en esquisse une par l'enveloppe à puissances divisées. La vérification en donne une autre, qui n'utilise que mathlib. On travaille sur un anneau intègre W de caractéristique nulle où les entiers premiers à p sont inversibles : c'est le cas de $W(k)$ et de $\mathbf{Z}_p$ (`padicInt_isUnit_natCast`). On pose

$$A^{(\nu)} = W[\Lambda_0,\dots,\Lambda_\nu]\big/\big(\Lambda_i^p - q_i\Lambda_{i+1}\ (i<\nu),\ \Lambda_\nu^p\big), \qquad W^{(\nu)} = A^{(\nu)}/(\Lambda_0 - p),$$

qui est bien le quotient de $W[\Lambda]$ par toutes les relations de la page (`presentation`), et $J = (\Lambda_0,\dots,\Lambda_\nu) \subset W^{(\nu)}$.

Théorème 35.2 (Grothendieck, page 4, universalité de la présentation ♦). *L'idéal J de $W^{(\nu)}$ porte une structure de puissances divisées δ telle que $\delta_{p^i}(p) = \Lambda_i$ pour $0 \leq i \leq \nu$ et $\delta_n(y) = 0$ pour $y \in J$ et $n \geq p^{\nu+1}$. Pour toute W-algèbre T munie d'un idéal I à puissances divisées γ tel que $p \in I$ et $\gamma_n(p) = 0$ pour $n \geq p^{\nu+1}$, il existe un unique morphisme de W-algèbres $W^{(\nu)} \to T$ compatible aux puissances divisées ; il envoie Λ_i sur $\gamma_{p^i}(p)$.*

Démonstration. Un plongement. Soit K le corps des fractions de W et $B = K[X]/(X^{p^{\nu+1}})$. L'application $\psi : \Lambda_i \mapsto X^{p^i}/(p^i)!$ respecte les relations, puisque $((p^i)!)^p q_i = (p^{i+1})!$, et définit $\psi : A^{(\nu)} \to B$. Elle est injective. D'une part les monômes Λ^a à exposants $0 \leq a_i < p$ engendrent $A^{(\nu)}$ comme W-module : leur W-module est stable par multiplication par chaque Λ_j, grâce à la retenue de la page 8 ($\Lambda_j^p = q_j\Lambda_{j+1}$, ou 0 si $j = \nu$). D'autre part $\psi(\Lambda^a)$ est un multiple non nul de $X^{\sum a_i p^i}$, et ces exposants sont distincts et $< p^{\nu+1}$ (écriture en base p). Un élément $\sum w_a\Lambda^a$ de noyau nul a donc tous ses w_a nuls.

37. Preuve vérifiée : `lean/Grothendieck/Folder5.lean`.

Les puissances divisées de $A^{(\nu)}$. Comme B est une $\mathbf{Q}$-algèbre, tout idéal de B porte les puissances divisées $x^n/n!$. On les ramène sur $\bar{I} = (\Lambda_0, \dots, \Lambda_\nu) \subset A^{(\nu)}$ par ψ : il suffit que $\gamma_n(\psi(y))$ soit dans $\psi(\bar{I})$ pour $y \in \bar{I}$. Par les formules de la somme et du produit, il suffit de le voir pour $y = \Lambda_i$, et comme $\gamma_n(\gamma_{p^i}(X))$ est un multiple entier de $\gamma_{np^i}(X)$, il suffit que chaque $\gamma_k(X) = X^k/k!$ vienne de $A^{(\nu)}$. C'est une récurrence sur k : si p^e est la plus grande puissance de p divisant k, on a $\binom{k}{p^e}\gamma_k = \gamma_{p^e}\,\gamma_{k-p^e}$, et $\binom{k}{p^e} \equiv k/p^e \not\equiv 0 \pmod p$ par le théorème de Lucas, donc inversible dans W ; et $\gamma_{p^e}(X) = \psi(\Lambda_e)$ si $e \le \nu$, tandis que $\gamma_k(X) = 0$ si $k \ge p^{\nu+1}$.

Passage au quotient. L'augmentation $\varepsilon : A^{(\nu)} \to W$, $\Lambda_i \mapsto 0$, a pour noyau $\bar{I}$. Si $(\Lambda_0 - p)a \in \bar{I}$, alors $-p\,\varepsilon(a) = 0$, donc $a \in \bar{I}$; et $\gamma_n((\Lambda_0 - p)a) = (\Lambda_0 - p)^n\gamma_n(a)$. Ainsi $(\Lambda_0 - p) \cap \bar{I}$ est un sous-idéal à puissances divisées, et celles-ci passent à $J = \bar{I}\,W^{(\nu)}$. On a $\delta_{p^i}(p) = \delta_{p^i}(\Lambda_0) = \Lambda_i$ par injectivité de ψ, et $\delta_n(y) = 0$ pour $n \ge p^{\nu+1}$ parce que $\psi(y)$ est un multiple de X.

L'universalité. Le morphisme $\Lambda_i \mapsto \gamma_{p^i}(p)$ respecte les relations : $\gamma_{p^i}(p)^p = q_i\,\gamma_{p^{i+1}}(p)$ (`dpow_pow_eq_q`), $\gamma_{p^\nu}(p)^p = q_\nu\gamma_{p^{\nu+1}}(p) = 0$ et $\gamma_1(p) = p$. Il commute aux $\delta_k(p)$ par la même récurrence sur k, et donc aux puissances divisées des générateurs Λ_i, ce qui suffit. Un morphisme compatible envoie nécessairement $\Lambda_i = \delta_{p^i}(p)$ sur $\gamma_{p^i}(p)$, d'où l'unicité. □

L'énoncé tient, sous une forme plus forte que celle de la page : ni la localité, ni l'artinianité, ni le corps résiduel n'interviennent, et l'hypothèse sur T ne porte que sur les $\gamma_n(p)$. Lean : `universal`, `dpW`ν, `dpW`ν`_p`, `dpW`ν`_eq_zero`, `presentation` ; pour les étapes, `boxSpan_eq_top` (la retenue), `deg_injective`, `psi_injective`, `dpow_split` et `choose_pow_mul_pow_modEq` (Lucas), `psi_hmem`, `dpIbar`, `isSubDPIdeal_Kp`, dans `Folder5.lean`.

Théorème 35.3 (Grothendieck, pages 5 et 6, la suffisance du lemme ♦). *Soient $\lambda_0, \dots, \lambda_\nu \in W$ avec $\lambda_0 = p$ et $\lambda_i^p = q_i\lambda_{i+1}$ (ainsi $\lambda_i = p^{p^i}/(p^i)!$), et $\Theta_i = \Lambda_i - \lambda_i$. Dans $W^{(\nu)}$, on a $p^i\Theta_i = 0$ pour $0 \le i \le \nu$ et $p^\nu\lambda_\nu^p = 0$; si $\lambda_\nu = p^m u$ avec u inversible, $p^{\nu+pm} = 0$.*

Démonstration. Récurrence sur i, comme à la page 6 : $\Theta_0 = \Lambda_0 - p = 0$. Si $p^i\Theta_i = 0$, la différence $\Lambda_i^p - \lambda_i^p = q_i\Theta_{i+1}$ est un multiple de $\Lambda_i - \lambda_i = \Theta_i$, donc $p^i q_i\Theta_{i+1} = 0$; comme $q_i = p\,r_i$ avec r_i premier à p ($v_p(q_i) = 1$), $p^{i+1}\Theta_{i+1} = 0$. Pour $i = \nu$, $\Lambda_\nu^p = 0$ donne de même $p^\nu\lambda_\nu^p = 0$. On n'a pas besoin de développer le binôme. □

Pour $\lambda_\nu = p^{p^\nu}/(p^\nu)!$, $m = p^\nu - (p^\nu - 1)/(p-1)$ (par `sub_one_mul_padicValNat_factorial_pow`) et $\nu + pm = c(\nu)$: c'est le « $p^{c(\nu)} \in I$ » de la page 6. Lean : `p_pow_mul_Θ_mem`, `p_pow_mul_lam_pow_mem`, `p_pow_mem_Kp`, énoncés comme appartenances à l'idéal $(\Lambda_0 - p)$ de $A^{(\nu)}$.

La nécessité, que la page laisse « au lecteur » avec un point d'exclamation en marge, est démontrée elle aussi. Pour un exposant $a = (a_0, \dots, a_\nu)$, $0 \le a_i < p$, notons $\mathrm{ord}(a)$ l'indice du premier exposant non nul de a, et $\mathrm{ord}(0) = c(\nu) = \nu + pm$.

Théorème 35.4 (Grothendieck, pages 5 et 6, le lemme et son corollaire ♦). *Soient λ_i comme ci-dessus, avec $\lambda_\nu = p^m u$, u inversible, et $\Theta_i = \Lambda_i - \lambda_i$.*

1. *Les monômes Θ^a, $0 \le a_i < p$, forment une base du W-module $A^{(\nu)}$.*
2. (Le lemme de la page 5.) *$\sum_a w_a\Theta^a$ appartient à $(\Lambda_0 - p)$ si et seulement si $p^{\mathrm{ord}(a)}$ divise w_a pour tout a : $w_a \in p^iW$ si a_i est le premier exposant non nul, et $w_0 \in p^{c(\nu)}W$.*
3. (Le corollaire de la page 6.) *$W^{(\nu)} \simeq \bigoplus_a W/p^{\mathrm{ord}(a)}W$ comme W-module.*
4. *Si p n'est pas inversible dans W, $p^k = 0$ dans $W^{(\nu)}$ si et seulement si $k \ge c(\nu)$: l'ordre de 1 est exactement $p^{c(\nu)}$.*

5. *Si W est un anneau de valuation discrète d'uniformisante p, $W^{(\nu)}$ est de longueur $\sum_a \mathrm{ord}(a) = p + p^2 + \cdots + p^\nu + pm$.*

Démonstration. La retenue dans les Θ_i. En développant $\Lambda_i^p = (\Theta_i + \lambda_i)^p$ et en utilisant $\lambda_i^p = q_i \lambda_{i+1}$, on trouve

$$\Theta_i^p = q_i \Theta_{i+1} - \sum_{0<k<p} \binom{p}{k} \lambda_i^{p-k} \Theta_i^k \quad (i < \nu), \qquad \Theta_\nu^p = -\lambda_\nu^p - \sum_{0<k<p} \binom{p}{k} \lambda_\nu^{p-k} \Theta_\nu^k.$$

Pour $i < \nu$ le terme constant λ_i^p disparaît : c'est ce qui rend la retenue compatible avec les conditions a) et b).

Un idéal. Soit S_n le sous-W-module engendré par les $p^{\min(\mathrm{ord}(a),n)}\Theta^a$. On montre, par récurrence descendante sur j, que $p^{\min(\mathrm{ord}(a),j,n)}\,\Theta_j\Theta^a \in S_n$ pour tout a. Si $a_j < p-1$, $\Theta_j\Theta^a$ est un monôme de la base, d'ordre au plus $\min(\mathrm{ord}(a), j)$. Si $a_j = p-1$, soit a' l'exposant a où l'on a remplacé a_j par 0 ; alors $\Theta_j\Theta^a = \Theta_j^p\Theta^{a'}$, et l'on remplace Θ_j^p par la formule ci-dessus. Les termes en $\Theta_j^k\Theta^{a'}$, $0<k<p$, sont des monômes de la base d'ordre au plus $\mathrm{ord}(a)$. Le terme $q_j\Theta_{j+1}\Theta^{a'}$ relève de l'hypothèse de récurrence : l'ordre ne monte que de 1 au plus, de j à $j+1$, et le facteur p de q_j le compense. Pour $j = \nu$, le terme $\lambda_\nu^p\Theta^{a'}$ porte le facteur p^{pm}, qui compense le passage de l'ordre ν à l'ordre $c(\nu) = \nu + pm$ quand $a' = 0$. Comme $\Lambda_j = \Theta_j + \lambda_j$, S_n est stable par multiplication par les Λ_j : c'est un idéal.

La base. S_0 est un idéal qui contient 1 : les Θ^a engendrent $A^{(\nu)}$. Comme les Λ^a en forment une base (c'est la seconde moitié de l'injectivité de ψ), l'application $(w_a) \mapsto \sum_a w_a\Theta^a$ est une surjection d'un module libre de rang $p^{\nu+1}$ sur un module libre de même rang, donc une bijection : sur un anneau commutatif, un endomorphisme surjectif d'un module de type fini est injectif.

Le lemme et ses conséquences. $S_{c(\nu)}$ est un idéal qui contient $\Theta_0 = \Lambda_0 - p$, donc contient $(\Lambda_0 - p)$: c'est la nécessité. La suffisance (théorème précédent) donne l'inclusion inverse. L'unicité des coordonnées dans la base des Θ^a donne alors (2), puis (3). Pour (4), on applique (2) à $p^k = p^k\,\Theta^0$: il faut et il suffit que $p^{c(\nu)}$ divise p^k. Pour (5), W/p^kW est de longueur k, et l'on compte : si $a_0 \neq 0$, l'ordre est 0, et si $a_0 = 0$, l'ordre est celui de $(a_1, \ldots, a_\nu)$ augmenté de 1. Par récurrence sur ν, $\sum_a \mathrm{ord}(a) + \nu + 1 = 1 + p + \cdots + p^\nu + c(\nu)$. □

L'énoncé tient. La seule propriété des q_i dont la nécessité ait besoin est $p \mid q_i$. La longueur $p + \cdots + p^\nu + pm$ vaut, par télescopage, la formule $c(\nu) + \sum_{i=1}^{\nu} i(p-1)p^{\nu-i}$ de la lecture ; pour $p = 2$ et $\nu = 1$, on retrouve la longueur 4 et $c(1) = 3$ de la note de la lecture. Pour les λ_i usuels, définis par $\lambda_i\,(p^i)! = p^{p^i}$, on a $m = p^\nu - v_p((p^\nu)!)$, et pour $W = \mathbf{Z}_p$ l'ordre de 1 est exactement $p^{c(\nu)}$. Lean : `normalForm`, `tmono_linearIndependent`, `span_tmono`, `Wνequiv`, `p_pow_eq_zero_iff`, `length_Wν`, `length_Wν_eq` ; pour les étapes, `Θ_pow_castSucc` et `Θ_pow_last` (la retenue), `Θ_mul_tmono_mem` et `mul_mem_S` (l'idéal), `mono_linearIndependent`, `Kp_le_S` (la nécessité), `S_le_Kp`, `sum_ord` (le dénombrement) ; pour les λ_i usuels, `exists_lamStd`, `p_pow_eq_zero_iff_std`, `length_Wν_std` et `padicInt_Wν`, dans `Folder5.lean`.

Reste hors de la vérification le lemme de la page 7 :

Théorème (Grothendieck, page 7, les quotients $W^{(\nu,r)}$ ♦). *Pour $1 \le r \le \nu$, soit $W^{(\nu,r)}$ le quotient de $W^{(\nu)}$ par $\Theta_1, \ldots, \Theta_r$. Alors $\sum w_a\Theta^a$ est dans $(\Theta_0, \ldots, \Theta_r)$ si et seulement si $w_a \in p^{i-r}W$ lorsque le premier exposant non nul a_i a un indice $i > r$, et $w_0 \in p^{c(\nu)-r}W$.*

◊ non vérifié en Lean

La forme normale de $W^{(\nu)}$ est démontrée ci-dessus. Pour les quotients $W^{(\nu,r)}$, l'édition n'a fait qu'une vérification à la machine, pour quelques (p, ν).

Théorème (Grothendieck, pages 49 et 50, dualité étale pour les sites annelés ♦). *Soient $f : (X, B) \to (Y, A)$ un morphisme lisse compactifiable de sites annelés, A un faisceau d'anneaux sur Y tué par un entier n premier aux caractéristiques résiduelles, et B un faisceau d'anneaux muni de $f^{-1}(A) \to B$. La dualité étale vaut pour f, avec $f^!(K) = R\mathrm{Hom}_{f^{-1}(A)}(B, f^{-1}(K) \otimes T_{X/Y}[2d])$, et se ramène aux cas $f^{-1}(A) \simeq B$ et $f = \mathrm{id}$. La lettre du 10 décembre 1965 l'énonce sans démonstration.*

◊ non vérifié en Lean

Mathlib n'a pas la dualité étale. On se reportera aux notes de Grothendieck (5, lot 3, p. 49).

Autres pistes de l'onglet Findings pour ce thème, non démontrées ici :

— Cote 8 : quand πA a des puissances divisées, le relèvement de Lubin–Tate existe et est unique par la seule théorie des déformations cristallines ; sans puissances divisées, l'argument donne l'unicité à isogénie près. La lecture de la page est à vérifier sur le fac-similé. Mathlib n'a pas la théorie des déformations cristallines. On se reportera aux notes de Grothendieck (8, lot 3, p. 43). ♦

— Cote 8 : deux groupes de Barsotti–Tate de dimension un et de hauteur $[K : \mathbf{Q}_p]$ sur $\mathbf{F}_q$, munis d'une action de A, sont isogènes si et seulement si $\varpi = \varpi'$, et $\mathrm{Hom}_A(G_0, G_0')$ est alors explicite. La lecture de la page est à vérifier sur le fac-similé. Mathlib n'a pas les groupes de Barsotti–Tate. On se reportera aux notes de Grothendieck (8, lot 2, p. 39). ♦

Théorème (Grothendieck, pages 1 et 4 à 7, valeurs propres unités de la cohomologie évanescente ♦). *On admet le théorème de Lefschetz faible cristallin avec torsion. Pour une section hyperplane lisse Y d'une variété projective lisse X de dimension n sur un corps parfait de caractéristique p, le nombre de valeurs propres du Frobenius qui sont des unités p-adiques sur la cohomologie cristalline évanescente est au moins le rang F-semi-simple de la cohomologie cohérente évanescente $\mathrm{Coker}(H^{n-1}(X, \mathcal{O}_X) \to H^{n-1}(Y, \mathcal{O}_Y))$, le défaut étant mesuré par la p-torsion de $H^n_{\mathrm{cris}}(X)$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 1 et 4 à 6). Le titre dit l'estimation « heuristique », et l'énoncé 8.4.4 a) de la page 1 y est sans argument. Mathlib n'a pas la cohomologie cristalline. On se reportera aux notes de Grothendieck (4, lot 1, p. 1).

Théorème (Grothendieck, pages 52 à 56, modules des variétés abéliennes ordinaires ♦). *Pour une polarisation de degré quelconque, divisible par p compris, l'anneau local en un point du schéma de modules des variétés abéliennes ordinaires polarisées en caractéristique p (degré de polarisation fixé, structure de niveau de Jacobi) est d'intersection complète et localement irréductible, et le schéma réduit est lisse : les modules formels des couples d'extensions compatibles forment le noyau d'un homomorphisme $\alpha - \beta$ de tores formels.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : ils donnent le noyau de $\alpha - \beta$, mais le texte des pages 52 à 56 est en grande partie illisible et reconstitué, et l'hypothèse que M_0 est étale est ajoutée par l'édition.

Théorème (Grothendieck, pages 49 et 50, un groupe formel hors des variétés abéliennes ♦). *Soient k un corps fini et E une courbe elliptique supersingulière sur k dont tous les endomorphismes sont définis sur k. La torsion du groupe formel de E par une unité θ de $\mathrm{End}(E) \otimes \mathbf{Z}_p$ de norme réduite transcendante donne une forme de $G_{1,1}$ qui ne se plonge dans le groupe formel d'aucune variété abélienne sur k ni sur aucune extension finie de k.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : ils donnent l'obstruction, d'après Weil, et disent « facile » l'existence de θ, qu'ils ne montrent pas.

Théorème (Grothendieck, pages 47 et 48, même groupe formel, non isogènes ♦). *Sur un corps algébriquement clos de caractéristique p, il existe des surfaces abéliennes simples de même groupe formel $\hat{\mathbf{G}}_m \times G_{1,1}$ qui ne sont pas isogènes.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : la discrétude de la classe d'isogénie n'y est pas justifiée, et la page compte une famille « de dim 2 au plus », chiffre de lecture douteuse, là où il faut 1.

Théorème (Grothendieck, pages 39 à 44 et 48 à 56, propriété universelle des complexes libres ♦). *Soient $\mathcal{P}$ la catégorie k-linéaire des complexes bornés de k-modules libres de type fini, Σ les suites exactes courtes scindées degré par degré et $\mathbb{C}^\bullet$ le complexe des disques. Pour toute catégorie $\mathcal{B}$ k-additive karoubienne munie d'une classe Σ de suites exactes où tout morphisme a un Σ-noyau, $F \mapsto F(\mathbb{C}^\bullet)$ est une équivalence entre les foncteurs k-linéaires $\mathcal{P} \to \mathcal{B}$ qui envoient Σ sur des suites exactes à gauche et les complexes de cochaînes de $\mathcal{B}$; les foncteurs Σ-exacts y correspondent aux Σ-résolutions.*

◊ non vérifié en Lean

L'encadré suit la forme de la page 55 ; la page 50 hésite et biffe « équivalence » pour « pleinement fidèle ». Les feuillets en esquissent une démonstration incomplète : les propositions 1 à 3 et la preuve des pages 52 à 55 sont en formules, et la page 52 note en marge « il faut condition de platitude ? ». La pleine fidélité, première moitié de a) et forme retenue par la page 50, est vérifiée en Lean et énoncée ci-dessous ; l'essentielle surjectivité (seconde moitié de a), là où servent les noyaux de $\mathcal{B}$) l'est aussi, pour $\mathcal{B}$ munie de noyaux et de sommes directes finies, dans le troisième encadré ; la forme karoubienne à classe Σ de l'énoncé et b) ne le sont pas.

Théorème (Grothendieck, pages 40 et 50 à 55, la pleine fidélité ♦). [a] *Soient k un anneau commutatif, $\mathcal{P}$ la catégorie des complexes de chaînes de k-modules libres de type fini, en degrés $\geqslant 0$ et nuls en grand degré, Σ la classe des suites $0 \to L' \to L \to L'' \to 0$ exactes en chaque degré, et $\mathbb{C}^\bullet$ le complexe des disques, $\mathbb{C}^n = (k \xrightarrow{\mathrm{id}} k)$ en degrés $n+1$, n. Alors :*

1. *(proposition 1, page 40)* $\mathrm{End}(\mathbb{C}^n) = k{\cdot}\mathrm{id}$, $\mathrm{Hom}(\mathbb{C}^n, \mathbb{C}^{n+1}) = k{\cdot}d^n$, *et* $\mathrm{Hom}(\mathbb{C}^n, \mathbb{C}^j) = 0$ *pour $j \notin \{n, n+1\}$; en particulier $d^{n+1}d^n = 0$;*
2. *pour toute catégorie k-linéaire $\mathcal{B}$, sans hypothèse de noyaux, le foncteur $F \mapsto F(\mathbb{C}^\bullet)$, des foncteurs k-linéaires $\mathcal{P} \to \mathcal{B}$ qui envoient chaque suite de Σ sur un diagramme noyau $0 \to F(L') \to F(L) \to F(L'')$ vers les complexes de cochaînes de $\mathcal{B}$, est pleinement fidèle.*

a. Preuve vérifiée : `lean/Grothendieck/Folder137.lean`.

Démonstration. (1) Un morphisme $f : \mathbb{C}^n \to X$ est déterminé par l'image du générateur 1 en degré $n+1$, sa composante de degré n s'en déduisant par la différentielle ; dans $\mathbb{C}^j$ cette image vit dans $(\mathbb{C}^j)_{n+1}$, qui vaut k pour $j = n$ (sommet) ou $j = n+1$ (base) et 0 sinon. (2) Tout L s'insère dans une suite de Σ

$$0 \to L \xrightarrow{\iota} I(L) \xrightarrow{\pi} L[1] \to 0, \qquad I(L)_m = L_m \oplus L_{m-1},$$
$$d(a,b) = (b,0), \quad \iota(a) = (a, da), \quad \pi(a,b) = b - da,$$

où $I(L)$, le cône de l'identité, est somme finie de disques : si (b) parcourt une base de chaque L_n, $\sum_{n,b} p_{n,b}\, e_{n,b} = \mathrm{id}_{I(L)}$, avec $e_{n,b} : \mathbb{C}^n \to I(L)$ envoyant le générateur sur $(0,b)$ et $p_{n,b} : I(L) \to \mathbb{C}^n$ donné par la coordonnée b^*. Soient F, G deux foncteurs comme dans l'énoncé et $\varphi : F(\mathbb{C}^\bullet) \to G(\mathbb{C}^\bullet)$ un morphisme de complexes. Par (1), φ commute à toute flèche entre disques, $c \cdot \mathrm{id}$, $c \cdot d^n$ ou 0, puisque F et G sont k-linéaires. On pose $\Phi_{I(L)} = \sum_{n,b} G(e_{n,b})\, \varphi_n\, F(p_{n,b})$; en insérant les deux décompositions de l'identité, Φ commute à toute flèche $I(L) \to I(M)$ et à toute flèche $\mathbb{C}^n \to I(M)$. Comme G envoie la suite ci-dessus sur un diagramme noyau, $G(\iota)$ est un monomorphisme noyau de $G(\pi)$; la flèche

$\Phi_{I(L)}F(\iota)$ est tuée par $G(\pi)$, car après le monomorphisme $G(\iota_{L[1]})$ elle devient $\Phi_{I(L[1])}F(\iota_{L[1]}\pi\iota) = 0$. Elle se relève donc en $\eta_L : F(L) \to G(L)$. La naturalité de η vient de $\iota_M g = I(g)\,\iota_L$, où $I(g) = g \oplus g$; on a $\eta_{\mathbb{C}^n} = \varphi_n$ en appliquant la commutation de Φ à $\iota : \mathbb{C}^n \to I(\mathbb{C}^n)$. C'est la plénitude. La fidélité suit de même : une transformation η vaut Φ sur $I(L)$ par la décomposition, puis est déterminée sur L par le monomorphisme $G(\iota)$. Le doute marginal de la page 52 (« il faut condition de platitude ? ») ne se pose pas pour cette moitié : on n'y utilise ni noyaux dans $\mathcal{B}$, ni platitude, ni la caractérisation par récurrence sur la longueur des pages 53 et 54, que la suite du cône remplace. Lean (`Folder137.lean`) définit $\mathcal{P}$ (`Perf`), les disques (`disc`, `dmap`, `univ`), Σ (`IsSigma`) et les foncteurs Σ-exacts à gauche (`SigmaLeftExact`, `Lex`), et démontre (1) (`disc_endo`, `disc_succ`, `disc_zero`), la suite du cône et sa décomposition (`isSigma_cone`, `total`) et (2) (ρ`FullyFaithful`, avec `discNat`, `phi_nat`, `extend`). L'essentielle surjectivité fait l'objet de l'encadré suivant ; ne sont pas démontrés la partie b), les propositions 2 et 3 (pages 42 à 44) et la version cosimpliciale des pages 45 et 46.

Théorème (Grothendieck, pages 50 à 55, l'essentielle surjectivité ♦). [a] *Avec les notations de l'encadré précédent, soit $\mathcal{B}$ une catégorie k-linéaire munie de noyaux et de sommes directes finies. Pour tout complexe de cochaînes $C^\bullet$ de $\mathcal{B}$, il existe un foncteur k-linéaire $\sigma(C^\bullet) : \mathcal{P} \to \mathcal{B}$, qui envoie chaque suite de Σ sur un diagramme noyau, tel que $\sigma(C^\bullet)(\mathbb{C}^\bullet) \simeq C^\bullet$. Par conséquent $F \mapsto F(\mathbb{C}^\bullet)$ est une équivalence de catégories.*

a. Preuve vérifiée : `lean/Grothendieck/Folder137.lean`.

Démonstration. Pour un objet T de $\mathcal{B}$, $M^\bullet = \mathrm{Hom}(T, C^\bullet)$ est un complexe de k-modules ; soit $\Phi_T(L) \subset \prod_n L_n \otimes_k M^n$ l'ensemble des familles (z_n) telles que $(1 \otimes d)\, z_n = (d \otimes 1)\, z_{n+1}$ dans $L_n \otimes M^{n+1}$. Comme $L_n \otimes M = \mathrm{Hom}_k(L_n^\vee, M)$ pour L_n libre de type fini, ce sont les morphismes de complexes $L^\vee \to M^\bullet$, c'est-à-dire les cycles de degré 0 de $\underline{\mathrm{Hom}}_k^\bullet(L^\bullet, C^\bullet)$ vus à travers T ; on définit $\sigma(C^\bullet)(L)$ comme un objet qui représente $T \mapsto \Phi_T(L)$. (i) Φ_T est exact à gauche sur Σ : une suite de Σ est scindée en chaque degré, L_n'' étant libre, donc reste exacte après $- \otimes_k M^n$; un élément de $\Phi_T(L)$ tué dans $\Phi_T(L'')$ provient d'un unique élément de $\Phi_T(L')$, la condition de cycle se transportant par injectivité. (ii) Le disque $\mathbb{C}^n$ est représenté par C^n : un cycle de $\mathbb{C}^n$ est déterminé par sa composante de degré n, $x \in \mathrm{Hom}(T, C^n)$, celle de degré $n+1$ valant dx ; par cette identification, d^n correspond à la différentielle de $C^\bullet$. (iii) $I(L)$ est représenté par la somme directe finie $\bigoplus_{n,b} C^n$, car à la relation $\sum_{n,b} p_{n,b}\, e_{n,b} = \mathrm{id}$ s'ajoute l'orthogonalité $p_{m,c}\, e_{n,b} = \delta_{(n,b),(m,c)}$. (iv) L est représenté par le noyau de la flèche $\sigma(I(L)) \to \sigma(I(L[1]))$ qui représente $I(L) \xrightarrow{\pi} L[1] \xrightarrow{\iota} I(L[1])$, par (i) appliqué aux suites du cône de L et de $L[1]$. Les flèches de $\sigma(C^\bullet)$ s'obtiennent par Yoneda ; la k-linéarité et l'exactitude à gauche sur Σ se lisent sur Φ, et $\sigma(C^\bullet)(\mathbb{C}^n) \simeq C^n$, compatiblement aux différentielles, parce que deux objets qui représentent le même foncteur sont isomorphes. Il n'y a pas de récurrence sur la longueur ni de platitude. Les sommes directes finies sont nécessaires en plus des noyaux que nomme la page 50 : un foncteur k-linéaire envoie $\mathbb{C}^0 \oplus \mathbb{C}^0$ sur une somme directe $F(\mathbb{C}^0) \oplus F(\mathbb{C}^0)$, qui n'existe pas dans la sous-catégorie pleine $\{0, k\}$ des k-espaces vectoriels (k un corps), laquelle a des noyaux ; le complexe réduit à k en degré 0 n'y est donc pas de la forme $F(\mathbb{C}^\bullet)$ (argument de l'édition, non formalisé). Lean (`Folder137.lean`) définit Φ (`Phi`, `PhiMap`, `PhiPre`) et la représentabilité (`Rep`), et démontre (i) (`PhiMap_injective`, `PhiMap_exact`), (ii) (`discRep`, `discRep_d`), (iii) (`eDec_pDec_self`, `eDec_pDec_ne`, `coneRep`) et (iv) (`kerRep`) ; il en tire $\sigma(C^\bullet)$ (σ`Fun`, σ`_sigmaLeftExact`, σ`Lex`), l'isomorphisme $\sigma(C^\bullet)(\mathbb{C}^\bullet) \simeq C^\bullet$ (σ`Iso`) et, avec ρ`FullyFaithful`, l'équivalence (ρ`Equivalence`). Ne sont pas démontrés : la forme karoubienne à classe Σ de suites exactes de $\mathcal{B}$ du premier encadré, la partie b), les propositions 2 et 3 (pages 42 à 44) et la version cosimpliciale des pages 45 et 46.

Conjecture (Grothendieck, pages 16 à 18, un site p-adique sans puissances divisées ♦). *Soit X_0 un schéma sur un corps parfait k de caractéristique p. La cohomologie du site des W-schémas formels affines p-adiquement complets $\mathrm{Spf}\, B$ munis d'une surjection $B \to A_0$ sur l'anneau d'un ouvert affine de X_0, de noyau nilpotent modulo p, sans puissances divisées ni*

surconvergence, est une cohomologie p-adique : elle redonne la cohomologie de Washnitzer–Monsky pour X_0 lisse affine, et $H_{\mathrm{DR}}(X/W)$ modulo la torsion quand X_0 a un relèvement propre et lisse X.

Mathlib n'a pas de cohomologie p-adique des schémas. On se reportera aux notes de Grothendieck (7, lot 1, p. 16).

Théorème (Grothendieck, pages 74 à 83, catégories polynomiales ♦). *Les catégories polynomiales strictes, catégories à produits finis munies d'une sous-catégorie additive de flèches de degré un et d'une graduation des* Hom *par l'homogénéité sous les scalaires, sont équivalentes aux $\otimes$-pd-catégories, catégories monoïdales symétriques additives munies d'un foncteur gradué exponentiel Γ^* et de flèches $\alpha_{p,q} : \Gamma^{pq} \to \Gamma^p\Gamma^q$; le passage inverse est $\mathbf{P}_p(X,Y) = \mathrm{Hom}(\Gamma^p X, Y)$.*

◊ non vérifié en Lean

La page 83 affirme l'équivalence sans la démontrer : « Les deux notions sont donc équivalentes ». Mathlib n'a aucune des deux notions. L'équivalence complète, avec les produits, l'additivité, les multidegrés, le produit tensoriel strict et la formule exponentielle, n'est pas vérifiée en Lean ; son cœur, la partie qui porte le passage inverse $\mathbf{P}_p(X,Y) = \mathrm{Hom}(\Gamma^p X, Y)$ et la règle de composition, l'est, et il est énoncé ci-dessous. On se reportera aux notes de Grothendieck (137, lot 4, p. 74).

Théorème (D'après les pages 77 à 83, forme réduite par l'édition, le cœur de l'équivalence ♦). [a] *Soit $\mathcal{C}$ une catégorie, celle des flèches de degré un. Appelons* catégorie polynomiale sur $\mathcal{C}$ *la donnée d'ensembles $\mathbf{P}_n(X,Y)$, d'une composition $\mathbf{P}_p(X,Y) \times \mathbf{P}_q(Y,Z) \to \mathbf{P}_{qp}(X,Z)$ associative, d'identités de degré un, et d'une bijection $\mathrm{Hom}_{\mathcal{C}}(X,Y) \simeq \mathbf{P}_1(X,Y)$ compatible à la composition ; elle est* représentable *si chaque foncteur $Y \mapsto \mathbf{P}_n(X,Y)$ sur $\mathcal{C}$ est représenté par un objet $\Gamma^n X$ et une flèche universelle $\gamma_n \in \mathbf{P}_n(X, \Gamma^n X)$. Appelons* structure à puissances divisées sur $\mathcal{C}$ *la donnée de foncteurs $\Gamma^n : \mathcal{C} \to \mathcal{C}$, de transformations naturelles $\alpha_{p,q} : \Gamma^{pq} \to \Gamma^p\Gamma^q$, d'un isomorphisme $\varepsilon : \Gamma^1 \simeq \mathrm{id}$, satisfaisant le carré d'associativité de la page 80 et les conditions d'unité $(**)$. Alors :*

1. *d'une structure à puissances divisées, $\mathbf{P}_p(X,Y) = \mathrm{Hom}(\Gamma^p X, Y)$ avec $g \circ f = g \circ \Gamma^q(f) \circ \alpha_{q,p}$ fait une catégorie polynomiale représentable, par $\Gamma^n X$ et $\gamma_n = \mathrm{id}$; si $\mathcal{C}$ est additive, cette composition est additive en g ;*
2. *d'une catégorie polynomiale représentable, les Γ^n sont des foncteurs, les $\alpha_{p,q}$ définis par la factorisation de $\gamma_p \circ \gamma_q$ sont naturels, $\Gamma^1 \simeq \mathrm{id}$, et le carré de la page 80 et $(**)$ sont vrais ;*
3. *les deux passages sont inverses l'un de l'autre : le premier suivi du second redonne exactement Γ, α et ε ; le second suivi du premier redonne la catégorie polynomiale de départ à isomorphisme près, par $\varphi \mapsto \varphi \circ \gamma_p$.*

a. Preuve vérifiée : `lean/Grothendieck/Folder137.lean`.

Démonstration. Une structure à puissances divisées est une comonade graduée par le monoïde multiplicatif $(\mathbf{N}, \cdot)$, et la catégorie polynomiale qu'elle définit en est la catégorie de Kleisli. (1) L'associativité de la composition des pages 81 et 82 est ce qui demande la naturalité de α : dans $h \circ (g \circ f)$ et $(h \circ g) \circ f$, on fait passer $\Gamma^{rq}(f)$ à travers $\alpha_{r,q}$ par naturalité, et il reste à comparer $\alpha_{r,q} \circ \alpha_{rq,p}$ et $\Gamma^r(\alpha_{q,p}) \circ \alpha_{r,qp}$, qui est le carré de la page 80. Les unités sont $(**)$ et la naturalité de ε. La représentabilité est immédiate : $\varphi \circ \gamma_n = \alpha_{1,n} \circ \varepsilon \circ \varphi = \varphi$, par $(**)$. (2) Tout se lit à travers la bijection $\varphi \mapsto \varphi \circ \gamma_n$ de $\mathrm{Hom}(\Gamma^n X, Y)$ sur $\mathbf{P}_n(X,Y)$: on définit $\Gamma^n(f)$ par $\Gamma^n(f) \circ \gamma_n = \gamma_n \circ f$, $\alpha_{p,q}$ par $\alpha_{p,q} \circ \gamma_{pq} = \gamma_p \circ \gamma_q$ (la page 80 : « ce qui revient au même »), et ε par $\varepsilon \circ \gamma_1 = \mathrm{id}$. Chaque identité à démontrer, fonctorialité, naturalité, carré, unités, devient après composition avec le γ convenable

une égalité entre composés de γ, qui découle de l'associativité de $\mathbf{P}$; par exemple les deux côtés du carré deviennent $\gamma_p \circ \gamma_q \circ \gamma_r$, parenthésé de deux façons. L'inverse de ε est la flèche de degré un qui correspond à γ_1. (3) Dans le premier passage, $\varphi \mapsto \varphi \circ \gamma_n$ est l'identité ; le second passage reconstruit donc Γ, α et ε à partir de $\gamma_n = \mathrm{id}$, et les retrouve par $(**)$. Dans l'autre sens, la bijection $\varphi \mapsto \varphi \circ \gamma_p$ envoie $g \circ \Gamma^q(f) \circ \alpha_{q,p}$ sur $(g \circ \gamma_q) \circ (f \circ \gamma_p)$, par le même calcul. Rien n'utilise l'additivité, le produit tensoriel ni la formule exponentielle : le cœur de l'équivalence vaut pour une catégorie $\mathcal{C}$ quelconque, et la règle de composition de la page 82 est forcée par la représentabilité. Les degrés sont portés par une équation $pq = n$, ce qui évite toute conversion d'indices. Lean (`Folder137.lean`) définit les deux notions (`PDCategory`, `PolynomialCategory`, `PolynomialCategory.Representation`) et démontre (1) (`PDCategory.toPoly`, `PDCategory.representation`, `PDCategory.toPoly_comp_add`), (2) (`Representation.toPD`) et (3) (`PDCategory.toPD_representation_Γ_map`, `PDCategory.toPD_representation_α`, `PDCategory.toPD_representation_ε`, `Representation.toPDToPolyIso`) ; un modèle trivial, tous les Γ^n égaux à l'identité, montre que les axiomes sont compatibles (`PDCategory.trivial`). Les axiomes a) à c) font l'objet de l'encadré suivant, et ce que Mathlib atteint de l'exemple des k-modules du second. Ne sont pas démontrés : la décomposition d) par multidegrés et l'homogénéité sous les scalaires, f) et g), la moitié $\mathbf{1} \simeq \Gamma^q(\mathbf{1})$ de $(***)$, le produit tensoriel strict, la formule exponentielle $\Gamma^*(X \oplus Y) \simeq \Gamma^* X \otimes \Gamma^* Y$ et, dans l'exemple des k-modules, le théorème de Roby.

Théorème (D'après la page 74, forme graduée par l'édition, les axiomes a) à c) ♦). [a] *Soit $\mathbf{P}$ une catégorie polynomiale représentable sur $\mathcal{C}$, au sens de l'encadré précédent. Si $\mathcal{C}$ a des produits binaires, alors pour tout n les projections, de degré un, font de $X \times Y$ un produit dans chaque $\mathbf{P}_n$: $\mathbf{P}_n(W, X \times Y) \simeq \mathbf{P}_n(W, X) \times \mathbf{P}_n(W, Y)$, et en degré un c'est l'accouplement de $\mathcal{C}$; l'objet final de $\mathcal{C}$ est final dans chaque $\mathbf{P}_n$. Si de plus $\mathcal{C}$ est préadditive, la loi $f + g = m \circ (f, g)$, où $m = \mathrm{pr}_1 + \mathrm{pr}_2 : X \times X \to X$ est de degré un, est une loi de groupe abélien sur $\mathbf{P}_n(W, X)$, qui prolonge l'addition de $\mathcal{C}$ en degré un, et*

$$(f + g) \circ h = f \circ h + g \circ h$$

pour h de degré quelconque. Pour la catégorie polynomiale d'une structure à puissances divisées, c'est l'addition de $\mathrm{Hom}(\Gamma^n W, X)$.

a. Preuve vérifiée : `lean/Grothendieck/Folder137.lean`.

Démonstration. Tout passe encore par la bijection $\varphi \mapsto \varphi \circ \gamma_n$ de $\mathrm{Hom}(\Gamma^n W, Y)$ sur $\mathbf{P}_n(W, Y)$, qui transforme la composition à droite par une flèche u de degré un en $u \circ -$. (a) Les composantes de $\varphi \circ \gamma_n$ sont donc $(\mathrm{pr}_1 \varphi) \circ \gamma_n$ et $(\mathrm{pr}_2 \varphi) \circ \gamma_n$: l'application $a \mapsto (\mathrm{pr}_1 \circ a, \mathrm{pr}_2 \circ a)$ est, à travers ces bijections, la propriété universelle du produit dans $\mathcal{C}$, d'où la bijection. De même pour l'objet final. (b) Par la même bijection, $m \circ (\varphi\gamma_n, \psi\gamma_n) = m(\varphi, \psi) \circ \gamma_n = (\varphi + \psi) \circ \gamma_n$: la loi $m \circ (f, g)$ est celle de $\mathrm{Hom}(\Gamma^n W, X)$ transportée, donc une loi de groupe abélien ; en degré un, $(\iota f, \iota g) = \iota(f, g)$ et $m \circ (f, g) = f + g$. (c) Pour h de degré p, les composantes de $(f, g) \circ h$ sont $f \circ h$ et $g \circ h$ par associativité, d'où $(f, g) \circ h = (f \circ h, g \circ h)$ par (a), puis $m \circ (f, g) \circ h = (f \circ h) + (g \circ h)$. La page tire de a) à c) que $\mathbf{P}(X, Y)$ est un groupe abélien, « fonctoriel en X par des homomorphismes, mais pas en Y » : c'est (c), et la composition n'est pas additive en h parce que Γ^q n'est pas additif. Lean (`Folder137.lean`) démontre (a) (`PolynomialCategory.pairMap_bijective`, `pairMap_ι`, `terminal_unique`), (b) (`PolynomialCategory.add_eq`, `ι_add`, `PDCategory.add_eq`) et (c) (`PolynomialCategory.comp_add`). Le tout est démontré degré par degré : la catégorie totale $\mathbf{P}(X, Y) = \bigoplus_n \mathbf{P}_n(X, Y)$ n'est pas construite, car composer une somme de flèches de degrés différents demande Γ^q d'une telle somme, et les multidegrés de d) ne sont pas formalisés.

Théorème (D'après les pages 80 et 84, l'exemple des k-modules, ce que Mathlib atteint ♦). [a] *Soient k un anneau commutatif, M un k-module et $\Gamma(M)$ son algèbre à puissances divisées,*

engendrée par les $m^{[n]}$. Pour toute application linéaire $\varphi : \Gamma(M) \to N$, l'application $m \mapsto \varphi(m^{[n]})$ est homogène de degré n, $\varphi((\lambda m)^{[n]}) = \lambda^n \varphi(m^{[n]})$, et sa composée avec une application linéaire $f : M' \to M$ est $(\varphi \circ \Gamma(f))((-)^{[n]})$. L'application $m \mapsto (m^{[q]})^{[p]}$ de M dans $\Gamma(\Gamma(M))$, image de $m^{[pq]}$ par $\alpha_{p,q}$, est homogène de degré pq. Enfin $m \mapsto m^{[1]}$ est additive.

a. Preuve vérifiée : `lean/Grothendieck/Folder137.lean`.

Démonstration. C'est la relation $(\lambda m)^{[n]} = \lambda^n m^{[n]}$ de $\Gamma(M)$, appliquée une fois, puis deux fois avec $(\lambda^q)^p = \lambda^{pq}$; la fonctorialité est $\Gamma(f)(m^{[n]}) = f(m)^{[n]}$, et l'additivité de $m \mapsto m^{[1]}$ vient de $(x+y)^{[1]} = x^{[1]}y^{[0]} + x^{[0]}y^{[1]}$. Lean (`Folder137.lean`, à partir de `DividedPowerAlgebra` de Mathlib) démontre `Modules.dp_comp_smul`, `Modules.dp_comp_map`, `Modules.dp_dp_smul` et `Modules.dp_one_add`. Ne sont pas démontrés : la graduation $\Gamma(M) = \bigoplus_n \Gamma^n M$, absente de Mathlib, la flèche $\alpha_{p,q} : \Gamma^{pq}M \to \Gamma^p\Gamma^q M$ elle-même, dont la définition demande la propriété universelle de $\Gamma^{pq}M$ pour les lois polynômes, le théorème de Roby $\mathrm{Hom}(\Gamma^p M, N) \simeq$ lois polynômes homogènes de degré p, et donc que les k-modules forment une $\otimes$-pd-catégorie.

Partie 18

Schémas en groupes et groupes algébriques

36 Cote 10 : les indécomposables de $\mathbb{G}_a \rtimes \mathbb{G}_m$ [38]

La cote 10, *Catégories tensorielles*, que l'inventaire date « [à partir de 1958] », finit sur sept feuillets consacrés au groupe $G = k \rtimes k^*$, k^* opérant sur k par $\lambda \mapsto \lambda^p$, en caractéristique nulle (10, lot 10, p. 191). La page 191 passe à l'algèbre de Lie, engendrée par X (de $\mathbb{G}_a$) et Y (de $\mathbb{G}_m$) avec $[Y, X] = pX$; les pages 192 à 194 classent les représentations indécomposables ; les pages 195 à 197 calculent l'anneau des classes. L'hypothèse $p \geq 1$ est de l'édition.
Conventions. Une représentation est un espace vectoriel muni de deux endomorphismes X et Y, et un morphisme une application linéaire qui commute aux deux. La chaîne $e_{n,k}$ est k^k, de base $z_0, \ldots, z_{k-1}$, avec $X z_j = z_{j+1}$ ($z_k = 0$) et $Y z_j = (n + pj)\, z_j$; c'est le $k[Z]/(Z^k)$ de la page, de poids $n, n+p, \ldots, n+p(k-1)$. Le produit tensoriel est muni de $X \otimes 1 + 1 \otimes X$ et de $Y \otimes 1 + 1 \otimes Y$, le dual de $-{}^tX$ et $-{}^tY$, et l'on pose $\xi = e_{0,2}$.

Énoncé (Grothendieck, page 194, les chaînes ♦). *En caractéristique nulle et pour $p \geq 1$, tout endomorphisme de $e_{n,k}$ est scalaire, de sorte que $e_{n,k}$ est indécomposable ; $e_{n,k} \simeq e_{n',k'}$ avec $k \geq 1$ entraîne $n = n'$ et $k = k'$; et le dual de $e_{n,k}$ est $e_{-n-p(k-1),k}$.*

L'énoncé tient tel que la lecture le donne (`string_end_scalar`, `string_indecomposable`, `string_iso_imp`, `string_dual`). La formule du dual vaut sur tout corps et pour tout p.

Énoncé (Énoncé de l'édition, d'après les pages 196 et 197, le terme dominant de ξ^n). *Sur un corps K quelconque et pour tout p, si $k \geq 2$ est inversible dans K, on a $\xi \otimes e_{n,k} \simeq e_{n,k+1} \oplus e_{n+p,k-1}$.*

Démonstration. Soient a, b la base de ξ, de poids 0 et p, avec $Xa = b$ et $Xb = 0$. Comme $X^2 = 0$ sur ξ, on a $X^c(a \otimes y) = a \otimes X^c y + c\, b \otimes X^{c-1} y$. Posons $v_j = X^j(a \otimes z_0)$, $0 \leq j \leq k$, et $w_i = X^i w_0$, $0 \leq i \leq k-2$, avec $w_0 = a \otimes z_1 - (k-1)\, b \otimes z_0$. Alors $v_j = a \otimes z_j + j\, b \otimes z_{j-1}$ et $w_i = a \otimes z_{i+1} + (i-k+1)\, b \otimes z_i$, d'où $X v_k = 0$ et $X w_{k-2} = 0$. La relation $[Y, X] = pX$ passe au produit tensoriel, et $a \otimes z_0$, w_0 sont propres pour Y, de valeurs n et $n+p$: les v_j et les w_i forment deux chaînes, de types $e_{n,k+1}$ et $e_{n+p,k-1}$. Enfin $v_{i+1} - w_i = k\, b \otimes z_i$ et $v_k = k\, b \otimes z_{k-1}$; comme k est inversible, les $b \otimes z_i$, puis les $a \otimes z_j = v_j - j\, b \otimes z_{j-1}$, sont dans l'espace engendré. Les $2k$ vecteurs v_j, w_i engendrent un espace de dimension $2k$: ils en forment une base, et l'application qui envoie les bases des deux chaînes sur eux est un isomorphisme de représentations. □

Remarque. Cet isomorphisme rend triangulaire, à coefficient dominant 1, l'écriture de ξ^n sur les $e_{0,i}$: $\xi \cdot e_{0,k} = e_{0,k+1} + \sigma_p\, e_{0,k-1}$ donne par récurrence $\xi^n = e_{0,n+1} + \sum_{i \leq n} c_{ni}\, e_{0,i}$, soit le $\alpha = 0$ que la page 197 obtient par les poids. La preuve n'utilise que l'inversibilité de k, ni la caractéristique nulle ni $p \geq 1$: l'énoncé est plus général que celui dont la page a besoin (`xi_tensor_string`).

Énoncé (Grothendieck, pages 192 à 194, lemmes 1 et 2 ♦). *En caractéristique nulle et pour $p \geq 1$, soit V une représentation de dimension finie non nulle, avec $[Y, X] = pX$, sur laquelle Y est diagonalisable à valeurs propres entières, $V = \bigoplus_{n \in \mathbf{Z}} \mathrm{Ker}(Y - n)$. Si V est indécomposable,*

38. Preuve vérifiée : `lean/Grothendieck/Folder10.lean`.

c'est-à-dire si ses seuls endomorphismes idempotents sont 0 *et* 1*, alors* $V \simeq e_{n,k}$ *pour un* $n \in \mathbf{Z}$ *et un* $k \geq 1$.

Démonstration. Comme X envoie le poids c sur le poids $c+p$ et que les poids de V sont en nombre fini, X est nilpotent ; soit m tel que $X^{m+1} = 0 \neq X^m$. Prenons un vecteur propre v de Y, de poids n, avec $X^m v \neq 0$, et une coordonnée ψ dans une base propre de Y telle que $\psi(X^m v) = 1$: on a $\psi \circ Y = \mu\,\psi$, et $\mu = n + pm$ est le poids de $X^m v$. Comme $X^a v$ est de poids $n + pa$, on obtient $\psi(X^a v) = 0$ pour $a \neq m$, la caractéristique étant nulle et $p \neq 0$. Posons $P(x) = \sum_{l=0}^{m} \psi(X^{m-l}x)\, X^l v$. Alors P commute à X (car $X^{m+1} = 0$) et à Y (car $X^a Y = (Y - pa)X^a$), et $P(X^l v) = X^l v$, de sorte que P est un idempotent non nul : $P = 1$. Les $X^l v$, $0 \leq l \leq m$, engendrent donc V ; ils sont libres, puisque $\psi(X^{m-l'} X^l v) = \delta_{ll'}$, et forment une chaîne de type $e_{n,m+1}$. □

Lean : `indecomposable_is_string` (avec une base propre de Y) et `indecomposable_is_string'` (avec $\sum_n \operatorname{Ker}(Y - n) = V$).

Remarque. La preuve ne suit pas celle de la page, qui construit la suite $E_0 \to E_1 \to \cdots$ et montre par récurrence que les u_i sont injectifs, puis bijectifs : elle scinde directement la plus longue chaîne par un supplémentaire stable. L'hypothèse que Y soit semi-simple est celle que la lecture tire du cas II pour une représentation rationnelle de G ; on ne peut l'omettre au niveau de l'algèbre de Lie, puisque $X = 0$ et Y un bloc de Jordan de taille 2 donnent une représentation indécomposable qui n'est pas une chaîne. Il en va de même de $p \geq 1$: pour $p = 0$, X n'est plus forcément nilpotent.

Ne sont pas démontrés ici : le passage d'une représentation rationnelle du groupe algébrique G à la représentation (V, X, Y) de son algèbre de Lie, avec Y semi-simple à poids entiers, et l'anneau $R(G) = \mathbf{Z}[\mathbf{Z}][\xi]$ lui-même, qui demande encore le théorème de Krull–Schmidt, absent de mathlib.

Page 65 : le H^2 d'un tore de norme un

L'Exemple 1 de la page 65 traite d'une catégorie tannakienne de lien un tore G de dimension 1, déployé par une extension quadratique Z/k. La suite exacte $0 \to G \to Z^* \to \mathbf{G}_m \to 0$, où $Z^* = R_{Z/k}\mathbf{G}_m$ et la flèche de droite est la norme, donne « par Hilbert 90 » que le noyau de $H^2(k, G) \to H^2(k, Z^*) = \operatorname{Br}(Z)$ est nul. La page en conclut que le caractère numérique détermine la catégorie. Lean démontre le pas cohomologique, à un niveau galoisien fini. Il ne démontre ni le passage à la cohomologie galoisienne de k, ni la conclusion tannakienne (finding `10-numerical-character-rank-one-torus`).

Conventions. Soient L/K une extension galoisienne finie, $\Gamma = \operatorname{Gal}(L/K)$ et $\chi\colon \Gamma \to \{\pm 1\}$ un caractère, le signe d'une sous-extension quadratique $Z \subset L$ (`quadChar`). Pour un Γ-module M (ici $M = L^\times$, noté additivement), on note M_χ le module M tordu par χ, soit $\gamma \star x = \chi(\gamma)\,\gamma x$, c'est-à-dire $\gamma(x)^{\chi(\gamma)}$ sur $L^\times$. On note $\operatorname{Ind} M$ le module $M \times M$, sur lequel γ agit par $(\gamma x, \gamma y)$ si $\chi(\gamma) = 1$ et par $(\gamma y, \gamma x)$ sinon. Sur $L^\times$, ce sont les L-points de G et de Z^* : $(Z \otimes_K L)^\times$ s'écrit dans la base des deux idempotents.

Énoncé (Grothendieck, page 65, Exemple 1, à un niveau fini ♦). [a]

(a) Pour tout Γ*-module* M*, la suite* $0 \to M_\chi \xrightarrow{x \mapsto (x,-x)} \operatorname{Ind} M \xrightarrow{(x,y)\mapsto x+y} M \to 0$ *est exacte. Si* $H^1(\Gamma, M) = 0$*, l'application* $H^2(\Gamma, M_\chi) \to H^2(\Gamma, \operatorname{Ind} M)$ *est injective.*

(b) Pour $M = L^\times$*, la suite est* $1 \to G(L) \to (Z \otimes_K L)^\times \xrightarrow{N} L^\times \to 1$*, et* $H^2(\Gamma, G(L)) \to$

$H^2(\Gamma, (Z \otimes_K L)^\times)$ *est injective.*

(c) Si χ est le signe d'une sous-extension quadratique Z, on a $H^2(\Gamma, \operatorname{Ind} L^\times) \simeq H^2(\mathrm{Gal}(L/Z), L^\times)$, et le composé $H^2(\Gamma, G(L)) \to H^2(\mathrm{Gal}(L/Z), L^\times)$ est injectif.

a. Preuve vérifiée : `lean/Grothendieck/Folder10.lean`.

Démonstration. (a) Le noyau de $(x, y) \mapsto x + y$ est formé des $(x, -x)$, et $(x, 0)$ est un antécédent de x. Les deux flèches sont équivariantes : si $\chi(\gamma) = -1$, l'échange des facteurs envoie $(\gamma x, -\gamma x)$ sur $(-\gamma x, \gamma x)$, image de $\gamma \star x = -\gamma x$, et ne change pas la somme. La suite exacte longue donne l'exactitude de $H^1(\Gamma, M) \xrightarrow{\delta} H^2(\Gamma, M_\chi) \to H^2(\Gamma, \operatorname{Ind} M)$, et le noyau est l'image d'un groupe nul. (b) La forme de Noether du théorème 90 de Hilbert donne $H^1(\mathrm{Gal}(L/K), L^\times) = 0$. (c) Soit τ hors de $\operatorname{Ker}\chi = \mathrm{Gal}(L/Z)$. L'application qui envoie (x, y) sur la fonction $h \mapsto hx$ si $\chi(h) = 1$ et $h \mapsto hy$ sinon est un isomorphisme de $\operatorname{Ind} M$ sur le coinduit de $M|_{\operatorname{Ker}\chi}$, d'inverse $f \mapsto (f(1), \tau^{-1} f(\tau))$. On conclut par le lemme de Shapiro. Un tel τ existe, puisque $Z \neq K$. □

Lean : `torusSeq_shortExact` et `torus_H2_injective` pour (a), `norm_one_torus_H2_injective`, `torusIncl_units` et `normMap_units` pour (b), `indShapiro` et `norm_one_torus_H2_injective_quadratic` pour (c).

Remarque. L'énoncé (a) vaut pour tout caractère χ, y compris le caractère trivial, cas où $Z = K \times K$ est déployée et où $G = \mathbf{G}_m$. Lean n'identifie pas le module $\operatorname{Ind} L^\times$ à $(Z \otimes_K L)^\times$: il prend le modèle des deux idempotents comme définition. Il n'identifie pas non plus $H^2(\mathrm{Gal}(L/Z), L^\times)$ au groupe de Brauer relatif $\mathrm{Br}(L/Z)$. Restent hors de portée le passage à la limite sur L, qui donne $H^2(k, G) \to \mathrm{Br}(Z)$, et l'énoncé tannakien que la page en tire : que le caractère numérique détermine $\mathcal{M}$ à équivalence près. Ce dernier demande les catégories tannakiennes, leurs gerbes et leurs liens, absents de mathlib.

37 Cote 90 : un groupe plat irréductible dont un saturé n'est pas de type fini [39]

La cote 90, *KG (X)*, est datée par l'inventaire « à partir de 1964 » ; ses notes sont écrites au dos de feuillets dactylographiés d'EGA IV, § 18. Elles préparent l'existence de résolutions équivariantes. La page 1 pose, sur un anneau de Dedekind A, la notion de *saturé* : pour un sous-module N d'un module sans torsion M, le saturé $\widetilde{N}$ est l'ensemble des $y \in M$ dont un multiple non nul est dans N. Le lemme 1 donne des conditions équivalentes pour que le saturé de tout sous-module de type fini soit de type fini (90, lot 1, p. 1). La page 9 applique ces conditions à l'algèbre B d'un groupe affine et plat G sur A, et dit dans une parenthèse (90, lot 1, p. 9) :

> *cela signifie que pour les composantes irréd. de G, leurs fibres sont non vides*

Pour un groupe de type fini, la parenthèse est raisonnable. Sans cette hypothèse, que la proposition ne pose pas, elle tombe en défaut.

Le contre-exemple. Soient R un anneau de valuation discrète, K son corps des fractions, ϖ une uniformisante et $k = R/\varpi R$ le corps résiduel. On pose

$$B = \{ f \in K[T] \ : \ f(0) \in R \},$$

39. Preuve vérifiée : `lean/Grothendieck/Folder90.lean`.

les polynômes à coefficients dans K dont le terme constant est entier. C'est la réunion des dilatations successives $R[T/\varpi^n]$ du groupe additif en l'origine : on autorise des dénominateurs arbitraires partout, sauf au point $T = 0$ de la fibre spéciale. Cet exemple figure déjà dans SGA 3 (exposé $\mathrm{VI_B}$, 13.3), où l'anneau est décrit comme $R \oplus K \oplus K \oplus \cdots$, non projectif ; Duong, Hai et dos Santos le rappellent (arXiv :1701.06518, exemple 1.1). La page de la cote 90, qui ne suppose pas G de type fini, le contredit donc dans le séminaire même de Grothendieck.

Contre-exemple 37.1 (SGA 3, exposé $\mathrm{VI_B}$, 13.3, contre la parenthèse de la page 9 [6])**.** *L'anneau B est intègre, de sorte que $\operatorname{Spec} B$ est irréductible ; il est plat sur R ; l'application $f \mapsto f(0) \bmod \varpi$ est surjective de B sur k, de noyau ϖB, de sorte que $B/\varpi B \simeq k$; et $K \otimes_R B \neq 0$. Les deux fibres sont donc non vides. Pour tout $f \in B$, il existe $b_i, c_i \in B$ en nombre fini tels que $f(x+y) = \sum_i b_i(x)\, c_i(y)$ pour tous $x, y \in K$: la comultiplication du groupe additif préserve B. Pourtant le saturé de $R \cdot T$ dans B est $K \cdot T$, qui n'est pas un R-module de type fini.*

Démonstration. B est un sous-anneau de $K[T]$, donc intègre. Il est sans torsion : si $r \neq 0$ et $rf = 0$ dans $K[T]$, alors $f = 0$, puisque r est inversible dans K. Sur un anneau principal, un module sans torsion est plat.

Soit $f \in B$ avec $f(0) \in \varpi R$, disons $f(0) = a\varpi$. Alors $g = \varpi^{-1} f$ a pour terme constant $a \in R$, donc $g \in B$ et $f = \varpi g \in \varpi B$. Réciproquement, un élément de ϖB a un terme constant dans ϖR. Le noyau de $f \mapsto f(0) \bmod \varpi$ est donc ϖB, et l'application est surjective puisque les constantes de R sont dans B. Pour la fibre générique, l'application $K \otimes_R B \to K[T]$, $\lambda \otimes f \mapsto \lambda f$, envoie $1 \otimes 1$ sur $1 \neq 0$.

Pour la comultiplication, écrivons $f = \sum_{k \le d} f_k T^k$ avec $f_0 \in R$. La formule du binôme donne $f(x+y) = \sum_k \sum_{j \le k} \binom{k}{j} f_k\, x^j y^{k-j}$. On répartit chaque terme en un produit de deux éléments de B : pour $k = j = 0$, $f_0 \cdot 1$; pour $j = 0 < k$, le facteur 1 en x et $f_k y^k$ en y, de terme constant nul ; pour $j \ge 1$, le facteur $\binom{k}{j} f_k x^j$, de terme constant nul, et y^{k-j}. Tous ces facteurs sont dans B.

Le saturé. Si $r \neq 0$ et $rf = aT$ avec $a \in R$, alors $f = (a/r)T \in K \cdot T$. Inversement, pour $c \in K$, écrivons $c = a/s$ avec $a, s \in R$, $s \neq 0$; alors $s \cdot cT = aT \in R \cdot T$. Le saturé est donc $K \cdot T$, contenu dans B puisque cT s'annule en 0. L'application $cT \mapsto c$ est un isomorphisme de R-modules de $K \cdot T$ sur K. Si K était de type fini sur R, il serait entier sur R ; or R est intégralement clos, donc ϖ^{-1} serait dans R, et ϖ serait inversible, ce qui n'est pas. □

Remarque. Le lemme 1 de la page 1 dit que, pour un module sans torsion sur un anneau de Dedekind, les saturés des sous-modules de type fini sont de type fini si et seulement si le module est réunion filtrante de sous-modules de type fini saturés. Ici $R \cdot T$ est de type fini et son saturé ne l'est pas : B ne satisfait pas les conditions du lemme 1, alors que $\operatorname{Spec} B$, qui n'a qu'une composante irréductible, a ses deux fibres non vides. Que B soit une algèbre de Hopf n'est vérifié que par l'identité de comultiplication, point par point sur K ; comme K est infini, c'est une identité de polynômes. L'antipode, $f(T) \mapsto f(-T)$, et la counité, $f \mapsto f(0)$, préservent visiblement B, mais ne sont pas écrites en Lean.

Le cas de type fini et réduit. Pour un groupe de type fini, la parenthèse se ramène à une question d'algèbre commutative sur l'idéal $d(A) = \bigcap_n \pi^n A$ des éléments infiniment divisibles par l'uniformisante. On en démontre ici le cœur, valable pour tout élément π d'un anneau commutatif.

Énoncé (Composantes et éléments infiniment divisibles, énoncé de l'édition)**.** [a] *Soient A un anneau commutatif, $\pi \in A$ et $d(A) = \bigcap_n \pi^n A$.*

(a) Si un idéal premier minimal $\mathfrak{p}$ de A vérifie $\mathfrak{p} + \pi A = A$, autrement dit si la composante irréductible $V(\mathfrak{p})$ de $\operatorname{Spec} A$ ne rencontre pas la fibre spéciale $V(\pi)$, alors $d(A) \neq 0$.

(b) Si A est noethérien et réduit et si tout premier minimal $\mathfrak{p}$ vérifie $\mathfrak{p} + \pi A \neq A$, alors $d(A) = 0$.

Pour A noethérien et réduit, $d(A) = 0$ si et seulement si toutes les composantes irréductibles de $\operatorname{Spec} A$ rencontrent la fibre spéciale.

a. Preuve vérifiée : `lean/Grothendieck/Folder90.lean`.

Démonstration. (a) Comme $\mathfrak{p} + \pi A = A$, il existe $c \in A$ tel que $1 - c\pi \in \mathfrak{p}$. Dans un anneau commutatif, tout élément d'un premier minimal est diviseur de zéro : il existe $a \neq 0$ tel que $a(1 - c\pi) = 0$. Alors $a = ac\pi$ et, par récurrence, $a = a(c\pi)^n = (ac^n)\,\pi^n$ pour tout n : a est un élément non nul de $d(A)$. L'idée : sur une composante qui évite la fibre spéciale, π est inversible, et une fonction portée par cette composante est divisible par toutes les puissances de π. Cette partie n'utilise ni l'hypothèse noethérienne ni le théorème de Krull.

(b) Soit $\mathfrak{p}$ un premier minimal. L'anneau $A/\mathfrak{p}$ est intègre et noethérien, et l'image de π y engendre un idéal propre, puisque $\mathfrak{p} + \pi A \neq A$. Le théorème d'intersection de Krull donne $\bigcap_n \bar{\pi}^n (A/\mathfrak{p}) = 0$; l'image de $d(A)$ dans $A/\mathfrak{p}$ est donc nulle, et $d(A) \subseteq \mathfrak{p}$. L'intersection des premiers minimaux est le nilradical, nul puisque A est réduit : $d(A) = 0$. □

Lean : `iInf_pow_ne_bot_of_minimalPrime` pour (a), `iInf_pow_eq_bot_of_minimalPrimes` pour (b) et `iInf_pow_eq_bot_iff` pour l'équivalence.

Remarque. Pour $A = R[G]$, algèbre d'un groupe affine et plat de type fini sur un anneau de valuation discrète complet R d'uniformisante π, la proposition 6.19 de Hai et dos Santos [66] et le théorème de Kaplansky sur les modules projectifs traduisent $d(A) = 0$ en deux propriétés : G est *spécialement localement fini*, et $R[G]$ est un R-module libre. Avec l'énoncé ci-dessus, on obtient le critère de la page 9 quand $R[G]$ est réduit, ce qui est toujours le cas en caractéristique générique nulle. Ces deux résultats sont cités, non formalisés. Le cas non réduit, en caractéristique générique p, reste ouvert.

Ne sont pas démontrés ici : le lemme 1 lui-même, et l'énoncé suivant de la cote.

Théorème (D'après les pages 13 à 23, sous-modules équivariants sur une base quelconque, forme précisée par la lecture ♦)**.** *Soient S un schéma et G un S-schéma en groupes plat et affine, dont l'algèbre est réunion filtrante de sous-cogèbres localement libres de rang fini à quotients plats, opérant sur un S-schéma X quasi-compact et quasi-séparé muni d'un faisceau ample relatif G-linéarisé. Tout sous-module quasi-cohérent d'un G-module quasi-cohérent E sur X est contenu dans un plus petit sous-module quasi-cohérent G-stable, compatible au changement de base plat sur S et de type fini quand le premier l'est.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 19 à 23). L'argument s'arrête sur « Rédiger mieux ce début ». Mathlib n'a pas les modules quasi-cohérents équivariants. On se reportera aux notes de Grothendieck (90, lot 1, p. 13).

Le plus petit sous-comodule, sur $\operatorname{Spec} A$ (pages 7–9 et 13–15) [40]

La page 13 (90, lot 1, p. 13) énonce, pour un groupe affine sur une base quelconque dont l'algèbre B est réunion filtrante de sous-modules B_i avec 1) B/B_i plat, 2) $\Delta B_i \subset B_i \otimes B_i$, 3) B_i localement libre de type fini, et pour un G-module quasi-cohérent E à action triviale :

> *1) tout sous-module quasi-cohérent F de E est contenu dans un plus petit sous-module quasi-cohérent F' stable par G; sa formation commute à tout changement de base plat; si F est de type fini, F' aussi; 2) si X est quasi-compact et quasi-séparé, E est réunion filtrante de sous-modules quasi-cohérents de type fini stables par G.*

La page n'en donne pas de démonstration ; la lecture propose la formule $F' = \sum_i U_i \cdot (F \cap E_i)$, $U_i = \check{B}_i$, tirée de la description des pages 7 et 9. On démontre ici le cas de l'anneau, $X = S = \operatorname{Spec} A$, que la page énonce et argumente. Mathlib a les cogèbres mais pas les comodules : un comodule est un A-module E muni d'une coaction $\delta\colon E \to B \otimes E$ counitaire et coassociative, et $N \subset E$ est un sous-comodule si δN est contenu dans l'image de $B \otimes N$.

Énoncé (Pages 13–15, cas affine)**.** [a] *Soient A un anneau commutatif et B une A-cogèbre, réunion filtrante de sous-modules B_i projectifs de type fini, avec B/B_i plat et $\Delta B_i \subset \operatorname{Im}(B_i \otimes B_i \to B \otimes B)$. Soit E un B-comodule.*

1. *Tout sous-module F de E est contenu dans un plus petit sous-comodule F', à savoir le sous-module engendré par les $(u \otimes \mathrm{id})(y)$, où $y \in B_i \otimes E$ relève δf, $f \in F$ et $u \in U_i = \operatorname{Hom}_A(B_i, A)$.*
2. *Si F est de type fini, F' l'est, et $F' = U_i \cdot F$ pour un seul indice i.*
3. *Tout élément de E est dans un sous-comodule de type fini ; ceux-ci sont stables par somme, et E en est la réunion filtrante.*
4. *Pour tout morphisme de comodules φ, $\varphi(F') = (\varphi F)'$.*
5. *Pour toute A-algèbre A', $A' \otimes E$ est un comodule sur la A'-cogèbre $A' \otimes B$, et l'image de $A' \otimes F'$ dans $A' \otimes E$ est le plus petit sous-comodule contenant l'image de $A' \otimes F$. Si A' est plat sur A, cette image est $A' \otimes F'$.*

a. Preuve vérifiée : `lean/Grothendieck/Folder90Comodules.lean`.

Démonstration. L'étape de platitude. Comme B/B_i est plat, $B_i \otimes M \to B \otimes M$ est injectif pour tout M (suite exacte $0 \to B_i \to B \to B/B_i \to 0$, lemme du serpent sur une présentation de M). Il en découle l'égalité de la lecture, $(B_i \otimes E) \cap (B \otimes N) = B_i \otimes N$: si $y \in B_i \otimes E$ a son image dans $B \otimes N$, son image dans $B_i \otimes (E/N)$ s'envoie sur 0 dans $B \otimes (E/N)$, donc est nulle, et y provient de $B_i \otimes N$ par exactitude à droite.

F' contient F. Pour $f \in F$, δf est une somme finie, donc dans un $B_i \otimes E$; la coünité restreinte à B_i donne $(\varepsilon \otimes \mathrm{id})(y) = (\varepsilon \otimes \mathrm{id})\,\delta f = f$.

Minimalité. Si $N \supset F$ est un sous-comodule et $y \in B_i \otimes E$ relève δf, $f \in F$, l'image de y est dans $B \otimes N$, donc $y \in B_i \otimes N$ par l'étape de platitude, et $(u \otimes \mathrm{id})(y) \in N$.

Stabilité. Le module projectif de type fini B_i a une base duale finie (b_k, b_k^*), et Δ se relève en $\Delta_i\colon B_i \to B_i \otimes B_i$ par projectivité. La coassociativité et l'injectivité de $B_i \otimes (B \otimes E) \to B \otimes (B \otimes E)$

40. Preuve vérifiée : `lean/Grothendieck/Folder90Comodules.lean`.

donnent $(\mathrm{id}\otimes\delta)(y)=(\Delta_i\otimes\mathrm{id})(y)$ dans $B_i\otimes B\otimes E$, d'où

$$\delta\big((u\otimes\mathrm{id})\,y\big)=\sum_k b_k\otimes\big((u*b_k^*)\otimes\mathrm{id}\big)(y),\qquad u*v=(u\otimes v)\circ\Delta_i,$$

et les coefficients sont encore des générateurs de F'.

Finitude. Si F est engendré par $f_1,\dots,f_m$, on choisit un i commun (la famille est filtrante) et des relèvements y_j de δf_j. Le sous-module G engendré par les $(b_k^*\otimes\mathrm{id})(y_j)$ contient tous les $(u\otimes\mathrm{id})(y_j)$, puisque $u=\sum_k u(b_k)\,b_k^*$; il est stable par la formule précédente et contient F ; donc $F'\subset G\subset F'$, et F' est de type fini. Le point 3 s'en déduit avec $F=Ae$.

Morphismes et changement de base. Un morphisme φ envoie les générateurs de F' sur des générateurs de $(\varphi F)'$, et $\varphi(F')$ est un sous-comodule contenant φF. Pour A', l'application $e\mapsto 1\otimes e$ est un morphisme de B-comodules $E\to A'\otimes E$; un sous-comodule de $A'\otimes E$ sur $A'\otimes B$ en est un sur B, par $(a\otimes b)\otimes n\mapsto b\otimes an$; et l'image de $A'\otimes F'$ est le A'-module engendré par $1\otimes F'$. Si A' est plat, $A'\otimes F'\to A'\otimes E$ est injectif. □

Remarque. L'énoncé 1 tient sur tout anneau commutatif tel que la lecture le complète, et la compatibilité au changement de base tient pour toute A-algèbre A' dès qu'on l'énonce avec des images ; la platitude de A' ne sert qu'à identifier l'image à $A'\otimes F'$. La platitude de B/B_i n'intervient que par l'injectivité de $B_i\otimes M\to B\otimes M$. Ne sont pas formalisés : les modules quasi-cohérents sur un schéma X au-dessus d'une base S quelconque (recollement, hypothèse « quasi-compact et quasi-séparé » de 2)), les énoncés 3) et 4), l'équivalence de la page 7 entre comodules i-admissibles et U_i-modules, et l'action de G sur X des pages 17 à 23, qui est l'objet de la trouvaille. Noms Lean : `Comodule`, `IsSubcomodule`, `Exhaustion`, `Exhaustion.closure`, `Exhaustion.isLeast_closure`, `Exhaustion.closure_fg`, `Exhaustion.exists_fg_isSubcomodule`, `IsSubcomodule.sup`, `Exhaustion.map_closure`, `Exhaustion.coact_coeff`, `Exhaustion.mem_range_lTensor_of_rTensor_mem`, `comoduleBaseChange`, `isLeast_closure_baseChange`, `baseChange_closure_injective`.

38 Cote 40 : la régularité des torseurs sous α_p ne passe pas à la somme [41]

La cote 40, *Calculs [affines sur des] fibrés principaux affines : notes manuscrites (s.d.)*, que l'inventaire date « [années 1960-1970] », compte vingt-sept pages de notes rapides, toutes de sa main. Elle traite des schémas en groupes affines comme algèbres de Hopf commutatives, de leurs actions et des espaces principaux homogènes (pages 1 à 15), puis du noyau α_p du Frobenius en caractéristique p (pages 16 à 18), de la classification $H^1(A,\alpha_p)=A/A^p$ (pages 18 à 23) et d'une version globale par la suite de Frobenius (pages 24 à 27). La remarque des pages 26 et 27 prend $A=k[[X]]$, k algébriquement clos, et les revêtements obtenus en extrayant une racine p-ième : au changement d'uniformisante près, ce sont les $A[T]/(T^p-X^n)$, et « si $n=1$, c'est un anneau local régulier. Sinon, il ne l'est pas, comme on voit facilement » (40, lot 2, p. 26). Pour $p=3$ et $n=2$, la page décrit le cusp. La page 27 ajoute que, pour la structure de revêtement sous α_p, ce revêtement est la somme de deux revêtements réguliers, ceux des racines p-ièmes de X et de $-X+X^2$, et que le produit fibré de ces deux anneaux C_1, C_2 sur A est « déjà un anneau non régulier [car isomorphe à $C_1[T]/(T^p)$, qui a des éléments nilpotents] »

41. Preuve vérifiée : `lean/Grothendieck/Folder40.lean`.

(40, lot 2, p. 27). La phrase de la page 26 qui introduit la somme comporte des mots illisibles ou incertains ; l'énoncé de la page 27 est lu.
Conventions. Un anneau local noethérien de dimension un est régulier si et seulement s'il est de valuation discrète ; c'est ce dernier énoncé qui est démontré. Un anneau local régulier est intègre, donc un anneau non intègre n'est pas régulier. Pour un polynôme unitaire g sur un anneau R, $R[T]/(g)$ est libre de base $1, T, \dots, T^{\deg g - 1}$; en particulier la classe d'un polynôme non nul de degré $< \deg g$ n'y est pas nulle.

Lemme 38.1. *Soient A un anneau de valuation discrète, ϖ une uniformisante, $u \in A^\times$ et $n \geq 1$. L'anneau $C = A[T]/(T^n - \varpi u)$ est de valuation discrète, d'idéal maximal (t), où t est la classe de T.*

Démonstration. Le polynôme $T^n - \varpi u$ est unitaire et d'Eisenstein pour l'idéal (ϖ) : ses coefficients non dominants sont dans (ϖ), et son terme constant $-\varpi u$ n'est pas dans (ϖ^2). Il est donc irréductible dans $A[T]$, qui est factoriel, donc premier, et C est intègre. L'anneau C est fini sur A, donc entier, et tout idéal maximal M de C se contracte en un idéal maximal de A, c'est-à-dire en (ϖ). Alors $\varpi \in M$, puis $t^n = \varpi u \in M$ et $t \in M$, puisque M est premier. Inversement, tout $x \in M$ s'écrit $x = a + ty$ avec $a \in A$ et $y \in C$; comme $a = x - ty \in M \cap A = (\varpi)$ et $\varpi = t^n u^{-1}$, on a $x \in (t)$. Ainsi $M = (t)$ pour tout idéal maximal M : C est local d'idéal maximal (t). Il est noethérien comme quotient de $A[T]$, et $t \neq 0$, puisque $t^n = \varpi u \neq 0$ et que $A \to C$ est injective. Un anneau local noethérien intègre dont l'idéal maximal est principal et non nul est de valuation discrète. □

Énoncé (Page 26, le cusp $T^n = X^2$)**.** *Soient k un corps quelconque, $n \geq 2$, $S = k[[X]][T]/(T^n - X^2)$ et y la classe de T.*

1. *Si n est impair, ni X ne divise y, ni y ne divise X dans S ; S n'est donc pas un anneau de valuation, ni a fortiori de valuation discrète.*
2. *Si $n = 2m$ est pair, $(y^m - X)(y^m + X) = 0$ et les deux facteurs sont non nuls ; S n'est pas intègre.*
3. *Si $n = 2$ et si k est de caractéristique 2, $(y - X)^2 = 0$ et $y - X \neq 0$.*

Démonstration. 1) L'homomorphisme $A = k[[X]] \to k[[Z]]$, $f(X) \mapsto f(Z^n)$, se prolonge en $\varphi : S \to k[[Z]]$ par $y \mapsto Z^2$, puisque $(Z^2)^n = (Z^n)^2$. Soit $B \subset k[[Z]]$ l'ensemble des séries dont les coefficients d'exposant impair $< n$ sont nuls. C'est un sous-anneau : dans le coefficient d'exposant m impair $< n$ d'un produit, chaque terme $a_i b_{m-i}$ a un indice impair $< n$. Il contient $f(Z^n)$, qui n'a que des exposants multiples de n, et Z^2 ; il contient donc $\varphi(S)$. Si $Xc = y$, alors $Z^n \varphi(c) = Z^2$, donc $Z^{n-2}\varphi(c) = 1$, égalité que le terme constant interdit, puisque $n \geq 3$. Si $yc = X$, alors $Z^2\varphi(c) = Z^n$ et $\varphi(c) = Z^{n-2}$, qui n'est pas dans B puisque $n - 2$ est impair et $< n$. Or, dans un anneau de valuation, de deux éléments l'un divise l'autre.

2) Le produit des polynômes unitaires $T^m - X$ et $T^m + X$ est $T^{2m} - X^2$, et leurs classes sont non nulles, étant de degré $m < 2m$.

3) $(T - X)^2 - (T^2 - X^2) = 2X(X - T)$ est nul en caractéristique 2, et $T - X$ est de degré $1 < 2$. □

Théorème 38.2 (Grothendieck, pages 26 et 27, la régularité ne passe pas à la somme des torseurs sous α_p ♦)**.** *Soient k un corps de caractéristique $p > 0$, $A = k[[X]]$, $C_1 = A[T]/(T^p - X)$ et $C_2 = A[T]/(T^p + X - X^2)$, de racines s et t.*

1. *C_1 et C_2 sont des anneaux locaux réguliers.*
2. *Leur somme dans $H^1(A,\alpha_p) = A/A^p$, l'anneau $A[T]/(T^p - X^2)$ de la classe de $X + (-X + X^2) = X^2$, n'est pas régulière.*
3. *Le produit fibré $C_1 \otimes_A C_2$ n'est pas réduit : $z = 1 \otimes t + (s - s^2) \otimes 1$ est non nul et $z^p = 0$. Dans C_1, on a $-X + X^2 = (-s + s^2)^p$.*
4. *Il y a un isomorphisme de C_1-algèbres $C_1 \otimes_A C_2 \simeq C_1[T]/(T^p)$ qui envoie z sur la classe de T.*

Démonstration. 1) C'est le lemme 38.1 pour $\varpi = X$, avec $u = 1$, puis avec $u = X - 1$, qui est inversible de terme constant -1 et vérifie $-X + X^2 = X(X - 1)$.

2) Si p est impair, c'est l'énoncé 38, 1). Si $p = 2$, l'anneau a un nilpotent non nul par l'énoncé 38, 3) ; il n'est donc pas intègre.

3) L'anneau C_1 est non nul et $p = 0$ dedans, donc de caractéristique p, et le Frobenius y est additif : $(-s + s^2)^p = (s^2 - s)^p = s^{2p} - s^p = X^2 - X$, puisque $s^p = X$. Le produit fibré est non nul (voir plus bas) et de caractéristique p pour la même raison, et $z = 1 \otimes t - (-s + s^2) \otimes 1$. Donc

$$z^p = 1 \otimes t^p - (-s + s^2)^p \otimes 1 = 1 \otimes a - a \otimes 1 = 0, \qquad a = -X + X^2 \in A,$$

car $a \otimes 1 = 1 \otimes a$ pour $a \in A$. Pour voir que $z \neq 0$, soit $D = C_1[T]/(T^p + X - X^2)$, l'extension des scalaires de C_2 à C_1. L'homomorphisme de A-algèbres $C_2 \to D$, $t \mapsto T$, et l'inclusion $C_1 \to D$ définissent $\psi : C_1 \otimes_A C_2 \to D$, $x \otimes y \mapsto x\,\psi_2(y)$. Alors $\psi(z) = T - (-s + s^2)$ est la classe d'un polynôme unitaire de degré $1 < p$, donc non nulle.

4) Soit $E = C_1[T]/(T^p)$, de racine τ, et $b = -s + s^2$. L'anneau E est non nul et de caractéristique p, donc $(\tau + b)^p = \tau^p + b^p = b^p = -X + X^2$ par 3) : l'homomorphisme de A-algèbres $\varphi_2 : C_2 \to E$, $t \mapsto \tau + b$, est bien défini, et avec l'inclusion $C_1 \to E$ il définit $\varphi : C_1 \otimes_A C_2 \to E$, $x \otimes y \mapsto x\,\varphi_2(y)$, qui est C_1-linéaire. Inversement, $z^p = 0$ par 3), donc $\tau \mapsto z$ définit un homomorphisme de C_1-algèbres $\chi : E \to C_1 \otimes_A C_2$. On a $\varphi(z) = (\tau + b) - b = \tau$, donc $\varphi \circ \chi$ fixe le générateur τ et est l'identité. De même $\chi \circ \varphi$ est C_1-linéaire et $\chi(\varphi(1 \otimes t)) = \chi(\tau + b) = z + b \otimes 1 = 1 \otimes t$; il est l'identité sur $C_1 \otimes 1$ et sur $1 \otimes C_2$, donc partout. □

Voir `root_add_pow_E`, `C₂toE`, `fibreToE`, `EtoFibre`, `fibreEquiv` et `fibreEquiv_z` dans `Folder40.lean`.

Remarque. Le théorème tient tel que la lecture l'énonce, et plus généralement. Le lemme 38.1 n'utilise ni la complétude de A, ni la caractéristique, ni k algébriquement clos, et vaut pour tout $n \geq 1$. L'énoncé 38 vaut sur tout corps et pour tout $n \geq 2$. Le calcul de $\psi(z)$ est celui de la lecture : dans D, $T^p = -X + X^2 = (-s + s^2)^p$, donc $(T - (-s + s^2))^p = 0$, et le changement de variable $T \mapsto T - (-s + s^2)$ donne $D \simeq C_1[T]/(T^p)$, l'anneau de la page. La lecture en déduit $C_1 \otimes_A C_2 \simeq C_1[T]/(T^p)$; le point 4) le démontre directement, sans passer par D ni par le changement de variable : on envoie t sur $\tau + (-s + s^2)$ et, en sens inverse, τ sur z. La piste demande si cet échec de la régularité sous la loi de groupe de $H^1(A,\alpha_p)$ est consigné dans la littérature sur les modèles de torseurs sous α_p.

Ne sont pas démontrés ici : les algèbres de Hopf, les actions et les deux critères des pages 1 à 15 ; la classification $H^1(A,\alpha_p) = A/A^p$ (pages 18 à 23), et donc l'identification de la loi de groupe de H^1 avec l'addition de A/A^p, que la page 22 dit ne pas avoir prouvée ; la suite de Frobenius (pages 24 à 26) ; la réduction de tout torseur de $k[[X]]$ à $A[T]/(T^p - X^n)$ par changement d'uniformisante ; la non-régularité de $A[T]/(T^p - X^n)$ pour $n \geq 2$ autre que $n = 2$.

39 Cote 46 : relever un cocycle à travers la réduction modulo $\mathfrak{m}$ [42]

La cote 46, *Schémas en groupes et fibrés principaux (Divers)*, quatre-vingt-quatorze pages sans pagination de sa main, réunit des liasses sur le Frobenius, les schémas de Brauer–Severi, la restriction des scalaires et, aux pages 71 à 92, des « Petits fourbis cohomologiques » : théorème 90 tordu, théorème de Lang, torsion des cocycles, version semi-locale. Les pages 90 à 92 en sont la dernière étape (46, lot 5, p. 90). Soient $\mathcal{O}$ un anneau local, d'idéal maximal $\mathfrak{m}$ et de corps résiduel k de caractéristique p, Γ un groupe fini et A une $(\mathcal{O},\Gamma)$-algèbre finie, non nécessairement commutative : la marge de la page 90 cite $A=\mathrm{M}_n(\mathcal{O})$. La page affirme que $H^1(\Gamma,A^*)\to H^1(\Gamma,(A/\mathfrak{m}A)^*)\times H^1(\Lambda,A^*)$ est injective, Λ un p-sous-groupe de Sylow, et « en particulier », quand p ne divise pas l'ordre de Γ, que la réduction $H^1(\Gamma,A^*)\to H^1(\Gamma,(A/\mathfrak{m}A)^*)$ l'est. La lecture modernisée n'en retient que la forme « noyau trivial ». On démontre ici ce cas particulier, par une autre voie que la page, et montre qu'il se passe des deux hypothèses que la page discute ; puis l'injectivité elle-même, que la page affirme, et enfin la forme de Sylow, sous la forme « noyau trivial ».

Cocycles et cobords. Le groupe Γ opère sur l'anneau A par automorphismes d'anneau, et donc sur le groupe A^* de ses inversibles. Un 1-cocycle est une application $c:\Gamma\to A^*$ telle que $c(gh)=c(g)\,g(c(h))$; c'est un homomorphisme quand l'action est triviale, et en général un homomorphisme « tordu » par l'action. Il est cohomologue au cocycle trivial, ou est un cobord, s'il existe $u\in A^*$ avec $c(g)=u^{-1}g(u)$ pour tout g. L'ensemble $H^1(\Gamma,A^*)$ des classes n'est pas un groupe quand A^* n'est pas commutatif, seulement un ensemble pointé, et « noyau trivial » y est plus faible qu'« injectif ». Dire que la classe de c meurt dans $H^1(\Gamma,(A/\mathfrak{m}A)^*)$, c'est dire que l'image $\bar c$ de c modulo $\mathfrak{m}A$ est un cobord : $\bar c(g)=\bar v^{-1}g(\bar v)$ pour un inversible $\bar v$ de $A/\mathfrak{m}A$. La question est de relever ce cobord.

La voie de la page : dévisser par les puissances de $\mathfrak{m}$. Supposons d'abord $\mathfrak{m}^N A=0$. La page corrige le cocycle couche par couche. Si c est déjà trivial modulo $\mathfrak{m}^nA$, on peut l'écrire $c(g)=1+a(g)$ avec $a(g)\in\mathfrak{m}^nA$. Modulo $\mathfrak{m}^{n+1}A$, le produit $a(g)\,g(a(h))$ disparaît, et la relation de cocycle devient additive : $a(gh)=a(g)+g(a(h))$. La couche $\mathfrak{m}^nA/\mathfrak{m}^{n+1}A$ est un groupe abélien, et même un espace vectoriel sur k. Sur un tel module, quand $|\Gamma|$ est inversible, tout cocycle additif est un cobord : on pose $w=-\frac{1}{|\Gamma|}\sum_\sigma a(\sigma)$, et la relation de cocycle donne $a(g)=g(w)-w$. Alors $1+w$ est inversible, et $(1+w)^{-1}g(1+w)=1+a(g)$ modulo $\mathfrak{m}^{n+1}A$: le cocycle est trivial une couche plus bas. Après N couches, il est trivial. L'inversibilité de $|\Gamma|$ est là où sert « p ne divise pas $|\Gamma|$ » : dans un espace vectoriel sur k, diviser par $|\Gamma|$ demande que $|\Gamma|\neq 0$ dans k. Pour le cas général, A fini sur $\mathcal{O}$ sans $\mathfrak{m}$ nilpotent, la lecture passe à la limite par Artin–Rees.

La voie suivie ici : une seule moyenne. La démonstration du théorème 90 de Hilbert fournit un raccourci. Pour un cocycle c et un élément quelconque w de A, posons $b=\sum_{\sigma\in\Gamma}c(\sigma)\,\sigma(w)$. Alors

$$c(g)\,g(b)=\sum_\sigma c(g)\,g(c(\sigma))\,g\sigma(w)=\sum_\sigma c(g\sigma)\,(g\sigma)(w)=b,$$

puisque $\sigma\mapsto g\sigma$ permute Γ. Si b est inversible, cela s'écrit $c(g)=b\,g(b)^{-1}$, et c est un cobord, avec $u=b^{-1}$. Tout revient à choisir w pour que b soit inversible. Si c est trivial modulo $\mathfrak{m}A$, on prend $w=1$: $b=\sum_\sigma c(\sigma)$ est congru à $|\Gamma|$, donc s'écrit $|\Gamma|(1+x)$ avec $x\in\mathfrak{m}A$, et il est inversible dès que $|\Gamma|$ l'est et que les éléments $1+x$, $x\in\mathfrak{m}A$, le sont. Dans le cas général, on relève $\bar v^{-1}$ en un $w\in A$; alors $b\equiv\sum_\sigma\bar v^{-1}\sigma(\bar v)\,\sigma(\bar v^{-1})=|\Gamma|\,\bar v^{-1}$, et $b=|\Gamma|w(1+x)$ avec $x\in\mathfrak{m}A$. Les couches de la page sont ainsi traitées d'un coup : la moyenne se fait dans A^* et

42. Preuve vérifiée : `lean/Grothendieck/Folder46.lean`.

non dans chaque quotient abélien.

Reste à voir que $1+\mathfrak{m}A$ est fait d'inversibles, et que w l'est. Quand $\mathfrak{m}^N A = 0$, un élément x de $\mathfrak{m}A$ vérifie $x^N = 0$, et $1+x$ a pour inverse $1 - x + x^2 - \cdots \pm x^{N-1}$. Quand A est fini sur $\mathcal{O}$, c'est le lemme de Nakayama : la multiplication à gauche par $1+x$ est une application $\mathcal{O}$-linéaire de A dans lui-même, surjective modulo $\mathfrak{m}A$ puisqu'elle y est l'identité, donc surjective ; $1+x$ a un inverse à droite, de même un inverse à gauche, et il est inversible. Un élément w inversible modulo $\mathfrak{m}A$, avec $ww' = 1+x$ et $w'w = 1+y$, $x, y \in \mathfrak{m}A$, est alors inversible des deux côtés.

Énoncé (D'après les pages 90 à 92, forme reconstituée par l'édition, cas où p ne divise pas l'ordre de Γ ♦). *Soient $\mathcal{O}$ un anneau local commutatif, de corps résiduel de caractéristique p, Γ un groupe fini d'ordre premier à p, et A une $\mathcal{O}$-algèbre, non nécessairement commutative, sur laquelle Γ opère par automorphismes d'anneau. On suppose $\mathfrak{m}^N A = 0$ pour un entier N, ou A fini sur $\mathcal{O}$. Alors le noyau de $H^1(\Gamma, A^*) \to H^1(\Gamma, (A/\mathfrak{m}A)^*)$ est trivial : un cocycle dont la réduction modulo $\mathfrak{m}A$ est un cobord est un cobord. Plus généralement, il en est ainsi de $H^1(\Gamma, A^*) \to H^1(\Gamma, B^*)$ pour tout morphisme d'anneaux surjectif $A \to B$ compatible à Γ et de noyau contenu dans $\mathfrak{m}A$.*

Démonstration. Soit c un cocycle et $\bar{v}$ un inversible de B avec $\bar{c}(g) = \bar{v}^{-1} g(\bar{v})$. Comme $|\Gamma|$ n'est pas divisible par p, son image dans le corps résiduel n'est pas nulle, et $|\Gamma|$ est inversible dans $\mathcal{O}$, donc dans A. Les éléments $1+x$, $x \in \mathfrak{m}A$, sont inversibles, par nilpotence ou par Nakayama. Relevons $\bar{v}^{-1}$ et $\bar{v}$ en w et w' ; ww' et $w'w$ sont de la forme $1+x$, donc w est inversible. L'élément $b = \sum_\sigma c(\sigma)\,\sigma(w)$ a pour image $\sum_\sigma \bar{v}^{-1}\,\sigma(\bar{v})\,\sigma(\bar{v}^{-1}) = |\Gamma|\,\bar{v}^{-1}$, la même que $|\Gamma|\,w$. Donc $b = m(1+m^{-1}x)$, avec $m = |\Gamma|\,w$ inversible et x dans le noyau, et b est inversible. L'identité $c(g)\,g(b) = b$ donne $c(g) = u^{-1} g(u)$ avec $u = b^{-1}$. □

Contre-exemple (De l'édition : l'hypothèse sur p est nécessaire). *Soit $\Gamma = \mathbb{Z}/2$, opérant trivialement sur $A = \mathcal{O} = \mathbb{Z}/4$, où $\mathfrak{m} = (2)$, $\mathfrak{m}^2 = 0$ et $p = 2 = |\Gamma|$. L'application c qui envoie l'élément non trivial de Γ sur -1 est un cocycle, trivial modulo $\mathfrak{m}$, puisque $-1 \equiv 1 \pmod 2$. Ce n'est pas un cobord : l'action étant triviale et A commutatif, $u^{-1}g(u) = 1$ pour tout u, et $-1 \neq 1$ dans $\mathbb{Z}/4$.*

Remarque. La démonstration n'utilise que deux choses : $|\Gamma|$ inversible dans A, et $1+x$ inversible pour x dans le noyau de $A \to B$. Elle ne se sert ni de l'hypothèse du texte, que Γ opère trivialement sur $A/\mathfrak{m}A$, ni de celle de la marge, que $A^\Gamma \to A/\mathfrak{m}A$ est surjectif, ni d'une action de Γ sur $\mathcal{O}$, ni de la noethérianité, et le cas fini se passe d'Artin–Rees. La page en a besoin parce qu'elle vise la forme de Sylow : la restriction $H^1(\Gamma, A) \to H^1(\Lambda, A)$, injective puisque $[\Gamma : \Lambda]$ est inversible, fournit un $w \in A$ quelconque avec $a(g) = g(w) - w$, et la surjectivité de $A^\Gamma \to A/\mathfrak{m}A$ sert à corriger ce w par un invariant pour que $\varepsilon(w) = 1$, donc pour que w soit inversible. Quand Λ est trivial, la moyenne donne directement un w dans $\mathfrak{m}^n A$, et la correction n'a pas lieu d'être.

Remarque. La marge qui porte la surjectivité de $A^\Gamma \to A/\mathfrak{m}A$ est écrite en huit lignes obliques dans la marge gauche de la page 90, reliée par un double trait à « Supposons de plus que » ; la transcription y relève une douzaine de mots illisibles et lit « plus généralement supposons » avec doute, « surjectif » étant souligné deux fois. L'hypothèse dont la forme de Sylow dépend repose donc sur une lecture fragile, que seul le fac-similé peut confirmer. Le cas démontré ici n'en dépend pas.

Remarque. Pour A commutatif, l'énoncé découle du lemme du § 3.6 de Lorenz [90], lu dans sa prépublication (arXiv :math/9808032) ; la version publiée n'a pas été consultée, et sa numérotation peut différer. Lorenz suppose S commutatif et la trace $S \to S^G$ surjective, ce qu'entraîne $|G|$ inversible, et montre que $H^1(G, \mathrm{GL}_n(S)) \to H^1(G, \mathrm{GL}_n(S/\mathrm{rad}\, S))$ est de noyau trivial, par les modules projectifs et Nakayama. Comme $\mathfrak{m}A$ est contenu dans le radical de Jacobson de A quand A est fini sur $\mathcal{O}$, le cas $n = 1$ donne le cas commutatif de l'énoncé encadré. Le cas d'une algèbre non commutative à action quelconque, celui de la marge ($A = \mathrm{M}_n(\mathcal{O})$ avec une action qui n'est pas forcément coefficient par coefficient), n'y est pas sous cette forme ; l'argument de moyenne est classique, et l'énoncé n'est pas présenté comme nouveau.

De noyau trivial à injectif. Dans un ensemble pointé, un noyau trivial ne dit pas que deux classes de même image sont égales. Les pages 86 à 89 passent de l'un à l'autre en *tordant* l'action par un cocycle c' : on fait opérer Γ sur A par $\gamma \star a = c'(\gamma)\,\gamma(a)\,c'(\gamma)^{-1}$, et dire que c et c' sont cohomologues revient à dire qu'un cocycle de l'action tordue est un cobord. On peut éviter de changer d'action en faisant la moyenne directement avec les deux cocycles.

Énoncé (Grothendieck, page 90, injectivité, cas où p ne divise pas l'ordre de Γ ♦). *Sous les hypothèses de l'énoncé précédent, avec A fini sur $\mathcal{O}$, l'application $H^1(\Gamma, A^*) \to H^1(\Gamma, B^*)$ est injective : si deux cocycles $c, c' : \Gamma \to A^*$ ont des réductions cohomologues dans B^*, ils sont cohomologues, c'est-à-dire que $c(g) = u^{-1}\,c'(g)\,g(u)$ pour un $u \in A^*$.*

Démonstration. Pour $w \in A$, posons $u = \sum_\sigma c'(\sigma)\,\sigma(w)\,c(\sigma)^{-1}$. La relation de cocycle donne $g(c(\sigma))^{-1} = c(g\sigma)^{-1}c(g)$, d'où

$$c'(g)\,g(u) = \sum_\sigma c'(g)\,g(c'(\sigma))\,(g\sigma)(w)\,g(c(\sigma))^{-1} = \sum_\sigma c'(g\sigma)\,(g\sigma)(w)\,c(g\sigma)^{-1}\,c(g) = u\,c(g).$$

Si u est inversible, cela s'écrit $c(g) = u^{-1}c'(g)\,g(u)$. Soit $v \in B^*$ avec $\bar{c}(g) = v^{-1}\,\bar{c}'(g)\,g(v)$; relevons v en w, inversible comme plus haut. Alors $\bar{c}'(\sigma)\,\sigma(v)\,\bar{c}(\sigma)^{-1} = v$ pour tout σ, de sorte que u a la même image que $|\Gamma|\,w$, et $u = |\Gamma| w(1+x)$ avec x dans le noyau : u est inversible. □

Avec $c' = 1$, on retrouve la moyenne de l'énoncé précédent. La moyenne u est celle du théorème 90 pour l'action tordue par c', écrite sans changer d'action.
La forme de Sylow. Reste le facteur $H^1(\Lambda, A^*)$ de la page 90. Quand p divise l'ordre de Γ, la moyenne sur Γ n'est plus possible, mais la moyenne sur les classes à gauche $g\Lambda$ l'est encore, puisque leur nombre $[\Gamma : \Lambda]$ est premier à p. Il faut pour cela que le terme $c(g)\,g(z)$ ne dépende que de la classe $g\Lambda$, c'est-à-dire que $c(\lambda)\,\lambda(z) = z$ pour $\lambda \in \Lambda$: la relation de cocycle donne alors $c(g\lambda)\,(g\lambda)(z) = c(g)\,g\big(c(\lambda)\,\lambda(z)\big) = c(g)\,g(z)$. C'est là que servent les deux hypothèses de la page. Que c soit un cobord sur Λ, $c(\lambda) = u^{-1}\lambda(u)$, permet de prendre $z = u^{-1}w$ avec w invariant par Λ ; que w puisse être choisi de réduction prescrite modulo $\mathfrak{m}A$, c'est la surjectivité de la marge.

Énoncé (D'après la page 90 et sa marge, forme « noyau trivial » ♦). *Soient $\mathcal{O}$ un anneau local commutatif, de corps résiduel de caractéristique p, Γ un groupe fini, Λ un sous-groupe d'indice premier à p, par exemple un p-sous-groupe de Sylow, et A une $\mathcal{O}$-algèbre finie, non nécessairement commutative, sur laquelle Γ opère par automorphismes d'anneau. On suppose que $A^\Lambda \to A/\mathfrak{m}A$ est surjectif, ce qu'entraîne la surjectivité de $A^\Gamma \to A/\mathfrak{m}A$ demandée par la marge. Alors une classe de $H^1(\Gamma, A^*)$ triviale dans $H^1(\Gamma, (A/\mathfrak{m}A)^*)$ et dans $H^1(\Lambda, A^*)$ est*

triviale. Il en est de même pour tout morphisme d'anneaux surjectif $\pi : A \to B$ compatible à Γ, de noyau contenu dans $\mathfrak{m}A$, tel que $A^\Lambda \to B$ soit surjectif.

Démonstration. Soient $u \in A^*$ avec $c(\lambda) = u^{-1}\lambda(u)$ pour $\lambda \in \Lambda$, et $\bar{v} \in B^*$ avec $\bar{c}(g) = \bar{v}^{-1}g(\bar{v})$. Choisissons $w \in A^\Lambda$ de réduction $\pi(u)\,\bar{v}^{-1}$, et posons $z = u^{-1}w$. Pour $\lambda \in \Lambda$,

$$c(\lambda)\,\lambda(z) = u^{-1}\lambda(u)\,\lambda(u^{-1})\,\lambda(w) = u^{-1}w = z,$$

de sorte que $b = \sum_{g\Lambda \in \Gamma/\Lambda} c(g)\,g(z)$ est bien défini. Comme plus haut, $c(\gamma)\,\gamma(b)$ est la même somme, réindexée par $g\Lambda \mapsto \gamma g\Lambda$, d'où $c(\gamma)\,\gamma(b) = b$. La réduction de z est $\bar{v}^{-1}$, celle de chaque terme est $\bar{v}^{-1}g(\bar{v})\,g(\bar{v}^{-1}) = \bar{v}^{-1}$, et celle de b est $[\Gamma : \Lambda]\,\bar{v}^{-1}$. L'indice est inversible dans A, z l'est puisque sa réduction l'est, et $b = m(1 + m^{-1}x)$ avec $m = [\Gamma : \Lambda]\,z$ et x dans le noyau : b est inversible, et $c(g) = b\,g(b)^{-1}$. □

Pour $\Lambda = \Gamma$, l'hypothèse sur Λ dit déjà que c est un cobord, et l'énoncé est vide ; pour Λ trivial, $A^\Lambda = A$ se surjecte toujours sur $A/\mathfrak{m}A$, et l'on retrouve le premier énoncé. La démonstration n'utilise pas l'hypothèse du texte que Γ opère trivialement sur le corps résiduel. Elle donne le noyau trivial et non l'injectivité : pour comparer deux cocycles c et c' égaux sur Λ, il faudrait un w qui commute aux $c(\lambda)$, ce que l'invariance par Λ ne fournit pas quand A n'est pas commutatif. Pour A commutatif, $H^1(\Gamma, A^*)$ est un groupe et le noyau trivial suffit.
L'injectivité dans la forme de Sylow. Pour comparer deux cocycles c et c', on tord la moyenne comme plus haut : $b = \sum_{g\Lambda} c'(g)\,g(z)\,c(g)^{-1}$. La relation de cocycle donne

$$c'(g)\,g\big(c'(h)\,h(z)\,c(h)^{-1}\big) = c'(gh)\,(gh)(z)\,c(gh)^{-1}\,c(g),$$

de sorte que le terme ne dépend que de la classe $g\Lambda$ dès que $c'(\lambda)\,\lambda(z)\,c(\lambda)^{-1} = z$ pour $\lambda \in \Lambda$, et qu'alors $c'(\gamma)\,\gamma(b) = b\,c(\gamma)$. Si $c(\lambda) = u^{-1}c'(\lambda)\,\lambda(u)$ sur Λ, on prend $z = wu$, et la condition devient $c'(\lambda)\,\lambda(w)\,c'(\lambda)^{-1} = w$: w doit être invariant par Λ pour l'action tordue par c', et non pour l'action donnée. C'est le point que la page ne vérifie pas en ramenant l'injectivité au noyau par torsion : l'hypothèse de la marge doit survivre à la torsion. Elle y survit dans deux cas : quand c' est un cobord $t^{-1}\lambda(t)$ sur Λ, les invariants tordus sont les $t^{-1}wt$, $w \in A^\Lambda$, ce qui contient le noyau $(c' = 1)$; quand A est commutatif, l'action tordue est l'action donnée.

Énoncé (D'après la page 90 et sa marge, injectivité, forme reconstituée par l'édition ♦)**.** *Soient $\mathcal{O}$, Γ, Λ, A et $\pi : A \to B$ comme dans l'énoncé précédent, sans supposer A commutatif, et c, c' deux cocycles $\Gamma \to A^*$ dont les images dans $H^1(\Gamma, B^*)$ et dans $H^1(\Lambda, A^*)$ coïncident. On suppose que tout élément de B se relève en un $w \in A$ tel que $c'(\lambda)\,\lambda(w)\,c'(\lambda)^{-1} = w$ pour $\lambda \in \Lambda$. Alors c et c' sont cohomologues. L'hypothèse est celle de la marge, $A^\Lambda \to B$ surjectif, quand c' est un cobord sur Λ ou quand A est commutatif ; dans ce dernier cas, $H^1(\Gamma, A^*) \to H^1(\Gamma, B^*) \times H^1(\Lambda, A^*)$ est injective.*

Démonstration. Soient $u \in A^*$ avec $c(\lambda) = u^{-1}c'(\lambda)\,\lambda(u)$ sur Λ, $\bar{v} \in B^*$ avec $\bar{c}(g) = \bar{v}^{-1}\,\bar{c}'(g)\,g(\bar{v})$, et w un relèvement tordu-invariant de $\bar{v}\,\pi(u)^{-1}$. Alors $z = wu$ vérifie $c'(\lambda)\,\lambda(z)\,c(\lambda)^{-1} = z$: multiplié à droite par $c(\lambda) = u^{-1}c'(\lambda)\lambda(u)$, c'est $c'(\lambda)\lambda(w)\lambda(u) = w\,c'(\lambda)\,\lambda(u)$. La réduction de z est $\bar{v}$, celle de chaque terme $c'(g)\,g(z)\,c(g)^{-1}$ est $\bar{v}$, celle de b est $[\Gamma : \Lambda]\,\bar{v}$, et b est inversible comme dans la démonstration précédente ; $c'(\gamma)\,\gamma(b) = b\,c(\gamma)$ s'écrit $c(\gamma) = b^{-1}c'(\gamma)\,\gamma(b)$. Si $c'(\lambda) = t^{-1}\lambda(t)$ et $w_0 \in A^\Lambda$ relève $\pi(t)\,y\,\pi(t)^{-1}$, l'élément $t^{-1}w_0t$ relève y et est invariant pour l'action tordue ; si A est commutatif, $c'(\lambda)\,\lambda(w)\,c'(\lambda)^{-1} = \lambda(w)$. □

On ne sait pas si l'hypothèse non tordue de la marge suffit en général quand A n'est pas commutatif ; la démonstration par la moyenne ne le donne pas, et l'on n'a pas cherché de contre-exemple.

Portée de la vérification. Lean définit les cocycles et les cobords à valeurs dans A^* pour un anneau quelconque muni d'une action par automorphismes (`IsCocycle`, `IsCoboundary`), sans recourir à la cohomologie des groupes de mathlib, qui est abélienne. Il démontre l'identité de moyenne (`mul_smul_sum`), sa conséquence (`isCoboundary_of_isUnit_sum`), le noyau trivial pour un morphisme surjectif compatible à Γ quand $1+\mathrm{Ker}$ est fait d'inversibles (`isCoboundary_of_map_isCoboundary`), la nilpotence de $\mathfrak{m}A$ quand $\mathfrak{m}^N A = 0$ et l'inversibilité de $1+\mathfrak{m}A$ pour A fini, par Nakayama (`isNilpotent_of_mem_smul_top`, `isUnit_one_add_of_mem_smul_top`), puis les deux formes de l'énoncé encadré (`ker_trivial_of_pow_smul_eq_bot`, `ker_trivial`), l'injectivité (`mul_smul_sum_twist`, `isCohomologous_of_map`, `injective`) et le contre-exemple (`not_isCoboundary_signCocycle`). La forme de Sylow, dans `Folder46.lean`, y est démontrée par la moyenne sur les classes (`mul_smul_sum_cosets`, `isCoboundary_of_restrict`), puis sur un anneau local pour un sous-groupe d'indice premier à p et pour un sous-groupe de Sylow (`ker_trivial_restrict`, `ker_trivial_sylow`). L'injectivité dans la forme de Sylow y est démontrée par la moyenne tordue sur les classes (`mul_smul_twist_cocycle`, `mul_smul_sum_cosets_twist`, `isCohomologous_of_restrict`), sous l'hypothèse de relèvement pour l'action tordue par c', sur un anneau local (`injective_restrict`, `injective_sylow`), puis sous l'hypothèse non tordue de la marge quand c' est un cobord sur Λ (`twisted_lift_of_isCoboundary`, `injective_sylow_of_isCoboundary`) et quand A est commutatif (`injective_sylow_comm`). L'hypothèse « p ne divise pas $|\Gamma|$ » y est écrite avec la caractéristique du corps résiduel de mathlib. Ne sont pas formalisés l'injectivité dans la forme de Sylow pour A non commutatif sous la seule hypothèse non tordue de la marge, dont on ignore si elle suffit, la base semi-locale des pages 84 à 89 et le passage à la limite par Artin–Rees, que le cas fini rend inutile.

Pages 84 à 89 : l'inertie. Avant ces trois pages, la cote en contient six autres (46, lot 5, p. 84) qui énoncent une version semi-locale du théorème 90. Soient $\mathcal{O}$ un anneau local, de corps résiduel k, sur lequel Γ opère ; Γ est alors son propre groupe de décomposition Γ_d, et opère sur k. Le groupe d'inertie Γ_i est le noyau de cette action : les γ qui opèrent trivialement sur k. L'action sur A est semi-linéaire, $\gamma(\lambda a) = \gamma(\lambda)\,\gamma(a)$ pour $\lambda \in \mathcal{O}$. La page affirme que la restriction $H^1(\Gamma, A^*) \to H^1(\Gamma_i, A^*)$ est injective. Sa démonstration tord l'action, passe par inflation-restriction à Γ/Γ_i opérant sur A^{Γ_i}, au-dessus de $\mathcal{O}^{\Gamma_i}$, admet (« on sait que ») que Γ/Γ_i opère fidèlement sur le corps résiduel de $\mathcal{O}^{\Gamma_i}$, puis traite le cas $\Gamma_i = \{e\}$: le cas d'un corps (pages 82 et 83), un dévissage le long des $\mathfrak{m}^n A$, et Artin–Rees pour conclure. On démontre ici l'énoncé quand k est infini et que l'ordre de Γ_i est inversible dans k, par une voie plus courte, qui n'a besoin ni de $\mathcal{O}^{\Gamma_i}$, ni du pas admis, ni du dévissage.

Deux outils suffisent. Le premier est l'indépendance des caractères de Dedekind. Les automorphismes de k définis par les éléments de Γ sont deux à deux distincts quand on les regroupe par classes modulo Γ_i. Si $\sum_\sigma a_\sigma\,\sigma(\mu) = 0$ pour tout $\mu \in k$, la somme des a_σ sur chaque classe est donc nulle, en particulier $\sum_{\sigma\in\Gamma_i} a_\sigma = 0$. Avec $a_\sigma = 1$, cela dit que la trace $\mu \mapsto \sum_\sigma \sigma(\mu)$ n'est pas identiquement nulle quand $|\Gamma_i| \neq 0$ dans k. Le second outil est un élément de trace un. Relevons dans $\mathcal{O}$ un μ de trace non nulle en λ_0. La trace $t = \sum_\sigma \sigma(\lambda_0)$ est inversible, puisque sa réduction ne s'annule pas, et invariante, donc $\lambda = \lambda_0 t^{-1}$ vérifie $\sum_\sigma \sigma(\lambda) = 1$. Cet élément remplace le $1/|\Gamma|$ de la moyenne : si $\bar{c}$ et $\bar{c}'$ sont cohomologues modulo $\mathfrak{m}A$, par $\bar{v} = \pi(w)$, la

moyenne

$$u = \sum_{\sigma \in \Gamma} c'(\sigma)\, \sigma(\lambda w)\, c(\sigma)^{-1}$$

vérifie $c'(\gamma)\,\gamma(u) = u\,c(\gamma)$, et sa réduction est $\sum_\sigma \sigma(\lambda)\,\bar{v} = \bar{v}$; elle est donc inversible, et c, c' sont cohomologues dans A^*. Il n'y a ni dévissage ni passage à la limite : le relèvement se fait en une seule moyenne.

Énoncé (D'après les pages 84 à 89, cas local, inertie modérée, corps résiduel infini ♦). *Soient $\mathcal{O}$ un anneau local commutatif, de corps résiduel k infini, Γ un groupe fini qui opère sur $\mathcal{O}$, Γ_i son groupe d'inertie, d'ordre inversible dans k, et A une $\mathcal{O}$-algèbre finie, non nécessairement commutative, munie d'une action semi-linéaire de Γ. Alors $H^1(\Gamma, A^*) \to H^1(\Gamma_i, A^*)$ est injective : deux cocycles cohomologues sur Γ_i le sont sur Γ. En particulier, si Γ opère fidèlement sur k, alors $H^1(\Gamma, A^*) = 1$. Le cas $\mathfrak{m} = 0$ est le théorème 90 pour une algèbre finie quelconque sur un corps infini.*

Démonstration. Soient c et c' deux cocycles, et $u_0 \in A^*$ avec $c(\gamma) = u_0^{-1} c'(\gamma)\,\gamma(u_0)$ pour $\gamma \in \Gamma_i$. Quitte à remplacer c' par $\gamma \mapsto u_0^{-1} c'(\gamma)\,\gamma(u_0)$, on peut supposer $c = c'$ sur Γ_i. Soit $B = A/\mathfrak{m}A$, une k-algèbre de dimension finie, et $\gamma \star x = c'(\gamma)\,\gamma(x)\,c(\gamma)^{-1}$ l'action tordue de Γ sur B. Elle est semi-linéaire sur k et fixe 1 sous Γ_i. Soit X l'ensemble de ses points fixes, les x avec $c'(\gamma)\,\gamma(x) = x\,c(\gamma)$.

Lemme de Speiser. Un élément v fixé par Γ_i est dans le k-sous-espace engendré par X. Sinon, une forme linéaire f s'annule sur X sans s'annuler en v. Pour tout $\mu \in k$, la moyenne $\sum_\sigma \sigma\star(\mu v)$ est dans X, d'où $\sum_\sigma \sigma(\mu)\, f(\sigma \star v) = 0$. Par Dedekind, $\sum_{\sigma \in \Gamma_i} f(\sigma \star v) = |\Gamma_i|\, f(v) = 0$, ce qui est absurde.

Un point fixe inversible. On a donc $1 = \sum_j t_j e_j$, avec des $e_j \in X$ et des $t_j \in k$. Le déterminant de la multiplication à gauche par $\sum_j x_j e_j$ est un polynôme P en les x_j, qui vaut 1 en t. Le corps fixe k^Γ est infini, puisque $[k : k^\Gamma] \le |\Gamma|$ et que k est infini. Le polynôme P ne s'annule donc pas partout sur $(k^\Gamma)^n$. Pour un tel point x, l'élément $\bar{u} = \sum_j x_j e_j$ est inversible et reste dans X, puisque ses coefficients sont invariants. Ainsi $\bar{c}$ et $\bar{c}'$ sont cohomologues dans B^*.

Relèvement. L'élément de trace un λ existe puisque $|\Gamma_i| \neq 0$ dans k, et la moyenne ci-dessus relève la cohomologie de B^* à A^*, puisque $1 + \mathfrak{m}A \subset A^*$ par Nakayama. Si Γ opère fidèlement sur k, alors $\Gamma_i = \{e\}$, et l'hypothèse sur Γ_i est vide. □

La démonstration n'utilise pas la noethérianité, ni une hypothèse de normalité, ni l'anneau $\mathcal{O}^{\Gamma_i}$: le pas que la page admet n'intervient pas dans ce cas. Le corps infini sert au choix d'un point fixe inversible. Pour un corps fini, la page invoque le théorème de Lang. L'ordre de Γ_i inversible sert au lemme de Speiser et à l'élément de trace un. Quand p divise $|\Gamma_i|$, la trace peut être identiquement nulle, et la page passe alors par $\mathcal{O}^{\Gamma_i}$.

Portée de la vérification. Dans `Folder46.lean`, Lean définit l'inertie (`inertia`) et démontre l'indépendance de Dedekind regroupée par fibres (`sum_inertia_eq_zero`, `exists_sum_smul_ne_zero`), le lemme de Speiser tordu (`mem_span_fixed`), le cas d'un corps infini (`isCohomologous_of_eqOn_inertia`), l'élément de trace un et le relèvement (`exists_sum_smul_eq_one`, `isCohomologous_of_map_of_sum_eq_one`), puis l'énoncé encadré (`isCohomologous_of_restrict_inertia`) et le cas d'une action fidèle sur k (`isCohomologous_of_faithful`). Comme plus haut, $A/\mathfrak{m}A$ est remplacé par un morphisme surjectif $\pi : A \to B$ compatible à Γ, de noyau contenu dans $\mathfrak{m}A$, vers une k-algèbre de dimension finie à action semi-linéaire.

La base semi-locale se traite de la même façon, sans complétion. Soient $\mathcal{O}$ un anneau commutatif, Γ un groupe fini qui opère sur $\mathcal{O}$, et $\mathfrak{m}$ un idéal maximal dont les conjugués $\sigma^{-1}(\mathfrak{m}) = \{a \mid \sigma(a) \in \mathfrak{m}\}$ sont tous les idéaux maximaux de $\mathcal{O}$; c'est la transitivité de la page 84, et $\mathcal{O}$ est alors semi-local. On note Γ_d le groupe de décomposition de $\mathfrak{m}$.

Énoncé (D'après les pages 84 à 89, base semi-locale et première flèche ♦). *Soient A une $\mathcal{O}$-algèbre finie, non nécessairement commutative, munie d'une action semi-linéaire de Γ, et $L \in \mathcal{O}$ tel que $\sigma(L) \in \mathfrak{m}$ pour $\sigma \notin \Gamma_d$ et $\sum_{\sigma\in\Gamma} \sigma(L) \equiv 1 \bmod \mathfrak{m}$. Deux cocycles $c, c' : \Gamma \to A^*$ dont les restrictions à Γ_d sont cohomologues modulo $\mathfrak{m}A$, a fortiori dans $A^*_{\mathfrak{m}}$, sont cohomologues dans A^*. Un tel L existe dès qu'il existe $\lambda \in \mathcal{O}$ de trace un modulo $\mathfrak{m}$ pour Γ_d, en particulier quand l'inertie Γ_i est d'ordre inversible dans $k = \mathcal{O}/\mathfrak{m}$. Si de plus k est infini, deux cocycles dont les restrictions à Γ_i sont cohomologues dans $(A/\mathfrak{m}A)^*$ sont cohomologues dans A^* : la composée $H^1(\Gamma, A^*) \to H^1(\Gamma_d, A^*_{\mathfrak{m}}) \to H^1(\Gamma_i, A^*_{\mathfrak{m}})$ est injective.*

Démonstration. Soit $w \in A$, inversible modulo $\mathfrak{m}A$, d'inverse w', avec $c'(\delta)\,\delta(w) \equiv w\,c(\delta)$ modulo $\mathfrak{m}A$ pour $\delta \in \Gamma_d$. La moyenne $u = \sum_{\sigma\in\Gamma} c'(\sigma)\,\sigma(Lw)\,c(\sigma)^{-1}$ vérifie $c'(\gamma)\,\gamma(u) = u\,c(\gamma)$. Modulo $\mathfrak{m}A$, les termes $\sigma \notin \Gamma_d$ disparaissent, puisque $\sigma(L) \in \mathfrak{m}$, et chacun des autres vaut $\sigma(L)\,w$; donc $u \equiv w$, et u est inversible modulo $\mathfrak{m}A$. Par l'invariance tordue, $u = c'(\sigma)\,\sigma(u)\,c(\sigma)^{-1}$, et $c(\sigma)\,\sigma(w')\,c'(\sigma)^{-1}$ est un inverse de u modulo $\sigma(\mathfrak{m})A$, des deux côtés. Un élément de A inversible modulo chacun des idéaux maximaux est inversible : la multiplication par u, à gauche comme à droite, est surjective modulo $\prod_\sigma \sigma(\mathfrak{m})$, contenu dans le radical de Jacobson, donc surjective par Nakayama. Ainsi c et c' sont cohomologues.

Pour construire L, les restes chinois donnent $e \in \mathcal{O}$, $e \equiv 1 \bmod \mathfrak{m}$ et $e \in \sigma^{-1}(\mathfrak{m})$ pour $\sigma \notin \Gamma_d$, puisque ces idéaux maximaux sont distincts de $\mathfrak{m}$; on prend $L = e\lambda$. Quand $|\Gamma_i|$ est inversible dans k, Dedekind donne $\mu \in k$ de trace non nulle pour Γ_d, et λ relève μ divisé par sa trace. Enfin, si k est infini, le cas d'un corps démontré plus haut, appliqué à Γ_d opérant sur $A/\mathfrak{m}A$, rend les restrictions à Γ_d cohomologues modulo $\mathfrak{m}A$ dès qu'elles le sont sur Γ_i. □

La page passe par le complété $\hat{A} = \prod_{\mathfrak{n}} \hat{A}_{\mathfrak{n}}$, où $\hat{A}^*$ est induit de Γ_d, puis redescend par Artin–Rees. L'élément e joue ici le rôle de l'idempotent du facteur $\hat{A}_{\mathfrak{m}}$, et la moyenne sur Γ celui du lemme de Shapiro. Ce lemme lui-même se démontre sans hypothèse sur les ordres : si $A = \prod_{\Gamma/\Gamma_d} \sigma(e)A$ pour un idempotent e dont les conjugués sont centraux et deux à deux orthogonaux quand ils sont distincts, Γ_d le stabilisateur de e, deux cocycles $\Gamma \to A^*$ dont les restrictions à Γ_d sont cohomologues dans $(eA)^*$ sont cohomologues dans A^*, par la moyenne $\sum_{g\Gamma_d} c'(g)\,g(z)\,c(g)^{-1}$ sur les classes, d'inverse $\sum_{g\Gamma_d} c(g)\,g(z^{-1})\,c'(g)^{-1}$.

Portée de la vérification. Dans `Folder46.lean`, Lean démontre le critère d'inversibilité sur une base semi-locale (`surjective_of_forall`, `isUnit_of_forall`), l'énoncé encadré pour un L donné (`isCohomologous_of_semilocal`), la construction de L par les restes chinois et par Dedekind (`exists_trace_one_semilocal`, `exists_trace_one_mod`), le cas modéré à corps résiduel infini (`isCohomologous_of_restrict_inertia_semilocal`) et le lemme de Shapiro pour un produit (`isCohomologous_of_shapiro`). Le groupe de décomposition est un sous-groupe D caractérisé par $\sigma \in D \iff \sigma^{-1}(\mathfrak{m}) = \mathfrak{m}$; le corps résiduel est un corps k muni d'une surjection $\mathcal{O} \to k$ de noyau $\mathfrak{m}$, compatible à D, et $A/\mathfrak{m}A$ est remplacé comme plus haut par un morphisme surjectif vers une k-algèbre de dimension finie, de noyau contenu dans $\mathfrak{m}A$. La localisation $A_{\mathfrak{m}}$ et la complétion n'interviennent pas : l'hypothèse porte sur la réduction modulo $\mathfrak{m}A$, plus faible.

N'est pas démontré ici, de la même cote :

Théorème (Grothendieck, pages 84 à 89, Hilbert 90 semi-local et inertie ; voir aussi Lorenz 1999 ♦). *Soient $\mathcal{O}$ un anneau semi-local noethérien, Γ un groupe fini qui opère fidèlement et transitivement sur ses idéaux maximaux, et A une $\mathcal{O}$-algèbre finie, non nécessairement commutative, munie d'une action semi-linéaire de Γ. Les applications $H^1(\Gamma, A^*) \to H^1(\Gamma_d, A^*_{\mathfrak{m}}) \to H^1(\Gamma_i, A^*_{\mathfrak{m}})$ vers les groupes de décomposition et d'inertie sont injectives comme applications d'ensembles pointés, et non seulement de noyau trivial.*

◊ non vérifié en Lean

La finitude de A sur $\mathcal{O}$ est ajoutée par l'édition, et un pas que la page admet (« on sait que ») peut demander une hypothèse de normalité. Lorenz considère ces applications pour un anneau commutatif et n'en donne que le noyau trivial. La seconde flèche est démontrée plus haut quand $\mathcal{O}$ est local, k infini et l'inertie modérée, et la base semi-locale avec la première flèche quand l'inertie est modérée (ou, plus généralement, quand Γ_d a un élément de trace un modulo $\mathfrak{m}$), ainsi que le lemme de Shapiro pour un produit. Restent non formalisés la première flèche dans le cas sauvage (complétion et descente par Artin–Rees), l'inertie sauvage, où la page passe à $\mathcal{O}^{\Gamma_i}$ et admet que Γ/Γ_i opère fidèlement sur son corps résiduel, et le corps résiduel fini (théorème de Lang). Mathlib n'a pas la cohomologie non abélienne $H^1(\Gamma, A^*)$. On se reportera aux notes de Grothendieck (46, lot 5, p. 84).

40 Cote 53 : un monoïde simplifiable est un groupe [43]

La cote 53, *Groupes algébriques : notes manuscrites (s.d.), lettre (1973)*, trente-trois pages, garde des notes pour un cours sur les groupes algébriques : sur un corps aux pages 2 à 15, sur un anneau aux pages 21 à 33 (distributions, comodules, plongements linéaires). Entre les deux, une lettre d'une autre main, de juin 1973, objecte au cours qu'un monoïde affine de type fini ne se plonge pas toujours dans GL_n : le monoïde $\{0, 1\}$ muni de la multiplication en est un exemple. La page 21 s'ouvre sur une « Rectification » : le plongement fermé multiplicatif se fait dans l'espace des matrices M_n, et non dans GL_n (53, lot 2, p. 21) ; à la page 30, le M de la proposition est écrit par-dessus un GL (53, lot 2, p. 30).

La page donne aussitôt la raison. Un monoïde G de présentation finie sur un anneau, « tel que les translations à g. (à dr.) sont » suivi de deux mots illisibles, par exemple un monoïde qui se plonge dans un groupe, serait un groupe ; la fin de la phrase, « objet gr.-pr. », est elle-même incertaine. La lecture modernisée complète les deux mots par « des monomorphismes » et propose une démonstration par le théorème d'Ax–Grothendieck (EGA IV, 10.4.11 [62]). L'énoncé repose donc sur une reconstruction : seul le fac-similé dira si les deux mots sont bien ceux-là. La vérification porte sur sa forme classique, pour les points sur un corps algébriquement clos.

Pourquoi un monoïde fermé de GL_n serait un groupe. Dans un groupe, on simplifie : $ax = ay$ entraîne $x = y$. Un sous-monoïde S de GL_n hérite de cette propriété, et la multiplication à gauche par $a \in S$ est une application injective de S dans lui-même. Si S était fini, une injection d'un ensemble fini dans lui-même serait une bijection, il existerait $b \in S$ avec $ab = 1$, et S serait un groupe. Pour un ensemble infini, l'argument tombe : dans $\mathbb{C}^*$, le sous-monoïde $\{1, 2, 4, 8, \ldots\}$ est simplifiable et n'est pas un groupe : la multiplication par 2 y est injective sans être surjective. Mais ce sous-monoïde n'est pas une variété : il n'est défini par aucun système d'équations polynomiales.

Le théorème d'Ax–Grothendieck. Sur un corps algébriquement clos K, une application polynomiale injective d'une variété affine dans elle-même est surjective [9, 19]. L'idée d'Ax est de se ramener au cas fini. Une application polynomiale ne fait intervenir qu'un nombre fini

43. Preuve vérifiée : `lean/Grothendieck/Folder53.lean`.

de coefficients. Sur la clôture algébrique de $\mathbb{F}_p$, ces coefficients vivent dans un corps fini $\mathbb{F}_q$, et la clôture est la réunion des $\mathbb{F}_{q^r}$: sur chacun, l'application envoie un ensemble fini dans lui-même, injectivement, donc surjectivement, et tout point de la variété est atteint. Le passage aux autres corps algébriquement clos, en caractéristique nulle en particulier, se fait par la logique : « injective entraîne surjective » s'écrit, à degrés bornés, comme un énoncé du premier ordre, vrai dans tous les corps algébriquement clos de caractéristique p pour p assez grand, donc dans ceux de caractéristique nulle. L'hypothèse « algébriquement clos » est nécessaire : sur $\mathbb{Q}$, $x \mapsto x^3$ est injective et ne prend pas la valeur 2. Mathlib contient ce théorème, démontré par la théorie des modèles, sous la forme `MvPolynomial.ax_grothendieck_zeroLocus` : pour le lieu des zéros $S \subset K^\iota$ d'un idéal de polynômes et une application polynomiale $S \to S$ injective, elle est surjective sur S.

Le cadre. Un monoïde de points d'une variété affine, à loi polynomiale, est un monoïde M muni d'une application injective $\varphi : M \to K^\iota$, ι fini, dont l'image est le lieu des zéros d'un idéal de $K[X_i]$, et de polynômes m_i en deux jeux de variables tels que $\varphi(xy) = m(\varphi(x), \varphi(y))$. La translation à gauche par x est alors, dans les coordonnées, l'application polynomiale $v \mapsto m(\varphi(x), v)$. On dit que M est simplifiable à gauche si $xy = xz$ entraîne $y = z$.

Énoncé (D'après la page 21, forme reconstituée par l'édition, sur les points ♦)**.** *Soient K un corps algébriquement clos et M un monoïde de points d'une variété affine sur K, à loi polynomiale. Si M est simplifiable à gauche, tout élément de M est inversible : M est un groupe.*

Démonstration. Soit $x \in M$. La translation $y \mapsto xy$ est injective, puisque M est simplifiable. Lue dans les coordonnées, c'est l'application polynomiale $v \mapsto m(\varphi(x), v)$ du lieu des zéros $\varphi(M)$ dans lui-même, injective sur ce lieu puisque φ l'est. Par Ax–Grothendieck, elle est surjective, et $\varphi(1)$ est atteint : il existe y avec $\varphi(xy) = \varphi(1)$, donc $xy = 1$. Alors $x(yx) = (xy)x = x = x \cdot 1$, et la simplification donne $yx = 1$. L'élément y est un inverse de x des deux côtés. □

Énoncé (D'après la page 21, sous-monoïdes fermés de GL_n)**.** *Sur un corps algébriquement clos K, un sous-monoïde de $\mathrm{GL}_n(K)$ fermé dans GL_n, c'est-à-dire défini par des équations polynomiales en les coefficients de la matrice et en l'inverse de son déterminant, est un sous-groupe.*

Démonstration. On repère une matrice inversible A par ses n^2 coefficients et par $t = \det(A)^{-1}$: GL_n devient le lieu des zéros de $t\det(A) - 1$ dans K^{n^2+1}, et le sous-monoïde S le lieu des zéros de ses équations et de celle-ci. La loi $(A, t)(B, s) = (AB, ts)$ est polynomiale, et S est simplifiable, comme partie d'un groupe. L'énoncé précédent donne, pour $A \in S$, un $B \in S$ avec $AB = 1$, c'est-à-dire $A^{-1} = B \in S$. □

Remarque. La démonstration n'utilise que la simplification à gauche, là où la page suppose les translations à gauche et à droite injectives. Le passage de $xy = 1$ à $yx = 1$ est un argument de monoïde, sans géométrie. Un sous-monoïde fermé de M_n contenu dans GL_n est fermé dans GL_n ; c'est un cas particulier du second énoncé. Un sous-monoïde fermé de M_n qui contient une matrice non inversible, comme $\{0, 1\}$, n'est évidemment pas un groupe : c'est pourquoi le cours doit plonger les monoïdes dans M_n.

Remarque. L'énoncé est classique. Brion [24, § 2.2, prop. 3] démontre par le même argument (une translation injective est surjective, par le théorème C d'Ax) qu'un élément d'un monoïde

algébrique qui a un inverse à gauche est inversible, et que si 1 est le seul idempotent, le monoïde est un groupe. Un monoïde simplifiable n'a pas d'autre idempotent que 1, car $e^2 = e = e \cdot 1$ donne $e = 1$; l'énoncé encadré en découle. Pour les monoïdes algébriques linéaires, le livre de Putcha [109] est la référence que Brion cite ; il n'a pas été relu ici. La fiche de la piste reste « non cherchée » pour la forme sur un anneau, avec des monomorphismes de schémas.

Portée de la vérification. Lean formalise un monoïde de points à loi polynomiale par les données (φ, I, m) ci-dessus et démontre les deux énoncés (`isUnit_of_isLeftCancelMul` et `inv_mem_of_isClosed`) par `ax_grothendieck_zeroLocus` ; les translations y sont écrites comme polynômes par substitution (`translation`, `eval_translation`). La forme de la page n'est pas formalisée : un schéma en monoïdes de présentation finie sur un anneau quelconque, des translations qui sont des monomorphismes de schémas, et la surjectivité des endomorphismes radiciels d'EGA IV, 10.4.11, qui la démontrerait. Mathlib n'a pas les schémas en monoïdes. Le plongement dans M_n de la page 30 n'est pas formalisé non plus.

Le critère d'irréductibilité géométrique de la page 9. La page 9 porte un « Rectificatif sur critère d'irréductibilité géom. » (53, lot 1, p. 9). La page n'écrit pas « X irréductible » ; sa démonstration l'utilise (« $p(X'_i) = X$ ») et la lecture l'ajoute, car sans cette hypothèse l'énoncé est faux (deux droites disjointes et un point de l'une). Sous la forme corrigée par l'édition, l'énoncé est le suivant.

Théorème (Page 9, forme corrigée par l'édition, critère d'irréductibilité géométrique ♦). *Soit X un schéma irréductible sur un corps k. Si un k-schéma géométriquement irréductible Z s'envoie dans X avec une image non contenue dans l'ensemble des points où passent plusieurs composantes irréductibles de $X_{\bar{k}}$, alors X est géométriquement irréductible ; un point géométriquement normal de X_{red} dans l'image suffit. Sans la seconde hypothèse, $x^2 + y^2 = 0$ sur $\mathbf{R}$, avec pour Z l'origine, est un contre-exemple.*

◊ non vérifié en Lean

La démonstration de la page se lit ainsi. Soient k' une extension finie galoisienne de k, de groupe G, $p : X' = X_{k'} \to X$ et $f' : Z' = Z_{k'} \to X'$. L'image $f'(Z')$ est irréductible, puisque Z' l'est, et stable par G, puisque f' est défini sur k. Elle est contenue dans une composante irréductible X'_i de X'. Chaque conjuguée gX'_i est encore une composante et contient $f'(Z')$; par l'hypothèse b), un point de $f'(Z')$ n'est que sur une composante, donc $gX'_i = X'_i$. Comme G agit transitivement sur les fibres de p, la composante X'_i est l'image réciproque de $p(X'_i)$, et $p(X'_i) = X$; donc $X' = X'_i$ est irréductible. Le passage de k' à $\bar{k}$ se fait par une extension radicielle, qui ne change pas la topologie.

Tout le cœur de l'argument est topologique, et c'est cette étape que Lean vérifie, dans une généralité qui ne mentionne plus de corps.

Énoncé (D'après la page 9, l'étape galoisienne, sous forme topologique). *Soient X' et X des espaces sobres, X irréductible, et $p : X' \to X$ une application fermée qui relève les générisations. Soit G un groupe opérant sur X' par homéomorphismes, transitivement sur chaque fibre de p. Si une partie irréductible S de X', stable par G, contient un point par lequel ne passe qu'une composante irréductible de X', alors X' est irréductible.*

Démonstration. Soit C une composante irréductible de X' contenant S, et $s \in S$ le point de l'hypothèse. Pour $g \in G$, gC est une composante, car $x \mapsto gx$ est un homéomorphisme ; elle contient $gS = S$, donc s, et l'unicité donne $gC = C$. Si $p(y) = p(x)$ avec $x \in C$, il existe g avec $y = gx \in gC = C$: la composante C est saturée pour p. Reste à voir que $p(C) = X$. Soient

c le point générique de C et η celui de X. Comme η se spécialise en $p(c)$ et que p relève les générisations, il existe x qui se spécialise en c avec $p(x) = \eta$. L'adhérence de x est irréductible et contient C, donc lui est égale par maximalité, et $x \in C$. Ainsi $p(C)$ est un fermé qui contient le point générique de X : c'est X. Comme C est saturée, $C = p^{-1}(p(C)) = X'$. □

Dans l'application, X' est $X_{k'}$ et p le morphisme de changement de base : il est fini, donc fermé, et plat, donc il relève les générisations ; les schémas sont sobres, et $\mathrm{Gal}(k'/k)$ opère transitivement sur les fibres. La page justifie $p(X'_i) = X$ par « p ouvert et fermé » ; la démonstration ci-dessus remplace l'ouverture par le relèvement des générisations, plus commode à formaliser et vrai ici par platitude.

Le contre-exemple. Sur $\mathbf{R}$, l'anneau $A = \mathbf{R}[x,y]/(x^2+y^2)$ est intègre : le morphisme $\mathbf{R}[x,y] \to \mathbf{C}[t]$, $x \mapsto t$, $y \mapsto it$, a pour noyau exactement (x^2+y^2). En effet, $y^2 + x^2$ est unitaire en y ; un polynôme du noyau a pour reste $a(x) + b(x)\,y$, qui s'envoie sur $a(t) + i\,t\,b(t)$; pour t réel, parties réelle et imaginaire donnent $a(t) = 0$ et $t\,b(t) = 0$, d'où $a = b = 0$. Le noyau d'un morphisme vers un anneau intègre est premier, et $X = \operatorname{Spec} A$ est irréductible. Sur $\mathbf{C}$, en revanche, $x^2+y^2 = (x+iy)(x-iy)$, et aucun des deux facteurs n'est nilpotent modulo x^2+y^2 : l'évaluation en $(1,-i)$, point du cône, envoie $x+iy$ sur 2, et l'évaluation en $(1,i)$ envoie $x-iy$ sur 2. Le nilradical n'est donc pas premier, et $\operatorname{Spec} \mathbf{C}[x,y]/(x^2+y^2)$ n'est pas irréductible : ce sont les deux droites $x = \pm iy$. Le point $Z = \operatorname{Spec} \mathbf{R}$ s'envoie sur l'origine, où elles se coupent : l'hypothèse b) y est en défaut.

Au niveau des schémas, le contre-exemple s'énonce avec la définition de Mathlib : un morphisme $X \to S$ est géométriquement irréductible si, pour tout corps K et tout $\operatorname{Spec} K \to S$, le produit fibré $X \times_S \operatorname{Spec} K$ est irréductible.

Énoncé (Page 9, le contre-exemple au niveau des schémas)**.** *On a un isomorphisme de* $\mathbf{C}$*-algèbres* $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[x,y]/(x^2+y^2) \simeq \mathbf{C}[x,y]/(x^2+y^2)$*. Le schéma* $X = \operatorname{Spec} \mathbf{R}[x,y]/(x^2+y^2)$ *est intègre, et il n'est pas géométriquement irréductible sur* $\mathbf{R}$*.*

Démonstration. L'application $z \otimes f \mapsto zf$ de $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[x,y]$ dans $\mathbf{C}[x,y]$ et l'application $\mathbf{C}$-linéaire $\mathbf{C}[x,y] \to \mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[x,y]$ qui envoie x sur $1 \otimes x$ et y sur $1 \otimes y$ sont des morphismes d'algèbres inverses l'un de l'autre : il suffit de le vérifier sur x, y et sur $\mathbf{C}$. Le produit tensoriel par $\mathbf{C}$ commute au passage au quotient : $\mathbf{C} \otimes_{\mathbf{R}} (\mathbf{R}[x,y]/I)$ est le quotient de $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[x,y]$ par l'idéal engendré par $1 \otimes I$, et l'isomorphisme précédent envoie $1 \otimes (x^2+y^2)$ sur x^2+y^2. L'anneau A est intègre (ci-dessus), donc X est intègre. Si X était géométriquement irréductible, la fibre de $X \to \operatorname{Spec} \mathbf{R}$ au-dessus de $\operatorname{Spec} \mathbf{C}$ serait irréductible ; c'est $\operatorname{Spec}(A \otimes_{\mathbf{R}} \mathbf{C})$, homéomorphe à $\operatorname{Spec} \mathbf{C}[x,y]/(x^2+y^2)$, qui ne l'est pas. □

Portée de la vérification. Lean démontre l'étape galoisienne (`irreducibleSpace_of_stable`, et `irreducibleSpace_of_map`, où S est l'image d'un espace irréductible Z'), avec le lemme `smul_mem_irreducibleComponents`, et le contre-exemple au niveau des anneaux (`isPrime_span_sumSq_real` par `ker_toLines`, et `not_irreducibleSpace_complex`). L'énoncé encadré de la page reste marqué non vérifié : Mathlib a désormais l'irréductibilité géométrique des schémas (`AlgebraicGeometry.GeometricallyIrreducible`), mais il manque, pour en déduire l'énoncé, l'action de $\mathrm{Gal}(k'/k)$ sur $X_{k'}$ et sa transitivité sur les fibres, le passage de toutes les extensions K de k aux extensions finies galoisiennes et l'étape radicielle. Le contre-exemple, lui, est démontré au niveau des schémas : l'isomorphisme $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[x][y] \simeq \mathbf{C}[x][y]$ (`baseChangeEquiv`, construit par `baseChangeHom` et

`baseChangeInv`), puis $\mathbf{C} \otimes_{\mathbf{R}} A \simeq \mathbf{C}[x,y]/(x^2+y^2)$ (`tensorQuotSumSqEquiv`, par `Algebra.TensorProduct.tensorQuotientEquiv`, `Ideal.quotientEquivAlg` et `baseChangeEquiv_tmul_sumSq`) ; l'intégrité de X (`isIntegral_spec_sumSq`) et l'absence d'irréductibilité géométrique (`not_geometricallyIrreducible_sumSq`, par `pullbackSpecIso` et `PrimeSpectrum.homeomorphOfRingEquiv`), réunies dans `isIntegral_and_not_geometricallyIrreducible_sumSq`, avec la définition `AlgebraicGeometry.GeometricallyIrreducible` de Mathlib. N'est pas formalisée la condition suffisante par un point géométriquement normal de X_{red}.

41 Cote 78 : le critère de fermeture $u_\alpha^n = 1$ sur un anneau, et les $2p$-gones en bande [44]

La cote 78, *[Polygones réguliers et polynômes cyclotomiques] : notes manuscrites (s.d.)*, que l'inventaire date « [à partir de 1977] », compte cent vingt-neuf pages. Elle cherche une définition du polygone régulier dans un plan affine sur un corps, ou un anneau, quelconque, sans longueurs ni angles : un n-gone dont chaque automorphisme combinatoire se prolonge d'une seule façon en une affinité. Dans le repère (s_0, s_1, s_{-1}) de trois sommets consécutifs, les pages 81 à 85 ramènent un tel polygone, quand il est « propre », à un seul paramètre α, l'invariant numérique, et la rotation s'écrit $u_\alpha(x,y) = (1 - y + \alpha x, x)$ (78, lot 5, p. 81). Les pages 109 à 113, sous le titre « Polynômes cyclotomiques », définissent des polynômes $F_n \in \mathbb{Z}[U]$, prouvent une identité entre trois produits consécutifs, écrivent les sommets et la matrice de u^n en fonction de α seul et énoncent, « soient k un anneau », que $u_\alpha^n = 1$ si et seulement si $F_n(\alpha) = 0$ (78, lot 6, p. 109, 78, lot 6, p. 111, 78, lot 6, p. 112). La page 112 conclut « la relation $F_n(\alpha) = 1$ » et le premier coefficient de Bézout de la page 113 a un indice douteux ; la lecture modernisée lit $F_n(\alpha) = 0$ et corrige le coefficient. Les pages 84 et 85, puis 94 à 99, décrivent deux polygones de caractéristique p dont les sommets sont alternativement sur deux droites parallèles : l'« impropre », et celui d'invariant $\alpha = -2$ (78, lot 5, p. 85, 78, lot 5, p. 95, 78, lot 5, p. 99).

Conventions. k est un anneau commutatif, $\alpha \in k$, et $S_m \in \mathbb{Z}[U]$, $m \in \mathbb{Z}$, les polynômes de Tchebychev de seconde espèce renormalisés : $S_0 = 1$, $S_1 = U$, $S_{m+1} = US_m - S_{m-1}$, de sorte que $S_{-1} = 0$. On pose

$$F_{2m} = S_{m-1}, \qquad F_{2m+1} = S_m + S_{m-1} \qquad (m \in \mathbb{Z}),$$

d'où $F_0 = 0$, $F_1 = F_2 = 1$, $F_3 = U + 1$, $F_4 = U$, $F_5 = U^2 + U - 1$, $F_6 = U^2 - 1$. On note u_α la bijection $(x,y) \mapsto (1 - y + \alpha x, x)$ de k^2, d'inverse $(x,y) \mapsto (y, 1 - x + \alpha y)$, $s_n = u_\alpha^n(0,0)$ pour $n \in \mathbb{Z}$, et $\sigma_1(x,y) = (y,x)$.

Énoncé (Page 109, les polynômes F_n)**.** *Les F_n sont ceux de la page : $F_{-n} = -F_n$ et, pour tout $t \in k$ inversible d'inverse t' et tout entier $m \geq 0$,*

$$F_{2m+2}(t+t')\,(t^2-1)\,t^m = t^{2m+2} - 1, \qquad F_{2m+1}(t+t')\,(t-1)\,t^m = t^{2m+1} - 1.$$

Démonstration. L'égalité $F_{-n} = -F_n$ se lit sur $S_{-m-2} = -S_m$. Dans chaque classe de parité, la récurrence de S donne $F_{n+4} = UF_{n+2} - F_n$. Les deux formules se vérifient pour $m = 0$ et $m = 1$; si A_m désigne le membre de gauche de l'une d'elles, la récurrence donne $A_{m+2} = (t+t')\,t\,A_{m+1} - t^2 A_m$, et $(t^2 + tt')(t^{j+2} - 1) - t^2(t^j - 1) = t^{j+4} - 1 + (tt' - 1)(t^{j+2} - 1)$. □

44. Preuve vérifiée : `lean/Grothendieck/Folder78.lean`.

Théorème 41.1 (Grothendieck, pages 109 à 113, le critère de fermeture sur un anneau ♦)**.**

1. *Pour tout $n \in \mathbb{Z}$, on a dans $\mathbb{Z}[U]$*

$$F_n F_{n+1} - U F_{n-1} F_n + F_{n-2} F_{n-1} = 1,$$

c'est-à-dire $A_n F_{n-1} + F_n F_{n+1} = 1$ avec $A_n = F_{n-2} - U F_n$; en particulier F_{n-1} et F_{n+1} sont étrangers.

2. *Pour tout $n \in \mathbb{Z}$ et tout $(x, y) \in k^2$, avec $X_n = F_n F_{n+1}(\alpha)$,*

$$u_\alpha^n(x, y) = (1 - x - y)\, s_n + x\, s_{n+1} + y\, s_{n-1},$$

où $s_n = (X_n, X_{n-1}) = \big(F_n F_{n+1}(\alpha), F_{n-1} F_n(\alpha)\big)$.

3. *Pour $n \in \mathbb{Z}$, les conditions suivantes sont équivalentes : a) $u_\alpha^n = \mathrm{id}$; b) $s_n = s_0$; c) $u_\alpha^n(s_i) = s_i$, pour un $i \in \mathbb{Z}$ donné ; d) $F_n(\alpha) = 0$.*

Démonstration. 1) Si $n = 2m$, les quatre polynômes sont S_{m-1}, $S_m + S_{m-1}$, $S_{m-1} + S_{m-2}$ et S_{m-2} ; en remplaçant S_m par $U S_{m-1} - S_{m-2}$, le membre de gauche devient $S_{m-1}^2 - U S_{m-1} S_{m-2} + S_{m-2}^2$. Si $n = 2m + 1$, il devient de même $S_m^2 - U S_m S_{m-1} + S_{m-1}^2$. Or $Q_m = S_m^2 - U S_m S_{m-1} + S_{m-1}^2$ ne dépend pas de m : $Q_{m+1} = S_{m+1}(S_{m+1} - U S_m) + S_m^2 = -S_{m+1} S_{m-1} + S_m^2 = Q_m$, et $Q_0 = 1$. C'est l'identité de Cassini des S_m. La relation de Bézout n'en est qu'une réécriture.

2) L'identité au rang $n+1$, évaluée en α, donne $X_{n+1} = \alpha X_n - X_{n-1} + 1$ pour tout n. Notons $V_n(x, y)$ le membre de droite. On a $V_0(x, y) = (x, y)$, puisque $X_0 = X_{-1} = 0$ et $X_1 = X_{-2} = 1$. La récurrence donne $u_\alpha \circ V_n = V_{n+1}$: la seconde coordonnée de $u_\alpha(V_n(x, y))$ est la première de $V_n(x, y)$, et la première est $1 - (\text{seconde}) + \alpha\,(\text{première})$, où l'on remplace chacun des trois termes $1 - X_{j-1} + \alpha X_j$ par X_{j+1}, pour $j = n$, $n+1$, $n-1$, les poids $1 - x - y$, x, y ayant pour somme 1. On conclut par récurrence vers le haut et, comme u_α est bijective, vers le bas.

3) a) $\Rightarrow$ b) est clair. d) $\Rightarrow$ a) : si $F_n(\alpha) = 0$, alors $X_n = X_{n-1} = 0$, puis $X_{n+1} = 1$ et $X_{n-2} = 1$ par la récurrence, et la formule de 2) se réduit à $u_\alpha^n(x, y) = (x, y)$. b) $\Rightarrow$ d) : si $F_n F_{n+1}(\alpha) = F_{n-1} F_n(\alpha) = 0$, on multiplie l'identité évaluée en α par $F_n(\alpha)$:

$$F_n(\alpha) = F_n(\alpha) \cdot F_n F_{n+1}(\alpha) + \big(F_{n-2}(\alpha) - \alpha F_n(\alpha)\big) \cdot F_{n-1} F_n(\alpha) = 0.$$

c) $\Leftrightarrow$ b) : u_α^n et u_α^i commutent, donc $u_\alpha^n(s_i) = u_\alpha^i(s_n)$, et u_α^i est injective. □

Remarque. Le théorème tient tel que la lecture l'énonce, sur tout anneau commutatif et pour tout $n \in \mathbb{Z}$, diviseurs de zéro compris : la réciproque passe par la relation de Bézout et non par une factorisation. Les colonnes de la formule 2) sont $s_{n+1} - s_n$, $s_{n-1} - s_n$ et s_n, soit $\big(F_{n+1}(F_{n+2} - F_n), F_n(F_{n+1} - F_{n-1})\big)$, $\big(F_n(F_{n-1} - F_{n+1}), F_{n-1}(F_{n-2} - F_n)\big)$ et $(F_n F_{n+1}, F_{n-1} F_n)$: c'est la première version de la matrice de la page 111, celle qui est barrée, que la lecture retient. La suite X_n vérifie une récurrence linéaire d'ordre deux avec second membre, et, avec la suite de Lucas $U_m = U_m(\alpha, 1)$ ($U_0 = 0$, $U_1 = 1$, $U_{m+1} = \alpha U_m - U_{m-1}$) [91], on a $F_{2m}(\alpha) = U_m$ et $F_{2m+1}(\alpha) = U_{m+1} + U_m$; la piste demande si l'équivalence sur un anneau quelconque y figure déjà, sous un autre nom. Le fichier vérifie aussi que $\sigma_1 u_\alpha \sigma_1 = u_\alpha^{-1}$ et $\sigma_1(s_n) = s_{-n}$, de sorte que u_α et σ_1 font opérer le groupe diédral sur les sommets, et que la forme $f_\alpha(x, y) = x^2 - x + y^2 - y - \alpha x y$ de la page 96 est invariante par u_α et nulle en tous les sommets. Enfin une affinité de k^2 est déterminée par ses valeurs en $s_0 = (0, 0)$, $s_1 = (1, 0)$ et $s_{-1} = (0, 1)$: un automorphisme du polygone combinatoire se prolonge au plus d'une façon.

Contre-exemple 41.2 (Page 113, le coefficient de la page). *Le couple $A_n = F_{n-2} - UF_{n-1}$, $B_n = F_n$ ne vérifie pas $A_nF_{n-1} + B_nF_{n+1} = 1$ pour $n = 4$.*

Démonstration. Pour $n = 4$, $(1 - U(U + 1))(U + 1) + U(U^2 + U - 1) = 1 - U - U^2$, qui vaut -1 en $U = 1$. □

Les deux polygones en bande. Pour $\alpha = -2$, $u_{-2}(x, y) = (1 - y - 2x, x)$; le polygone impropre de la page 85 a pour rotation $v(x, y) = (1 - y, -x)$, et l'on pose $t_n = v^n(0, 0)$. Une *caractéristique* p est un entier $p \geq 0$ tel que, pour $m \in \mathbb{Z}$, l'image de m dans k soit nulle si et seulement si p divise m ; on suppose k non nul.

Énoncé (Pages 84, 85 et 94 à 99, existence des $2p$-gones en bande ♦). *Soit k un anneau non nul de caractéristique p.*

1. *Pour $m \in \mathbb{Z}$, $s_{2m} = (-m, m)$ et $s_{2m+1} = (1 + m, -m)$: les sommets pairs sont sur la droite $x + y = 0$, les impairs sur la droite parallèle $x + y = 1$ (figure 3), et $f_{-2}(x, y) = (x + y)(x + y - 1)$.*
2. *$u_{-2}^n = \mathrm{id}$ si et seulement si $2p$ divise n, ce qui équivaut à $F_n(-2) = 0$; u_{-2} est d'ordre $2p$, et $s_n = s_m$ si et seulement si $2p$ divise $n - m$.*
3. *Trois sommets consécutifs ne sont jamais alignés : le déterminant de $(s_{n+1} - s_n, s_{n-1} - s_n)$ vaut 1. La partie linéaire $(x, y) \mapsto (-2x - y, x)$ est de déterminant 1.*
4. *Pour le polygone impropre, v^{2m} est la translation de vecteur $m\,(1, -1)$, $t_{2m} = (m, -m)$ et $t_{2m+1} = (m + 1, -m)$, sur les deux mêmes droites ; $v^n = \mathrm{id}$ si et seulement si $2p$ divise n, v est d'ordre $2p$, $t_n = t_m$ si et seulement si $2p$ divise $n - m$, trois sommets consécutifs ne sont pas alignés (déterminant ± 1), $\sigma_1 v \sigma_1 = v^{-1}$, et la partie linéaire $(x, y) \mapsto (-y, -x)$ est de déterminant -1.*

Démonstration. 1) Par récurrence sur m dans les deux sens : $u_{-2}(-m, m) = (1 + m, -m)$ et $u_{-2}(1 + m, -m) = (-(m + 1), m + 1)$. La factorisation de f_{-2} est immédiate.

2) Par 1), $s_{2m} = (0, 0)$ équivaut à $m = 0$ dans k, c'est-à-dire à $p \mid m$, ou encore à $2p \mid 2m$; et $s_{2m+1} = (0, 0)$ imposerait $m = 0$ et $1 + m = 0$, donc $1 = 0$. Le théorème ci-dessus (b ⇔ a ⇔ d) donne $u_{-2}^n = \mathrm{id} \iff 2p \mid n \iff F_n(-2) = 0$, d'où l'ordre. Enfin $s_n = s_m$ équivaut à $u_{-2}^{n-m}(s_m) = s_m$, donc à $2p \mid n - m$ par la condition c).

3) Pour $n = 2m$, les deux vecteurs sont $(1 + 2m, -2m)$ et $(2m, 1 - 2m)$, de déterminant $1 - 4m^2 + 4m^2 = 1$; le cas impair est analogue.

4) $v(1 - y + m, -x - m) = (x + m + 1, y - m - 1)$ et $v(x + m, y - m) = (1 - y + m, -x - m)$ donnent par récurrence $v^{2m}(x, y) = (x + m, y - m)$ et $v^{2m+1}(x, y) = (1 - y + m, -x - m)$. Les sommets s'en déduisent, et l'on raisonne comme en 2) : $t_{2m} = (0, 0)$ si et seulement si $p \mid m$, $t_{2m+1} \neq (0, 0)$, et v^{2m} est l'identité dès que $m = 0$ dans k. Les déterminants se calculent sur les sommets : les vecteurs sont $(1, 0)$ et $(0, 1)$ en un sommet pair, $(0, -1)$ et $(-1, 0)$ en un sommet impair. □

Le polygone d'invariant $\alpha = -2$, dessiné sur $\mathbf{Q}$ dans les coordonnées $(x - y,\ x + y)$: les sommets pairs sur la droite $x + y = 0$, les impairs sur $x + y = 1$, de s_{-2} à s_5. Sur $\mathbf{Q}$ il ne se referme pas ; en caractéristique p, $s_{n+2p} = s_n$ et c'est un $2p$-gone.

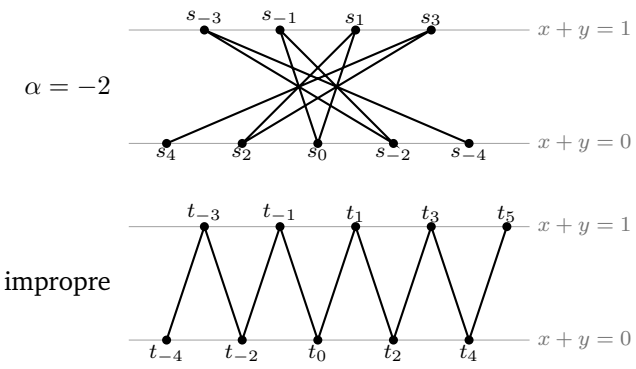
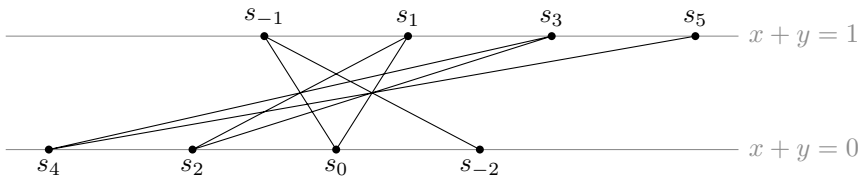


FIGURE 3 – Les deux polygones en bande de l'énoncé, sur $\mathbf{Z}$, dans les coordonnées $(x-y,\ x+y)$ du repère (s_0, s_1, s_{-1}), où les deux droites sont horizontales. En haut, $s_n = u_{-2}^n(0,0)$: $s_{2m} = (-m, m)$ et $s_{2m+1} = (1+m, -m)$ vont et viennent de part et d'autre de s_0, les pairs sur $x+y=0$, les impairs sur $x+y=1$. En bas, le polygone impropre $t_n = v^n(0,0)$ avance en zigzag d'un seul côté, sur les deux mêmes droites. En caractéristique p, les deux suites sont périodiques de période $2p$ et l'on obtient un $2p$-gone dans la bande. Figure de l'édition ; Grothendieck dessine à la page 95 les axes, la droite D de direction a et les points s_0, $-s_0$ (78, lot 5, p. 95).



Remarque. L'existence tient en toute caractéristique, sans supposer p premier ni impair. Pour $p=2$, $\alpha = -2 = 0$ et l'on retrouve le carré, d'ordre $4 = 2p$, comme le note la lecture ; pour $p=0$, les deux rotations sont d'ordre infini et les sommets forment les deux ∞-polygones en escalier de la page 85. Le déterminant -1 ne sépare le polygone impropre des polygones unimodulaires que si $2 \neq 0$, c'est-à-dire pour p impair. Les formules 1) et 4) montrent que les deux polygones ont le même ensemble de sommets : $s_{2m+1} = t_{2m+1}$ et $s_{2m} = t_{-2m}$. Le premier zigzague en parcourant les deux droites en sens contraires, $(0,0)$, $(1,0)$, $(-1,1)$, $(2,-1)$, et ainsi de suite ; le second monte en escalier en les parcourant dans le même sens, $(0,0)$, $(1,0)$, $(1,-1)$, $(2,-1)$, et ainsi de suite. Ils ne diffèrent que par l'ordre des sommets et par le déterminant de la rotation.

Ne sont pas démontrés ici : l'énoncé de la piste selon lequel le $2p$-gone impropre est le seul polygone régulier fini non unimodulaire, que la lecture ajoute et qui demande la classification des réalisations régulières ; la proposition de la page 83, qui met les réalisations épinglées en bijection avec les couples (α, β) vérifiant $\alpha\beta = 0$ et $\beta(\beta+2) = 0$; la factorisation $F_n = \prod_{d|n,\, d\geq 3} \Psi_d$ et le polynôme semi-cyclotomique Ψ_n des pages 114 à 120, avec la réduction $\Psi_p \equiv (U-2)^{(p-1)/2}$ modulo p ; le p-gone de la parabole (pages 95 et 100), dont la piste est retrouvée dans la littérature ; les gerbes et la descente des pages 39 à 48.

42 Cote 64 : la configuration octaédrale en caractéristique 5 [45]

La cote 64, *Modules courbes elliptiques en caractéristiques $\neq 2$: notes manuscrites (s.d.)*, cent cinquante-six pages que l'inventaire date « [à partir de 1980-1982] », consacre sa partie II

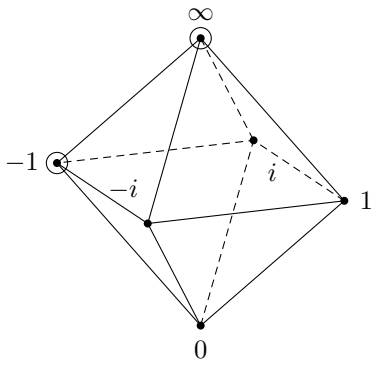
45. Preuve vérifiée : `lean/Grothendieck/Folder64.lean`.

aux structures octaédrales dans $\mathbf{P}^1$ (pages 43 à 52, 64, lot 3, p. 44). Une action fidèle du groupe de Klein se met localement sous la forme $\sigma_1(z) = -z$, $\sigma_2(z) = 1/z$, et la somme des axes est la configuration octaédrale $\Delta = \{0, \infty, \pm 1, \pm i\}$. Pour identifier $\mathrm{Aut}(X, \Delta)$ au groupe des rotations de l'octaèdre, la page 48 calcule le fixateur de deux sommets non opposés, ∞ et -1 : un tel automorphisme s'écrit $z \mapsto az + (a-1)$, et s'il n'est pas l'identité il permute $\{0, 1, i, -i\}$. Les quatre conditions sur a qui en résultent ont, dit la page, une intersection vide hors des caractéristiques 2 et 5. La marge borne le calcul par « car. $\neq 3$ et 5 », et la lecture ajoute l'hypothèse « 5 inversible » partout où elle sert.

Théorème 42.1 (Grothendieck, page 48)**.** *Soit K un corps où $2 \neq 0$, et $i \in K$ avec $i^2 = -1$. Si $z \mapsto az + (a-1)$ envoie $\{0, 1, i, -i\}$ dans lui-même, alors $5(a-1) = 0$. En particulier, si $5 \neq 0$ dans K, le fixateur de ∞ et -1 dans $\mathrm{Aut}(\mathbf{P}^1_K, \Delta)$ est trivial.*

Démonstration. Les quatre points sont distincts, puisque $2 \neq 0$. Si $a = 0$, l'image de 0 est -1, qui n'est aucun des quatre points. Sinon l'application est injective, donc permute les quatre points, et conserve leur somme, qui vaut 1 ; or elle la change en $a \cdot 1 + 4(a-1) = 5a - 4$. D'où $5(a-1) = 0$. □

Les six points de Δ sont les sommets d'un octaèdre dont les sommets opposés sont 0 et ∞, 1 et -1, i et $-i$. Le fixateur de deux sommets non opposés, ∞ et -1 (cerclés), permute les quatre autres.



Contre-exemple 42.2 (énoncé de l'édition, d'après la note de la lecture à la page 49)**.** *En caractéristique 5, le fixateur de ∞ et -1 n'est pas trivial : $z \mapsto 2z + 1$ permute $\{0, 1, i, -i\}$. Sur $\mathbf{F}_5$, avec $i = 2$, la configuration Δ est $\mathbf{P}^1(\mathbf{F}_5)$ tout entier ; les bijections de $\mathbf{P}^1(\mathbf{F}_5)$ induites par $\mathrm{GL}_2(\mathbf{F}_5)$, qui préservent toutes Δ, sont au nombre de 120 et non de 24, et le fixateur de ∞ et -1 est formé de l'identité et des $z \mapsto az + (a-1)$ pour $a = 2, 3, 4$.*

Démonstration. Comme $i^2 = -1 = 4$, $i = \pm 2$. Pour $i = 2$, l'application $z \mapsto 2z + 1$ envoie $0 \mapsto 1 \mapsto 3 = -i \mapsto 2 = i \mapsto 0$; de même pour $i = -2$. Sur $\mathbf{F}_5$, les six points $\infty, 0, 1, -1, 2, -2$ sont les six points de $\mathbf{P}^1(\mathbf{F}_5)$. Le décompte des bijections induites et du fixateur se fait sur les 625 matrices de $M_2(\mathbf{F}_5)$; Lean le vérifie par calcul (`card_pgl`, `card_fixer`). □

Remarque. La démonstration du théorème 42.1 n'utilise que $2 \neq 0$ et $5 \neq 0$: la caractéristique 3, que la marge exclut, n'a pas à l'être. Le contre-exemple confirme l'hypothèse « 5 inversible » de la lecture : sans elle, $\mathrm{Aut}(X, \Delta)$ est $\mathrm{PGL}_2(\mathbf{F}_5)$, d'ordre 120, et non le groupe des rotations de l'octaèdre, d'ordre 24.

Ne sont pas démontrés ici : la forme normale locale de la page 46, l'égalité $\mathrm{Aut}(X, \Delta) = \mathrm{Aut}^+_{\mathrm{oct}}(\Delta)$ qui suit du théorème, et les énoncés relatifs au-dessus d'une base, qui restent ouverts :

Théorème (Grothendieck, pages 44 à 52, configurations octaédrales sur une base ; voir aussi Beauville [13] ⧫). *Soit X un fibré en droites projectives sur un schéma S de caractéristiques résiduelles différentes de 2. Se correspondent bijectivement : les sous-schémas en groupes de $\mathrm{Aut}_S(X)$ localement isomorphes à $(\mathbf{Z}/2)^2$, ceux localement isomorphes à $\mathfrak{S}_4$, et les configurations octaédrales régulières, diviseurs étales de degré 6 munis d'une antipodie. Les couples (X, Δ) dont le torseur d'orientation est identifié à μ_4^* équivalent aux revêtements étales finis de degré 4 de S.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 46 à 49). Le corollaire 2 n'est pas démontré, et l'hypothèse qui en fait une équivalence est une addition marginale de lecture incertaine. Là où la page identifie $\mathrm{Aut}_S(X, \Delta)$ au groupe des rotations de l'octaèdre, l'édition suppose 5 inversible, hypothèse nécessaire par le contre-exemple 42.2. Beauville traite le cas d'un corps, sans base. Mathlib n'a pas les formes de $\mathbf{P}^1$ sur une base.

Théorème (Grothendieck, pages 74 à 79 et 84 à 91, épinglages de Legendre ; voir aussi Antieau–Meier [3] ⧫). *Sur $\mathbf{Z}[1/2]$, les courbes elliptiques munies d'un épinglage de Jacobi de niveau 2 et d'un épinglage de Legendre (un vecteur tangent à l'origine, tordu par un μ_4-torseur fixé, dont le carré correspond à l'espace tangent de $E/\pm 1$ en l'image de l'origine) forment un groupoïde rigide représenté par $U_{0,3} \times \mu_4^*$. Le groupe $\mu_4 \times \mathfrak{S}_3$ opère sur ce schéma, $\mathfrak{S}_3$ tautologiquement sur $U_{0,3}$ et par la signature sur μ_4^*.*

◊ non vérifié en Lean

La représentabilité est affirmée sans démonstration (page 85). Antieau et Meier (2020, définition 4.4, proposition 4.5 et lemme 4.7 dans la numérotation de arXiv :1608.00851) décrivent, sur $\mathbf{Z}[1/2]$, l'espace de Legendre $X = \mathbf{A}^1 \smallsetminus \{0, 1\}$ comme le C_2-torseur des racines carrées de $p\,\omega^{\otimes 2}$ au-dessus de $\mathcal{M}(2) \simeq BC_{2,X}$, et notent que l'action de $\mathfrak{S}_3$ ne se relève pas strictement à X ; l'épinglage tordu par μ_4^*, qui rend l'action de $\mu_4 \times \mathfrak{S}_3$ stricte sur $U_{0,3} \times \mu_4^*$, n'y figure pas. Le $\mathfrak{S}_3$ qui opère ici sur $U_{0,3}$ est celui des sections 50 et 74. Mathlib n'a pas les espaces de modules de courbes elliptiques. On se reportera aux notes de Grothendieck (64, lot 4, p. 74).

43 Cote 80 : un contre-exemple au théorème des arrangements cruciaux [46]

La cote 80, *Systèmes de pseudo-droites*, n'est pas datée de sa main ; l'inventaire la date « à partir de 1981 », et une notice administrative du 13 mai 1981, à la page 27, appuie cette date. Un arrangement de pseudo-droites est une famille finie de courbes fermées simples du plan projectif réel qui se coupent deux à deux en un seul point ; les droites en sont l'exemple. Les pages 20 à 28 cherchent les arrangements « cruciaux » et leur donnent des noms (80, lot 2, p. 22) : I_N, $\mathrm{I}_{p,q}$ et $\mathrm{II}'_{p,q}$ sont formés de deux faisceaux, c'est-à-dire que deux sommets suffisent pour que chaque pseudo-droite passe par l'un d'eux ; II_4 et II_5 sont quatre et cinq pseudo-droites en position générale, sans trois concourantes ; III_6 est le quadrangle complet, les six droites qui joignent quatre points dont trois ne sont jamais alignés (quatre points triples) ; IV_7 est un quadrilatère complet et ses trois diagonales. La page 24 énonce (80, lot 2, p. 24) :

> *Théorème : supposons qu'il n'existe pas deux sommets tels que les ps. droites passent par l'un d'eux [...]. Supposons de plus que K ne contienne pas de sous-arrangement du type* II_5 *; elle est de l'un des types suivants :* III_6, IV_7.

Pour le réfuter, des droites suffisent (figure 4). On écrit une droite $u_0 x + u_1 y + u_2 z = 0$ du plan

46. Preuve vérifiée : `lean/Grothendieck/Folder80.lean`.

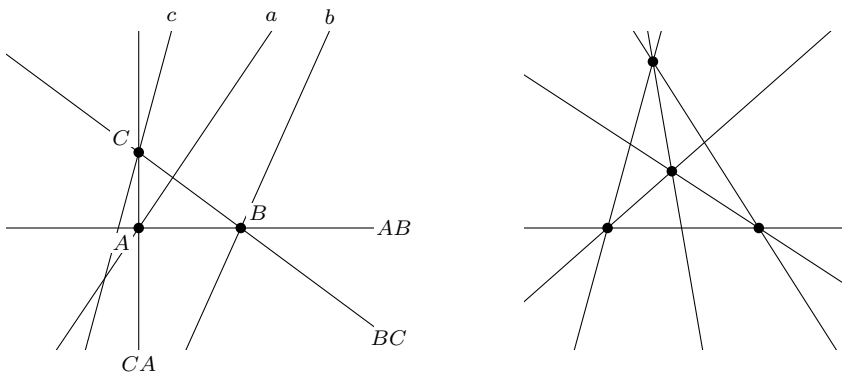
projectif comme un triplet d'entiers u ; trois droites u, v, w sont concourantes si et seulement si le déterminant de la matrice de lignes u, v, w est nul. Toutes les vérifications deviennent alors des calculs finis sur des entiers.

Contre-exemple 43.1 (Énoncé de l'édition, page 24)**.** *Soient $A = (0, 0)$, $B = (1, 0)$, $C = (0, 1)$ dans le plan affine, et les six droites*

$$AB : y = 0, \quad BC : x+y = 1, \quad CA : x = 0, \quad a : y = 2x, \quad b : y = 3x-3, \quad c : y = 5x+1,$$

les trois dernières passant respectivement par A, B et C. Cet arrangement a exactement trois points triples, A, B et C ; il n'existe pas deux sommets par l'un desquels passe chacune des six droites ; cinq quelconques d'entre elles contiennent trois droites concourantes, de sorte qu'il ne contient pas de II_5 ; il n'est ni III_6, qui a quatre points triples, ni IV_7, qui a sept droites.

Démonstration. Les triplets sont $(0, 1, 0)$, $(1, 1, -1)$, $(1, 0, 0)$, $(2, -1, 0)$, $(3, -1, -3)$ et $(5, -1, 1)$. Parmi les vingt triples de droites, trois seulement ont un déterminant nul : $\{AB, CA, a\}$, $\{AB, BC, b\}$ et $\{BC, CA, c\}$, qui concourent en A, B et C. Deux droites distinctes sont toujours non proportionnelles, puisque chacune forme avec l'autre et une troisième un déterminant non nul. Un sommet est l'intersection de deux droites, et une droite y passe si elle est l'une des deux ou si elle forme avec elles un triple concourant. Chaque point triple porte trois droites et chaque point double deux, et deux points triples distincts ont une droite commune, un côté du triangle : deux sommets portent au plus cinq droites, jamais six. Cinq droites parmi six en omettent une. Si c'est un côté, disons BC, les droites AB, CA et a restent et concourent en A ; si c'est a, il reste AB, BC et b, qui concourent en B, et de même pour b et c. Enfin il y a trois points triples et non quatre, et six droites et non sept. En Lean, ces assertions sont décidées par calcul sur les entiers. □



le contre-exemple III_6

FIGURE 4 – À gauche, les six droites du contre-exemple, tracées d'après leurs équations : trois points triples seulement, A, B et C, aucun couple de sommets par lesquels passent toutes les droites, et trois droites concourantes parmi cinq quelconques. À droite, III_6, le quadrangle complet, qui a quatre points triples. Figure de l'édition ; Grothendieck dessine aux pages 22 à 28 les faisceaux et les arrangements cruciaux qu'il nomme (80, lot 2, p. 22, 80, lot 2, p. 24).

Remarque. Le contre-exemple contient un $\mathrm{II}'_{3,2}$, trois pseudo-droites par un point et deux par un autre sans droite de jonction : les cinq droites AB, CA, a, b, c n'ont qu'un triple concourant, $\{AB, CA, a\}$. La forme encadrée de la page 24, et la version corrigée par la lecture où l'on

exclut aussi $\mathrm{II}'_{3,2}$, ne sont donc pas atteintes. La lecture corrige aussi la parenthèse de la page parce que IV_7 contient lui aussi un $\mathrm{II}'_{3,2}$, et cela se vérifie de la même façon : pour le carré $A=(0,0)$, $B=(1,0)$, $C=(1,1)$, $D=(0,1)$, avec $E=AB\cap CD$ et $F=AD\cap BC$ à l'infini, les sept droites AB, BC, CD, DA, AC, BD, EF ont six points triples, et parmi elles AB, AD, AC, BD, EF n'ont que le triple $\{AB, AD, AC\}$.

Le calcul porte sur des droites. Un arrangement de droites est un arrangement de pseudo-droites, et le contre-exemple vaut donc pour l'énoncé de la page tel qu'il est écrit ; les pseudo-droites en général ne sont pas formalisées. Viennent ensuite les autres énoncés de la cote, avec ce qu'en dit Lean.

Théorème (Grothendieck, pages 20, 24 et 28, arrangements sans bigones ♦). [a] *Tout arrangement de pseudo-droites du plan projectif réel sans pseudo-droite bigonale est l'arrangement simple de quatre pseudo-droites (II_4), ou contient un sous-arrangement de l'un de trois types : cinq pseudo-droites en position générale (II_5), un faisceau de trois et un faisceau de deux sans la droite qui joint leurs centres ($\mathrm{II}'_{3,2}$), ou le quadrangle complet (III_6).*

a. Preuve vérifiée : `lean/Grothendieck/Folder80Maps2.lean`.

La page tire cet énoncé du théorème de la page 24, faux tel qu'il est écrit, et ne donne pour le lemme de la page 28 qu'une « idée » ; le nom $\mathrm{II}'_{3,2}$ est de la lecture. L'édition le démontre, sans Lean, avec le lemme de numérotation. Un arrangement sans bigones n'est pas un quasi-faisceau (chaque droite du faisceau n'y porte que le centre et son point sur la transversale) ; il a donc un point double $p=a\cap b$ (Kelly et Rottenberg, théorème 3.6 [82] ; voir aussi Bokowski et Pokora [17]). La droite a porte au moins deux autres sommets q_i, q_j ; deux pseudo-droites $c\ni q_i$ et $d\ni q_j$ qui coupent b en des points distincts forment avec a, b quatre pseudo-droites en position générale Q, et s'il n'en existe pas, toutes passent par un même point de b, qui est alors bigonale. Une autre pseudo-droite qui ne passe par aucun ou par un seul des six sommets de Q donne II_5 ou $\mathrm{II}'_{3,2}$; sinon c'est une diagonale du quadrilatère Q, passant par deux sommets opposés ; une diagonale seule serait bigonale, deux donnent III_6. Pour la numérotation, on part de III_6 s'il est présent (toute pseudo-droite coupe ses six côtés en au moins trois points), sinon de Q, en ajoutant en dernier la diagonale éventuelle ; ajouter une pseudo-droite n'ôte aucun sommet aux autres, si bien que chaque arrangement partiel est sans bigones. Une énumération par ordinateur de tous les arrangements d'au plus neuf pseudo-droites le confirme. La version combinatoire est vérifiée en Lean (`Folder80Maps2.lean`) pour les cartes combinatoires de la page 60 : une carte généralisée (drapeaux et trois involutions) de caractéristique d'Euler 1, dont les drapeaux sont étiquetés par les pseudo-droites, chacune connexe et passant une fois par chacun de ses sommets, deux d'entre elles se coupant en un seul sommet ; « sans bigone » veut dire que chaque pseudo-droite porte au moins trois sommets, ce qui exclut aussi les faisceaux (`map_dichotomy`). L'inégalité de Melchior, tirée de $\chi=1$ et de ce que les faces ont au moins trois côtés (le squelette n'a ni boucle ni arête multiple), donne un point double (`melchior`) ; le reste est de l'incidence pure : quatre pseudo-droites en position générale, puis une cinquième, qui donne II_5, $\mathrm{II}'_{3,2}$ ou une diagonale ; deux diagonales donnent III_6, une seule est bigonale (`dichotomy`). Le lemme de numérotation de la page 28 et le passage d'un arrangement topologique à sa carte ne sont pas formalisés. On se reportera aux notes de Grothendieck (80, lot 1, p. 20).

Théorème (D'après les pages 24 et 26, cas latticiel, condition b) lue par l'édition ♦). *Pour un arrangement de pseudo-droites du plan projectif réel, les cellules fermées de la décomposition induite se coupent deux à deux suivant le vide ou une seule cellule fermée si et seulement si aucune pseudo-droite n'est bigonale et l'arrangement n'est pas l'arrangement simple de quatre pseudo-droites II_4.*

◊ non vérifié en Lean

La page 26 l'énonce sans démonstration. Vérifié en Lean (`Folder80Maps1.lean`) : l'énoncé est faux dans le sens « si », déjà pour de vraies droites. L'arrangement $\mathrm{II}'_{3,2}$, formé des droites $x=0$, $x=z$, $x=2z$

et $y = 0$, $y = z$, n'a pas de pseudo-droite bigonale et n'est pas II_4, mais ses deux faces « de coin » ont pour intersection les deux centres $[0 : 1 : 0]$ et $[1 : 0 : 0]$, qui ne forment pas une cellule (`lattice_criterion_false`) ; la page 24 le dit pourtant latticiel. Le critère juste, démontré dans le modèle des covecteurs (signes des points, fermeture topologique comprise), est : on est dans le cas latticiel si et seulement s'il n'existe pas deux points par l'un desquels passe chaque pseudo-droite, c'est-à-dire si l'arrangement n'est d'aucun des types I_N, $\mathrm{I}_{p,q}$, $\mathrm{II}'_{p,q}$, l'hypothèse même du théorème de la page 24 (`lattice_iff`, `lattice_iff_not_twoPencil`). Le sens « seulement si » de la page tient : une pseudo-droite bigonale, ou II_4, fournit deux tels points (`not_lattice_of_bigonal`, `not_lattice_of_four`). Le critère abstrait vaut pour tout ensemble de vecteurs de signes symétrique et stable par composition, donc pour toute pseudo-droite par la représentation de Folkman–Lawrence, qui n'est pas formalisée. On se reportera aux notes de Grothendieck (80, lot 2, p. 24).

Théorème (Grothendieck, pages 39 à 54, squelette d'un arrangement sans bigones ♦). *Un arrangement combinatoire de pseudo-droites du plan projectif réel sans pseudo-droite bigonale est déterminé par son* 1*-squelette muni de la décomposition des arêtes en pseudo-droites, et cela fonctoriellement : le foncteur des arrangements sans bigones vers les arrangements de dimension* 1 *sans bigones est pleinement fidèle, de sorte que tout automorphisme du squelette décomposé vient de la carte.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 41 à 54). Les conditions (A1) à (A6) y sont dites satisfaites « bien entendu », sans démonstration, et l'indépendance des choix en (34) n'est pas vérifiée. Partiellement vérifié en Lean (`Folder80Maps3.lean`), pour les cartes combinatoires de la page 60 (carte généralisée de caractéristique d'Euler 1 étiquetée par les pseudo-droites, sans bigone, chaque pseudo-droite allant tout droit en chaque sommet). Le foncteur est fidèle (`faithful`). Le « théorème général des cartes » de la page 41 est démontré : un isomorphisme de squelettes décomposés vient d'un isomorphisme de cartes si et seulement s'il respecte les chemins de trois arêtes consécutives d'une face (`lift_iff`) ; la pleine fidélité revient donc à lire ces chemins sur le squelette. En homologie modulo 2, $\chi = 1$ donne $\dim Z_1/B_1 \leqslant 1$, la relation $c_2 = c(K)$ de la page 42 (`finrank_Z1_le`) ; une pseudo-droite est un cycle qui ne borde pas (`lineChain_not_mem`), et une pseudo-droite coupe le bord d'une réunion de faces en un nombre pair de points (`parity`). D'où la condition (A5) de la page 50 : si une quatrième pseudo-droite Δ évite les trois sommets d'un triangle, un cycle triangulaire borde si et seulement si Δ en coupe un nombre pair de côtés (`triangle_iff`) ; l'orientation canonique du triangle se lit donc sur le squelette et ne dépend pas de Δ. Les segments d'une pseudo-droite se lisent sur le squelette (`seg_unique`), et tout isomorphisme de squelettes décomposés respecte cette orientation (`SkelIso.triangle_map`). Le théorème de la page 54 est démontré pour les arrangements simples (`full_simple`) : le triangle découpé par un chemin de face borde (`path_bounds`, par un comptage de parité le long de la droite de l'arête médiane), les coins en un sommet de deux droites se lisent sur le squelette (`corner2`), et tout isomorphisme de squelettes décomposés se relève. Restent les points multiples ((A1)–(A3) en un sommet d'au moins trois droites), (A6) et le quadrangle complet III_6. La condition (A4) est démontrée en des sommets de multiplicité quelconque : deux arêtes quittant les extrémités d'une arête du même côté découpent un triangle qui borde, et de côtés opposés un triangle qui ne borde pas (`side_bounds`, `side_not`) ; le côté se lit donc sur le squelette dès qu'une quatrième droite évite le triangle. Restent (A1)–(A3) aux points multiples (l'ordre cyclique déduit des côtés), (A6) et le quadrangle complet III_6. Le théorème de la page 54 est démontré, points multiples compris, dès que tout triangle a une quatrième droite évitant ses sommets (`full_of_fourth'`) : si tout triangle a une quatrième droite évitant ses sommets, tout isomorphisme de squelettes décomposés se relève de façon unique. L'ingrédient est (A1)–(A3) : les côtés d'une arête se lisent par les triangles qui bordent (`side_tri`), et deux arêtes en un sommet sont adjacentes si aucune arête n'est entre elles (`between_iff`, `SkelIso.corner_map`). Restent les arrangements où un triangle a toutes les autres droites par ses sommets, dont le quadrangle complet III_6 : c'est (A6). L'hypothèse de quatrième droite découle d'une condition intrinsèque : un triangle ayant un sommet double a toujours une quatrième droite évitant ses sommets (`fourth_at`). D'où la pleine fidélité dès que tout triangle a un sommet sur exactement deux

droites (`full_of_simpleCorner`). Restent les arrangements ayant un triangle sans quatrième droite : ses trois sommets sont multiples et toutes les autres droites passent par eux. C'est (A6) et le quadrangle complet III_6, entre autres. Plus précisément, restent non formalisés les conditions (A1) à (A4), qui lisent sur le squelette l'ordre circulaire en un sommet et le transport le long d'une arête, et les cas (A6) et III_6 de l'orientation canonique ; le théorème de la page 54 n'est donc pas démontré en entier. Mathlib n'a pas les arrangements de pseudo-droites ni les cartes. On se reportera aux notes de Grothendieck (80, lot 2, p. 39).

Le cas restant se démontre par un autre chemin, celui des chirotopes (`Folder80Signs.lean`). Un chirotope attribue un signe à chaque triple de pseudo-droites sans point commun : il dit dans quel sens tourne le triangle qu'elles forment. Un isomorphisme de squelettes décomposés conserve, le long de chaque pseudo-droite, l'ordre circulaire de ses sommets au retournement près. En rang 2, cela veut dire que les deux chirotopes, restreints aux triples qui contiennent cette pseudo-droite, ne diffèrent que par un signe global et par le retournement de certaines des autres pseudo-droites. Le produit ψ des deux chirotopes, corrigé par ces signes, s'écrit alors en chaque pseudo-droite i sous la forme $\psi(i,j,l) = \delta^i_j \delta^i_l$. Si une quatrième pseudo-droite évite les sommets d'un triangle, les quatre triples formés par ces quatre pseudo-droites ont la même valeur, et leur produit vaut 1 : on retrouve (A5) sous une autre forme (`eq_zero_of_fourth`). Sinon, on coupe le triangle a, b, c en deux le long d'une pseudo-droite x qui passe par $b \cap c$ et par un troisième sommet de a. Les triangles a, b, x et a, x, c ont chacun une quatrième pseudo-droite, qui passe par $a \cap c$ pour le premier et par $a \cap b$ pour le second (`eq_zero`). Dans le quadrangle complet, les trois pseudo-droites auxiliaires sont les côtés qui passent par le quatrième point. Les deux chirotopes diffèrent donc d'une réorientation (`reorientation_of_locallyEquivalent`), et le théorème de Folkman et Lawrence fournit l'homéomorphisme. Le pas de rang 2 est démontré lui aussi. Le long d'une pseudo-droite, les autres se rangent en classes, une par sommet, et la somme des signes sur un cycle de quatre arêtes dit si deux sommets en séparent deux autres. Une fonction de signes dont toutes ces sommes s'annulent, sur un graphe multiparti complet d'au moins trois parts, est une constante plus une coupure (`const_add_cut`). Deux chirotopes qui ont les mêmes relations de séparation le long de chaque pseudo-droite diffèrent donc d'une réorientation (`reorientation_of_sameSeparation`). Le théorème de Folkman et Lawrence n'est pas formalisé, et l'argument, qui est celui de l'édition, n'a pas été relu par un spécialiste.

La page 44 décrit l'ordre circulaire en un sommet multiple, la donnée que les conditions (A1) à (A3) lisent sur le squelette (figure 5). Soit s un sommet par lequel passent $\nu = \nu_s$ pseudo-droites D_i, $i \in I_s$. Autour de s, les 2ν demi-arêtes se suivent dans un ordre circulaire, et chaque pseudo-droite, qui traverse s tout droit, en occupe deux opposées. En tournant dans un sens fixé, qui est le choix de u_0, on passe d'une pseudo-droite D_i à la suivante $D_{u_0(i)}$: le polygone de sommets I_s est ainsi orienté. On passe aussi d'une orientation de D_i, c'est-à-dire d'une demi-arête sortante, à une orientation de la suivante, d'où une bijection α_i des deux orientations de D_i sur celles de $D_{u_0(i)}$. Après ν pas on a fait un demi-tour, et l'on retrouve D_{i_0} orientée dans l'autre sens : le composé des ν bijections échange les deux orientations. C'est la condition (28) de la page : les $\nu - 1$ premières bijections déterminent la dernière, qui doit faire du composé l'échange et non l'identité. Le polygone se referme donc comme un ruban de Möbius. Cette condition n'est pas formalisée. On se reportera aux notes de Grothendieck (80, lot 3, p. 44).

44 Cote 82 : $\mathfrak{sl}(2)$ et la conique en caractéristique 2, cas déployé [47]

La cote 82, *SO(3) ≃ GP(1)*, notes que l'inventaire date « [vers 1982] », compare les formes de $\mathrm{SO}(3)$ et de $\mathrm{PGL}(2)$ sur une base quelconque. Aux pages 77 et 78, sur une base où $2 = 0$, elle prend le module $\tilde{\mathfrak{g}}$ des matrices 2×2 de trace nulle avec $\varphi(u, v) = \mathrm{Tr}(uv)$: comme $\mathrm{Tr}\, 1 = 2 = 0$, $\mathcal{O}_S \cdot 1 \subset \tilde{\mathfrak{g}}$ est le noyau de φ (58). Le morphisme (59), qui envoie un sous-groupe de Borel, c'est-à-dire une droite isotrope $L \subset \tilde{\mathfrak{g}}$, sur son orthogonal, se factorise par $\mathbf{P}(\tilde{\mathfrak{g}}/\mathcal{O}_S)$ (60), et la page affirme que (60) est le Frobenius relatif, non un monomorphisme (82, lot 4, p. 77). L'édition

47. Preuve vérifiée : `lean/Grothendieck/Folder82.lean`.

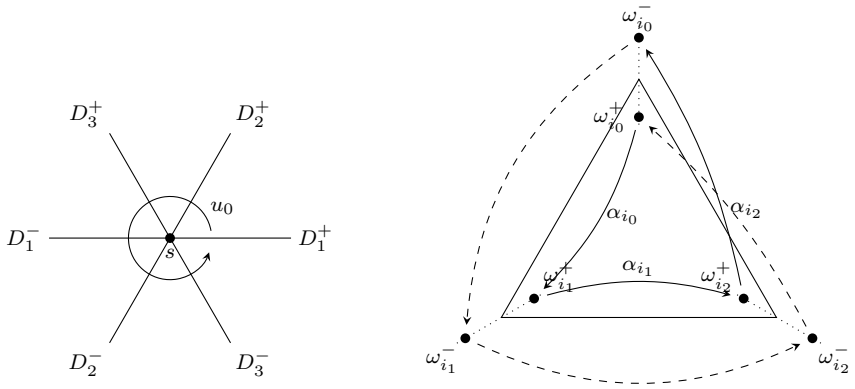


FIGURE 5 – Le cas $\nu = 3$. À gauche, les trois pseudo-droites par le sommet s et leurs six demi-arêtes, D_i^+ et D_i^- opposées ; u_0 tourne d'une demi-arête à la suivante. À droite, le polygone de sommets I_s orienté par u_0, avec en chaque coin les deux orientations $\omega_i^\pm$ de D_i ; les bijections α_i suivent la rotation, et la dernière échange l'intérieur et l'extérieur : le composé des trois est l'échange, condition (28). Figure de l'édition ; à la page 44 Grothendieck dessine ce polygone comme un hexagone aux côtés fléchés, deux points sur la bissectrice extérieure de chaque coin (80, lot 3, p. 44).

le vérifie dans le cas déployé, sur tout anneau commutatif R où $2 = 0$, dans les coordonnées $u = x\tilde{X} + y\tilde{Y} + z\tilde{H}$, $\tilde{X} = E_{12}$, $\tilde{Y} = E_{21}$, $\tilde{H} = \mathrm{diag}(1, -1)$, pour lesquelles $u^2 = (xy + z^2) \cdot 1$.

Aux pages 26 et 27, sur une base où $2 = 0$, une forme de $\mathfrak{sl}(2)$ équivaut à un couple (V, E), V de rang 2 et E une extension de V par $\det V$; le groupe des automorphismes d'une forme est un groupe affine « lisse de dim rel. 6 », celui d'un plan affine symplectique $\mathrm{SL}(V) \ltimes V$, « lisse de dim 5 ». La lecture identifie $\mathfrak{sl}(2)$ à l'algèbre de Heisenberg : son centre $\mathcal{O}\tilde{H}$ est son algèbre dérivée et le crochet induit $\Lambda^2 V \simeq \mathcal{O}\tilde{H}$.

Théorème 44.1 (D'après les pages 26 et 27, cas déployé ♦). *Soit R un anneau commutatif où $2 = 0$. Dans $\mathfrak{sl}_2(R)$, $[u, u'] = (xy' - yx')\tilde{H}$ pour $u = x\tilde{X} + y\tilde{Y} + z\tilde{H}$, et le centre $R\tilde{H}$ est fait de crochets. Tout endomorphisme d'algèbres de Lie de $\mathfrak{sl}_2(R)$ s'écrit de façon unique $u \mapsto g(x, y) + (ax + by + \det g \cdot z)\tilde{H}$, avec $g \in M_2(R)$ et $a, b \in R$, la composition étant celle de $\mathrm{GL}(V) \ltimes \mathrm{Hom}(V, \det V)$; c'est un automorphisme si et seulement si $\det g$ est inversible. Ainsi $\mathrm{Aut}(\mathfrak{sl}_2)(R) \simeq \mathrm{GL}_2(R) \ltimes R^2$, et les automorphismes qui fixent $\tilde{H}$ forment $\mathrm{SL}_2(R) \ltimes R^2$. Les dérivations forment un R-module libre de rang 6, celles qui annulent $\tilde{H}$ un module libre de rang 5.*

L'énoncé tient : voir `bijective_iff`, `bijective_fix_iff`, `autFun_comp`, `finrank_der` et `finrank_derFix` dans `Folder82.lean`. Les dimensions 6 et 5 de la page sont celles des algèbres de Lie. Ne sont pas démontrés : les formes sur une base, $\mathfrak{gp}(1)$ et le couplage, le caractère lisse des schémas d'automorphismes.

Théorème 44.2 (D'après les pages 77 et 78, cas déployé ♦). *Soit R un anneau commutatif où $2 = 0$. Alors $\tilde{H} = 1$ et le noyau de φ sur $\tilde{\mathfrak{g}}$ est $R \cdot 1$. Pour $s, t \in R$, l'élément $s^2\tilde{X} + t^2\tilde{Y} + st\tilde{H}$ est de carré nul, et son orthogonal pour φ est l'hyperplan $t^2x + s^2y = 0$, qui contient 1 et ne dépend que de $(s^2 : t^2)$: (60) est $(s : t) \mapsto (s^2 : t^2)$. Sur $R = \mathbf{F}_2[\varepsilon]/(\varepsilon^2)$, les points distincts $(1 : \varepsilon)$ et $(1 : 0)$ de $\mathbf{P}^1(R)$ ont le même orthogonal : (60) n'est pas un monomorphisme.*

L'énoncé tient tel que la note de la lecture le donne (`ker_phi`, `orth_iff`, `orth_smul`, `not_mono`, dans `Folder82.lean`). Le calcul de l'orthogonal vaut pour tous s, t, sans hypothèse d'unimodularité.

Théorème (Grothendieck, page 78, (61)). *Pour une algèbre de quaternions sur une base de caractéristique 2, il existe un isomorphisme canonique $\mathbf{P}(\tilde{\mathfrak{g}}/\mathcal{O}_S) \simeq X^{(2)}$, et (60) est le Frobenius relatif $X \to X^{(2)}$: il est fini, plat de rang 2 et radiciel.*

◊ non vérifié en Lean

La page 78 l'affirme sans démonstration. Sur un corps, la projection depuis le noyau de la conique est classique ; la forme relative et canonique ne l'est pas. Mathlib n'a pas les coniques sur une base ni le Frobenius relatif des schémas. On se reportera aux notes de Grothendieck (82, lot 4, p. 77).

45 Cote 84 : le produit des algèbres quadratiques, en coordonnées [48]

La cote 84, *[Formes quadratiques] : notes manuscrites (s.d.)*, cent quatre-vingt-douze pages que l'inventaire date « [à partir de 1982-vers 1986] », étudie les formes quadratiques binaires et les algèbres quadratiques au-dessus d'une base quelconque, sans diviser par 2. Sa deuxième partie construit le produit $A_1 * A_2$ de deux algèbres quadratiques. La page 47 encadre $T_0^2 \equiv \delta \pmod 4$; la page 48 énonce, quand 2 est régulier, l'équivalence entre revêtements quadratiques et triplets (L, δ, T_0) (84, lot 3, p. 47, 84, lot 3, p. 48). La page 63 pose « sauf erreur » $b = b_1 b_2$ et en tire c par $4c = b^2 - \delta$; l'encadré écrit « $4c_1c_1$ », le membre de droite et le calcul donnent $4c_1c_2$ (84, lot 4, p. 63). La page 64 vérifie par une identité polynomiale que l'élément $u_1b_2 + u_2b_1 + 2u_1u_2$ annule l'équation du produit quand u_1 et u_2 annulent les leurs (84, lot 4, p. 64). Page 84, elle calcule des générateurs de $\mathrm{Im}(\sigma_1 \otimes \sigma_2 - \mathrm{id})$; page 85, elle énonce la proposition sur les coinvariants, avec un décompte de rangs au-dessus de $X_0 = V(2)$; page 86, le corollaire sur les invariants, « et inversement si on sait que ceci reste vrai après toute changement de base » (84, lot 5, p. 84, 84, lot 5, p. 85, 84, lot 5, p. 86). Page 89, le théorème donne $b = b_1b_2$, $c = c_1b_2^2 + c_2b_1^2 - 4c_1c_2$ et $\delta = \delta_1\delta_2$ (84, lot 5, p. 89) ; page 102, l'image $i(\mathcal{U}) = 2U_1U_2 + b_1U_2 + b_2U_1$ du générateur dans $A_1 \otimes A_2$ (84, lot 6, p. 102). Pages 65 à 79, elle introduit les extensions χ-trivialisées et leur produit ; page 78, le cas scindé donne $b = b_1 \otimes b_2$, et une note marginale de la page 79, oblique et en partie illisible, donne le critère d'inversibilité (84, lot 4, p. 78, 84, lot 4, p. 79). Pages 125 à 131, elle refait le produit en coordonnées pour un quotient M quelconque et commence la relation de cocycle sans l'achever ; page 169, elle met en place les produits poussé et tiré (84, lot 7, p. 125, 84, lot 7, p. 129, 84, lot 7, p. 131, 84, lot 9, p. 169).

Algèbres quadratiques libres. Pour $b, c \in R$, on note $A(b,c) = R[U]/(U^2 + bU + c)$, de base $(1, U)$, et $\delta(b,c) = b^2 - 4c$. Le changement de variable $V = \varepsilon U + t$, $\varepsilon \in R^\times$, $t \in R$, envoie l'équation de U sur celle de V avec

$$(b', c') = (\varepsilon b - 2t,\ \varepsilon^2 c - \varepsilon b t + t^2).$$

Dans le cas libre, $L = A/R$ est engendré par l'image de U, T_0 est la réduction de la trace $-b$ modulo 2, donc $T_0 \equiv b$ modulo 2, et changer de base de L revient à multiplier par ε. Le triplet (L, δ, T_0) de la page 48 devient, à isomorphisme près, la classe de $(\delta, b \bmod 2)$ sous $(\delta, b) \mapsto (\varepsilon^2\delta, \varepsilon b)$.

Énoncé (Pages 47 à 53, *le théorème des triplets, cas libre* ⧫). *Soit R un anneau commutatif.*

1. *Les R-algèbres $A(b,c)$ et $A(b',c')$ sont isomorphes si et seulement si (b',c') se déduit de (b,c) par un changement de variable $V = \varepsilon U + t$.*
2. *(Page 47) Pour tous b, c, $b^2 - \delta(b,c) = 4c$. Si $\tau^2 - \delta \in 4R$, alors $(\tau + 2a)^2 - \delta \in 4R$ pour tout a. Si $\tau^2 - \delta \in 4R$, il existe c avec $\delta(\tau, c) = \delta$.*

48. Preuve vérifiée : `lean/Grothendieck/Folder84.lean`.

3. *(Page 48) Supposons que 2 ne divise pas zéro dans R. Alors $A(b,c) \simeq A(b',c')$ si et seulement s'il existe $\varepsilon \in R^\times$ avec $\delta(b',c') = \varepsilon^2\delta(b,c)$ et $b' \equiv \varepsilon b$ modulo $2R$. Avec $\varepsilon = 1$ (la base de L fixée), il existe une translation $V = U+t$ de (b,c) sur (b',c') si et seulement si $\delta(b',c') = \delta(b,c)$ et $b' \equiv b$ modulo $2R$, et cette translation est unique.*
4. *(Page 53, sur $\mathbb{Z}$) Un entier δ est de la forme $b^2 - 4c$ si et seulement si $\delta \equiv 0$ ou 1 modulo 4, et $A(b,c) \simeq A(b',c')$ si et seulement si $\delta(b,c) = \delta(b',c')$.*
5. *Sur $\mathbb{F}_2$, $(1,0)$ et $(1,1)$ ont le même $\delta = 1$ et le même b, et $A(1,0) = \mathbb{F}_2[U]/(U^2+U)$ n'est pas isomorphe à $A(1,1) = \mathbb{F}_2[U]/(U^2+U+1)$.*

Démonstration. (1) Tout élément de $A(b,c)$ s'écrit $a+eU$, et $a+eU = 0$ entraîne $a = e = 0$: le polynôme unitaire U^2+bU+c de degré 2 ne divise aucun polynôme non nul de degré au plus 1, et le reste de la division par lui donne l'écriture. Si $V = \varepsilon U+t$ convient, $\varepsilon U+t$ annule $V^2+b'V+c'$ dans $A(b,c)$: le calcul donne $\varepsilon^2(U^2+bU+c)$. On obtient un morphisme $A(b',c') \to A(b,c)$, $V \mapsto \varepsilon U+t$; le changement inverse $U = \varepsilon^{-1}V-\varepsilon^{-1}t$ donne le morphisme réciproque, et les deux composés fixent les générateurs. Réciproquement, soit $\varphi : A(b,c) \to A(b',c')$ un isomorphisme. Écrivons $\varphi^{-1}(V) = t+\varepsilon U$ et $\varphi(U) = s+\eta V$. Alors $U = \varphi^{-1}(\varphi(U)) = (s+\eta t)+\eta\varepsilon U$, donc $\eta\varepsilon = 1$ et ε est inversible. L'image par φ^{-1} de l'équation de V, où l'on remplace U^2 par $-bU-c$, donne

$$(t^2+b't+c'-\varepsilon^2 c) + (2t\varepsilon+b'\varepsilon-\varepsilon^2 b)\,U = 0,$$

d'où $b' = \varepsilon b - 2t$ après multiplication par η, puis $c' = \varepsilon^2 c - \varepsilon b t + t^2$.

(2) Ce sont des identités : $(\tau+2a)^2 - \tau^2 = 4(a\tau+a^2)$, et si $\tau^2-\delta = 4k$, on prend $c = k$.

(3) Un changement de variable donne $\delta(b',c') = \varepsilon^2\delta(b,c)$ en développant, et $b' = \varepsilon b+2(-t)$; cela vaut sur tout anneau. Réciproquement, si $b' = \varepsilon b+2s$ et $\delta(b',c') = \varepsilon^2\delta(b,c)$, posons $t = -s$. Alors $b' = \varepsilon b - 2t$, et l'égalité des discriminants s'écrit $4c' = 4(\varepsilon^2 c - \varepsilon b t + t^2)$. Comme 2 est régulier, 4 l'est, et $c' = \varepsilon^2 c - \varepsilon b t + t^2$. Le cas $\varepsilon = 1$ est le même calcul ; deux translations t, t' vérifient $2t = 2t'$, donc $t = t'$.

(4) Si b est pair, $b^2-4c \equiv 0$; s'il est impair, $b^2-4c \equiv 1$ modulo 4. Inversement $\delta = 0^2-4(-\delta/4)$ ou $\delta = 1^2 - 4\cdot\frac{1-\delta}{4}$. Les unités de $\mathbb{Z}$ sont ±1, donc $\varepsilon^2 = 1$ et l'énoncé (3) se réduit à $\delta = \delta'$ et $b' \equiv b$ modulo 2. Cette congruence découle de $\delta = \delta'$: $(b'-b)(b'+b) = 4(c'-c)$ est pair, donc l'un des facteurs l'est, et $b'-b$, $b'+b$ ont la même parité.

(5) Dans $\mathbb{F}_2$, la seule unité est 1 et $t^2 = t$ pour tout t ; un changement de variable envoie donc $(1,c)$ sur $(1,c-t+t^2) = (1,c)$. Par (1), $A(1,0) \not\simeq A(1,1)$. □

Remarque. Dans le cas libre, la classification des algèbres quadratiques par $(\delta, b \bmod 2)$ quand 2 est régulier découle de la proposition 3.11 et du théorème 4.3 de Voight (2016) [120]. La vérification porte sur le cas libre du théorème de la page 48 : L trivial, l'algèbre donnée par une base $(1,U)$, et la correspondance sur les classes d'isomorphisme. Le cas L inversible non trivial, sur une base affine, est démontré plus bas, ainsi que la compatibilité aux changements de base et la reconstruction de E, A, de la trace, de la norme et du produit par divisions (pages 49 à 52) ; l'équivalence de catégories fibrées sur un schéma ne l'est pas. L'énoncé (1) vaut sur tout anneau et ne demande pas que 2 soit régulier ; l'hypothèse sert à l'injectivité de $(b,c) \mapsto (\delta, b \bmod 2)$ sur les classes, et l'exemple de $\mathbb{F}_2$, où $\mathbb{F}_2 \times \mathbb{F}_2$ et $\mathbb{F}_4$ ont les mêmes δ et T_0, montre qu'elle est nécessaire. La surjectivité, (2), vaut sur tout anneau. Sur $\mathbb{Z}$, on retrouve que les discriminants sont les entiers congrus à 0 ou 1 modulo 4 et qu'un anneau quadratique est déterminé par son discriminant ; T_0 y est déterminé par δ, comme la lecture le dit.

Conventions. R est un anneau commutatif quelconque. Les algèbres A_i ont pour bases $(1, U_i)$ avec $U_i^2 + b_i U_i + c_i = 0$, de sorte que $\mathrm{Tr}(U_i) = -b_i$ et que la conjugaison est $\sigma_i(1) = 1$, $\sigma_i(U_i) = -b_i - U_i$; on pose $\delta_i = b_i^2 - 4c_i$. C'est la convention de la lecture (pages 98 à 102). Du côté des extensions, E_i a pour base (e_i, x_i), où e_i engendre L_i et x_i est le scindage ; $\psi(e_i) = 0$, $\psi(x_i) = 1$, $T_i = 2x_i - b_i e_i$ et $\sigma_i(x) = \psi(x)T_i - x$, donc $\sigma_i(e_i) = -e_i$ et $\sigma_i(x_i) = x_i - b_i e_i$ (page 84). On écrit $E_1 \otimes E_2 = R^4$ dans la base $(e_1 \otimes e_2, e_1 \otimes x_2, x_1 \otimes e_2, x_1 \otimes x_2)$, $\sigma_1 \otimes \sigma_2$ par le produit de Kronecker des deux matrices, et $E_1 * E_2 = R^2$ dans la base $(e_1 \otimes e_2, x_1 * x_2)$. L'application $E_1 \otimes E_2 \to E_1 * E_2$ est celle de la page 63, $(x_1 + u_1) * (x_2 + u_2) = x_1 * x_2 + u_1 b_2 + u_2 b_1 + 2u_1 u_2$: elle envoie (a, a', a'', a''') sur $(2a + b_2 a' + b_1 a'',\ a''')$. Du côté des algèbres, $A = A_1 * A_2$ a pour base $(1, \mathcal{U})$, $A_1 \otimes A_2$ la base $(1, U_1, U_2, U_1U_2)$, et i envoie (λ, μ) sur $(\lambda, \mu b_2, \mu b_1, 2\mu)$.

Énoncé (Pages 63, 64, 89 et 102, *la formule du produit* ♦). *Soient A_1, A_2 deux R-algèbres commutatives et $u_i \in A_i$ avec $u_i^2 + b_i u_i + c_i = 0$, $b_i, c_i \in R$. Posons $U_1 = u_1 \otimes 1$, $U_2 = 1 \otimes u_2$ dans $A_1 \otimes_R A_2$, $b = b_1 b_2$ et $c = c_1 b_2^2 + c_2 b_1^2 - 4c_1 c_2$.*

1. *(Page 64) Dans tout anneau commutatif, avec $Q_i = u_i^2 + b_i u_i + c_i$ et $u = 2u_1u_2 + b_1u_2 + b_2u_1$,*
$$u^2 + bu + c = b_2^2 Q_1 + b_1^2 Q_2 + 4\big(Q_1Q_2 - c_1Q_2 - c_2Q_1\big).$$
2. *(Page 102) L'élément $\mathcal{U} = 2U_1U_2 + b_1U_2 + b_2U_1$ vérifie $\mathcal{U}^2 + b\mathcal{U} + c = 0$ dans $A_1 \otimes_R A_2$; il existe donc un unique morphisme de R-algèbres $R[\mathcal{U}]/(\mathcal{U}^2 + b\mathcal{U} + c) \to A_1 \otimes_R A_2$ envoyant $\mathcal{U}$ sur cet élément.*
3. *(Pages 63 et 89) $b^2 - 4c = \delta_1\delta_2$, et $c_1\delta_2 + c_2\delta_1 + 4c_1c_2 = c_1b_2^2 + c_2b_1^2 - 4c_1c_2$.*

Démonstration. (1) et (3) sont des identités entre polynômes à coefficients entiers ; on les vérifie en développant. (2) Les inclusions $A_1 \to A_1 \otimes A_2$ et $A_2 \to A_1 \otimes A_2$ sont des morphismes de R-algèbres ; elles transportent les équations de u_1 et u_2 en $U_1^2 + b_1U_1 + c_1 = 0$ et $U_2^2 + b_2U_2 + c_2 = 0$. L'identité (1), appliquée dans l'anneau $A_1 \otimes A_2$ à U_1 et U_2, donne $\mathcal{U}^2 + b\mathcal{U} + c = 0$, puisque $Q_1 = Q_2 = 0$. La propriété universelle de $R[\mathcal{U}]/(\mathcal{U}^2 + b\mathcal{U} + c)$ donne le morphisme. □

Remarque. La formule du produit est publiée par Voight (2016, construction 3.12 et théorème 3.24) [120], qui l'attribue à A. Hahn (1994), le monoïde général à O. Loos (1996), et son existence à une lettre de P. Deligne à M. Rost et à M. Bhargava (2005). L'identité de la page 64 vaut sans hypothèse sur u_1, u_2, dans tout anneau commutatif, et la vérification ne divise jamais par 2 : le produit est défini sur $\mathbb{Z}$. La lecture de « $4c_1c_1$ » en $4c_1c_2$ est confirmée : avec $4c_1c_2$, l'identité (1) et la relation $b^2 - 4c = \delta_1\delta_2$ tiennent, et la première forme de l'encadré est égale à la seconde. Seule la partie en coordonnées de la piste est démontrée ; la construction intrinsèque de $X_1 * X_2$ et l'unicité de la forme quadratique de la page 89 ne le sont pas.

Théorème 45.1 (Grothendieck, pages 84 et 85, *proposition* ♦). *Dans les coordonnées ci-dessus, l'application induite*
$$(E_1 \otimes E_2)/\operatorname{Im}(\sigma_1 \otimes \sigma_2 - \mathrm{id}) \to E_1 * E_2$$
est bien définie, et elle est bijective si et seulement si $2R + b_1R + b_2R = R$.

Démonstration. On calcule $\sigma_1 \otimes \sigma_2 - \mathrm{id}$ sur la base : $e_1 \otimes e_2 \mapsto 0$, $e_1 \otimes x_2 \mapsto (b_2, -2, 0, 0)$, $x_1 \otimes e_2 \mapsto (b_1, 0, -2, 0)$, $x_1 \otimes x_2 \mapsto (b_1b_2, -b_1, -b_2, 0)$; ce sont les générateurs de la page 84. L'application $(a, a', a'', a''') \mapsto (2a + b_2a' + b_1a'', a''')$ les annule, d'où l'application induite.

Elle a même image que $E_1 \otimes E_2 \to E_1 * E_2$. Si elle est surjective, $(1,0)$ est atteint, donc $2a + b_2a' + b_1a'' = 1$ pour des $a, a', a'' \in R$, et $2R + b_1R + b_2R = R$. Réciproquement, si $2g_0 + b_1g_1 + b_2g_2 = 1$, l'image de $(y_0g_0, y_0g_2, y_0g_1, y_1)$ est (y_0, y_1).

Sous la condition, montrons que le noyau est dans $\mathrm{Im}(\sigma_1 \otimes \sigma_2 - \mathrm{id})$; l'injectivité de l'application induite en résulte. Écrivons $f = (2, b_2, b_1)$ et $g = (g_0, g_2, g_1)$, de sorte que $f \cdot g = 1$. Un élément du noyau est $(a_0, a_1, a_2, 0)$ avec $f \cdot a = 0$. Les relations de Koszul $\kappa_{jk} = f_k\varepsilon_j - f_j\varepsilon_k$ de f dans R^3 sont $\kappa_{01} = (b_2, -2, 0)$, $\kappa_{02} = (b_1, 0, -2)$ et $\kappa_{12} = (0, b_1, -b_2)$; les deux premières sont les images de $e_1 \otimes x_2$ et $x_1 \otimes e_2$, la troisième celle de $x_1 \otimes x_2 - b_1\, e_1 \otimes x_2$. Or

$$a = \sum_{j<k} (g_k a_j - g_j a_k)\, \kappa_{jk},$$

car la i-ème coordonnée du second membre est $a_i(f \cdot g) - g_i(f \cdot a) = a_i$. L'élément a est donc l'image d'une combinaison explicite des vecteurs de base. □

Énoncé (Page 86, *corollaire* ♦). *Dans les coordonnées ci-dessus, disons que $A \to (A_1 \otimes A_2)^{\sigma_1 \otimes \sigma_2}$ est un isomorphisme si i est injectif et si son image est le sous-module des invariants de $\sigma_1 \otimes \sigma_2$.*

1. *Si $2R + b_1R + b_2R = R$, c'est un isomorphisme.*
2. *C'est un isomorphisme après tout changement de base $R \to S$ si et seulement si $2R + b_1R + b_2R = R$.*
3. *Sur $R = \mathbb{Z}[X]$, avec $b_1 = X$ et $b_2 = 0$, c'est un isomorphisme, alors que 2, X et 0 engendrent un idéal propre.*

Démonstration. Un vecteur (p, q, r, s) (coefficients de 1, U_1, U_2, U_1U_2) est invariant si et seulement si $-b_1q - b_2r + b_1b_2s = 0$, $2q = b_2s$ et $2r = b_1s$. L'image $(\lambda, \mu b_2, \mu b_1, 2\mu)$ de i vérifie ces relations.

(1) Soit $2g_0 + b_1g_1 + b_2g_2 = 1$. Si $i(\lambda, \mu) = 0$, alors $\lambda = 0$ et $\mu = \mu(2g_0 + b_1g_1 + b_2g_2) = 0$. Soit (p, q, r, s) invariant. Des relations on tire $b_1q = b_2r$, car $b_1b_2s = 2b_1q$ (on multiplie $2q = b_2s$ par b_1). Posons $\mu = sg_0 + rg_1 + qg_2$. Alors $2\mu = s$, $b_1\mu = r$ et $b_2\mu = q$; par exemple $b_2\mu - q = g_0(b_2s - 2q) + g_1(b_2r - b_1q) = 0$, en remplaçant q par $q(2g_0 + b_1g_1 + b_2g_2)$. Donc $(p, q, r, s) = i(p, \mu)$.

(2) La condition passe à tout S : l'image de $1 = 2g_0 + b_1g_1 + b_2g_2$ est une relation du même type, et (1) s'applique. Réciproquement, si l'idéal $I = (2, b_1, b_2)$ n'est pas R, prenons $S = R/I$, qui n'est pas nul. Dans S, $2 = b_1 = b_2 = 0$, et le vecteur $U_2 = (0, 0, 1, 0)$ est invariant. S'il était $i(\lambda, \mu)$, sa coordonnée sur U_2 serait $\mu b_1 = 0$, et l'on aurait $1 = 0$ dans S.

(3) Avec $b_1 = X$, $b_2 = 0$, les relations deviennent $2q = 0$, $2r = Xs$. L'anneau $\mathbb{Z}[X]$ est intègre, donc $q = 0$ et i est injectif ($2\mu = 0$ entraîne $\mu = 0$). L'élément 2 est premier dans $\mathbb{Z}[X]$ et ne divise pas X ; de $2 \mid Xs$ on tire $s = 2\mu$, puis $r = X\mu$ en simplifiant par 2, et $(p, q, r, s) = i(p, \mu)$. Enfin, si $2g_0 + Xg_1 = 1$, le coefficient constant donne $2\, g_0(0) = 1$ dans $\mathbb{Z}$, ce qui est impossible. □

Remarque. La proposition de la page 85 tient en coordonnées sur tout anneau commutatif, dans les deux sens, sans changement de base, sans hypothèse de rang et sans la réduction au cas $2 = 0$ que la page annonce. Le noyau est engendré par les relations de Koszul de la suite unimodulaire $(2, b_2, b_1)$. Lorsque les deux algèbres sont séparables, l'identification du produit aux invariants de $\sigma_1 \otimes \sigma_2$ est énoncée par Voight (théorème 3.24 (iii)) [120] ; voir aussi Kanzaki et C. Small (1972), qu'il cite. Pour le corollaire de la page 86, la condition suffit sur R lui-même,

et la réciproque demande l'hypothèse de la page, « après toute changement de base » : l'exemple de $\mathbb{Z}[X]$ montre que l'isomorphisme sur R seul n'entraîne pas la condition. Un changement de base vers $R/(2, b_1, b_2)$ suffit. La formulation ponctuelle (en tout point de $V(2)$, l'un des $T_{i,0}$ engendre $L_{i,0}$) n'est pas démontrée ; elle équivaut à la condition en coordonnées dès que L_1, L_2 sont triviaux et munis de scindages, comme la page le dit aussi. Le passage de l'énoncé sur les coinvariants à l'énoncé sur les invariants par dualité n'est pas formalisé : les deux sont démontrés séparément, en coordonnées.

Extensions χ-scindées en coordonnées. Soit $\chi \in R$. On prend une extension scindée $0 \to L \to M \oplus L \to M \to 0$, $\alpha(\xi) = (0, \xi)$, $\psi(\eta, \xi) = \eta$, de R-modules quelconques. Un χ-scindage est un couple (π, ϖ), $\pi : M \oplus L \to L$, $\varpi : M \to M \oplus L$, avec $\pi\alpha = \chi$, $\psi\varpi = \chi$ et $\alpha\pi + \varpi\psi = \chi$ (page 169). Pour $b : M \to L$, on pose $\pi_b(\eta, \xi) = b(\eta) + \chi\xi$ et $\varpi_b(\eta) = (\chi\eta, -b(\eta))$. La transvection T_w, pour $w : M \to L$, est $(\eta, \xi) \mapsto (\eta, \xi + w(\eta))$. Le produit de deux objets $b_1 : M_1 \to L_1$ et $b_2 : M_2 \to L_2$ est $b_1 \otimes b_2 : M_1 \otimes M_2 \to L_1 \otimes L_2$ (page 78, « Il n'y a pas plus simple ! », et page 129). Pour $M = L = R$, un objet est un scalaire b, et l'objet unité est $b = 1$, $\pi(u, \lambda) = \lambda + \chi u$ (page 78).

Énoncé (Pages 77–79 et 123–131, extensions χ-scindées ♦).
1. *Le couple (π_b, ϖ_b) est un χ-scindage. Réciproquement, tout χ-scindage (π, ϖ) de $M \oplus L$ est de cette forme, avec $b = \pi|_M$.*
2. *Il existe un endomorphisme f de $M \oplus L$ induisant l'identité sur L et sur M et tel que $\pi_{b'} \circ f = \pi_b$ si et seulement si $b = b' + \chi w$ pour un $w : M \to L$; c'est alors T_w. On a aussi $T_w \circ \varpi_b = \varpi_{b'}$ et $T_w \circ T_{w'} = T_{w+w'}$.*
3. *(Page 129) Pour $u_i : M_i \to L_i$, $(b_1 + \chi u_1) \otimes (b_2 + \chi u_2) = b_1 \otimes b_2 + \chi u$ avec $u = b_1 \otimes u_2 + u_1 \otimes b_2 + \chi\, u_1 \otimes u_2$.*
4. *(Page 131) Si l'on change d'abord par u_i, puis par u_i' en partant de $b_i' = b_i + \chi u_i$, la somme des deux données est celle du changement par $u_i + u_i'$: $u'' = u + u'$.*
5. *(Page 78) Le produit est associatif, commutatif et unitaire : à travers les isomorphismes d'associativité et de commutativité des produits tensoriels, $(b_1 \otimes b_2) \otimes b_3$ correspond à $b_1 \otimes (b_2 \otimes b_3)$ et $b_1 \otimes b_2$ à $b_2 \otimes b_1$; à travers $R \otimes M \simeq M$ et $R \otimes L \simeq L$, $\mathrm{id}_R \otimes b$ correspond à b.*
6. *(Page 79) Pour $M = L = R$, disons $b \sim b'$ s'il existe $\varepsilon \in R^\times$ et $w \in R$ avec $\varepsilon b = b' + \chi w$ (un isomorphisme qui agit par ε sur L). La relation est compatible au produit, et la classe de b est inversible, c'est-à-dire $bb' \sim 1$ pour un b', si et seulement si $bR + \chi R = R$, si et seulement si b est inversible dans $R/\chi R$: la section $T_0 = -b_0$ engendre L_0 sur $V(\chi)$.*

Démonstration. (1) Les trois relations se vérifient sur $(\eta, 0)$ et $(0, \xi)$; par exemple $\alpha\pi_b(\eta, \xi) + \varpi_b(\eta) = (0, b\eta + \chi\xi) + (\chi\eta, -b\eta) = \chi(\eta, \xi)$. Si (π, ϖ) est un χ-scindage, $\pi(0, \xi) = \chi\xi$ donne $\pi = \pi_b$. La relation $\alpha\pi + \varpi\psi = \chi$ appliquée à $(\eta, 0)$ donne $\varpi(\eta) = \chi(\eta, 0) - (0, b\eta)$, et $\varpi = \varpi_b$.

(2) Si f induit l'identité sur L et sur M, alors $f(0, \xi) = (0, \xi)$ et la première coordonnée de $f(\eta, 0)$ est η, donc $f = T_w$ avec $w(\eta)$ la seconde coordonnée de $f(\eta, 0)$. On a $\pi_{b'}(T_w(\eta, \xi)) = b'\eta + \chi\xi + \chi w\eta = \pi_{b'+\chi w}(\eta, \xi)$, d'où la condition $b = b' + \chi w$, en évaluant en $(\eta, 0)$. Inversement T_w convient. Le calcul de $T_w \circ \varpi_b$ et de $T_w \circ T_{w'}$ est direct.

(3) et (4) Le produit tensoriel d'applications linéaires est bilinéaire ; on développe. Pour (4), on compare $u + u'$, où $u' = (b_1 + \chi u_1) \otimes u_2' + u_1' \otimes (b_2 + \chi u_2) + \chi\, u_1' \otimes u_2'$, avec $(b_1 \otimes (u_2 + u_2')) + ((u_1 + u_1') \otimes b_2) + \chi\, (u_1 + u_1') \otimes (u_2 + u_2')$; les deux développements ont les mêmes neuf termes.

(5) Ce sont la naturalité des isomorphismes d'associativité et de commutativité, qui sont dans mathlib, et un calcul sur les tenseurs purs pour l'unité.

(6) Si $\varepsilon_i b_i = b'_i + \chi w_i$, alors $\varepsilon_1\varepsilon_2 b_1 b_2 = b'_1 b'_2 + \chi(b'_1 w_2 + w_1 b'_2 + \chi w_1 w_2)$. Si $\varepsilon b b' = 1 + \chi w$, alors $b(\varepsilon b') + \chi(-w) = 1$. Si $bg + \chi h = 1$, alors $bg = 1 + \chi(-h)$, et $bg \sim 1$ avec $\varepsilon = 1$. Enfin $bR + \chi R = R$ équivaut à l'existence de g avec $bg \equiv 1$ modulo χR. □

Remarque. Seule la partie en coordonnées de la piste est démontrée, pour une extension scindée de modules quelconques, sans diviser par χ ni par 2. Le recollement de ces coordonnées en un produit $E_1 * E_2$ sur une base non affine et la compatibilité des contraintes entre elles (la quatrième compatibilité de la page 177 n'est pas écrite) ne le sont pas ; la construction par somme amalgamée et la propriété universelle des applications bi-affines (pages 68 à 76) sont démontrées sur une base affine à la fin de la section. La relation de cocycle de la page 131, que la page commence sans l'achever, est vraie avec les signes $b'_i = b_i + \chi u_i$. Le critère d'inversibilité de la note marginale de la page 79 est démontré dans le cas $L = M = R$ (pour L quelconque, voir le théorème de la fin de la section) : l'inverse de la classe de b est la classe de g dès que $bg \equiv 1$ modulo χ, et l'on n'a besoin d'aucune unité ε autre que 1 pour le construire.

Énoncé (Pages 125, 127 et 169, *produit poussé et produit tiré* ♦)**.** *En coordonnées, le produit poussé porte le χ-scindage de $b = b_1 \otimes b_2$ et le produit tiré celui de $-b$ (page 125).*

1. *Si $\gamma\chi = 2$, la transvection $T_{\gamma b}$ envoie le χ-scindage π_b sur π_{-b} : $\pi_{-b} \circ T_{\gamma b} = \pi_b$.*
2. *(Page 125, « commute ! », figure 6) Si $\gamma\chi = 2$, pour un changement de scindage qui remplace b par $b + \chi u$ du côté poussé et $-b$ par $-b - \chi u$ du côté tiré, $T_{\gamma b} \circ T_u = T_{-u} \circ T_{\gamma(b+\chi u)}$.*
3. *Pour les objets unités ($M = L = R$, $b_1 = b_2 = \mathrm{id}$), il existe un endomorphisme de $R \oplus R$ qui induit l'identité sur L et sur M et envoie le scindage poussé sur le scindage tiré si et seulement s'il existe γ avec $\gamma\chi = 2$. Sur $\mathbb{Z}$, avec $\chi = 4$, il n'en existe pas.*

Démonstration. (1) Par l'énoncé précédent, $\pi_{-b} \circ T_{\gamma b} = \pi_{-b+\chi\gamma b} = \pi_{-b+2b} = \pi_b$. (2) Les transvections se composent par addition : il faut $\gamma b + u = -u + \gamma b + \gamma\chi u$, ce qui est $\gamma\chi u = 2u$. (3) Par l'énoncé précédent, un tel endomorphisme existe si et seulement si $\mathrm{id} = -\mathrm{id} + \chi w$ pour un $w : R \to R$; en 1, cela donne $w(1)\chi = 2$, et inversement $w = \gamma\,\mathrm{id}$ convient. Sur $\mathbb{Z}$, $4\gamma = 2$ n'a pas de solution. □

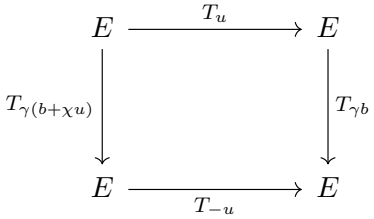


FIGURE 6 – Le carré « commute ! » de la page 125, point 2 de l'énoncé, pour $\gamma\chi = 2$. Les transvections T_w de l'extension E se composent par addition, et le carré commute parce que $\gamma b + u = -u + \gamma b + \gamma\chi u$. La transvection $T_{\gamma b}$ fait passer du χ-scindage b du produit poussé au scindage $-b$ du produit tiré (point 1) ; changer le scindage par u d'un côté et par $-u$ de l'autre ne change pas cette comparaison. Figure de l'édition ; Grothendieck dessine sur la même page deux cubes de suites $L_i \to E_i \to M_i$ (84, lot 7, p. 125).

Remarque. L'hypothèse $\gamma\chi = 2$, que la lecture prend à la page 127 pour l'isomorphisme de la page 169, est suffisante, et elle est nécessaire dès les objets unités, parmi les isomorphismes qui induisent l'identité sur $L_1 \otimes L_2$ et $M_1 \otimes M_2$: la comparaison demande que 2 soit multiple de χ. Le signe $-b$ du produit tiré est pris de la page 125 ; la construction du produit tiré comme produit fibré (page 169) et l'identification de la flèche du milieu du diagramme de la page 167 avec l'opérateur F_{11} ne sont pas formalisées.

Ne sont pas démontrés ici : l'équivalence de catégories fibrées du théorème de la page 48 sur une base non affine et le lien de la page 45 entre algèbres et triplets (L, P_1, Q) pour L non trivial (le cas L inversible sur une base affine, les changements de base et la reconstruction des pages 49 à 52 sont démontrés à la fin de la section), la construction intrinsèque du produit $X_1 * X_2$ et des extensions χ-scindées sur une base non affine (sur une base affine, la somme amalgamée des pages 68 à 70 et la propriété universelle des pages 75 et 76 sont démontrées à la fin de la section), la construction du produit tiré comme produit fibré et l'opérateur F_{11} (pages 141 à 169), l'unicité de la forme quadratique du théorème de la page 89, la formulation ponctuelle de la proposition de la page 85 et du corollaire de la page 86, l'énoncé du corollaire pour $\underline{\mathrm{Hom}}(-, M)$, le passage des coinvariants aux invariants par dualité, la trace et la norme de $A_1 \otimes A_2$ sur A (pages 104 et 105), la quatrième partie du dossier et le reste de la troisième.
Le cas L inversible, sur une base affine. Sur $X = \operatorname{Spec} R$, la page 45 décrit un revêtement quadratique par un triplet (L, P_1, Q) : L inversible, P_1 un torseur sous L et $Q : P_1 \to L^{\otimes 2}$ une fonction polynôme de degré 2 de partie homogène $u \mapsto u^2$. Sur une base affine le torseur est trivial ; le choix d'une origine x_0 identifie P_1 à L et écrit $Q(x_0 + u) = u \otimes u + b \otimes u + c$, avec $b = 2x_0 - T \in L$ et $c \in L \otimes L$ (`qform`). Un morphisme $(L, b, c) \to (L', b', c')$ est un isomorphisme $\varphi : L \to L'$ accompagné de l'application de torseurs $x_0 + u \mapsto x'_0 + t + \varphi(u)$, $t \in L'$, qui transporte Q sur Q' : $Q'(t + \varphi u) = (\varphi \otimes \varphi)(Q(u))$ pour tout u (`IsCoverHom`). Le triplet associé est (L, δ, T_0) avec $\delta = b \otimes b - 4c$ (`discL`) et T_0 la classe de b dans $L/2L = \Gamma(V(2), L_0)$; la condition $T_0^2 \equiv \delta \bmod 4$ dit qu'un relèvement τ de T_0 vérifie $\tau \otimes \tau - \delta \in 4\,(L \otimes L)$ (`TripletCond`). Un morphisme de triplets est un isomorphisme φ avec $(\varphi \otimes \varphi)(\delta) = \delta'$ et $\varphi_0(T_0) = T'_0$, où $\varphi_0 : L/2L \to L'/2L'$ est induit par φ (`mod2`).

Théorème 45.2 (Grothendieck, pages 45 à 53, classification par triplets, base affine ⧫)**.** *Soit R un anneau commutatif, et L, L' des R-modules inversibles.*

1. *Sur tout R, (φ, t) est un morphisme si et seulement si $\varphi(b) = b' + 2t$ et $(\varphi \otimes \varphi)(c) = c' + b' \otimes t + t \otimes t$; les morphismes forment un groupoïde, d'identité $(\mathrm{id}, 0)$, de composé $(\psi, s) \circ (\varphi, t) = (\psi\varphi, s + \psi t)$ et d'inverse $(\varphi^{-1}, -\varphi^{-1}t)$.*
2. *(Page 47) Sur tout R, (L, δ, T_0) vérifie $T_0^2 \equiv \delta \bmod 4$, et la condition ne dépend pas du relèvement τ choisi. Un morphisme (φ, t) de revêtements est un morphisme de triplets.*
3. *(Page 48) Supposons que 2 ne divise pas zéro dans R. Tout morphisme de triplets φ se relève en un unique morphisme (φ, t) de revêtements. Tout triplet (L, δ, T_0) avec $T_0^2 \equiv \delta \bmod 4$ provient d'un revêtement de même L, et cela vaut sur tout R. Le foncteur $(L, b, c) \mapsto (L, \delta, T_0)$ est donc une équivalence de groupoïdes ; en particulier deux revêtements sont isomorphes si et seulement si leurs triplets le sont.*

Démonstration. On utilise deux faits sur un module inversible L. D'abord $L \otimes L$ est symétrique : $x \otimes y = y \otimes x$ (`Module.Invertible.tmul_comm` de mathlib, par localisation en un idéal maximal, où L devient libre de rang 1). C'est ce qui donne un sens au produit $b\,u$ de la page. Ensuite, si $x \otimes w = 0$ pour tout $w \in L$, alors $x = 0$ (`eq_zero_of_tmul_eq_zero`) : on écrit $1 = \sum \gamma_i(w_i)$

avec $\gamma_i \in L^\vee$, ce que permet l'inversibilité, et l'on applique $\mathrm{id} \otimes \gamma_i$ à $x \otimes w_i = 0$, d'où $x = \sum \gamma_i(w_i)\, x = 0$.

(1) En $u = 0$, la condition donne $t \otimes t + b' \otimes t + c' = (\varphi \otimes \varphi)(c)$. En $u = \varphi^{-1}(w)$, les termes en $w \otimes w$ et les termes constants se simplifient, et il reste, par symétrie, $(\varphi(b) - b' - 2t) \otimes w = 0$ pour tout w, donc $\varphi(b) = b' + 2t$. La réciproque se vérifie en développant. Pour le composé, $s + \psi t + \psi\varphi u = s + \psi(t + \varphi u)$, et $(\psi \otimes \psi)(\varphi \otimes \varphi) = \psi\varphi \otimes \psi\varphi$. Pour l'inverse, on applique la condition à $u = -\varphi^{-1}t + \varphi^{-1}w$ et l'on compose par $\varphi^{-1} \otimes \varphi^{-1}$ (`isCoverHom_iff`, `isCoverHom_refl`, `isCoverHom_trans`, `isCoverHom_symm`).

(2) Le relèvement $\tau = b$ donne $b \otimes b - \delta = 4c$. Si $\tau' = \tau - 2a$, la symétrie donne $\tau' \otimes \tau' - \tau \otimes \tau = 4(a \otimes a - \tau \otimes a)$. Si $\varphi(b) = b' + 2t$ et $(\varphi \otimes \varphi)(c) = c' + b' \otimes t + t \otimes t$, alors

$$(\varphi \otimes \varphi)(\delta) = (b' + 2t) \otimes (b' + 2t) - 4(c' + b' \otimes t + t \otimes t) = b' \otimes b' - 4c' = \delta',$$

et $\varphi(b) - b' = 2t \in 2L'$ (`tripletCond_iff_forall`, `tripletCond_discL`, `isCoverHom_triplet`).

(3) Un module inversible est projectif, donc facteur direct d'un module libre ; si 2 est régulier dans R, il l'est sur tout module libre, donc sur L' et sur $L' \otimes L'$, qui est inversible (`two_smul_injective_of_projective`). Soit φ un morphisme de triplets. La condition sur T_0 donne t avec $\varphi(b) = b' + 2t$. Alors

$$4\,(\varphi \otimes \varphi)(c) = \varphi(b) \otimes \varphi(b) - \delta' = (b' + 2t) \otimes (b' + 2t) - b' \otimes b' + 4c' = 4\,(c' + b' \otimes t + t \otimes t),$$

et l'on simplifie par 4 : (φ, t) est un morphisme par (1). Si (φ, t') en est un autre, $2t = 2t'$, donc $t = t'$. Enfin, si τ relève T_0 et $\tau \otimes \tau - \delta = 4k$, le revêtement (L, τ, k) a pour triplet (L, δ, T_0) ; c'est la formule $c = (\tau^2 - \delta)/4$ de la page, sans division (`triplet_full_faithful`, `triplet_ess_surj`, `triplet_classification`, `cover_iso_iff_triplet_iso`). □

Remarque. Le cas L non trivial ne demande rien de plus que le cas libre, une fois les produits $b\,u$ lus dans $L \otimes L$: la symétrie de $L \otimes L$ remplace la commutativité de R, et la projectivité de L et de $L \otimes L$ transporte la régularité de 2. Comme dans le cas libre, l'hypothèse sur 2 ne sert qu'à la pleine fidélité, et l'exemple de $\mathbb{F}_2$ montre qu'elle est nécessaire ; la surjectivité essentielle vaut sur tout anneau. Seule la symétrie utilise le rang 1 : pour le sens « morphisme de revêtements ⇒ morphisme de triplets », il suffit que L' soit inversible. L'énoncé démontré porte sur les triplets (L, P_1, Q) de la page 45, l'origine de P_1 choisie, sur une base affine.

Changement de base. Soit $R \to S$ un morphisme d'anneaux commutatifs. Pour un R-module L, on note $L_S = S \otimes_R L$, $b_S = 1 \otimes b$ pour $b \in L$, et $c \mapsto c_S$ l'application R-linéaire $L \otimes_R L \to L_S \otimes_S L_S$, $x \otimes y \mapsto (1 \otimes x) \otimes (1 \otimes y)$ (`bc2`) ; pour $\varphi : L \simeq L'$, $\varphi_S = \mathrm{id}_S \otimes \varphi$.

Énoncé (Pages 45 à 48, *compatibilité aux changements de base* ⧫)**.** *Soit $R \to S$ un morphisme d'anneaux commutatifs, L, L' des R-modules, L' inversible.*

1. *$\delta(b_S, c_S) = \delta(b, c)_S$; si $\tau \otimes \tau - \delta \in 4\,(L \otimes L)$ pour un relèvement τ de T_0, alors $\tau_S \otimes \tau_S - \delta_S \in 4\,(L_S \otimes L_S)$: la condition $T_0^2 \equiv \delta \bmod 4$ passe à S.*
2. *Si (φ, t) est un morphisme de revêtements $(L, b, c) \to (L', b', c')$, alors (φ_S, t_S) est un morphisme $(L_S, b_S, c_S) \to (L'_S, b'_S, c'_S)$. Si φ est un morphisme de triplets, φ_S en est un.*

Le foncteur $(L, b, c) \mapsto (L, \delta, T_0)$ commute donc aux changements de base, sur les objets et sur les morphismes.

Démonstration. L'application $c \mapsto c_S$ est bien définie : $(1 \otimes rx) \otimes (1 \otimes y) = r\,(1 \otimes x) \otimes (1 \otimes y)$, le scalaire r agissant sur $L_S \otimes_S L_S$ par son image dans S. Par récurrence sur les tenseurs, elle commute à $\varphi \otimes \varphi$: $((\varphi \otimes \varphi)\,c)_S = (\varphi_S \otimes \varphi_S)(c_S)$. (1) Par linéarité, $(b \otimes b - 4c)_S = b_S \otimes b_S - 4c_S$; si $\tau' - \tau = 2a$, alors $\tau'_S - \tau_S = 2a_S$, et $\tau \otimes \tau - \delta = 4k$ donne $\tau_S \otimes \tau_S - \delta_S = 4k_S$. (2) L'_S est inversible sur S (mathlib), et l'on applique le critère en coordonnées du théorème précédent sur S : $\varphi_S(b_S) = (\varphi b)_S = b'_S + 2t_S$ et $(\varphi_S \otimes \varphi_S)(c_S) = ((\varphi \otimes \varphi)c)_S = c'_S + b'_S \otimes t_S + t_S \otimes t_S$. Pour un morphisme de triplets, $(\varphi_S \otimes \varphi_S)(\delta_S) = ((\varphi \otimes \varphi)\delta)_S = \delta'_S$, et $\varphi(\tau) - \tau' = 2a$ donne $\varphi_S(\tau_S) - \tau'_S = 2a_S$ (`discL_baseChange`, `tripletCond_baseChange`, `isCoverHom_baseChange`, `tripletHom_baseChange`). □

La reconstruction des pages 49 à 52. Dans le cas libre, $A = A(b,c)$, $\delta = b^2 - 4c$, et Tr, N sont la trace et la norme de A sur R (celles de mathlib, `Algebra.trace` et `Algebra.norm`). Pour $y = a + eU \in A$, on pose $\beta = \mathrm{Tr}(y)$ et $\gamma = e$, de sorte que $y = (\beta + \gamma z)/2$ avec $z = 2U + b$, $z^2 = \delta$ (`recon`) ; pour $x \in E = \check{A}$, on pose $\lambda = \psi(x) = x(1)$ et $\zeta = (2x - \lambda\,\mathrm{Tr})(U) = 2x(U) + \lambda b$, la coordonnée de $2x - \psi(x)T \in L$ (`eCoord`). La fonction de la page 45, dans le scindage $x_0 = (1,0)$, est $Q(x) = x(U)^2 + b\,x(1)x(U) + c\,x(1)^2$, c'est-à-dire $Q(x_0 + u) = u^2 + bu + c$ (`qE`), et $\varphi_N(y) = \mathrm{Tr}(y)\,\mathrm{Tr} - \mathrm{Tr}(y\,\cdot)$ est la forme polaire de la norme (`phiN`).

Théorème 45.3 (Grothendieck, pages 46 et 49 à 52, reconstruction de E, A, de la trace, de la norme et du produit ⧫). *Soit R un anneau commutatif et $b, c \in R$.*

1. $\mathrm{Tr}(a + eU) = 2a - eb$ *et* $N(a + eU) = a^2 - abe + ce^2$.
2. *(Page 49) Sur tout R, les couples (β, γ) des éléments de A sont ceux qui vérifient $\beta \equiv \gamma b$ modulo 2, et les couples (λ, ζ) des éléments de E ceux qui vérifient $\zeta \equiv \lambda b$ modulo 2 ; b est un relèvement de T_0. Si 2 est régulier, $y \mapsto (\beta, \gamma)$ et $x \mapsto (\lambda, \zeta)$ sont injectives.*
3. *(Pages 50 et 51) L'unité a pour couple $(2, 0)$, et, sans division,*
$$2\beta(yy') = \beta\beta' + \gamma\gamma'\delta, \qquad 2\gamma(yy') = \beta\gamma' + \gamma\beta', \qquad 4N(y) = \beta^2 - \gamma^2\delta.$$
4. *(Pages 50 et 52)* $2\,x(y) = \lambda\beta + \gamma\zeta$, *et* $4Q(x) = \zeta^2 - \lambda^2\delta$.
5. *(Pages 46 et 50) $\varphi_N(y)$ a pour couple $(\beta, -\gamma\delta)$, et $Q(\varphi_N(y)) = -N(y)\,\delta$.*
6. *(Pages 49 à 52, L inversible) Soit $\tau \in L$ et $\delta \in L \otimes L$ avec $\tau \otimes \tau - \delta \in 4\,(L \otimes L)$, et (β, γ), $(\beta', \gamma') \in R \times \check{L}$ avec $\beta \equiv \gamma(\tau)$ et $\beta' \equiv \gamma'(\tau)$ modulo 2. Alors $\beta^2 - \gamma^2\delta \in 4R$, $\beta\beta' + \gamma\gamma'\delta \in 2R$ et $\beta\gamma' + \beta'\gamma \in 2\check{L}$; si 2 est régulier, des moitiés β'', γ'' de ces deux derniers vérifient encore $\beta'' \equiv \gamma''(\tau)$ modulo 2. Si $\zeta \in L$ et $\zeta \equiv \lambda\tau$ modulo $2L$, alors $\zeta \otimes \zeta - \lambda^2\delta \in 4\,(L \otimes L)$.*

Démonstration. (1) Dans la base $(1, U)$, la multiplication par $y = a + eU$ envoie 1 sur $a + eU$ et U sur $-ec + (a - eb)U$, puisque $U^2 = -bU - c$; la trace et le déterminant de la matrice $\begin{pmatrix} a & -ec \\ e & a - eb \end{pmatrix}$ sont $2a - eb$ et $a^2 - abe + ce^2$ (`trace_qalg`, `norm_qalg`). (2) $\beta = 2a - eb = eb + 2(a - eb)$; inversement, si $\beta = \gamma b + 2s$, l'élément $(s + \gamma b) + \gamma U$ convient. Si $\beta = \gamma = 0$, alors $2a = 0$, donc $a = 0$ quand 2 est régulier. Du côté de E, $\mathrm{Tr}(U) = -b$ donne $\zeta = 2x(U) + \lambda b$; la forme $\lambda\,1^\vee + s\,U^\vee$ a pour couple $(\lambda, \lambda b + 2s)$, et x est connu par $x(1)$ et $x(U)$ (`recon_range`, `recon_injective`, `eCoord_range`, `eCoord_injective`). (3) à (5) Ce sont des identités entre polynômes en a, e, a', e', b, c et $x(1), x(U)$, une fois écrits $yy' = (aa' - ee'c) + (ae' + a'e - ee'b)U$, $\varphi_N(y)(1) = 2a - eb$ et $\varphi_N(y)(U) = 2ec - ab$ (`recon_one`, `recon_mul`, `recon_norm`, `coupling`, `four_qE`, `phiN_`

`coords`). (6) On écrit $\beta = \gamma(\tau) + 2s$, $\beta' = \gamma'(\tau) + 2s'$, $\delta = \tau \otimes \tau - 4k$, et $\gamma\gamma'\delta$ pour $(\gamma \otimes \gamma')(\delta)$. Alors $\beta^2 - \gamma^2\delta = 4(\gamma(\tau)s + s^2 + \gamma^2 k)$ et $\beta\beta' + \gamma\gamma'\delta = 2(\gamma(\tau)\gamma'(\tau) + s\gamma'(\tau) + s'\gamma(\tau) + 2ss' - 2\gamma\gamma' k)$. La symétrie de $\check{L} \otimes \check{L}$, à laquelle on applique $f \otimes g \mapsto g(\tau)f$, donne $\gamma'(\tau)\gamma = \gamma(\tau)\gamma'$, d'où $\beta\gamma' + \beta'\gamma = 2(\gamma(\tau)\gamma' + s\gamma' + s'\gamma)$. Évaluée en τ, la seconde moitié donne $2\gamma''(\tau) = \beta\gamma'(\tau) + \beta'\gamma(\tau)$, et $2(\beta'' - \gamma''(\tau)) = 4(ss' - \gamma\gamma' k)$; on simplifie par 2. Enfin, si $\zeta = \lambda\tau + 2a$, la symétrie $a \otimes \tau = \tau \otimes a$ donne $\zeta \otimes \zeta - \lambda^2\delta = 4(\lambda^2 k + \lambda\,\tau \otimes a + a \otimes a)$ (`div_norm`, `div_prod_fst`, `div_prod_snd`, `div_prod_mem`, `div_qform`). □

Remarque. Chaque division des pages 49 à 52 est donc légitime, comme la page le vérifie « à chaque étape », et dans le cas libre la description de A et de E par les couples (β, γ) et (λ, ζ) redonne l'algèbre, sa trace, sa norme et son produit. Le signe de $Q(\varphi_N(x)) = -N(x)\,\delta$, couvert page 46 et écrit $+$ page 52, est confirmé. Pour L non trivial, seule la légitimité des divisions et la stabilité du produit sont démontrées ; que les couples (β, γ) forment un anneau isomorphe à l'algèbre du revêtement ne l'est pas, faute de l'équivalence de la page 45.

Énoncé (Pages 45 et 48, *la forme globale* ♦). *Sur un schéma ou un topos localement annelé où 2 n'est pas diviseur de zéro, la catégorie fibrée des revêtements quadratiques est équivalente à celle des triplets (L, P_1, Q) (page 45), donc à celle des triplets (L, δ, T_0), compatiblement aux changements de base.* ◊ non vérifié en Lean

Ne sont pas démontrés : l'équivalence de la page 45 entre algèbres quadratiques localement libres de rang 2 et triplets (L, P_1, Q), quand L n'est pas trivial (le cas libre est l'énoncé des pages 47 à 53 ci-dessus) ; elle demande que $\mathcal{O} \to A$ soit scindé et que $A/\mathcal{O}$ soit inversible, ce qui n'est pas formalisé ; le passage d'une base affine à un schéma, où P_1 n'a plus d'origine globale et les morphismes se recollent. La compatibilité aux changements de base entre bases affines est démontrée plus haut ; c'est le recollement qui manque pour en faire une équivalence de catégories fibrées sur un schéma.

La catégorie des extensions χ-scindées. On reprend les coordonnées ci-dessus, sur un anneau commutatif R et pour $\chi \in R$. Un objet est un triplet (M, L, b), $b : M \to L$ linéaire, c'est-à-dire l'extension scindée $0 \to L \to M \oplus L \to M \to 0$ munie du χ-scindage (π_b, ϖ_b) (`ChiExt`). Un morphisme $(M, L, b) \to (M', L', b')$ est un triplet (f, φ, w), $f : M \to M'$, $\varphi : L \to L'$, $w : M \to L'$, avec $\varphi \circ b = b' \circ f + \chi w$; il représente l'application $F(\eta, \xi) = (f\eta, \varphi\xi + w\eta)$ de $M \oplus L$ dans $M' \oplus L'$. Le composé de (f, φ, w) puis (g, ψ, v) est $(gf, \psi\varphi, \psi w + vf)$. Le produit est $(M_1 \otimes M_2, L_1 \otimes L_2, b_1 \otimes b_2)$ (page 78), celui de deux morphismes est $(f_1 \otimes f_2, \varphi_1 \otimes \varphi_2, w)$ avec $w = b_1' f_1 \otimes w_2 + w_1 \otimes b_2' f_2 + \chi\, w_1 \otimes w_2$, la donnée u de la page 129 ; l'unité est (R, R, id), $\pi(u, \lambda) = \lambda + \chi u$. Les contraintes d'associativité, d'unité et de commutativité sont celles du produit tensoriel sur M et sur L, avec $w = 0$.

Théorème 45.4 (Grothendieck, pages 65 à 79, produit des extensions χ-scindées, base affine ♦). *Soit R un anneau commutatif et $\chi \in R$.*

1. *Une application linéaire $F : M \oplus L \to M' \oplus L'$ qui induit f sur M et φ sur L est de la forme $(\eta, \xi) \mapsto (f\eta, \varphi\xi + w\eta)$; elle respecte les χ-rétractions, $\pi_{b'} F = \varphi \pi_b$, si et seulement si $\varphi b = b' f + \chi w$, et de même pour les χ-sections, $F\varpi_b = \varpi_{b'} f$.*
2. *Les extensions scindées munies d'un χ-scindage, avec ces morphismes et le produit $b_1 \otimes b_2$, forment une catégorie monoïdale symétrique.*
3. *Un morphisme (f, φ, w) est un isomorphisme dès que f et φ en sont.*
4. *(Page 79) Soit L un R-module et $b \in L$. L'objet (R, L, b) est inversible pour le produit,*

c'est-à-dire $(R, L, b) * Y \simeq (R, R, \mathrm{id})$ pour un objet Y, si et seulement si L est un module inversible et b engendre L modulo χ, $L = Rb + \chi L$, c'est-à-dire si la section $T_0 = -b_0$ engendre $L_0 = L/\chi L$ sur $V(\chi)$.

Démonstration. (1) $F(0,\xi) = (0, \varphi\xi)$, et la première coordonnée de $F(\eta, 0)$ est $f\eta$; on pose $w\eta$ la seconde. Alors $\pi_{b'} F(\eta,\xi) = b' f\eta + \chi\varphi\xi + \chi w\eta$ et $\varphi\pi_b(\eta,\xi) = \varphi b\eta + \chi\varphi\xi$; de même $F\varpi_b(\eta) = (\chi f\eta, -\varphi b\eta + \chi w\eta)$ et $\varpi_{b'}(f\eta) = (\chi f\eta, -b' f\eta)$ (`eq_extMap`, `extMap_pi_iff`, `extMap_varpi_iff`).

(2) Le composé est un morphisme : $\psi\varphi b = \psi(b'f + \chi w) = (b''g + \chi v)f + \chi\,\psi w = b''(gf) + \chi(\psi w + vf)$. Le produit de deux morphismes en est un : $(b_1 \otimes b_2)(\varphi_1 \otimes \varphi_2) = (b_1' f_1 + \chi w_1) \otimes (b_2' f_2 + \chi w_2)$, qu'on développe par bilinéarité de $\otimes$ sur les morphismes, ce qui donne $(b_1' \otimes b_2')(f_1 \otimes f_2) + \chi w$: c'est le calcul de la page 129, sans division. Les axiomes portent sur trois composantes. Sur M et sur L, ce sont ceux de la catégorie monoïdale symétrique des R-modules (`ModuleCat` de mathlib). Sur w, il reste deux identités. La fonctorialité du produit, $(p_1 \otimes p_2)(q_1 \otimes q_2) = p_1 q_1 \otimes p_2 q_2$, se ramène, après avoir remplacé $b_i'\varphi_i'$ par $f_i' b_i'' + \chi w_i'$, à l'égalité de deux sommes de huit termes. La naturalité de l'associativité développe les deux membres en sept termes $(x_1 \otimes x_2) \otimes x_3$ et $x_1 \otimes (x_2 \otimes x_3)$, $x_i \in \{b_i' f_i, w_i\}$, que l'associativité du produit tensoriel identifie. Toutes les autres identités, pentagone, triangle, hexagones, symétrie, n'ont que des w nuls (`ChiExt.instMonoidalCategory`, `ChiExt.instSymmetricCategory`, avec `tensorHom_comp_tensorHom'` et `associator_naturality'`).

(3) Si f et φ sont inversibles, $(f^{-1}, \varphi^{-1}, -f^{-1} w \varphi^{-1})$ est un morphisme, en composant $\varphi b = b' f + \chi w$ par f^{-1} et φ^{-1}, et c'est l'inverse : les composantes w des deux composés sont $w\varphi^{-1} - w\varphi^{-1} = 0$ et $-f^{-1}w + f^{-1}w = 0$ (`ChiExt.isIso_of`).

(4) Nécessité. Soit $Y = (M', L', b')$ et (f, φ, w) un isomorphisme $(R, L, b) * Y \to (R, R, \mathrm{id})$. Sa composante $\varphi : L \otimes L' \to R$ est un isomorphisme, donc L est inversible (`Module.Invertible.left` de mathlib). Sa composante $f : R \otimes M' \to R$ est surjective : il existe m' avec $f(1 \otimes m') = 1$. Posons $y = b'(m')$; la relation $\varphi(b \otimes b') = f + \chi w$, évaluée en $1 \otimes m'$, donne $\varphi(b \otimes y) = 1 + \chi c$. Pour $x \in L$, la symétrie $x \otimes b = b \otimes x$ de $L \otimes L$ (`Module.Invertible.tmul_comm`), à laquelle on applique $u \otimes v \otimes y \mapsto \varphi(v \otimes y)\, u$, donne $(1 + \chi c)\, x = \varphi(x \otimes y)\, b$, donc $x = \varphi(x \otimes y)\, b + \chi(-cx) \in Rb + \chi L$. Suffisance. Écrivons $1 = \sum \gamma_i(x_i)$ avec $\gamma_i \in L^\vee$, ce que permet l'inversibilité de L, et $x_i = r_i b + \chi y_i$. Alors $\beta = \sum r_i \gamma_i$ vérifie $\beta(b) = 1 - \chi \sum \gamma_i(y_i) = 1 + \chi c$. (Lean le dit sans choisir de somme : l'idéal $\beta(b)$, $\beta \in L^\vee$, plus χR, contient l'image de l'accouplement $L^\vee \otimes L \to R$, qui est R.) Soit $Y = (R, L^\vee, 1 \mapsto \beta)$. Le morphisme $(R \otimes R \simeq R,\ L \otimes L^\vee \simeq R,\ c \cdot (R \otimes R \simeq R))$ vérifie la relation, puisque $(rb) \otimes (s\beta) \mapsto rs\,\beta(b) = rs + \chi\, c\, rs$, et c'est un isomorphisme par (3). Enfin $L = Rb + \chi L$ équivaut à ce que la classe de b engendre $L/\chi L$ (`ChiExt.invertible_iff_generates`, `generates_iff_span`, `ChiExt.invertible_iff_span`). □

Remarque. La note marginale de la page 79 dit « L inversible et T_0 base de L_0 » ; la preuve ci-dessus montre que l'inversibilité de L est nécessaire, et qu'avec elle il suffit que b engendre L modulo χ : on n'a pas à localiser, ni à rendre b unitaire hors de $V(\chi)$ comme le fait la lecture. L'inverse est $(R, L^\vee, \beta)$ pour toute forme β avec $\beta(b) \equiv 1$ modulo χ ; pour $L = R$, c'est la classe de g avec $bg \equiv 1$ de l'énoncé précédent. Rien n'est divisé par χ ni par 2, et χ peut être nul : pour $\chi = 0$, l'objet est inversible si et seulement si b est une base de L. Le critère n'utilise que les objets dont le quotient est R, qui sont tous scindés sur une base affine.

Le produit intrinsèque, sur une base affine. Une extension χ-trivialisée de $\mathcal{O}$ par L est la donnée de $\iota : L \to E$, $\psi : E \to R$ et $\pi : E \to L$ linéaires avec $\psi\iota = 0$ et $\pi\iota = \chi$ (`ChiTriv`) ; rien

n'est scindé, et l'exactitude n'est supposée que là où elle sert. Pour deux d'entre elles, on pose $K = (L_1 \otimes E_2) \oplus (E_1 \otimes L_2)$, d'image $E_1 \otimes_0 E_2$ dans $E_1 \otimes E_2$ par $j = (\iota_1 \otimes \mathrm{id}, \mathrm{id} \otimes \iota_2)$, et $\mu = (\mathrm{id} \otimes \pi_2, \pi_1 \otimes \mathrm{id}) : K \to L_1 \otimes L_2$ (page 68). Le produit est le quotient

$$E_1 * E_2 = \big((E_1 \otimes E_2) \oplus (L_1 \otimes L_2)\big)/\{(j(k), -\mu(k))\},$$

où $x_1 * x_2$ est la classe de $(x_1 \otimes x_2, 0)$ (`Amal`, `starA`, `incl`).

Théorème 45.5 (Grothendieck, pages 68 à 76, le produit par somme amalgamée, base affine ♦). *Soit R un anneau commutatif et $\chi \in R$.*

1. *$E_1 * E_2$ est la somme amalgamée de $E_1 \otimes E_2$ et de $L_1 \otimes L_2$ le long de K, dans la catégorie des R-modules. Elle porte, sans division et sans scindage, $\psi(x_1 * x_2) = \psi_1(x_1)\psi_2(x_2)$, l'application $L_1 \otimes L_2 \to E_1 * E_2$ et la χ-rétraction $\pi(x_1 * x_2) = \pi_1(x_1) \otimes \pi_2(x_2)$, $\pi = \chi$ sur $L_1 \otimes L_2$ (page 70) : c'est une extension χ-trivialisée.*
2. *(Pages 72 à 74) $u_1 * x_2 = u_1 \otimes \pi_2(x_2)$, $x_1 * u_2 = \pi_1(x_1) \otimes u_2$, et $(x_1 + u_1) * (x_2 + u_2) = x_1 * x_2 + u_1 \otimes \pi_2(x_2) + \pi_1(x_1) \otimes u_2 + \chi\, u_1 \otimes u_2$.*
3. *Toute suite exacte $0 \to L \to E \to R \to 0$ est scindée. Pour des scindages x_1, x_2, de rétractions p_1, p_2, on a $E_1 * E_2 \simeq R \times (L_1 \otimes L_2)$, avec ψ la première projection, $L_1 \otimes L_2$ le second facteur et $\pi(\lambda, u) = \lambda\, b_1 \otimes b_2 + \chi u$, $b_i = \pi_i(x_i)$. En particulier $0 \to L_1 \otimes L_2 \to E_1 * E_2 \to R \to 0$ est exacte, scindée par $x_1 * x_2$, et $b = b_1 \otimes b_2$ (page 78) : c'est le produit $(\mathcal{O}, L_1, b_1) \otimes (\mathcal{O}, L_2, b_2)$ de la catégorie des extensions χ-scindées ci-dessus.*
4. *(Pages 75 et 76) Soit N un R-module, $f : P_1 \times P_2 \to N$, où $P_i = \psi_i^{-1}(1)$, et $\alpha : L_1 \otimes L_2 \to N$ linéaire, avec*

$$f(x_1 + u_1, x_2) = f(x_1, x_2) + \alpha(u_1 \otimes \pi_2(x_2)),$$
$$f(x_1, x_2 + u_2) = f(x_1, x_2) + \alpha(\pi_1(x_1) \otimes u_2).$$

Si les extensions sont exactes, il existe une unique application linéaire $g : E_1 * E_2 \to N$ avec $g(x_1 * x_2) = f(x_1, x_2)$ sur $P_1 \times P_2$ et $g = \alpha$ sur $L_1 \otimes L_2$. Réciproquement, toute application linéaire g définit ainsi un tel couple (f, α).

Démonstration. (1) Une application linéaire hors du quotient est un couple (g, h) avec $g \circ j = h \circ \mu$; c'est la propriété universelle de la somme amalgamée, et le cocône correspondant est colimite dans `ModuleCat` (`isPushout`). Le couple $(\psi_1 \otimes \psi_2, 0)$ convient, puisque $\psi_i \iota_i = 0$; le couple $(\pi_1 \otimes \pi_2, \chi)$ aussi, puisque $\pi_1\iota_1(u_1) \otimes \pi_2(x_2) = \chi\, u_1 \otimes \pi_2(x_2) = \chi\, \mu(u_1 \otimes x_2)$, et de même de l'autre côté. (2) C'est la relation $(j(k), -\mu(k)) = 0$ pour $k = u_1 \otimes x_2$ et $k = x_1 \otimes u_2$, puis la bilinéarité. (3) Si $\psi(x_0) = 1$, l'endomorphisme $e \mapsto e - \psi(e)x_0$ est à valeurs dans $\ker \psi = \iota(L)$, et l'on en tire la rétraction p (`ChiTriv.splittingOf`) ; alors $e = \iota p(e) + \psi(e)x_0$ et $\pi = \chi p + \psi\, b$. L'application $e_1 \otimes e_2 \mapsto (\psi_1(e_1)\psi_2(e_2),\ p_1(e_1) \otimes \pi_2(e_2) + \psi_1(e_1)\, b_1 \otimes p_2(e_2))$, avec l'identité sur $L_1 \otimes L_2$, passe au quotient : sur $e_1 \otimes \iota_2 u_2$, la seconde coordonnée vaut $(\chi p_1(e_1) + \psi_1(e_1)b_1) \otimes u_2 = \pi_1(e_1) \otimes u_2$. Son inverse est $(\lambda, u) \mapsto \lambda\, x_1 * x_2 + u$: par (2), $e_1 * e_2 = \psi_1(e_1)\psi_2(e_2)\, x_1 * x_2 + p_1(e_1) \otimes \pi_2(e_2) + \psi_1(e_1)\, b_1 \otimes p_2(e_2)$. On lit ψ, ι et π dans ces coordonnées ; l'identification avec le produit de la catégorie précédente est $R \otimes R \simeq R$ sur M et l'identité sur $L_1 \otimes L_2$ (`splitEquiv`, `split_coords`, `prod_exact`, `prodSplitting_b`, `ChiExt.ofSectionTensorIso`). (4) Existence : $g(\lambda, u) = \lambda f(x_1, x_2) + \alpha(u)$ dans les coordonnées de (3) ;

pour $y_i = x_i + \iota_i p_i(y_i)$ dans P_i, les deux relations donnent $f(y_1, y_2) = f(x_1, x_2) + \alpha(b_1 \otimes p_2(y_2)) + \alpha(p_1(y_1) \otimes \pi_2(y_2))$, qui est $g(y_1 * y_2)$. Unicité : par la formule de (3) pour $e_1 * e_2$, g est connu par $g(x_1 * x_2) = f(x_1, x_2)$ et par α. La réciproque est (2) (`biaffine_universal`, `biaffine_of_linear`). □

Remarque. La construction de la page 68 est démontrée telle quelle, sans division et sans choisir de scindage, pour χ quelconque, nul ou diviseur de zéro ; sur une base affine, toute extension de $\mathcal{O}$ est scindée, et le produit intrinsèque y coïncide avec le produit en coordonnées $b_1 \otimes b_2$, ce qui transporte au produit intrinsèque la structure de catégorie monoïdale symétrique démontrée plus haut. La remarque de la page 76, que la donnée de α n'est pas superflue, se retrouve dans l'énoncé : g est déterminé par f et α ensemble, μ n'étant pas surjectif en général. La variante de la page où l'on exige aussi $\pi_\Pi(f(x_1, x_2)) = \pi_1(x_1) \otimes \pi_2(x_2)$ n'est pas formalisée.

Énoncé (Pages 65 à 79, *le produit intrinsèque* ♦). *Soit $\chi \in \Gamma(\mathcal{O})$ sur un schéma ou un topos annelé quelconque. Les extensions $0 \to L \to E \to M \to 0$, non nécessairement scindées, munies d'un χ-scindage, forment une catégorie monoïdale symétrique pour le produit $E_1 * E_2$ construit par somme amalgamée de $E_1 \otimes E_2$ et $L_1 \otimes L_2$ le long de $E_1 \otimes_0 E_2$, sans division ; dans le cas scindé, il redonne $b = b_1 \otimes b_2$.* ◊ non vérifié en Lean

Ne sont pas démontrés : la fonctorialité et les contraintes du produit par somme amalgamée écrites intrinsèquement, sans passer par les coordonnées ; les extensions d'un quotient M quelconque ; le passage d'une base affine à un schéma, où les extensions de $\mathcal{O}$ par L ne sont plus scindées globalement et où les coordonnées se recollent par la relation de cocycle de la page 131. La construction par somme amalgamée, son identification avec le produit en coordonnées et la propriété universelle des applications bi-affines sont démontrées sur une base affine (théorème ci-dessus).

46 Cote 160 : le déterminant de Moore et les coefficients de Dickson [49]

La cote 160, *Schémas [en] groupes : notes manuscrites (s.d.)*, est rangée dans le groupe « Dérivateurs » que l'inventaire date de 1990-[1991] ; ses vingt-deux pages traitent des sous-groupes finis de $\mathbb{G}_a$ en caractéristique p. Aux pages 7 à 9, le déterminant de Moore $\Delta_n(\xi) = \det(\xi_j^{p^i})$ donne par la règle de Cramer les coefficients A_i de la relation $\xi_k^{p^n} + A_{n-1}\xi_k^{p^{n-1}} + \cdots + A_0\xi_k = 0$, et la page 9 affirme sans raison que Δ_n divise les numérateurs (160, lot 1, p. 9). Les pages 14 et 15 transposent la construction à un faisceau E localement libre de rang n muni de $u : E^{(p)} \simeq E$: Δ_n^E est homogène de degré $\frac{p^n-1}{p-1}$, les A_i^E, définis hors du diviseur des zéros de Δ_n^E, s'étendent à $V(E)$ tout entier, et $A_0^E = \pm(\Delta_n^E)^{p-1}$ (160, lot 1, p. 14). On traite ici le cas où E est trivialisé et u l'identité.

Théorème 46.1 (D'après les pages 9, 14 et 15, E trivialisé ♦). *Soit p premier. Sur tout anneau commutatif, $\Delta_n(c\xi) = c^{(p^n-1)/(p-1)}\Delta_n(\xi)$. Il existe des polynômes $A_0, \ldots, A_{n-1} \in \mathbf{F}_p[X_1, \ldots, X_n]$ tels que, pour toute $\mathbf{F}_p$-algèbre S et tout $\xi \in S^n$, $\xi_k^{p^n} + \sum_i A_i(\xi)\,\xi_k^{p^i} = 0$ pour tout k ; si $\Delta_n(\xi)$ est inversible, les $A_i(\xi)$ sont les seuls coefficients de cette relation. Enfin $A_0 = (-1)^n\Delta_n^{p-1}$.*

L'énoncé tient : voir `moore_smul'`, `dickson_relation_eval`, `dickson_unique` et `A_zero_eval` dans `Folder160.lean`, avec le signe $(-1)^n$ que page et lecture laissent en $\pm$.

49. Preuve vérifiée : `lean/Grothendieck/Folder160.lean`.

Remarque. Les A_i sont les coefficients de $\prod_{\lambda\in\mathbf{F}_p^n}(T-\lambda\cdot X)$, et $\Delta_{n+1}(T,X_1,\dots,X_n) = (-1)^n\Delta_n\prod_\lambda(T-\lambda\cdot X)$: les p^n formes $\lambda\cdot X$ sont des racines distinctes d'un polynôme de degré p^n en T dont le coefficient dominant $\pm\Delta_n$ est non nul (par récurrence sur n). La factorisation de la page 7 et sa constante c ne servent pas.

Le signe du corollaire de la page 13. Pour un sous-groupe étale $M = \operatorname{Ker} f_a$ de $\mathbb{G}_a$ de rang p^n, $f_a = x^{p^n}+a_{n-1}x^{p^{n-1}}+\cdots+a_0x$, la page 13 affirme que les trivialisations de $\Lambda^n_{\mathbf{F}_p}M$ correspondent bijectivement aux racines $(p-1)$-ièmes de a_0 (160, lot 1, p. 13). Le signe laissé en $\pm$ à la page 9 compte ici. Sur un corps, une base $e=(e_1,\dots,e_n)$ de M donne la trivialisation $e_1\wedge\cdots\wedge e_n$, et $\Delta_n(e)$ en est la valeur ; le théorème précédent donne $a_0 = A_0(e) = (-1)^n\Delta_n(e)^{p-1}$.

Contre-exemple 46.2 (Énoncé de l'édition, page 13)**.** *Sur $\mathbf{F}_3$, avec $n=1$ et $M=\mathbf{F}_3 = \operatorname{Ker}(x^3-x)$, on a $a_0=-1$, qui n'a pas de racine carrée dans $\mathbf{F}_3$, alors que $\Lambda^1M = M$ a deux trivialisations, ses deux éléments non nuls. Le corollaire est faux dès que p et n sont impairs.*

En effet $A_0(1) = (-1)^1\cdot 1^2 = -1$, et les carrés de $\mathbf{F}_3$ sont 0 et 1. En général, si $y^{p-1}=a_0$, alors $(y/\Delta_n)^{p-1} = (-1)^n$, et -1 n'est pas une puissance $(p-1)$-ième dans $\mathbf{F}_p$ pour p impair.

Énoncé (Énoncé de l'édition, forme corrigée sur un corps)**.** *Soient K un corps de caractéristique p, $n\geq 1$ et $e\in K^n$ avec $\Delta_n(e)\neq 0$. Pour une matrice g à coefficients dans $\mathbf{F}_p$, notons $g\cdot e$ la famille $\left(\sum_k g_{jk}e_k\right)_j$. Alors $\Delta_n(g\cdot e) = \det(g)\,\Delta_n(e)$; $\Delta_n(e)$ est une racine $(p-1)$-ième de $(-1)^na_0$, où $a_0=A_0(e)$; toute racine $(p-1)$-ième de $(-1)^na_0$ est de la forme $\Delta_n(g\cdot e)$ avec $g\in\mathrm{GL}_n(\mathbf{F}_p)$; et $\Delta_n(g\cdot e)=\Delta_n(h\cdot e)$ si et seulement si $\det g = \det h$. Les trivialisations correspondent donc aux racines $(p-1)$-ièmes de $(-1)^na_0$, les fibres étant les orbites de $\mathrm{SL}_n(\mathbf{F}_p)$.*

Démonstration. Les coefficients de g sont fixes par Frobenius, donc $\left(\sum_k g_{jk}e_k\right)^{p^i} = \sum_k g_{jk}e_k^{p^i}$: la matrice de Moore de $g\cdot e$ est celle de e multipliée par la transposée de g, et les déterminants se multiplient. La deuxième assertion est le théorème précédent, puisque $(-1)^nA_0(e) = \Delta_n(e)^{p-1}$. Soit y avec $y^{p-1} = \Delta_n(e)^{p-1}$; alors $y\neq 0$, et $c = y/\Delta_n(e)$ vérifie $c^{p-1}=1$, donc $c^p=c$. Les solutions de $c^p=c$ dans K sont les p éléments de $\mathbf{F}_p$, puisqu'un polynôme de degré p a au plus p racines : $c\in\mathbf{F}_p^\times$, et la matrice diagonale $g=\operatorname{diag}(c,1,\dots,1)$ donne $\Delta_n(g\cdot e) = c\,\Delta_n(e) = y$. La dernière assertion vient de la première, $\Delta_n(e)$ étant non nul et $\mathbf{F}_p\to K$ injectif. □

Lemme 46.3 (Changement de base)**.** *Soient K un corps de caractéristique p et $e,f\in K^n$ deux familles $\mathbf{F}_p$-libres engendrant le même sous-$\mathbf{F}_p$-espace $M\subset K$. Il existe $g\in\mathrm{GL}_n(\mathbf{F}_p)$ tel que $f = g\cdot e$, et alors $\Delta_n(f) = \det(g)\,\Delta_n(e)$.*

Démonstration. Les familles e et f sont deux bases de M ; la matrice de passage P, de colonnes les coordonnées des f_j dans la base e, est inversible, et $f_j = \sum_k P_{kj}e_k$, soit $f = {}^tP\cdot e$ avec $\det{}^tP = \det P$ inversible. La formule pour Δ_n est alors la première assertion de l'énoncé précédent. Voir `exists_act_eq_of_span_eq` et `moore_eq_of_span_eq`, qui s'appuient sur `Basis.toMatrix`, `Basis.invertibleToMatrix` et `Basis.sum_toMatrix_smul_self` de Mathlib. □

Les valeurs $\Delta_n(f)$, pour f parcourant les bases de M, sont donc exactement les $\Delta_n(g\cdot e)$ pour une base fixée e : avec l'énoncé précédent, elles forment l'ensemble des racines $(p-1)$-ièmes de $(-1)^na_0$, et deux bases ont même valeur si et seulement si elles diffèrent d'un élément de $\mathrm{SL}_n(\mathbf{F}_p)$.

Le théorème de Dickson. Les pages 9 à 12 en tirent les invariants de $\Gamma_n = \mathrm{GL}_n(\mathbf{F}_p)$ et de $S\Gamma_n = \mathrm{SL}_n(\mathbf{F}_p)$, opérant sur $\mathbf{F}_p[X_1, \dots, X_n]$ par $X_j \mapsto \sum_k g_{jk} X_k$ (160, lot 1, p. 9).

Théorème 46.4 (Dickson, pages 9 à 12 ♦). *Soit p premier. Un polynôme $f \in \mathbf{F}_p[X_1, \dots, X_n]$ est invariant par $\mathrm{GL}_n(\mathbf{F}_p)$ si et seulement s'il appartient à la sous-algèbre engendrée par $A_0, \dots, A_{n-1}$, et ceux-ci sont algébriquement indépendants : $\mathbf{F}_p[X_1, \dots, X_n]^{\mathrm{GL}_n(\mathbf{F}_p)} = \mathbf{F}_p[A_0, \dots, A_{n-1}]$ est une algèbre de polynômes. De même $\mathbf{F}_p[X_1, \dots, X_n]^{\mathrm{SL}_n(\mathbf{F}_p)} = \mathbf{F}_p[\Delta_n, A_1, \dots, A_{n-1}]$, algèbre de polynômes en $\Delta_n, A_1, \dots, A_{n-1}$.*

Esquisse. La démonstration vérifiée est la démonstration galoisienne, non celle de la page, qui passe par le Main Theorem de Zariski. Les A_i sont invariants : g permute les formes $\lambda \cdot X$, donc fixe $\prod_\lambda (T - \lambda \cdot X)$; et $\Delta_n(g \cdot X) = \det(g)\, \Delta_n(X)$. Chaque X_k est racine du polynôme unitaire $\prod_\lambda (T - \lambda \cdot X)$, à coefficients dans $\mathbf{F}_p[A]$; $\mathbf{F}_p[X]$ est donc entier sur $\mathbf{F}_p[A]$, et les n éléments A_i, qui engendrent une algèbre sur laquelle une algèbre de degré de transcendance n est algébrique, sont algébriquement indépendants ; de même pour $\Delta_n, A_1, \dots, A_{n-1}$, puisque $A_0 = (-1)^n \Delta_n^{p-1}$. Le corps $\mathbf{F}_p(X)$ est le corps de décomposition sur $\mathbf{F}_p(A)$ de ce polynôme, séparable puisque sa dérivée est la constante $A_0 \neq 0$; c'est une extension galoisienne. Un automorphisme σ de $\mathbf{F}_p(X)$ au-dessus de $\mathbf{F}_p(A)$ envoie chaque X_k sur une racine, soit une forme $\lambda_k \cdot X$; il agit donc comme la matrice g de lignes λ_k, qui est inversible puisque σ est injectif. Un invariant f est fixé par tous les σ, donc appartient à $\mathbf{F}_p(A)$; entier sur $\mathbf{F}_p[A]$, algèbre de polynômes donc intégralement close, il appartient à $\mathbf{F}_p[A]$. Pour SL_n, on prend le corps $\mathbf{F}_p(\Delta_n, A_1, \dots, A_{n-1})$: un σ qui le fixe fixe Δ_n, donc $\det g = 1$. Voir `dickson_theorem`, `dickson_algebraicIndependent`, `dickson_theorem_SL` et `dicksonSL_algebraicIndependent`, qui s'appuient sur `IsGalois.of_separable_splitting_field`, `IsGalois.mem_bot_iff_fixed` et le degré de transcendance de Mathlib. □

Le lemme de la page 11 sur $A_\alpha(X_1, \dots, X_{n-s}, 0, \dots, 0)$, les degrés $p^n - p^i$ des A_i et la démonstration géométrique de la page (quasi-finitude, surjectivité par les sous-groupes de $\mathbb{G}_a$, Main Theorem de Zariski) ne sont pas formalisés.

Ne sont pas démontrés ici : la version relative pour (E, u) non trivial et la trivialisation $(\Lambda^n \check{E})^{\otimes(p-1)} \simeq \mathcal{O}_S$ par $\Lambda^n \check{u}$; la bijection $a \mapsto \mathrm{Ker}\, f_a$ des pages 2 à 6 ; la forme relative du corollaire de la page 13 sur une base S, et l'identification de $\Delta_n(e)$ à une trivialisation de $\Lambda^n_{\mathbf{F}_p} M$ au sens de la puissance extérieure.

47 Cote 69 : les automorphismes du graphe des vingt-sept droites qui fixent un triangle [50]

La cote 69, *Graphes cubiques : notes manuscrites (s.d.)*, cent dix-neuf pages, étudie le graphe C des vingt-sept droites d'une surface cubique, deux droites étant liées quand elles se coupent, et son groupe d'automorphismes W, d'ordre $51\,840$. Aux pages 25 et 26, elle marque un triangle t (trois droites deux à deux concourantes) et décrit (C, t) par un ensemble t à trois éléments, un plan V sur $\mathbf{F}_2$ et un torseur sous une extension centrale $\widetilde{\Psi}$ d'ordre 32, produit de Baer de trois copies de Q_8 (69, lot 2, p. 25, 69, lot 2, p. 26). La page 25 donne le groupe W'_t des automorphismes qui fixent t point par point comme extension de $\mathfrak{S}_4$ par $\mathbf{F}_2^3$, et le corollaire de la page 26 en tire l'ordre du groupe W_t des automorphismes de (C, t).

50. Preuve vérifiée : `lean/Grothendieck/Folder69.lean`.

Conventions. Les sommets sont a_i, b_i ($0 \le i \le 5$) et c_{ij} ($i < j$) ; a_i et b_j sont liés si $i \neq j$, a_i et b_i sont liés à c_{jk} si $i \in \{j,k\}$, c_{ij} et c_{kl} sont liés si $\{i,j\} \cap \{k,l\} = \emptyset$, et il n'y a pas d'autre arête. C'est le modèle classique des vingt-sept droites ; chaque sommet a dix voisins. On prend $t = \{a_0, b_1, c_{01}\}$.

Théorème 47.1 (Grothendieck, page 26)**.** *Le groupe W_t des automorphismes de C qui conservent le triangle t est d'ordre $32 \cdot 36 = 1152$.*

L'énoncé tient : voir `card_Wt` et `card_aut` dans `Folder69.lean`. Le sous-groupe W_t' est d'ordre $192 = 8 \cdot 24$, comme le donne la suite exacte de la page 25 (`card_pointwise`). La vérification est un calcul fini : la base $a_0, b_1, a_1, a_2, a_3, a_4$ a des orbites de tailles $3, 2, 8, 4, 3, 2$; chaque orbite est contenue dans l'ensemble des sommets qui ont les mêmes incidences avec les points déjà fixés, et parcourue par des automorphismes explicites que le noyau vérifie ; un automorphisme qui fixe la base fixe tout, car la base sépare les sommets. La cote 74 retrouve 1152 par un autre chemin, les 96 autotopies de la table de Klein (§ 54).

Ne sont pas démontrés ici : la description de (C, t) par $(t, V, \widetilde{P})$ et l'équivalence de catégories de la page 26, l'identification de $\widetilde{\Psi}$ au produit de Baer des relevés de Q_8, la suite exacte $1 \to \widetilde{\Psi} \to W_t \to \mathfrak{S}_t \times \mathfrak{S}_{V^*} \to 1$, et le rapprochement de W_t avec $W(F_4)$.

48 Cote 89 : trois vecteurs de somme nulle dans un module libre de rang deux[51]

La cote 89, *[Hexagone] combinatoire. [Ensembles 3-3] : notes manuscrites (s.d.)*, vingt pages non datées du groupe de cotes 69 à 102 que l'inventaire date de 1976 à vers 1986, part de la structure la plus pauvre qui soit : six objets rangés en deux groupes de trois. Les pages 2 à 14 y lisent un hexagone, puis un plan sur $\mathbf{F}_3$. Les pages 15 à 18 reprennent la question sur un anneau quelconque : comment reconstituer un module libre de rang 2 à partir de l'ensemble de ses droites, muni de quelques données combinatoires (89, lot 1, p. 15). Pour définir l'addition à partir des seules droites, la page 16 s'appuie sur une relation entre trois vecteurs, qu'elle dit se vérifier « de suite ». C'est elle que l'on démontre ici.

Les données. Soient Λ un anneau commutatif et V un Λ-module libre de rang 2. Une *droite* de V est un facteur direct libre de rang 1 ; pour une droite x, on note D_x le sous-module et T_x l'ensemble de ses générateurs. Deux générateurs d'une même droite diffèrent d'une unité de Λ, de sorte que T_x est un torseur sous le groupe Λ^* des unités. Le déterminant $\det V = \Lambda^2 V$ est libre de rang 1, et l'on note $u \wedge v$ l'image de (u, v) ; dans une base, $u \wedge v = u_0 v_1 - u_1 v_0$. Deux droites x et y sont *disjointes* si $V = D_x \oplus D_y$, ce qui revient à dire que $u \wedge v$ engendre $\det V$ pour $u \in T_x$ et $v \in T_y$, ou encore que $u \wedge v$ est une unité quand on identifie $\det V$ à Λ par une base. Sur un corps, deux droites sont disjointes dès qu'elles sont distinctes ; sur un anneau local, il faut que leurs réductions modulo l'idéal maximal le soient.

L'image du triangle. Sur $\mathbf{R}$, $u \wedge v$ est l'aire orientée du parallélogramme construit sur u et v. Trois vecteurs de somme nulle sont les côtés d'un triangle parcouru dans l'ordre (figure 7). Deux côtés consécutifs engendrent alors toujours le même parallélogramme, d'aire double de celle du triangle et de même orientation : $u \wedge v = v \wedge w = w \wedge u$. La relation de la page dit que la réciproque est vraie, et qu'elle l'est sur tout anneau dès que u et v forment une base.

51. Preuve vérifiée : `lean/Grothendieck/Folder89.lean`.

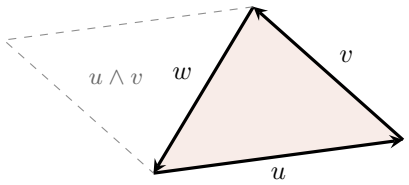


FIGURE 7 – Trois vecteurs de somme nulle, côtés d'un triangle parcouru dans l'ordre. Le parallélogramme construit sur u et v, complété en pointillé, a pour aire orientée $u \wedge v$, le double de celle du triangle ; les paires (v, w) et (w, u) donnent la même.

Énoncé (Grothendieck, page 16, la relation fondamentale)**.** *Soient Λ un anneau commutatif, V un Λ-module libre de rang 2, x et y deux droites disjointes, z une droite, et $u \in T_x$, $v \in T_y$, $w \in T_z$. Alors*

$$u \wedge v = v \wedge w = w \wedge u \iff u + v + w = 0.$$

La page ajoute que ces relations entraînent que z est disjointe de x et de y. La lecture modernisée démontre l'équivalence en écrivant $w = au + bv$ dans la base (u, v) : les égalités équivalent à $a = b = -1$. La démonstration suivie ici, celle de la preuve vérifiée, passe par une identité qui vaut pour trois vecteurs quelconques.

Démonstration. On choisit une base de V, qui identifie $\det V$ à Λ. Pour trois vecteurs quelconques u, v, w de V, on a l'identité de Cramer

$$(v \wedge w)\, u + (w \wedge u)\, v + (u \wedge v)\, w = 0.$$

Elle exprime que trois vecteurs d'un plan sont liés, avec pour coefficients les mineurs de rang 2, et se vérifie coordonnée par coordonnée : pour la première, les six termes de $(v_0w_1 - v_1w_0)u_0 + (w_0u_1 - w_1u_0)v_0 + (u_0v_1 - u_1v_0)w_0$ s'annulent deux à deux. Si les trois produits extérieurs valent un même d, l'identité devient $d\,(u + v + w) = 0$, et $d = u \wedge v$ est une unité puisque x et y sont disjointes, d'où $u + v + w = 0$. Réciproquement, si $w = -(u + v)$, alors $v \wedge w = -\,v \wedge u = u \wedge v$ et $w \wedge u = -\,v \wedge u = u \wedge v$. □

Remarque. L'énoncé tient sous une hypothèse plus faible que celle de la page : w n'a pas besoin d'engendrer une droite, et seule sert l'inversibilité de $u \wedge v$. Celle-ci ne peut être omise. Sur $\mathbf{Z}$, avec $u = v = w = (1, 0)$, les trois produits extérieurs sont nuls, donc égaux, alors que $u + v + w = (3, 0)$. La conséquence que la page ajoute se lit sur les égalités : si $u + v + w = 0$, alors $v \wedge w$ et $w \wedge u$ sont égaux à $u \wedge v$, donc inversibles, et z est disjointe de y et de x. Elle n'est pas vérifiée en Lean.

La preuve vérifiée travaille dans R^2, pour un anneau commutatif R quelconque, avec le produit extérieur $u_0v_1 - u_1v_0$ (`wedge`) ; c'est le cas général, puisque V est libre de rang 2. Elle établit l'identité de Cramer coordonnée par coordonnée (`cramer`), puis l'équivalence sous la seule hypothèse que $u \wedge v$ est une unité (`fundamental_relation`). Les noms sont ceux de `Folder89.lean`.

Ne sont pas démontrés ici : la disjonction de z que la page ajoute ; la reconstruction de V, sur un corps, à partir de l'ensemble de ses droites, des torseurs T_x, du torseur des générateurs de $\det V$, de la relation de disjonction et des isomorphismes de $T_x \wedge T_y$ sur ce dernier torseur (page 17), avec la seule propriété de ces données que la page 18 écrit ; les hexagones et les ensembles 3-3 des pages 2 à 8, leur groupe d'automorphismes d'ordre 36 ; les plans sur $\mathbf{F}_3$ des

pages 9 à 14 ; les polygones combinatoires des pages 19 et 20. Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 11 à 16, polarisations hodgiennes ♦). *Soient G un groupe algébrique réel muni d'homomorphismes $\mathbb{G}_m \xrightarrow{i} G \xrightarrow{\varepsilon} \mathbb{G}_m$, $\eta = i(-1)$ et $G' = \operatorname{Ker}\varepsilon$. Deux éléments C, C' de $G'(\mathbb{R})$ de carré η qui définissent des polarisations de $\mathrm{Rep}(G)$ sont, après conjugaison par $G'(\mathbb{R})^\circ$, liés par $C' = zC$ avec z central d'ordre divisant 2, et $z \neq 1$ donne une autre polarisation : les polarisations hodgiennes forment un torseur sous un groupe d'éléments centraux de 2-torsion. Sur toute $\otimes$-catégorie graduée sur $K \subset \mathbb{R}$, les $\otimes$-automorphismes z de l'identité tels que $z^2 = 1$, triviaux sur $K(1)$, opèrent librement sur les polarisations.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 15 et 16). La conjugaison de la page 15 tient en trois lignes abrégées où quatre mots sont illisibles, et le groupe qui opère, la 2-torsion de $Z \cap G'$, est le choix de l'édition. Mathlib n'a pas les catégories tannakiennes ni leurs polarisations. On se reportera aux notes de Grothendieck (10, lot 1, p. 11).

Théorème (Grothendieck, pages 62 à 65, caractère numérique et tore de rang un ♦). *Une catégorie tannakienne sur un corps k dont le lien est un tore de dimension 1 est déterminée à équivalence près par son caractère numérique : l'ensemble des classes d'objets simples, les constantes de structure de $K(\mathcal{M})$, les centres Z_σ des algèbres d'endomorphismes avec leurs classes de Brauer, et le rang. Pour le tore G des éléments de norme 1 d'une extension quadratique Z/k, l'application $H^2(k, G) \to H^2(k, R_{Z/k}\mathbb{G}_m) = \mathrm{Br}(Z)$ est en effet injective, par Hilbert 90.*

◊ non vérifié en Lean

La page passe par « on vérifie aussitôt » l'équivalence entre le caractère numérique et les données $(G, u_\sigma(\xi))$. Mathlib n'a pas les catégories tannakiennes ni leurs gerbes. On se reportera aux notes de Grothendieck (10, lot 4, p. 62).

Théorème (Grothendieck, pages 10 à 12, groupe de Picard de l'espace de Grothendieck–Springer ♦). *Soient S un schéma normal intègre, G un S-schéma en groupes réductif dont le tore maximal abstrait T n'est pas déployé, et Γ l'image de $\pi_1(S)$ dans $\mathrm{Aut}\, X^*(T)$. L'application $\mathrm{Pic}(\mathrm{Bor}) \to \mathrm{Pic}(\tilde{G})$ est injective, de conoyau contenu dans $H^1(\Gamma, X^*(T))$, et bijective quand ce H^1 est nul. Un fibré en droites sur Bor est ample si et seulement si son image réciproque sur $\tilde{G}$ l'est, sans hypothèse de normalité sur S.*

◊ non vérifié en Lean

La condition $H^1(\Gamma, X^*(T)) = 0$ vient d'une marge et de la page 12, lues avec plusieurs mots incertains ou illisibles ; la réciproque pour S régulier, que la marge annonce, n'est pas reprise ici. Mathlib n'a pas les schémas en groupes réductifs ni leurs schémas de Borel. On se reportera aux notes de Grothendieck (123, lot 1, p. 10).

Théorème (Grothendieck, pages 21, 28, 30 et 34, rigidifications de Kostant ♦). *Soient G un groupe simple adjoint de nombre de Coxeter h premier à la caractéristique, et z l'ordre du groupe $\mathfrak{z}$ tel que $N(T) \cap N(T')$ soit extension de $(\mathbf{Z}/h)^*$ par $\mathbf{Z}/h \times \mathfrak{z}$. Le groupe G opère librement sur les quadruplets (T, B, T', B') formés de tores maximaux T, T' en apposition au sens de Kostant et de sous-groupes de Borel $B \supset T$, $B' \supset T'$. Le quotient est fini étale de rang $\mathrm{card}(W)^2/(h\, z\, \varphi(h))$, et de rang $\mathrm{card}(W)^2/(h\, z)$ quand on se donne aussi un générateur de $T \cap N(T') \simeq \mu_h$.*

◊ non vérifié en Lean

La lettre à Kostant du 22 octobre 1969 (page 21) et la page 34 donnent ce compte sans démonstration. L'édition le déduit de la théorie de Kostant et de Springer [86, 115], par un argument que Lean ne vérifie

pas. Soit $x = \rho^\vee(e^{2i\pi/h})$ l'élément principal de T ; un $t \in T$ qui normalise T' envoie l'élément cyclique E' sur un multiple de lui-même, d'où $\alpha_i(t) = \theta(t)^{-1} = \lambda$ avec $\lambda^h = 1$, et $T \cap N(T') = \langle x \rangle$. L'image de $N(T) \cap N(T')$ dans W est formée des w tels que $w(x) \in \langle x \rangle$: le stabilisateur de x est le groupe $\Omega \simeq P^\vee/Q^\vee$, d'ordre z, car le centralisateur de x dans le groupe adjoint n'est pas connexe, et x n'est conjugué à x^k que pour k premier à h ; chacun de ces w se relève, par la conjugaison des sous-espaces de Cartan des $\mathfrak{g}^{\zeta^j}$ sous $Z_G(x)^\circ = T$. D'où l'ordre $h\,z\,\varphi(h)$, et le compte, puisque le stabilisateur d'un quadruplet est $T \cap T' = 1$. Un comptage par ordinateur sur $\mathbf{F}_q$ donne 2, 4 et 12 orbites pour A_2, B_2 et G_2. Reste la question que la lettre pose à Kostant : B et B' sont-ils toujours en position générale ? C'est vrai pour A_2, où les vecteurs propres de E' sont les vecteurs de Fourier. Mathlib n'a pas les tores maximaux ni les sous-groupes de Borel des groupes algébriques. On se reportera aux notes de Grothendieck (123, lot 2, p. 21).

Énoncé (Le nombre annoncé aux pages 21 et 34, en petit rang, vérification de l'édition). [a] *Soient W le groupe de Weyl d'un type simple, h son nombre de Coxeter et z l'ordre du centre du groupe simplement connexe. Pour les types A_1 à A_8, B_2 à B_8, C_3 à C_8, D_4 à D_8, E_6, E_7, E_8, F_4 et G_2, l'entier $h\,z\,\varphi(h)$ divise $\mathrm{card}(W)^2$. Le quotient vaut 1, 2, 4 et 12 pour A_1, A_2, B_2 et G_2.*

a. Preuve vérifiée : `lean/Grothendieck/Folder123Kostant.lean`.

Démonstration. Les données sont les valeurs classiques : $\big((n+1)!,\, n+1,\, n+1\big)$ pour $(\mathrm{card}\, W, h, z)$ en type A_n, $(2^n n!,\, 2n,\, 2)$ en types B_n et C_n, $(2^{n-1} n!,\, 2n-2,\, 4)$ en type D_n, et $(51\,840, 12, 3)$, $(2\,903\,040, 18, 2)$, $(696\,729\,600, 30, 1)$, $(1152, 12, 1)$, $(12, 6, 1)$ pour E_6, E_7, E_8, F_4, G_2. Pour A_2, par exemple, $36/(3 \cdot 3 \cdot \varphi(3)) = 36/18 = 2$, et pour G_2, $144/(6 \cdot 1 \cdot 2) = 12$. Lean décide que chaque reste est nul (`integral_A`, `integral_B`, `integral_C`, `integral_D`, `integral_exceptional`) et calcule les quatre valeurs (`small_cases`). Les données sont entrées à la main et ne sont pas tirées des systèmes de racines. L'intégralité est une condition nécessaire pour que le nombre soit un nombre d'orbites, et les valeurs pour A_2, B_2 et G_2 sont celles du comptage sur $\mathbf{F}_q$ rappelé plus haut. Lean ne vérifie ni l'action libre de G sur les quadruplets, ni le compte lui-même, et l'encadré précédent reste non vérifié. Les noms sont ceux de `Folder123Kostant.lean`.

Théorème (Grothendieck, pages 10 à 13, pas de résolution de Steinberg sans changement de base ♦). *Sur une base S, il n'existe pas de résolution du morphisme de Steinberg $G \to T/W$ qui soit un isomorphisme au-dessus de G^{reg} et dont le lieu exceptionnel soit de codimension ≥ 2 fibre par fibre : son groupe de Picard serait fini modulo $\mathrm{Pic}(S)$, alors que celui de l'espace de Grothendieck–Springer $\tilde{G}$ contient le réseau des poids et son cône ample. Le changement de base $T \to T/W$ est ainsi rendu nécessaire par une comparaison de groupes de Picard, et non par la monodromie.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 10 à 13). La phrase de conclusion s'interrompt, et l'argument demande une résolution régulière et projective sur G, hypothèses que la page ne formule pas. Mathlib n'a pas les schémas en groupes réductifs ni leurs groupes de Picard. On se reportera aux notes de Grothendieck (123, lot 1, p. 10).

Théorème (Grothendieck, pages 71 à 77, catégorie de Picard de Brandt ♦). *Soit C une catégorie de Deuring sur un anneau de Dedekind, équivalente à celle des modules inversibles sur un ordre $\mathfrak{o}$ d'une algèbre E dont tous les automorphismes sont intérieurs et dont les bimodules inversibles contenus dans E commutent entre eux. Le 2-groupe $\mathrm{Eqv}(C)$ des autoéquivalences porte une structure symétrique strictement commutative, indépendante de l'objet choisi pour l'identifier aux bimodules. Les catégories de Deuring d'un même type sont donc des catégories-torseurs sous une même catégorie de Picard stricte, la catégorie de Picard de Brandt.*

◊ non vérifié en Lean

C'est l'édition qui affirme, d'après Auslander–Goldman et Reiner, que la condition de commutation vaut pour les ordres maximaux. Mathlib n'a pas les catégories de Picard ni les catégories-torseurs. On se reportera aux notes de Grothendieck (15, lot 4, p. 71).

Théorème (Grothendieck, pages 116 à 118, foncteurs fibres réels ♦). *Soit une catégorie motivique sur $\mathbf{Q}$ de lien commutatif G, de caractère de Tate ε et de cocaractère des poids j avec $\varepsilon j(\lambda) = \lambda^2$, et soit $U = \mathrm{Ker}(\varepsilon|_{G^\circ})$, où U° est un tore compact. La catégorie admet un foncteur fibre à valeurs dans les espaces vectoriels réels si et seulement si U est connexe ; sinon $U \simeq U^\circ \times \mu_2$. Sa sous-catégorie de poids pairs, de groupe $G/j(\mu_2)$, en admet donc toujours un.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (page 116). La condition intermédiaire (ii) des deux propositions est en partie illisible, l'édition la rétablit, et l'implication qui y passe est la sienne. Mathlib n'a pas les catégories tannakiennes ni les foncteurs fibres. On se reportera aux notes de Grothendieck (15, lot 6, p. 116).

Théorème (Grothendieck, pages 27 à 36, semi-continuité des rangs ♦). *Pour un schéma en groupes lisse, séparé et de présentation finie sur une base quelconque, la dimension de la partie affine et les rangs nilpotent, affine-nilpotent et unipotent sont semi-continus supérieurement ; le rang abélien, le rang abélien plus réductif et le rang semi-simple sont semi-continus inférieurement.*

◊ non vérifié en Lean

SGA 3, X 8.7, énonce ces inégalités sans démonstration. La réduction à un trait suppose les invariants localement constructibles, propriété que ni la page ni la lecture ne vérifient, et l'équivalence entre les inégalités (3) et (9) que la page affirme n'est pas justifiée. Mathlib n'a pas les schémas en groupes lisses ni leur décomposition de Chevalley. On se reportera aux notes de Grothendieck (27, lot 2, p. 27).

Théorème (Grothendieck, pages 10 à 14, liens sur un corps de Tsen ♦). *Sur un corps C_1, tout lien algébrique, lisse ou non, provient d'un k-schéma en groupes, et $H^2(k, L)$ se réduit alors à sa classe neutre.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 11 à 14), par deux principes de réduction pour les gerbes de réalisations. Le deuxième cas suppose une conjugaison des sous-groupes de Cartan infinitésimaux qui n'est pas établie, et le troisième n'est pas lu. Mathlib n'a pas les liens ni la cohomologie non abélienne de degré 2. On se reportera aux notes de Grothendieck (45, lot 1, p. 10).

Théorème (D'après les pages 3 à 10, forme corrigée par l'édition, surjectivité en H^1 en dimension un ♦). *Soit k un corps tel que $\mathrm{Br}(k') = 0$ pour toute extension finie séparable k'/k. Pour tout épimorphisme $G \to G'$ de schémas en groupes algébriques sur k, non nécessairement lisses ni linéaires, à noyau non nécessairement commutatif, l'application $H^1(k, G) \to H^1(k, G')$ de cohomologie plate est surjective.*

◊ non vérifié en Lean

La page suppose $\mathrm{cd}(k) \leq 1$; l'hypothèse sur les groupes de Brauer, la dimension ≤ 1 au sens de Serre, est de l'édition. Les feuillets en esquissent une démonstration incomplète (pages 3 à 9). Le lemme 4 invoque une conjugaison des sous-algèbres de Cartan qui n'est pas établie et qui tombe en défaut en général en caractéristique p, et l'énoncé de la page 9 conclut que $H^1(k, G) \to H^1(k, G')$ est un épimorphisme pour tout épimorphisme $G \to G'$ de groupes algébriques sur k. Mathlib n'a pas la cohomologie plate des schémas en groupes. On se reportera aux notes de Grothendieck (45, lot 1, p. 3).

Théorème (Grothendieck, page 13, principe d'identité et lemme B ♦). *Soit X un espace annelé quasi-compact, de faisceau structural cohérent et d'anneaux locaux noethériens, qui*

◊ non vérifié en Lean

vérifie un principe d'identité : pour tout Idéal cohérent J et tout point y de $Y = \mathrm{Supp}(\mathcal{O}/J)$ où $\mathcal{O}_{Y,y}$ est intègre, il existe un voisinage ouvert U de y dans Y sur lequel toute section nulle près de y est nulle. Alors toute suite croissante de sous-faisceaux cohérents d'un faisceau cohérent est stationnaire, et $\Gamma(X, \mathcal{O}_X)$ est noethérien.

La page énonce le lemme B et son corollaire sans démonstration, et propose les polycylindres analytiques compacts comme cas d'application ; le passage au corollaire par le lemme A est de la lecture. Mathlib n'a pas les faisceaux cohérents sur un espace annelé, et le pas central, celui où sert le principe d'identité, n'est pas vérifié en Lean ; l'édition ne vérifie pas non plus que les conditions de la page suffisent sur un espace annelé quelconque. Lean vérifie ce qui entoure ce pas, énoncé ci-dessous. On se reportera aux notes de Grothendieck (55, lot 1, p. 13).

Théorème (D'après la page 13, forme réduite par l'édition, le lemme B moins le principe d'identité ♦). [a] *Soient X un espace quasi-compact et $(S_k)_{k\in\mathbf{N}}$ une suite croissante de sous-faisceaux d'un préfaisceau d'ensembles sur X. On suppose qu'en chaque point x les germes des S_k se stabilisent, et que cette stabilisation se propage uniformément : pour tout x et tout k, il existe un voisinage ouvert W de x tel que tout S_l, $l \geq k$, qui a en x les mêmes germes que S_k, coïncide avec S_k sur W. Alors la suite (S_k) est stationnaire. Sans l'hypothèse d'uniformité, la conclusion tombe en défaut. Enfin, si les idéaux de type fini I d'un anneau A s'envoient de façon croissante sur des objets $\widetilde{I}$ d'une classe où toute suite croissante est stationnaire, avec $\Gamma(\widetilde{I}) = I$, alors A est noethérien.*

a. Preuve vérifiée : `lean/Grothendieck/Folder55.lean`.

Démonstration. Un sous-faisceau est ici une famille d'ensembles de sections, stable par restriction et locale : une section y appartient dès qu'elle y appartient localement. En chaque point x, on prend l'indice k_x où les germes se stabilisent, puis le voisinage W_x que donne l'uniformité pour k_x : sur W_x, tous les S_l, $l \geq k_x$, coïncident avec S_{k_x}. Par quasi-compacité, un nombre fini de W_x recouvrent X ; soit K le plus grand des k_x correspondants. Pour $l \geq K$, une section de S_l sur un ouvert U appartient, sur chaque $U \cap W_x$, à $S_l = S_{k_x} \subset S_K$, donc à S_K par localité : la suite est stationnaire à partir de K. La stabilisation des germes est ce que donne l'hypothèse (iv) : la fibre d'un faisceau cohérent est un module de type fini sur l'anneau noethérien $\mathcal{O}_{X,x}$, où toute suite croissante de sous-modules est stationnaire. Pour le contre-exemple, on prend le compactifié d'Alexandrov $\mathbf{N} \cup \{\infty\}$, le faisceau de toutes les fonctions à valeurs dans $\{0, 1\}$, et pour S_k les fonctions qui ne valent 1 qu'aux points $0, \ldots, k-1$. En un entier n, les germes sont constants à partir de $k = n+1$; en ∞, une section de S_k est nulle sur le voisinage ouvert obtenu en retirant les points $0, \ldots, k-1$, et les germes sont tous ceux de S_0. Pourtant la fonction indicatrice de $\{k\}$ est dans S_{k+1} et pas dans S_k : les sous-faisceaux s'accumulent en ∞, ce que le principe d'identité est là pour interdire. Pour le corollaire, une suite croissante d'idéaux de type fini I_k donne la suite croissante des $\widetilde{I_k}$, stationnaire, et $I_k = \Gamma(\widetilde{I_k})$ l'est aussi ; la condition des chaînes ascendantes sur les idéaux de type fini suffit à rendre A noethérien. Les noms sont `stationary_of_locally_stationary` (le pas de quasi-compacité), `stationary_of_germs` (le lemme B sous l'hypothèse d'uniformité), `germs_stabilize_of_noetherian` (le rôle de (iv)), `not_stationary_without_uniformity` (le contre-exemple) et `isNoetherianRing_of_tilde` (le corollaire), dans `Folder55.lean`. Ne sont pas démontrés : que le principe d'identité (v) entraîne l'hypothèse d'uniformité, ce qui demanderait les faisceaux cohérents, les supports des $\mathcal{O}/\mathcal{J}$ et une décomposition primaire dans les fibres, et que le lemme A fournisse $I \mapsto \widetilde{I}$ avec $\Gamma(\widetilde{I}) = I$. Le principe (v) ne parle que des sections sur un voisinage U fixé, pas sur les ouverts plus petits où vivent les sous-faisceaux qui s'accumulent ; l'édition ne sait pas s'il suffit sur un espace annelé quelconque.

Partie 19

Surfaces de Riemann, uniformisation et modules des courbes

49 Cote 93 : la différence schwarzienne en dérivées divisées [52]

La cote 93, du groupe « Géométrie et topologie combinatoire », étudie la dérivée schwarzienne et les connexions projectives sur une courbe lisse X au-dessus d'une base S. Pour deux uniformisantes t, s, la lecture note $G(t,s) = \left(-2\,s'''/s' + 3\,(s''/s')^2\right) dt^2$. Page 72, la page remplace les dérivées par les opérateurs $D_t^{(i)} = \frac{1}{i!}\frac{d^i}{dt^i}$ sur une base variable, les dérivées de Hasse (Hasse et Schmidt, 1937 [69]), observe que les coefficients 2 et 3 de G l'interdisent, et prend $G_0 = \frac{1}{12}G$; elle fixe le signe par la valeur test $G_0(t,t^3) = \frac{2}{3t^2}\,dt^2$, après un premier essai sur $G_0(t,t^2)$ (93, lot 4, p. 72). Pages 115 à 117, la mise au net énonce l'invariance par les homographies (1) et la relation de cocycle (2) (93, lot 6, p. 115). Page 120, elle écrit $G(t,s) = 12\,G_0(t,s)$ avec $G_0(t,s) = -D_t^{(3)}s/D_t^{(1)}s + (D_t^{(2)}s/D_t^{(1)}s)^2$ (93, lot 6, p. 120). Une marge de la page 121, marquée « OK », dit que les fonctions annulées par $D^{(1)}$, $D^{(2)}$, $D^{(3)}$ forment $\mathcal{O}^{(p)}$ si $p \neq 2,3$ et $\mathcal{O}^{(p^2)}$ sinon ; la Proposition des pages 121 à 123 en tire la rigidité locale (93, lot 7, p. 121, 93, lot 7, p. 123). On démontre ici le noyau algébrique de ces pages dans le modèle local $R[X]$, sur un anneau commutatif quelconque : la formule $G = 12\,G_0$, la relation de cocycle, l'invariance par les homographies, les deux valeurs tests, la description de la marge de la page 121, le fait qu'en caractéristique 2 et 3 une translation par une puissance p-ième change G_0, et la rigidité de la Proposition des pages 121 à 123 dans l'anneau tronqué $A[T]/(T^n)$, c'est-à-dire pour $\alpha = 0$.

Le titre d'inventaire du dossier est *Connexions de Gauss-Manin et équations de Picard-Fuchs. Opération de Cartier*, et la cote ouvre ici l'axe des connexions, de la p-courbure et de la monodromie. Une connexion ∇ sur un fibré E est une règle pour dériver ses sections le long d'un champ de vecteurs D. Sur les nombres complexes, elle est à courbure nulle quand E admet localement une base de sections de dérivée nulle ; prolongées le long d'un lacet, ces sections reviennent transformées, et cette transformation est la monodromie. Sur une famille de variétés, la cohomologie des fibres porte une connexion canonique, celle de Gauss–Manin : les pages 161 à 166 la construisent d'après Katz et Oda (1968) [81], et les pages 218 à 220 en tracent un plan. En caractéristique p, le composé de D avec lui-même p fois est encore une dérivation, notée $D^{[p]}$, et la p-courbure mesure l'écart entre $\nabla(D)^p$ et $\nabla(D^{[p]})$. La page 188 énonce que les connexions de courbure et de p-courbure nulles sont celles qui proviennent d'un module sur le quotient de Frobenius X' : c'est la descente de Cartier, sous la forme que lui donne Katz (1970) [79], §5. Les pages 193 et 194 demandent si une connexion définie sur les entiers, de p-courbure nulle pour presque tout p, a une monodromie finie ; c'est la conjecture de Grothendieck–Katz, démontrée par Katz (1972) [80] pour les connexions de Gauss–Manin et ouverte en général. La descente de Cartier n'est formalisée que sur le fibré trivial, quand l'anneau a une coordonnée ; la remarque des pages 193 et 194 l'est en rang un, avec la formule de Jacobson qui calcule la p-courbure, puis, à titre d'illustration, sur le fibré trivial de rang quelconque, avec trois exemples calculés en rang deux ; la conjecture est énoncée plus bas. Les autres énoncés démontrés portent

52. Preuve vérifiée : `lean/Grothendieck/Folder93.lean`.

sur les connexions projectives d'une courbe : une connexion projective désigne les coordonnées locales qui se déduisent les unes des autres par des homographies, et la différence schwarzienne $G(t,s)$ mesure l'écart entre les structures définies par t et par s. S'y ajoute le morphisme dérivé des pages 233 à 235, qui compare les complexes de De Rham de deux relèvements.

Le même axe traverse trois cotes sans section propre. La cote 162-5 (partie « Catégories et foncteurs ») place les connexions intégrables et les groupes formels dans le cadre des catégories formelles, et y compare un complexe de De Rham à un complexe de Hochschild dans la catégorie dérivée. La cote 60 (partie « Cohomologie étale et ℓ-adique ») lit la monodromie locale d'un faisceau ℓ-adique sur une courbe dans sa représentation de Weil–Deligne. La cote 34 (partie « Groupes fondamentaux et théorie de Galois ») décrit la monodromie modérée d'une famille dégénérée en caractéristique résiduelle p, sur une base de dimension quelconque.

Conventions. R est un anneau commutatif et X joue le rôle de l'uniformisante t. Pour $f \in R[X]$, $D^{(k)}f$ est la dérivée de Hasse, définie sans division par $k!$ par $D^{(k)}X^n = \binom{n}{k}X^{n-k}$; on a $k!\,D^{(k)}f = f^{(k)}$. On pose

$$N(f) = (D^{(2)}f)^2 - D^{(3)}f \cdot D^{(1)}f, \qquad G_0(f) = N(f)\,(D^{(1)}f)^{-2},$$

où l'inverse est pris quand $D^{(1)}f$ est inversible (Lean utilise `Ring.inverse`, qui vaut 0 sinon). Ainsi $G_0(f)$ est le coefficient de dt^2 dans $G_0(t,f)$, et $N(f)$ est ce coefficient débarrassé de son dénominateur. On note de même $N_{\mathrm{cl}}(f) = 3\,(f'')^2 - 2\,f'''f'$ et $G(f) = N_{\mathrm{cl}}(f)\,(f')^{-2}$. Pour $s,u \in R[X]$, $s \circ u$ est le polynôme composé. On dit que f est *tué* si $D^{(1)}f = D^{(2)}f = D^{(3)}f = 0$. On note f_i le coefficient de X^i dans f.

Énoncé (Page 120, le facteur 12 ♦). *Pour tout $f \in R[X]$, $N_{\mathrm{cl}}(f) = 12\,N(f)$ et $G(f) = 12\,G_0(f)$.*

Démonstration. On a $f' = D^{(1)}f$, $f'' = 2\,D^{(2)}f$ et $f''' = 6\,D^{(3)}f$ (par un lemme de mathlib sur les dérivées de Hasse). Donc $3\,(f'')^2 - 2\,f'''f' = 12\,(D^{(2)}f)^2 - 12\,D^{(3)}f\,D^{(1)}f$. La seconde égalité s'en déduit en multipliant par $(f')^{-2}$. □

Lemme 49.1. *Pour $s,u \in R[X]$, en notant $s_i = (D^{(i)}s)\circ u$ et $u_i = D^{(i)}u$:*

$$D^{(1)}(s\circ u) = s_1u_1, \quad D^{(2)}(s\circ u) = s_1u_2 + s_2u_1^2, \quad D^{(3)}(s\circ u) = s_1u_3 + 2\,s_2u_1u_2 + s_3u_1^3.$$

Démonstration. Les trois identités sont additives en s et valent pour s constant. On les démontre ensemble par récurrence sur les monômes, en passant de s à Xs. On a $(Xs)\circ u = u\cdot(s\circ u)$, et la formule de Leibniz $D^{(k)}(fg) = \sum_{i+j=k} D^{(i)}f\,D^{(j)}g$ donne, avec $D^{(1)}X = 1$ et $D^{(2)}X = D^{(3)}X = 0$, $D^{(1)}(Xs) = s + XD^{(1)}s$, $D^{(2)}(Xs) = D^{(1)}s + XD^{(2)}s$, $D^{(3)}(Xs) = D^{(2)}s + XD^{(3)}s$. On développe les deux membres par Leibniz et l'hypothèse de récurrence ; ils coïncident comme polynômes en u, les u_i, $s\circ u$ et les s_i. □

Énoncé (Pages 115 à 117, la relation de cocycle ♦). *Pour $s,u \in R[X]$:*

1. *$N(s\circ u) = N(s)\circ u\cdot(D^{(1)}u)^4 + \big((D^{(1)}s)\circ u\big)^2 N(u)$, sans hypothèse ;*
2. *si $D^{(1)}s$ et $D^{(1)}u$ sont inversibles, $G_0(s\circ u) = G_0(s)\circ u\cdot(D^{(1)}u)^2 + G_0(u)$.*

De plus $N(X) = 0$, donc $G_0(X) = 0$.

Démonstration. (1) On reporte les formules du lemme 49.1 dans $N(s\circ u)$. Avec les notations du lemme,

$$(s_1u_2 + s_2u_1^2)^2 - (s_1u_3 + 2s_2u_1u_2 + s_3u_1^3)\,s_1u_1 = u_1^4(s_2^2 - s_3s_1) + s_1^2(u_2^2 - u_3u_1),$$

les termes croisés $\pm 2 s_1 s_2 u_1^2 u_2$ se compensant. (2) On a $D^{(1)}(s \circ u) = s_1 u_1$; s_1 est inversible comme image de l'inversible $D^{(1)} s$ par l'homomorphisme $f \mapsto f \circ u$, qui envoie l'inverse de $(D^{(1)} s)^2$ sur l'inverse de s_1^2. On divise (1) par $(s_1 u_1)^2$. □

Remarque. Là où 6 est inversible, la relation de cocycle et l'invariance par les homographies sont les propriétés classiques de la dérivée schwarzienne, qui porte le nom de H. A. Schwarz. Dans (2), $G_0(s) \circ u \cdot (D^{(1)} u)^2$ est le coefficient de dt^2 dans $G_0(u, s \circ u)$, puisque $du = D^{(1)} u \, dt$; l'énoncé est donc la relation $G_0(t, r) = G_0(t, u) + G_0(u, r)$ pour $r = s \circ u$. La forme (1) n'utilise aucune hypothèse d'inversibilité : la relation de cocycle est une identité entre polynômes des coefficients, valable sur $\mathbf{Z}$ et donc sur toute base, en caractéristique 2 et 3 comprises. L'inversibilité ne sert qu'à diviser.

Énoncé (Page 115, invariance par les homographies ♦). *Soient $s, p, q \in R[X]$ avec $s\,q = p$ et $D^{(2)} p = D^{(3)} p = D^{(2)} q = D^{(3)} q = 0$. Alors $q^2 N(s) = 0$. En particulier, si $a, b, c, d \in R[X]$ sont tués, si $cX + d$ est inversible et si $s\,(cX + d) = aX + b$, alors $G_0(s) = 0$; c'est le cas pour $a, b, c, d \in R$.*

Démonstration. On applique $D^{(2)}$ et $D^{(3)}$ à $s\,q = p$ par Leibniz : $D^{(2)} s\,q + D^{(1)} s\,D^{(1)} q = 0$ et $D^{(3)} s\,q + D^{(2)} s\,D^{(1)} q = 0$. Alors

$$q^2 N(s) = D^{(2)} s\,q \left(D^{(2)} s\,q + D^{(1)} s\,D^{(1)} q\right) - D^{(1)} s\,q \left(D^{(3)} s\,q + D^{(2)} s\,D^{(1)} q\right) = 0.$$

Si a est tué, Leibniz donne $D^{(2)}(aX) = D^{(1)} a = 0$ et $D^{(3)}(aX) = D^{(2)} a = 0$; les hypothèses valent donc pour $p = aX + b$ et $q = cX + d$. Si q est inversible, $N(s) = 0$, d'où $G_0(s) = 0$. Les constantes sont tuées. □

Énoncé (Page 72, les valeurs tests). *Dans $R[X]$, $N(X^2) = 1$ et $D^{(1)}(X^2) = 2X$; $N(X^3) = 6X^2$ et $D^{(1)}(X^3) = 3X^2$. Donc $G_0(t, t^2) = \frac{1}{4t^2}\, dt^2$ là où 2 est inversible, et $G_0(t, t^3) = \frac{2}{3t^2}\, dt^2$ là où 3 est inversible.*

Démonstration. $D^{(k)} X^n = \binom{n}{k} X^{n-k}$. Pour X^2 : $D^{(2)} = 1$, $D^{(3)} = 0$. Pour X^3 : $D^{(1)} = 3X^2$, $D^{(2)} = 3X$, $D^{(3)} = 1$, et $9X^2 - 3X^2 = 6X^2$. □

Énoncé (Marge de la page 121, les fonctions tuées ♦). *Soit R de caractéristique p première.*

1. *$f \in R[X]$ est tué si et seulement si, pour tout n tel que le coefficient de X^n dans f soit non nul, p divise n si $p > 3$, 4 divise n si $p = 2$, 9 divise n si $p = 3$.*
2. *Si u est tué, tout polynôme $f \circ u$ est tué ; c'est le cas des polynômes en X^p ($p > 3$), en X^4 ($p = 2$), en X^9 ($p = 3$).*
3. *Si $p = 2$, $D^{(1)}(X^2) = 0$, $D^{(1)}(X + X^2) = 1$ et $G_0(X + X^2) = 1$.*
4. *Si $p = 3$, $D^{(1)}(X^3) = D^{(2)}(X^3) = 0$, $D^{(3)}(X^3) = 1$, $D^{(1)}(X + X^3) = 1$ et $G_0(X + X^3) = -1$.*

Démonstration. (1) Le coefficient de X^n dans $D^{(k)} f$ est $\binom{n+k}{k}$ fois celui de X^{n+k} dans f ; donc $D^{(k)} f = 0$ si et seulement si $\binom{n}{k} a_n = 0$ pour tout n, où a_n est le coefficient de X^n. Dans un anneau de caractéristique p, un entier c non divisible par p est inversible, car il l'est dans $\mathbf{F}_p$; donc $\binom{n}{k} a_n = 0$ équivaut à $p \mid \binom{n}{k}$ ou $a_n = 0$. Ainsi f est tué si et seulement si p divise n, $\binom{n}{2}$ et $\binom{n}{3}$ pour tout n tel que $a_n \neq 0$. Le théorème de Lucas (`Choose.choose_modEq_choose_mod_mul_choose_div_nat` de Mathlib) donne $\binom{n}{k} \equiv \binom{n \bmod p}{k \bmod p} \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \pmod p$. Si $p > 3$ et $p \mid n$,

cela vaut $\binom{0}{k} = 0$ pour $k = 2, 3$: la condition se réduit à $p \mid n$. Si $p = 2$: $\binom{n}{2} \equiv \lfloor n/2 \rfloor$ quand n est pair, donc $2 \mid n$ et $2 \mid \binom{n}{2}$ équivalent à $4 \mid n$, et alors $\binom{n}{3} \equiv \binom{0}{1}\lfloor n/2 \rfloor = 0$. Si $p = 3$: $\binom{n}{3} \equiv \lfloor n/3 \rfloor$ quand $3 \mid n$, donc $3 \mid n$ et $3 \mid \binom{n}{3}$ équivalent à $9 \mid n$, et alors $\binom{n}{2} \equiv \binom{0}{2} = 0$. (2) Par le lemme 49.1, les trois dérivées de $f \circ u$ sont des combinaisons de u_1, u_2, u_3, nuls ; et X^m est tué par (1). (3) et (4) sont des calculs de coefficients binomiaux : $N(X + X^2) = 1$ sur tout anneau et $D^{(1)}(X + X^2) = 1 + 2X$; $N(X + X^3) = 6X^2 - 1$ et $D^{(1)}(X + X^3) = 1 + 3X^2$. □

Remarque. La vérification confirme la page 120 sans hypothèse sur la base : $G = 12\,G_0$ est une identité sur $\mathbf{Z}$, et G_0 est défini partout, en caractéristique 2 et 3 comprises. La relation de cocycle vaut sous la forme (1), sans dénominateur ; l'invariance par les homographies ne demande que $D^{(2)}$ et $D^{(3)}$ nuls sur le numérateur et le dénominateur, ce qui couvre les homographies à coefficients dans $\mathcal{O}'$, les fonctions tuées, en toute caractéristique. La valeur test de la page 72 est confirmée, $G_0(t, t^3) = \frac{2}{3t^2}\,dt^2$, ainsi que la correction de la lecture pour le premier essai : $G_0(t, t^2) = \frac{1}{4t^2}\,dt^2$, là où la page écrit $\frac{1}{2t}\,dt^2$. Dans le modèle local, la marge de la page 121 est exacte : les fonctions tuées sont les polynômes en X^p si $p > 3$, en X^4 si $p = 2$, en X^9 si $p = 3$. Les points (3) et (4) montrent que ce niveau p^2 est nécessaire pour l'invariance : en caractéristique 2, t^2 a une différentielle nulle mais la translation $t \mapsto t + t^2$ donne $G_0 = dt^2$; en caractéristique 3, $t \mapsto t + t^3$ donne $G_0 = -dt^2$. Le groupe qui laisse G_0 invariant n'est donc pas celui des homographies à coefficients dans $\mathcal{O}^{(p)}$ pour $p = 2, 3$. Ces énoncés portent sur l'invariance ; la rigidité réciproque est traitée plus bas dans l'anneau tronqué. Le cadre est $R[X]$: les unités de $R[X]$ sont rares, et l'hypothèse « $D^{(1)}$ inversible » n'y est satisfaite que pour des f particuliers ; les formes sans dénominateur, (1) du cocycle et $q^2 N(s) = 0$, n'ont pas cette limite. Le passage aux séries formelles, à $A[T]/(T^{p^N} - \alpha)$ pour $\alpha \neq 0$ ou à une courbe lisse n'est pas formalisé.

Le modèle tronqué. La Proposition des pages 121 à 123 porte sur $B = A[T]/(T^{p^N} - \alpha)$, et la page se ramène d'abord à $\alpha = 0$ (93, lot 7, p. 122). On travaille dans $B_n = A[T]/(T^n)$, en écrivant ses éléments comme classes de polynômes $s \in A[X]$. Comme t est nilpotent dans B_n, un élément de B_n est inversible si et seulement si son terme constant l'est ; $D^{(1)}s$ est donc inversible dans B_n si et seulement si $s_1 \in A^*$. Le lemme suivant dit que, pour $n = p^N > 3$ en caractéristique p, la condition $G_0(t, s) = 0$ dans B_n s'écrit $X^n \mid N(s)$. L'énoncé de rigidité est formulé dans $A[X]$ avec ces deux traductions.

Lemme 49.2. *Soit A de caractéristique p première et $n = p^N$. Pour $k < n$ et $g \in A[X]$, $D^{(k)}(X^n g) = X^n D^{(k)} g$. Si $n > 3$, X^n divise $N(s + X^n g) - N(s)$ pour tous $s, g \in A[X]$.*

Démonstration. La première assertion est l'énoncé général rappelé à la suite de la démonstration : par Leibniz, elle revient à la nullité des $D^{(i)}(X^n)$ pour $0 < i < p^N$. Si $n > 3$, on l'applique à $k = 1, 2, 3$: $D^{(k)}(s + X^n g) = D^{(k)}s + X^n D^{(k)} g$, et en développant, $N(s + X^n g) - N(s)$ est X^n fois $2\,D^{(2)}s\,D^{(2)}g + X^n (D^{(2)}g)^2 - D^{(3)}s\,D^{(1)}g - D^{(3)}g\,D^{(1)}s - X^n D^{(3)}g\,D^{(1)}g$. □

Résultat général, démontré en Lean dans
`Upstream/HasseDerivXPowMul.lean` *; la démonstration n'est pas reprise ici.*

Énoncé (Page 122, le premier terme non affine ♦). *Soient A un anneau commutatif, $s \in A[X]$, $a, b, c, d \in A$, $q = cX + d$ et $r = s\,q$.*

1. $q\,N(s) = D^{(2)}s \cdot D^{(2)}r - D^{(1)}s \cdot D^{(3)}r$.
2. *Si X^{j+3} divise $r - (aX + b)$, le coefficient de X^j dans $q\,N(s)$ est $-\binom{j+3}{3}\,s_1\,r_{j+3}$.*

Démonstration. (1) On a $D^{(1)}q = c$ et $D^{(2)}q = D^{(3)}q = 0$, donc par Leibniz $D^{(2)}r = D^{(2)}s\,q + c\,D^{(1)}s$ et $D^{(3)}r = D^{(3)}s\,q + c\,D^{(2)}s$. Alors $D^{(2)}s\cdot D^{(2)}r - D^{(1)}s\cdot D^{(3)}r = q\,\big((D^{(2)}s)^2 - D^{(3)}s\,D^{(1)}s\big)$, les termes en c se compensant. (2) Soit $e = r - (aX+b)$. Les dérivées $D^{(2)}$ et $D^{(3)}$ tuent $aX+b$, donc $D^{(k)}r = D^{(k)}e$ pour $k = 2, 3$. Le coefficient de X^i dans $D^{(k)}e$ est $\binom{i+k}{k}e_{i+k}$, nul si $i+k < j+3$. Donc X^{j+1} divise $D^{(2)}e$ et X^j divise $D^{(3)}e$, dont le coefficient de X^j est $\binom{j+3}{3}e_{j+3} = \binom{j+3}{3}r_{j+3}$, puisque $j+3 \geq 2$. Dans (1), le premier produit n'a pas de terme en X^j, et le terme en X^j du second est $(D^{(1)}s)_0\binom{j+3}{3}r_{j+3} = s_1\binom{j+3}{3}r_{j+3}$. □

Énoncé (Pages 121 à 123, la rigidité ♦). *Soient A un anneau commutatif et n un entier tel que $\binom{k}{3}$ soit inversible dans A pour $3 \leq k < n$. Soit $s \in A[X]$ avec $s_1 \in A^*$, et supposons nuls les coefficients de X^m dans $N(s)$ pour $m+3 < n$ (c'est le cas si $X^n \mid N(s)$). Posons $c = -s_2/s_1$, $b = s_0$, $a = s_1 + c\,s_0$. Alors $a - bc = s_1$ et X^n divise $s\,(cX+1) - (aX+b)$: dans B_n, $s = (at+b)/(ct+1)$. En particulier :*

1. *si A est de caractéristique p première et $n = p$, sans autre hypothèse sur A ; et si de plus $p > 3$, pour $s_1 \in A^*$, $X^p \mid N(s)$ équivaut à l'existence de $a, b, c \in A$ avec $X^p \mid s\,(cX+1) - (aX+b)$;*
2. *pour $n = 4$, sur tout anneau A (niveau p^2 pour $p = 2$) ;*
3. *si A est de caractéristique 3 et $n = 9$ (niveau p^2 pour $p = 3$) ;*
4. *si A est une $\mathbf{Q}$-algèbre, dans $A[X]$ même : $N(s) = 0$ et $s_1 \in A^*$ entraînent $s\,(cX+1) = aX + b$.*

Plus généralement, si A est de caractéristique p, $n = p^N > 3$, $d \in A^*$ et $X^n \mid s\,(cX+d) - (aX+b)$, alors $X^n \mid N(s)$.

Démonstration. Soit $r = s\,(cX+1)$, de coefficients $r_0 = s_0 = b$, $r_1 = s_1 + c\,s_0 = a$ et $r_2 = s_2 + c\,s_1 = 0$; on a $a - bc = s_1$. On montre par récurrence sur $i < n$ que le coefficient de X^i dans $r - (aX+b)$ est nul. Pour $i \leq 2$ c'est le calcul précédent. Pour $i = j+3 < n$, l'hypothèse de récurrence dit que X^{j+3} divise $r - (aX+b)$. Les coefficients de $N(s)$ de degré $\leq j$ sont nuls, donc aussi le coefficient de X^j dans $(cX+1)\,N(s)$; par l'énoncé précédent, $\binom{j+3}{3}s_1 r_{j+3} = 0$, et $r_{j+3} = 0$ puisque $\binom{j+3}{3}$ et s_1 sont inversibles. (1) Pour $3 \leq k < p$, p ne divise pas $\binom{k}{3}$: sinon il diviserait $\binom{k}{3}\cdot 3!\,(k-3)! = k!$, d'où $p \leq k$. Un entier premier à p est inversible dans A, car il l'est dans $\mathbf{F}_p$. (2) Seul $k = 3$ intervient, et $\binom{3}{3} = 1$. (3) Pour $k = 3, \ldots, 8$, $\binom{k}{3} = 1, 4, 10, 20, 35, 56$, premiers à 3. (4) $\binom{k}{3} \neq 0$ pour $k \geq 3$, donc inversible dans $\mathbf{Q}$ et dans A ; les hypothèses valent pour tout n, et on prend n plus grand que le degré de $f = s\,(cX+1) - (aX+b)$: tous les coefficients de f sont nuls. Pour la dernière assertion, écrivons $s\,q = aX + b + X^n g$ avec $q = cX + d$. Par l'énoncé précédent et le lemme 49.2, $q\,N(s) = D^{(2)}s\cdot X^n D^{(2)}g - D^{(1)}s\cdot X^n D^{(3)}g$, divisible par X^n. Le polynôme q, de terme constant d inversible, est premier à X, donc à X^n (énoncé général rappelé à la suite de la démonstration) ; donc X^n divise $N(s)$. La réciproque de (1) en est le cas $N = 1$, $d = 1$. □

Résultat général, démontré en Lean dans
`Upstream/PolynomialIsCoprimeX.lean` *; la démonstration n'est pas reprise ici.*

Contre-exemple 49.3 (Page 121, le déterminant ♦). *Si $u \in A$ et si X^3 divise $uX\,(cX+d) - (aX+b)$ avec $ad - bc = 1$, alors u est un carré dans A. En particulier, dans $\mathbf{F}_5[T]/(T^5)$, $s = 2t$ vérifie $N(s) = 0$ et $D^{(1)}s = 2 \in \mathbf{F}_5^*$, et $s = (2t+0)/(0\cdot t + 1)$, mais s n'est égal à aucune homographie $(at+b)/(ct+d)$ avec $a, b, c, d \in \mathbf{F}_5$ et $ad - bc = 1$.*

Démonstration. Les coefficients de X^0, X^1 donnent $b = 0$ et $a = ud$. Alors $u = u\,(ad - bc) = u^2 d^2 = (ud)^2$. Dans $\mathbf{F}_5$, 2 n'est pas un carré (les carrés sont 0, 1, 4), et $X^5 \mid \cdot$ entraîne $X^3 \mid \cdot$. $N(2X) = 0$ car $D^{(2)}$ et $D^{(3)}$ tuent $2X$. □

Remarque. Dans le modèle tronqué avec $\alpha = 0$, la Proposition des pages 121 à 123 est confirmée sur tout anneau de caractéristique p : l'hypothèse « A local, plus généralement $\mathrm{Pic}(A) = 0$ » ne sert pas, l'homographie se normalise par $d = 1$ et son déterminant est s_1. Cette hypothèse ne sert qu'au passage de α à 0, démontré plus bas. La démonstration suit la page, avec une différence : au lieu de normaliser s en $t + at^d + \cdots$ en composant par des homographies, on multiplie s par $cX + 1$ et l'on suit les coefficients de $r = s\,(cX + 1)$; l'égalité $q\,N(s) = D^{(2)}s\,D^{(2)}r - D^{(1)}s\,D^{(3)}r$ remplace la relation de cocycle, et le coefficient $a\binom{d}{3}$ de la page devient $s_1\binom{j+3}{3}r_{j+3}$ avec $d = j + 3$. Seuls les coefficients de $N(s)$ de degré $< n - 3$ servent. Pour $p = 2$ seul $\binom{3}{3} = 1$ intervient, comme le dit la page 123, et l'énoncé vaut alors sur tout anneau ; pour $p = 3$, les restes $\binom{k}{3} \bmod 3 = 1, 1, 1, 2, 2, 2$ pour $k = 3, \ldots, 8$ confirment la colonne de droite de la page 123. L'hypothèse $p > 3$ du point (1) ne sert pas à l'implication directe, vide pour $n = p \leq 3$; elle sert à ce que $D^{(3)}$ passe au quotient B_p, ce qui demande $p > 3$, d'où le niveau p^2 pour $p = 2, 3$. La normalisation « avec $ad - bc = 1$ », ajoutée sur la page 121, est fausse en général : le déterminant est une unité, carré seulement si s_1 l'est, et l'énoncé correct porte sur $\mathrm{PGL}_2(A)$. En caractéristique nulle, la conclusion dans $A[X]$ permet c nilpotent : sur $A = \mathbf{Q}[\varepsilon]/(\varepsilon^2)$, $s = X + \varepsilon X^2$ vérifie $s\,(1 - \varepsilon X) = X$; si A est intègre, $c = 0$ et s est affine.

Ces énoncés sont, dans `Folder93.lean` : `Ncl_eq` et `G_eq` pour le facteur 12 ; `chain`, `N_comp` et `G0_comp` pour la relation de cocycle ; `N_homography`, `G0_homography` et `G0_homography_const` pour l'invariance ; `N_X_sq` et `N_X_cube` pour les valeurs tests ; `killed_iff`, `killed_iff_of_gt`, `killed_iff_two`, `killed_iff_three`, `Killed.comp`, `char_two` et `char_three` pour la marge de la page 121 ; `hasseDeriv_X_pow_mul` et `N_add_X_pow_mul` pour le lemme 49.2 ; `N_mul_lin` et `step` pour la page 122 ; `rigidity_core`, `rigidity`, `rigidity_of_gt`, `rigidity_four`, `rigidity_nine`, `rigidity_char_zero`, `N_of_homography_trunc` et `rigidity_iff_of_gt` pour la rigidité ; `det_one_square` et `det_one_counterexample` pour le déterminant.

La marge de la page 121 est le seul point où ces énoncés rejoignent la descente de Cartier. En caractéristique p, les fonctions de dérivée nulle forment $\mathcal{O}^{(p)}$, le faisceau des fonctions du quotient de Frobenius, que la descente de Cartier prend pour faisceau de constantes ; la marge demande en outre $D^{(2)}$ et $D^{(3)}$ nuls, et trouve $\mathcal{O}^{(p^2)}$ pour $p = 2, 3$. Lean le vérifie dans $R[X]$, sans faisceau ni Frobenius relatif.

La p-courbure en rang un et la question de la page 193

Les pages 193 et 194 partent d'une remarque et posent une question (93, lot 10, p. 193). La remarque : si une connexion définie sur les entiers a une monodromie finie, sa réduction modulo p est de p-courbure nulle pour presque tout p. La question : la réciproque est-elle vraie ? On démontre ici la remarque dans le cas le plus simple, celui d'un fibré de rang un trivial, avec le calcul qui la sous-tend, la formule de Jacobson. La question reste ouverte ; on l'énonce à la fin.

Le cadre. Soient A un anneau commutatif et D une dérivation de A, c'est-à-dire une application additive telle que $D(xy) = x\,Dy + y\,Dx$; on peut penser à $A = k[x]$ ou $k(x)$ et à $D = d/dx$. On note μ_c la multiplication par $c \in A$, vue comme un opérateur sur A. Une connexion sur le fibré trivial de rang un, dont les sections sont les éléments de A, se donne par une 1-forme ω : elle dérive une section f le long de D par $\nabla_D f = Df + \omega(D)\,f$. On écrit $a = \omega(D)$, de sorte

que $\nabla_D = D + \mu_a$. Une section y est *horizontale* si $\nabla_D y = 0$, soit $Dy + ay = 0$. Sur les nombres complexes, avec $D = d/dx$, les solutions sont les multiples de $\exp(-\int a)$; elles sont algébriques quand la monodromie est finie, par exemple pour $a = -\frac{1}{2x}$, où $y = \sqrt{x}$.
Pourquoi la caractéristique p. En itérant la règle de Leibniz, $D^n(xy) = \sum_k \binom{n}{k} D^k x\, D^{n-k} y$. Pour $n = p$ premier, les coefficients $\binom{p}{k}$ avec $0 < k < p$ sont divisibles par p ; si $p = 0$ dans A, il ne reste que $D^p(xy) = x\, D^p y + y\, D^p x$, et D^p est encore une dérivation. La connexion sait donc dériver le long de D^p, par $\nabla_{D^p} = D^p + \mu_{\omega(D^p)}$, et l'on peut comparer cet opérateur à la puissance p-ième $(\nabla_D)^p$. La différence

$$\psi(D) = (\nabla_D)^p - \nabla_{D^p}$$

est la *p-courbure*. Elle commute aux multiplications : c'est une multiplication par un élément de A, et non plus un opérateur différentiel. Elle joue le rôle d'un commutateur. La courbure $[\nabla_D, \nabla_{D'}] - \nabla_{[D,D']}$ mesure le défaut de ∇ à respecter le crochet des champs de vecteurs ; ψ mesure son défaut à respecter la puissance p-ième. Si E a localement une base de sections horizontales, ψ les annule ; comme elle est linéaire, elle est nulle. C'est l'idée de la remarque de la page 194.

Énoncé (D^p est une dérivation, classique)**.** *Si A est de caractéristique p premier, pour tous $x, y \in A$, $D^p(xy) = x\, D^p y + y\, D^p x$.*

Énoncé (Formule de Jacobson en rang un, classique)**.** *Si A est de caractéristique p premier, pour tout $a \in A$, on a l'égalité d'opérateurs sur A*

$$(D + \mu_a)^p = D^p + \mu_{a^p + D^{p-1}(a)}.$$

La formule est un cas particulier de celle de Jacobson (1941) [75] pour la puissance p-ième d'une somme dans une algèbre de caractéristique p. Elle donne la p-courbure en rang un : $\psi(D) = \mu_{a^p + D^{p-1}(a) - \omega(D^p)}$. Pour $D = d/dx$ sur $k[x]$ ou $k(x)$, on a $D^p = 0$ (la dérivée p-ième de x^n contient le facteur $n(n-1)\cdots(n-p+1)$, divisible par p), et il reste $\psi = a^p + a^{(p-1)}$. Le premier terme est p-linéaire en a, le second linéaire. C'est la forme que la page 208 donne à la p-courbure d'une connexion $d + \omega$ sur $\mathcal{O}$, $K_0(\omega) = \omega^{\otimes p} - F^*_{X/S}(\widetilde{C}\omega)$, « somme d'une opération p-linéaire et d'une opération linéaire » (93, lot 11, p. 208). L'identification du terme linéaire à l'opérateur de Cartier n'est pas vérifiée en Lean.

Idée de la démonstration. Écrivons $L = D + \mu_a$. La règle de Leibniz dit que $L\,\mu_c = \mu_c\, L + \mu_{Dc}$: faire passer L à droite d'une multiplication coûte une dérivée. Par récurrence, $L^n \mu_c = \sum_k \binom{n}{k} \mu_{D^k c}\, L^{n-k}$, d'où, en caractéristique p, $D^p \mu_c = \mu_c D^p + \mu_{D^p c}$: c'est le premier énoncé, appliqué à y. Pour le second, on introduit une variable t qui commute à tout et l'on considère $(D + t\mu_a)^p$, polynôme en t à coefficients opérateurs. Son terme constant est D^p et son coefficient de t^p est $\mu_a^p = \mu_{a^p}$. Sa dérivée en t est $\sum_{i<p} L_t^i\, \mu_a\, L_t^{p-1-i}$, avec $L_t = D + t\mu_a$; la même règle de commutation et l'identité $\sum_{i<n} \binom{i}{k} = \binom{n}{k+1}$ la ramènent à $\sum_k \binom{p}{k+1} \mu_{D^k a} L_t^{p-1-k}$, où seul le terme $k = p-1$ survit : la dérivée vaut $\mu_{D^{p-1}a}$ et ne dépend pas de t. Le coefficient de t est donc $\mu_{D^{p-1}a}$, et ceux de t^i pour $2 \le i \le p-1$ sont nuls, puisque i fois chacun d'eux est nul et que i est inversible modulo p. On fait $t = 1$. □

Théorème 49.4 (Grothendieck, pages 193 et 194, la remarque)**.** *Soient S intègre, de type fini et dominant sur* $\operatorname{Spec}\mathbf{Z}$*, de point générique η, X lisse sur S et E localement libre sur X*

♢ non vérifié en Lean

muni d'une connexion relative à courbure nulle. Si E_η devient trivial sur un revêtement fini étale de X_η, il existe un voisinage U de η tel que, pour tout $s \in U$ de caractéristique $p > 0$, la p-courbure de E_s sur $X_s/k(s)$ soit nulle.

La page l'affirme sans démonstration. En voici le cas que Lean vérifie ; c'est un énoncé de l'édition.

Énoncé (Le sens facile en rang un, modèle de l'édition)**.** *Soient A de caractéristique p premier, $y \in A$ inversible d'inverse z, et $a \in A$ avec $Dy + ay = 0$. Pour la connexion de forme $\omega = -dy/y$, qui vérifie $\omega(D) = a$ et $\omega(D^p) = -D^p(y)\,z$, la p-courbure est nulle :*

$$(D + \mu_a)^p = D^p + \mu_{-D^p(y)\,z}.$$

Avec la formule de Jacobson, $a^p + D^{p-1}(a) = -D^p(y)\,z$; si de plus $D^p = 0$, comme pour d/dx sur $\mathbf{F}_p(x)$, alors $a^p + D^{p-1}(a) = 0$.

Démonstration. La section y trivialise la connexion. Pour toute f, $y\,D(zf) = Df + y\,D(z)\,f$, et $y\,D(z) = -z\,Dy = a$ en dérivant $yz = 1$; donc $D + \mu_a = \mu_y\,D\,\mu_z$. En élevant à la puissance p, les facteurs $\mu_z\mu_y = 1$ se simplifient : $(D + \mu_a)^p = \mu_y\,D^p\,\mu_z = D^p + \mu_{y\,D^p(z)}$, par la règle de commutation de D^p. Enfin D^p est une dérivation et $D^p(1) = 0$, donc $y\,D^p(z) + z\,D^p(y) = D^p(yz) = 0$. Pour la seconde affirmation, on compare les deux expressions de $(D + \mu_a)^p$ en les appliquant à 1. □

Pour d/dx sur $\mathbf{F}_p(x)$ et $y = x^m$ avec m entier, on a $a = -m/x$. Le calcul direct le confirme : $a^{(p-1)} = -m\,(p-1)!\,x^{-p} = m\,x^{-p}$ par le théorème de Wilson, $a^p = -m^p x^{-p}$, et la somme $(m - m^p)\,x^{-p}$ est nulle par le petit théorème de Fermat. Sur $\mathbf{Q}$, la connexion $d/dx - c/x$ avec c rationnel a pour solution x^c, qui est algébrique ; modulo tout p qui ne divise pas le dénominateur de c, c devient un élément de $\mathbf{F}_p$, donc la classe d'un entier m, et la p-courbure est nulle par ce calcul.

Ces énoncés sont, dans `Folder93.lean`, espace `PCurvature` : `iterate_leibniz` et `pDerivation` pour le premier, sur un anneau commutatif A avec `CharP A p` et une dérivation `D : Derivation ℤ A A` ; `jacobson` pour la formule de Jacobson, dans `Module.End ℤ A` ; `pCurvature_eq_zero`, `jacobson_logDeriv` et `jacobson_logDeriv_of_pow_eq_zero` pour le sens facile. Les règles de commutation sont démontrées dans un anneau quelconque, pour un élément L et une famille M_c avec $LM_c = M_cL + M_{Dc}$ (`pow_mul_eq_sum`, `pow_char_mul`, `sum_pow_mul_pow`) ; la variable t est celle des polynômes à coefficients dans l'anneau non commutatif des opérateurs.

Ici Lean ne vérifie que le rang un, sur le fibré trivial, et pour un seul champ D ; la sous-section suivante passe au rang quelconque sur le fibré trivial. Ni la p-courbure d'un fibré non trivial, ni sa p-linéarité en D et l'existence du tenseur demandé page 208, ni le passage d'une connexion sur X/S à ses réductions E_s ne sont formalisés. Le théorème encadré, en rang quelconque et avec un revêtement fini étale, ne l'est pas non plus.

Conjecture (Question de la page 193, conjecture de Grothendieck–Katz)**.** *Soient K un corps de nombres, X une variété lisse sur K et (E, ∇) un fibré vectoriel sur X muni d'une connexion intégrable. On choisit un modèle de (X, E, ∇) sur un anneau $\mathcal{O}_K[1/N]$. Si, pour presque tout idéal premier $\mathfrak{p}$, la réduction de (E, ∇) modulo $\mathfrak{p}$ est de p-courbure nulle, alors (E, ∇) a une monodromie finie : de façon équivalente, E admet une base de sections horizontales algébriques, ou encore (E, ∇) devient trivial sur un revêtement fini étale de X.*

Katz l'a démontrée pour les connexions de Gauss–Manin (1972) [80]. Le cas où la monodromie est résoluble, qui contient le rang un, a été établi par D. et G. Chudnovsky pour les courbes (1985) [30], puis par J.-B. Bost (2001) [21] et Y. André (2004) [2]. Le cas général est ouvert, et Lean ne le démontre pas. Il l'énonce seulement, sur un ouvert de la droite affine, sous le nom `PCurvatureConjecture`. On y prend $A = R[x][1/g]$, où R est intègre, de type fini sur $\mathbf{Z}$ et de caractéristique nulle, avec $D = d/dx$ et $\nabla = D + \Gamma$ sur A^n. L'hypothèse demande que, pour presque tout p, la matrice Γ_p de la sous-section suivante ait ses coefficients dans pA : comme D^p s'annule modulo p, c'est exactement dire que la p-courbure de la réduction est nulle. La conclusion est celle de Katz, une base de solutions algébriques dans une extension de corps où D se prolonge. L'énoncé est une proposition et non un axiome, de sorte qu'aucune preuve n'en dépend.

La p-courbure en rang deux, illustration de l'édition

La page 193 pose sa question pour une connexion de rang quelconque. On reprend donc le calcul du rang un sur le fibré trivial de rang n, et l'on calcule trois exemples en rang deux. Rien de ceci n'est écrit sur la page : ce sont des énoncés de l'édition, qui illustrent la notion dont la page parle.

Le cadre. Les sections sont les vecteurs $v = (v_1, \dots, v_n)$ de A^n, et D agit coordonnée par coordonnée. Une connexion est donnée par une matrice $\Gamma \in M_n(A)$, la valeur de la forme de connexion sur D, et elle dérive une section par $\nabla v = Dv + \Gamma v$. Une section horizontale est une solution du système différentiel $Dv = -\Gamma v$. Pour $D = d/dx$ et $n = 2$, un tel système équivaut à une équation du second ordre : avec $\Gamma = \left(\begin{smallmatrix} 0 & 1 \\ x & 0 \end{smallmatrix}\right)$, il s'écrit $v_1' = -v_2$, $v_2' = -x v_1$, d'où $v_1'' = x v_1$, l'équation d'Airy.

Pourquoi ∇^p est linéaire. Faire passer ∇ à droite d'une multiplication par $c \in A$ coûte, comme en rang un, la dérivée de c : $\nabla(cv) = c\,\nabla v + (Dc)\,v$, car la matrice Γ commute à la multiplication par c. En itérant, $\nabla^k(cv) = \sum_j \binom{k}{j} (D^j c)\,\nabla^{k-j} v$, et pour $k = p$ les coefficients binomiaux intermédiaires sont nuls modulo p : il reste $\nabla^p(cv) = c\,\nabla^p v + (D^p c)\,v$. Le même calcul vaut pour D seul, qui est la connexion de matrice nulle. Dans la différence $\psi = \nabla^p - D^p$, les deux termes $(D^p c)\,v$ se compensent, et $\psi(cv) = c\,\psi(v)$. Sur les nombres complexes, $\nabla^p - D^p$ serait un opérateur différentiel d'ordre $p - 1$; en caractéristique p, c'est une matrice. Lorsque $D^p = 0$, comme pour d/dx sur $\mathbf{F}_p[x]$, la connexion dérive le long de D^p par l'opérateur nul, et ψ est exactement la p-courbure $\nabla(D)^p - \nabla(D^p)$; sinon les deux diffèrent de la matrice $\omega(D^p)$, qui ne change pas la linéarité.

La mesure d'un défaut de solutions. En caractéristique p, l'équation $Dv = -\Gamma v$ est bien plus contrainte que sur $\mathbf{C}$: la dérivée de x^p est nulle, les « constantes » forment l'anneau $\mathbf{F}_p[x^p]$, et l'on peut se demander si le système a une base de solutions, c'est-à-dire une matrice inversible Y dont les colonnes sont horizontales. La p-courbure est l'obstruction : s'il existe une telle base, ψ est nulle. La réciproque, qui est le théorème de Cartier de la page 188, fait l'objet de la sous-section suivante.

Énoncé (La p-courbure du fibré trivial de rang n, illustration de l'édition)**.** *Soient A de caractéristique p premier, D une dérivation de A, $\Gamma \in M_n(A)$ et $\nabla = D + \Gamma$ sur A^n.*

1. *L'opérateur $\psi = \nabla^p - D^p$ est A-linéaire : $\psi(cv) = c\,\psi(v)$.*
2. *On pose $\Gamma_0 = 1$ et $\Gamma_{k+1} = D(\Gamma_k) + \Gamma\,\Gamma_k$, où D agit sur chaque coefficient. Alors $\psi(v) = \Gamma_p\,v$ pour tout v.*

3. *Si $Y \in M_n(A)$ vérifie $D(Y) + \Gamma Y = 0$, alors $\Gamma_p Y = -D^p(Y)$. Si de plus Y est inversible et $D^p = 0$, alors $\Gamma_p = 0$.*

Démonstration. (1) est le calcul ci-dessus, écrit dans l'anneau des opérateurs additifs sur A^n avec la règle de commutation déjà employée en rang un. (2) Par récurrence, $\nabla^k e_j$ est la j-ième colonne de Γ_k : appliquer ∇ à la colonne j d'une matrice M donne la colonne j de $D(M)+\Gamma M$. Comme $D^p e_j = 0$ (les coordonnées de e_j sont 0 et 1), $\psi(e_j)$ est la colonne j de Γ_p, et l'on conclut par linéarité en écrivant $v = \sum_j v_j e_j$. (3) Chaque colonne y_j de Y est horizontale, donc $\nabla^p y_j = 0$ et $\psi(y_j) = -D^p y_j$; par (2), c'est la colonne j de $\Gamma_p Y$. Si $D^p = 0$, $\Gamma_p Y = 0$, et l'on multiplie à droite par l'inverse de Y. □

La récurrence de (2) donne un moyen pratique de calculer la p-courbure d'un système différentiel : on dérive la matrice $p-1$ fois en la corrigeant à chaque pas.

Énoncé (Trois exemples en rang deux, illustration de l'édition)**.** *Soit A de caractéristique p premier, avec une dérivation D.*

1. *Si $\Gamma = \operatorname{diag}(a, b)$, alors $\Gamma_p = \operatorname{diag}\big(a^p + D^{p-1}a,\ b^p + D^{p-1}b\big)$: la p-courbure est faite des deux p-courbures de rang un.*
2. *Si $\Gamma = \left(\begin{smallmatrix} 0 & f \\ 0 & 0 \end{smallmatrix}\right)$, alors $\Gamma_p = \left(\begin{smallmatrix} 0 & D^{p-1}f \\ 0 & 0 \end{smallmatrix}\right)$. Sur $\mathbf{F}_p[x]$, avec $D = d/dx$ et $f = x^{p-1}$, on trouve $\Gamma_p = \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) \neq 0$, et il n'existe aucune matrice inversible de sections horizontales.*
3. *Si $Dx = 1$ et $\Gamma = \left(\begin{smallmatrix} 0 & 1 \\ x & 0 \end{smallmatrix}\right)$ (Airy), alors*

$$\Gamma_3 = \begin{pmatrix} -1 & x \\ x^2 & 1 \end{pmatrix} \text{ en caractéristique } 3, \qquad \Gamma_5 = \begin{pmatrix} x & x^2 \\ x^3 - 1 & -x \end{pmatrix} \text{ en caractéristique } 5.$$

Démonstration. (1) La récurrence reste diagonale, et sur chaque coefficient elle calcule $(D + \mu_a)^k(1)$; la formule de Jacobson donne la valeur pour $k = p$. (2) Comme $\Gamma^2 = 0$ et que Γ annule toute matrice de la forme $\left(\begin{smallmatrix} 0 & g \\ 0 & 0 \end{smallmatrix}\right)$, on a $\Gamma_{k+1} = \left(\begin{smallmatrix} 0 & D^k f \\ 0 & 0 \end{smallmatrix}\right)$ par récurrence. Pour $f = x^{p-1}$, $D^{p-1}f = (p-1)! = -1$ par le théorème de Wilson ; comme $D^p = 0$ sur $\mathbf{F}_p[x]$, l'énoncé précédent interdit une base de sections horizontales. (3) Sur un anneau quelconque, la récurrence donne

$$\Gamma_2 = \begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}, \quad \Gamma_3 = \begin{pmatrix} 2 & x \\ x^2 & 1 \end{pmatrix}, \quad \Gamma_4 = \begin{pmatrix} x^2 & 2 \\ 4x & x^2 \end{pmatrix}, \quad \Gamma_5 = \begin{pmatrix} 6x & x^2 \\ x^3 + 4 & 4x \end{pmatrix},$$

et l'on réduit modulo 3 et modulo 5. □

Le deuxième exemple montre une p-courbure qui ne se lit pas sur les morceaux de rang un. La droite engendrée par e_1 et le quotient sont des connexions triviales, de p-courbure nulle, mais l'extension ne l'est pas. Les sections horizontales vérifient $v_2' = 0$ et $v_1' = -f v_2$: il faut une primitive de f, et x^{p-1} n'en a pas dans $\mathbf{F}_p[x]$, puisque la primitive attendue x^p/p n'a pas de sens. C'est l'analogue du logarithme, primitive de $1/x$ qui n'est pas algébrique sur $\mathbf{C}$. La p-courbure, ici nilpotente, détecte exactement ce défaut.

Dans le troisième exemple, la trace de Γ_p est nulle et son déterminant vaut $-1 - x^3 = -(1+x)^3$ pour $p = 3$ et $-x^5$ pour $p = 5$: le polynôme caractéristique, $T^2 - (1+x)^3$ ou $T^2 - x^5$, a ses coefficients dans $\mathbf{F}_p[x^p]$. Ce fait général n'est pas démontré en Lean. Sur $\mathbf{C}$, les fonctions d'Airy ne sont pas algébriques ; la conjecture de Grothendieck–Katz prévoit donc une p-courbure non nulle pour une infinité de p, et le calcul le constate pour $p = 3$ et $p = 5$.

Ces énoncés sont, dans `Folder93.lean`, espace `PCurvature` : `nabla`, `nabla_comm`, `pCurvature` et `pCurvature_smul` pour la linéarité ; `curvMat` et `pCurvature_apply` pour la récurrence ; `curvMat_mul_horizontal` et `curvMat_eq_zero_of_horizontal` pour le sens facile ; `curvMat_diagonal_char`, `curvMat_unipotent_char`, `curvMat_unipotent_X_pow`, `not_horizontal_unipotent_X_pow`, `curvMat_airy`, `curvMat_airy_three` et `curvMat_airy_five` pour les exemples. Les trois premiers énoncés sont en rang n quelconque, sur A^n vu comme `Fin n →` `A`, et réemploient la règle de commutation `pow_char_mul` du rang un.

Ne sont pas formalisés : la p-linéarité de ψ en D, le fait que le polynôme caractéristique de ψ a ses coefficients dans A^p, et les fibrés non triviaux.

La réciproque de Cartier sur le fibré trivial

Une base de sections horizontales force la p-courbure à s'annuler. La page 188 affirme la réciproque, sous la forme de la descente de Cartier : une connexion de courbure et de p-courbure nulles provient d'un module sur le quotient de Frobenius, et elle a donc localement une base de sections horizontales (93, lot 10, p. 188). On la démontre ici dans le cas le plus simple, celui du fibré trivial A^n sur un anneau qui a une coordonnée.

Le cadre. L'anneau A est commutatif, de caractéristique p, muni d'une dérivation D telle que $D^p = 0$ et d'un élément x tel que $Dx = 1$. C'est le cas de d/dx sur $\mathbf{F}_p[x]$, sur $\mathbf{F}_p(x)$ et sur $\mathbf{F}_p[[x]]$. Pour $k < p$, l'entier $k!$ n'est pas divisible par p et il est inversible dans A : on peut écrire $x^k/k!$, et c'est tout ce dont on aura besoin. Comme $D^p = 0$, la p-courbure de $\nabla = D + \Gamma$ est $\psi = \nabla^p$, et elle est nulle si et seulement si $\nabla^p v = 0$ pour tout v.

L'idée : la formule de Taylor. Sur les nombres réels, une fonction se retrouve à partir de ses dérivées en 0 : $f(x) = \sum_k f^{(k)}(0)\, x^k/k!$. En caractéristique p, on ne peut pas diviser par $p!$, et la série s'arrête d'elle-même au rang $p-1$; l'hypothèse $\nabla^p = 0$ dit justement que les termes suivants seraient nuls. Cartier en tire un opérateur qui fabrique des sections horizontales,

$$P = \sum_{k=0}^{p-1} \frac{(-x)^k}{k!}\, \nabla^k.$$

On peut le lire comme « la valeur en $x = 0$ » : $P(v)$ est la section horizontale qui coïncide avec v au point $x = 0$, quand ce point a un sens.

Pourquoi $P(v)$ est horizontal. La règle de Leibniz $\nabla(c\,w) = c\,\nabla w + (Dc)\,w$ et le calcul $D\big((-x)^k/k!\big) = -(-x)^{k-1}/(k-1)!$ donnent

$$\nabla P(v) = \sum_{k=0}^{p-1} \frac{(-x)^k}{k!}\, \nabla^{k+1} v \;-\; \sum_{k=1}^{p-1} \frac{(-x)^{k-1}}{(k-1)!}\, \nabla^k v = \frac{(-x)^{p-1}}{(p-1)!}\, \nabla^p v = 0.$$

Les deux sommes se compensent terme à terme, sauf le dernier terme de la première, qui est nul par hypothèse.

Pourquoi les $P(\nabla^j v)$ suffisent. La formule de Taylor se retourne :

$$v = \sum_{j=0}^{p-1} \frac{x^j}{j!}\, P(\nabla^j v).$$

En développant, le membre de droite vaut $\sum_{j,k} \frac{x^j (-x)^k}{j!\,k!}\, \nabla^{j+k} v$. Les termes où $j + k \geq p$ sont nuls,

puisque $\nabla^p = 0$. Pour $m = j + k < p$, le coefficient de $\nabla^m v$ est $\sum_{j+k=m} \frac{x^j (-x)^k}{j!\,k!} = \frac{(x-x)^m}{m!}$ par la formule du binôme : il vaut 1 pour $m = 0$ et 0 sinon. C'est l'identité $e^{xT} e^{-xT} = 1$, tronquée modulo T^p, où elle a un sens sans dénominateur divisible par p.

Énoncé (D'après la page 188, réciproque de Cartier sur le fibré trivial)**.** *Soient A un anneau commutatif de caractéristique p premier, D une dérivation de A telle que $D^p = 0$, et $x \in A$ tel que $Dx = 1$.*

1. *Si la connexion $\nabla = D + \Gamma$ sur A^n est de p-courbure nulle, tout $v \in A^n$ s'écrit $v = \sum_{j<p} \frac{x^j}{j!}\, w_j$ avec $\nabla w_j = 0$: les sections horizontales engendrent A^n.*
2. *Si A est local (un corps comme $\mathbf{F}_p(x)$, ou $\mathbf{F}_p[[x]]$), la connexion $D + a$ de rang un a une base horizontale, c'est-à-dire un inversible y tel que $Dy + ay = 0$, si et seulement si sa p-courbure $a^p + D^{p-1}(a)$ est nulle.*

Démonstration. Le premier point est le calcul qui précède, avec $w_j = P(\nabla^j v)$. Pour le second, le sens direct est la remarque démontrée plus haut. Réciproquement, la formule de Jacobson donne $(D+a)^p = D^p + a^p + D^{p-1}(a) = 0$, et le premier point appliqué à $v = 1$ écrit $1 = \sum_j \frac{x^j}{j!}\, y_j$ avec des y_j horizontaux. Dans un anneau local, les non-inversibles forment l'idéal maximal, et une somme de non-inversibles n'est pas inversible ; l'un des y_j est donc inversible. □

L'exemple $a = -m/x$ sur $\mathbf{F}_p(x)$, vu plus haut, en est le cas typique : sa p-courbure est nulle, et la réciproque retrouve la solution x^m. Sur $\mathbf{F}_p[x]$, en revanche, le second point dégénère. Les inversibles de $\mathbf{F}_p[x]$ sont les constantes non nulles, de dérivée nulle, et une base horizontale force $a = 0$. Inversement, si $a^p + a^{(p-1)} = 0$, le premier point fournit une section horizontale non nulle y, qui vérifie $y' = -ay$, et la comparaison des degrés impose $a = 0$: en rang un sur $\mathbf{F}_p[x]$, la p-courbure n'est nulle que pour la connexion triviale. Le premier point, lui, dit quelque chose sur $\mathbf{F}_p[x]$ en tout rang.

Portée de la vérification. Lean démontre ces énoncés dans `Folder93.lean`, espace `PCurvature` : `exp_mul_exp` pour l'identité tronquée, `proj`, `mul_proj` et `taylor` pour le projecteur et la formule de Taylor, écrits dans un anneau d'opérateurs quelconque où $[\nabla, c] = Dc$, `horizontal_generate` et `horizontal_span` pour le premier point en rang un et en rang n, `horizontal_unit_iff` pour le second, et `horizontal_unit_iff_Fp` pour le cas de $\mathbf{F}_p[x]$. Ne sont pas démontrés : le fait que les sections horizontales forment un module libre de rang n sur $A^D \supseteq \mathbf{F}_p[x^p]$, avec $A^n = A \otimes M^\nabla$, qui est la descente de Cartier proprement dite, les fibrés non triviaux et les anneaux sans coordonnée globale.

Hors du fibré trivial traité plus haut, en rang un et en rang quelconque, aucun énoncé du dossier sur la connexion de Gauss–Manin ou sur la p-courbure n'est démontré ici : ni la filtration du complexe de De Rham relatif et la connexion qu'elle définit (pages 161 à 166), ni la descente de Cartier de la page 188 au-delà du fibré trivial, ni les foncteurs de Picard relatifs à connexion et l'existence d'un tenseur de p-courbure en rang quelconque (pages 205 à 212), ni le plan des pages 218 à 220. Ne sont pas démontrés non plus : l'unicité de l'homographie au scalaire près (« uniques … scalaire », page 121) ; la rigidité dans $A[X]$ ou dans les séries formelles en caractéristique p, avec des coefficients tués non constants, et sur une courbe lisse en caractéristique p ; l'injectivité espérée page 121 du quotient de $\mathcal{P}_{X/S}$ par les homographies à coefficients dans $\mathcal{O}'_X$ dans $\mathrm{Conn}^0_{X/S}$; la construction des torseurs $\mathrm{Conn}_{X/S}$ et $\mathrm{Conn}_{0,X/S}$; l'unicité de G_0 au signe près sur $\mathbf{Z}$ (page 72) et l'unicité en caractéristique p de la remarque 3 (page 73).

Les pages 233 à 235 cherchent à comparer les complexes de De Rham de deux relèvements X', X'' d'un même X_0 sur un épaississement de carré nul (93, lot 12, p. 233, 93, lot 12, p. 234). Localement on dispose d'isomorphismes $p : X' \to X''$, qui forment un torseur $\mathcal{P}$ sous un faisceau abélien $\mathcal{G}$: deux d'entre eux diffèrent d'un $g \in \mathcal{G}$. Chaque p donne un isomorphisme de complexes $u(p)$, et changer p en $p+g$ modifie $u(p)$ par une homotopie explicite $k(g)$:

$$u(p+g) - u(p) = d\,k(g) + k(g)\,d.$$

Si $\mathcal{P}$ avait une section globale, on prendrait $u(p)$ et l'on aurait fini, puisque deux choix sont homotopes. Il n'y en a pas en général, et la page veut éviter les recouvrements. Elle introduit pour cela l'extension $0 \to \mathcal{G} \to \bar{\mathcal{G}} \xrightarrow{j} \mathbf{Z} \to 0$ telle que $j^{-1}(1) = \mathcal{P}$, le complexe $\mathcal{L} = [\mathcal{G} \to \bar{\mathcal{G}}]$, quasi-isomorphe à $\mathbf{Z}$, et l'application $\varphi : \mathcal{L} \to \underline{\mathrm{Hom}}^\bullet(K', K'')$ égale à k en degré -1 et à u sur $\mathcal{P}$. Elle s'arrête sur « un homom. de la cat. dérivée ».

On formalise la version où $\mathcal{P}$ est un torseur sous un groupe abélien G, et non sous un faisceau. Ici K' et K'' sont des complexes d'une catégorie additive, $\underline{\mathrm{Hom}}^n(K', K'')$ est le groupe des familles de flèches de degré n, et δ sa différentielle, $\delta(k) = dk + kd$ en degré -1.

Théorème 49.5 (D'après les pages 234 et 235, cas d'un groupe abélien ♦). *Soient $\mathcal{P}$ un torseur sous un groupe abélien G, $k : G \to \underline{\mathrm{Hom}}^{-1}(K', K'')$ additive et $u : \mathcal{P} \to \underline{\mathrm{Hom}}^0(K', K'')$, avec $u(p+g) - u(p) = \delta(k(g))$ et chaque $u(p)$ morphisme de complexes. L'extension $\bar{G}$ de $\mathbf{Z}$ par G avec $j^{-1}(1) = \mathcal{P}$ se construit sans choisir de point, et $[G \to \bar{G}]$ est quasi-isomorphe à $\mathbf{Z}$. Il existe $\varphi^0 : \bar{G} \to \underline{\mathrm{Hom}}^0(K', K'')$ additif, égal à u sur $\mathcal{P}$ et à $\delta \circ k$ sur G ; (k, φ^0) est un morphisme de complexes. La classe de $u(p)$ dans la catégorie d'homotopie, et dans la catégorie dérivée, ne dépend pas de p.*

L'énoncé tient : voir `j_eq_zero_iff`, `j_eq_one_iff`, δ`_φ0`, `quotient_map_eq` et `derived_map_eq` dans `Folder93.lean`. On prend pour $\bar{G}$ le quotient de $G \times \mathbf{Z}^{(\mathcal{P})}$ par les relations $[p+g] - [p] = g$. L'homotopie entre $u(p')$ et $u(p)$ est $k(p'-p)$.

Pour un groupe, le torseur a toujours un point, et l'énoncé se réduit à l'indépendance du choix. Ce que les pages visent, un torseur sous un faisceau sans section globale, n'est pas formalisé, pas plus que l'application aux complexes de De Rham. La chemise de ces pages annonce la connexion canonique en cohomologie de De Rham ; y voir une construction de la connexion de Gauss–Manin est une inférence de la lecture, que les pages n'écrivent pas, et Lean n'en vérifie rien.

Théorème 49.6 (Grothendieck, pages 71 à 73 et 120 à 123, schwarzien à dérivées divisées ♦). *La différence schwarzienne écrite avec les dérivées divisées $D^{(i)} = \frac{1}{i!}\frac{d^i}{dt^i}$, $G_0(t,s) = -D^{(3)}s/D^{(1)}s + (D^{(2)}s/D^{(1)}s)^2 = G/12$, est un cocycle à valeurs dans $\omega^{\otimes 2}$ défini sur toute base, caractéristiques 2 et 3 comprises. Sur un anneau local A de caractéristique p (on a alors $\mathrm{Pic}(A) = 0$), pour tout $\alpha \in A$, un $s \in A[T]/(T^{p^N} - \alpha)$ avec $D^{(1)}s$ inversible et $G_0(t,s) = 0$ s'écrit $(at+b)/(ct+d)$ avec $a, b, c, d \in A$ et $ct+d$ inversible, pour $N = 1$ si $p > 3$ et pour $N = 2$ si $p = 2$ ou 3.*

Énoncé (Grothendieck, pages 121 à 123, anneau non local ♦). *La même conclusion vaut sur tout anneau A de caractéristique p tel que $\mathrm{Pic}(A) = 0$.*

Démonstration de la page (pages 120 à 123). Le facteur 12, la relation de cocycle et la rigidité pour $\alpha = 0$ sont démontrés plus haut ; la page écrit $G = 12\,G_0$ sans le calcul (p. 120). Elle se

◊ non vérifiée en Lean

ramène à $\alpha = 0$ (« OPS ») sans argument, puis, par deux changements de variable homographiques, à $s \equiv t \bmod t^3$ (p. 122). Si $s = t + at^d + \cdots$ avec $d \geq 3$, la comparaison de $D^{(3)}s\, D^{(1)}s$ et de $(D^{(2)}s)^2$ modulo t^{d-2} donne $a\binom{d}{3} = 0$, d'où $a = 0$ pour $p > 3$ (p. 122) ; pour $p = 2$ ou 3, avec T^{p^2}, la page conclut par le critère de Lucas, le cas $p = 3$ refait en marge (p. 123). L'unicité de G_0 au signe près (p. 72) n'est pas démontrée.

Réduction à $\alpha = 0$. Posons $q = p^N$ et $B = A[T]/(T^q - \alpha)$, et notons β la classe de T. Sur B lui-même, $T^q - \alpha = (T - \beta)^q$ par Frobenius : l'extension $A \to B$ est celle qui rend le cas $\alpha = 0$ applicable. L'application de Taylor $\theta(f) = f(\beta + Y)$, de $A[T]$ dans $B[Y]$, a pour coefficients les classes des $D^{(k)}f$, commute aux dérivées divisées et envoie $T^q - \alpha$ sur Y^q. Le polynôme $\theta(s)$ vérifie donc, sur la base B et modulo Y^q, les hypothèses du cas $\alpha = 0$, et la rigidité démontrée plus haut donne

$$\theta(s)\,(cY + 1) \equiv aY + s \pmod{Y^q}, \qquad c = -\frac{D^{(2)}s}{D^{(1)}s}, \quad a = D^{(1)}s + cs,$$

avec $a, c \in B$: c'est l'homographie osculatrice en β, de vecteur de coefficients $v = (a,\ s - aT,\ c,\ 1 - cT)$ en la variable T, et l'on a $s\,(v_3T + v_4) = v_1T + v_2$ identiquement. Reste à descendre v de B à A. En dérivant la congruence une et deux fois en Y, on obtient pour chaque coordonnée

$$(cY + 1)\,\theta(v_j) \equiv v_j \pmod{Y^q},$$

ce qui dit que l'homographie osculatrice en $\beta + Y$ est la même, à un scalaire près. Pour $\ell = \lambda c + \mu(1 - cT)$, $\lambda, \mu \in A$, le produit $x = \ell^{q-1}v_j$ vérifie alors $(cY + 1)^q\,\theta(x) \equiv x$, et $(cY + 1)^q = 1 + c^qY^q$: $\theta(x) \equiv x$, c'est-à-dire $D^{(k)}x = 0$ dans B pour $0 < k < q$. Un élément de B ainsi tué est dans A (on le voit sur le représentant de degré $< q$). Le vecteur $\ell^{q-1}v$ est donc dans A^4, et donne $s = (aT + b)/(cT + d)$ avec $cT + d = \ell^{q-1}$; de même $\ell^q \in A$. Il reste à choisir ℓ inversible. Avec $\gamma = c^q \in A$, on a $(1 - cT)^q = 1 - \gamma\alpha$. Si A est local, γ ou $1 - \gamma\alpha$ est inversible, et l'on prend $\ell = c$ ou $\ell = 1 - cT$.

Si l'on suppose seulement $\mathrm{Pic}(A) = 0$, on considère le sous-A-module I de B formé des $x = c'T + d$ ($c', d \in A$) tels que $s\,x = a'T + b'$ avec $a', b' \in A$: ce sont les dénominateurs des homographies égales à s. Le coefficient de Y^2 dans $\theta(s)\,\theta(x) \equiv a'(\beta + Y) + b' \pmod{Y^q}$, où $q > 2$, donne $D^{(2)}s \cdot x + D^{(1)}s \cdot c' = 0$, donc $c\,x = c' \in A$ et $(1 - cT)\,x = d \in A$: le module $J = Ac + A(1 - cT)$ vérifie $IJ \subseteq A$. Par ce qui précède, c^{q-1} et $(1 - cT)^{q-1}$ sont dans I, et $\alpha\, c^{q-1} \cdot c + (1 - cT)^{q-1}(1 - cT) = \alpha\gamma + 1 - \gamma\alpha = 1$, donc $IJ = A$. Le module I est un sous-A-module inversible de B, et sa classe dans $\mathrm{Pic}(A)$ est triviale : il est alors de la forme Au avec u inversible dans B (suite exacte $A^\times \to B^\times \to \{\text{sous-modules inversibles}\} \to \mathrm{Pic}(A)$). Comme $u \in I$, on a $u = cT + d$ et $s\,u = aT + b$ avec $a, b, c, d \in A$. □

Portée de la vérification. Lean démontre la réduction dans `Folder93.lean`, espace `Alpha`, avec B = `AdjoinRoot`$(T^q - \alpha)$: `θ_coeff`, `θ_D`, `θ_P` pour l'application de Taylor, `descent` pour la descente, `rigidity_alpha` pour l'énoncé sur un anneau quelconque de caractéristique p où $\binom{k}{3}$ est inversible pour $3 \leq k < q$, avec ℓ quelconque, et `rigidity_alpha_local`, `rigidity_alpha_of_gt`, `rigidity_alpha_four`, `rigidity_alpha_nine` pour l'anneau local et les cas $p > 3$, $p = 2$, $p = 3$, puis `rigidity_alpha_pic`, `rigidity_alpha_pic_of_gt`, `rigidity_alpha_pic_four`, `rigidity_alpha_pic_nine` pour un anneau tel que $\mathrm{Pic}(A) = 0$ (hypothèse `Subsingleton (CommRing.Pic A)`), par le sous-module inversible I et `Submodule.ker_unitsToPic` de Mathlib. Le passage au faisceau sur une courbe, où t n'est qu'une coordonnée locale, n'est pas formalisé.

Remarque. La caractérisation des polynômes tués par les dérivées de Hasse d'ordre $0 < k < p^e$ en caractéristique p (ce sont les polynômes en X^{p^e}) vaut sous cette forme générale, avec le critère de divisibilité qu'elle utilise, tiré du théorème de Lucas (1878) [91] sur les coefficients binomiaux modulo p. Pour $p = 3$ elle porte sur les ordres $k < 9$, quand la marge n'emploie que $D^{(1)}$, $D^{(2)}$, $D^{(3)}$.

Remarque. Deux lemmes servent à la démonstration de la rigidité : le passage des dérivées de Hasse d'ordre $< p^e$ à travers la multiplication par X^{p^e}, et le critère selon lequel un polynôme P est premier à $X - a$ si et seulement si $P(a)$ est inversible. Pour $a = 0$, il dit qu'un polynôme de terme constant inversible est premier à X, donc à X^n, ce qu'emploie la démonstration.

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Exemple (Grothendieck, pages 30 à 32 et 35, carte des structures spéciales de $M_{0,5}$ ♦). Comme points de base et générateurs d'une présentation du groupoïde de Teichmüller de cinq points sur la sphère, construite à partir de pièces de dimension modulaire ≤ 1, la cote propose une carte de 542 structures spéciales en neuf orbites sous $\mathfrak{S}_5$ sur trois niveaux (12 pentagonales, 20 bitétraédriques et 30 pyramidales ; $60 + 60 + 120$; $60 + 120 + 60$), reliées par 1620 flèches en quatorze orbites.

◊ non vérifié en Lean

Les relations sont annoncées et jamais écrites. Pour trois types de flèches, les sources et buts dessinés ne correspondent pas aux facteurs du décompte, que l'édition reproduit sans le vérifier, et « 1620 » surcharge un « 1580 » barré. Mathlib n'a pas le groupoïde de Teichmüller. On se reportera aux notes de Grothendieck (148, lot 2, p. 30).

Énoncé (Grothendieck, pages 30 et 32, les décomptes de la carte). [a] *Si chacun des neuf types de structures spéciales de la page 30 compte* $120/|G|$ *structures, où* G *est son groupe d'automorphismes holomorphes, d'ordres* 10*,* 6 *et* 4 *au niveau* 2*,* 2*,* 2 *et* 1 *au niveau* 1*,* 2*,* 1 *et* 2 *au niveau* 0*, les trois niveaux portent* 62*,* 240 *et* 240 *structures,* 542 *en tout. Les quatorze types de flèches de la page 32, comptés comme la lecture les tabule, forment trois groupes de* 180*,* 420 *et* 1020 *flèches,* 1620 *en tout.*

a. Preuve vérifiée : `lean/Grothendieck/Folder148Chart.lean`.

Démonstration. Le groupe $\mathfrak{S}_5$, d'ordre 120, permute les structures d'un même type, et G est le stabilisateur de l'une d'elles ; d'où les $120/|G|$ structures du type, que la page inscrit dans son tableau. Ces nombres sont 12, 20, 30 ; 60, 60, 120 ; 60, 120, 60 (`counts_eq`), de sommes 62, 240 et 240 par niveau et 542 en tout (`vertices`). Les flèches de la page 32 se comptent par groupes : $60+120 = 180$ pour les flèches entre structures de niveau 2, $60+120+60+60+120 = 420$ et $120+120+120+120+360+120+60 = 1020$ pour les deux autres, soit quatorze types et 1620 flèches (`arrows_eq`). Lean décide ces égalités d'entiers. Il ne vérifie ni la liste des neuf types, ni leurs groupes d'automorphismes, ni le nombre de flèches de chaque type. Le 360 du septième type du dernier groupe est celui que la lecture restitue sous une ligne surchargée, et pour trois types les sources et buts du tableau ne s'accordent pas avec les facteurs du décompte ; la carte elle-même reste donc non vérifiée. Les noms sont ceux de `Folder148Chart.lean`.

Définition (Grothendieck, pages 40 et 49 à 60, groupoïde de Teichmüller multimarqué ♦). Dans le groupoïde de Teichmüller des surfaces découpées, chaque cercle de découpe ou de bord a porte un nombre quelconque $r(a) \geq 0$ de points marqués, qui forment un torseur sous le groupe tordu $\mathbf{Z}_a/r(a)$. Les opérations élémentaires sont, outre le découpage et le recollement, l'effacement partiel uniforme, restriction au sous-groupe d'ordre r' divisant r, et le surmarquage uniforme, extension le long de $\mathbf{Z}/r \to \mathbf{Z}/dr$. Le recollement de deux

cercles est défini à isomorphisme unique près dès qu'ils portent le même nombre de points et qu'on se donne un anti-isomorphisme de leurs torseurs.

La définition du surmarquage uniforme et la phrase qui ramène le recollement à $r(a) = r(a')$ contiennent des mots illisibles, et la restriction au sous-groupe d'ordre r' corrige la page. Mathlib n'a pas le groupoïde de Teichmüller des surfaces découpées, et Lean ne vérifie pas la définition elle-même. Il vérifie l'unique énoncé qu'elle contient, l'unicité du recollement, dont la page affirme qu'il est « bien déterminé » sans dire pourquoi (encadré suivant). On se reportera aux notes de Grothendieck (148, lot 2, p. 40 et 148, lot 3, p. 58).

Théorème (Grothendieck, pages 55 à 58, unicité du recollement ♦). [a] *Soient a et a' deux cercles orientés portant chacun $r \geq 1$ points marqués, ceux de a formant un torseur R_a sous $\mathbf{Z}/r$, et soit $u : R_a \to R_{a'}$ un anti-isomorphisme de torseurs. L'espace des homéomorphismes $a \to a'$ qui renversent l'orientation et induisent u sur les points marqués est non vide et contractile. En particulier deux recollements le long de u sont isotopes parmi les recollements le long de u.*

a. Preuve vérifiée : `lean/Grothendieck/Folder148.lean`.

Lean vérifie l'énoncé dans le modèle des relèvements. Le cercle est $\mathbf{R}/\mathbf{Z}$, orienté par $\mathbf{R}$; ses points marqués sont donnés par leurs relèvements $p : \mathbf{Z} \to \mathbf{R}$, strictement croissants avec $p(k+r) = p(k)+1$, à des positions quelconques (`Marking`). Le point $p(k)$ porte l'étiquette $k \bmod r$, et le générateur de $\mathbf{Z}/r$ fait passer au point suivant dans le sens de l'orientation. Un anti-isomorphisme u vérifie $u(x+1) = u(x) - 1$, donc $u(x) = c - x$ (`antiIso_eq`). Un homéomorphisme renversant l'orientation se relève en $F : \mathbf{R} \to \mathbf{R}$ continue, strictement décroissante, avec $F(x+1) = F(x) - 1$; deux relèvements diffèrent d'un entier, et on normalise par $F(p(k)) = q(c-k)$ pour tout k, où $c \in \mathbf{Z}$ relève u. L'espace $\mathcal{G}(p,q,c)$ de ces F, muni de la topologie compacte-ouverte, est l'espace de l'énoncé (`gluings`). Il est non vide (`gluings_nonempty`). On interpole p de façon affine par morceaux, en un homéomorphisme croissant h_p de $\mathbf{R}$ avec $h_p(k) = p(k)$ et $h_p(y+r) = h_p(y) + 1$ (`Marking.interpHomeomorph`), de même pour q, et $F = h_q \circ (c - \cdot) \circ h_p^{-1}$ convient. Il est convexe (`convex_gluings`) : si F et G conviennent et $s+t = 1$ avec $s,t \geq 0$, alors $sF+tG$ est encore strictement décroissante, vérifie $(sF+tG)(x+1) = (sF+tG)(x) - 1$ et prend en $p(k)$ la valeur $q(c-k)$. C'est l'argument de la lecture, qui raisonne arc par arc : la convexité vaut sur chaque arc entre deux points marqués consécutifs. Un convexe non vide est contractile par l'homotopie rectiligne (`contractibleSpace_gluings`), donc connexe par arcs (`isPathConnected_gluings`). Chaque élément est un homéomorphisme de $\mathbf{R}$ (`toHomeomorph`). Enfin, tout homéomorphisme décroissant qui envoie les points marqués de a sur ceux de a' induit un anti-isomorphisme $k \mapsto c - k$ (`exists_antiIso`), de sorte que les espaces $\mathcal{G}(p,q,c)$ épuisent les recollements qui respectent les marquages. Lean vérifie ensuite l'énoncé sur le cercle lui-même, $\mathbf{R}/\mathbf{Z}$ (`AddCircle 1`). Un homéomorphisme du cercle y renverse l'orientation s'il admet un relèvement continu strictement décroissant, et l'espace de l'énoncé est celui des bijections continues ayant un tel relèvement et envoyant $p(k)$ sur $q(c-k)$ (`circleGluings`), muni de la topologie compacte-ouverte. Passer au quotient est un homéomorphisme de $\mathcal{G}(p,q,c)$ sur cet espace (`gluingsHomeomorph`), qui est donc contractile (`contractibleSpace_circleGluings`). Trois points font la preuve. Un relèvement strictement décroissant d'un homéomorphisme est de degré -1 : $F(x+1) - F(x)$ est un entier constant $n < 0$, et si $n \leq -2$ le théorème des valeurs intermédiaires donne $t \in [0,1]$ avec $F(t) = F(0) - 1$, contre l'injectivité (`lift_add_one`). Les entiers $F(p(k)) - q(c-k)$ ne dépendent pas de k, puisque deux consécutifs diffèrent de moins de 1, et on normalise en retranchant leur valeur (`exists_gluing_of_mem`). Enfin si deux relèvements normalisés ont des images à distance uniforme $< \varepsilon \leq 1/2$, leur différence, nulle en $p(0)$ et partout à moins de ε d'un entier, reste par connexité à moins de ε de 0 (`abs_sub_lt_of_dist_lt`) ; c'est la continuité de l'inverse. Lean ne vérifie pas le groupoïde. Les noms sont ceux de `Folder148.lean`.

Théorème (Grothendieck, page 49, recollement de cercles sans points marqués ♦). [a] *L'espace des homéomorphismes du cercle qui renversent l'orientation a le type d'homotopie du cercle, et son groupe fondamental est* $\mathbf{Z}$*. L'espace des recollements de deux cercles sans points marqués n'est donc pas contractible, contrairement au cas* $r \geq 1$.

a. Preuve vérifiée : `lean/Grothendieck/Folder148.lean`.

La page prend $r(a) = 0$ sans commentaire, avec le groupe $\mathbf{Z}_a/0 = \mathbf{Z}$; l'énoncé est celui de la lecture. Lean le vérifie sur `AddCircle 1`, avec la même définition de l'orientation (`circleReversing`). L'application $f \mapsto (f(0), f - f(0))$ est un homéomorphisme sur le produit du cercle par l'espace des homéomorphismes renversants qui fixent 0 (`circleReversingHomeomorph`). Ce dernier est l'espace de l'encadré précédent pour $r = 1$, $p = q = \mathrm{id}$ et $c = 0$, donc contractile, d'où l'équivalence d'homotopie avec le cercle (`circleReversingHomotopyEquiv`) et, par le groupe fondamental du cercle de Mathlib (`AddCircle.windingNumberIso`), l'isomorphisme $\pi_1 \simeq \mathbf{Z}$ (`circleReversing_fundamentalGroup`). Lean ne vérifie pas que le générateur, la rotation complète d'un des deux bords, est le twist de Dehn le long du cercle de recollement, ni que le recollement devient unique une fois donné un torseur de cadrages sous $\mathbf{Z}$; ces deux points sont ceux de la lecture.

Partie 20

Champs, gerbes et catégories fibrées

50 Cote 62 : l'invariant j d'une conique munie d'une trisection étale [53]

La cote 62, *Courbes elliptiques (généralités – vieille rédaction)*, notes que l'inventaire date « [à partir de 1963] », décrit aux pages 41 à 53 les triplets (X, X', s) formés d'une conique, d'une trisection étale et d'une section disjointe de X', sur une base où 6 est inversible. Dans une coordonnée qui envoie X' sur $\{0, 1, \infty\}$, les six substitutions anharmoniques t, $1/t$, $1-t$, $t/(t-1)$, $1/(1-t)$, $(t-1)/t$ forment $\mathfrak{S}_3$, et la page 39 calcule le quotient (11),

$$j(t) = -\frac{1}{27}\Big(\frac{(t+1)(2t-1)(t-2)}{t(t-1)}\Big)^2,$$

revêtement galoisien de groupe $\mathfrak{S}_3$ non ramifié au-dessus de $\mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$; l'involution $\kappa(t) = (t-2)/(2t-1)$ donne $j(\kappa t) = 1/j(t)$ (12) (62, lot 2, p. 39). L'invariant du triplet est $j(s)$, et il détermine le triplet là où $j(j-1)$ est inversible (62, lot 3, p. 41). Lean démontre cet énoncé fibre à fibre, sur un corps K où 6 est inversible, pour $t \notin \{0, 1\}$.

Théorème 50.1 (D'après les pages 39 à 47, l'invariant j ♦). *Soit K un corps où 6 est inversible, et soient $s, t \in K \smallsetminus \{0, 1\}$. Alors $j(s) = j(t)$ si et seulement si s est l'une des six images anharmoniques de t ; en particulier j est invariant par $\mathfrak{S}_3$. On a $j(t) = 0$ si et seulement si $t \in \{-1, 2, \frac{1}{2}\}$, et $j(t) = 1$ si et seulement si $t^2 - t + 1 = 0$; aucune substitution non triviale ne fixe t si et seulement si $j(t)(j(t)-1) \neq 0$. Enfin $j = 1 - j_{\mathrm{cl}}/1728$, avec $j_{\mathrm{cl}}(t) = 256\,(t^2-t+1)^3/t^2(t-1)^2$, et $j(\kappa t)\,j(t) = 1$ pour $t \notin \{-1, 2, \frac{1}{2}\}$.*

L'énoncé tient tel que la lecture le donne (`j_eq_iff`, `stabilizer_trivial_iff`, `j_eq_one_sub_jcl`, `j_kappa_mul`, dans `Folder62.lean`). La différence $j(s) - j(t)$ vaut $\frac{4}{27}$ fois le produit des six facteurs $s - g(t)$, dénominateurs chassés, divisé par $(s(s-1)\,t(t-1))^2$; l'invariance et les fibres s'en déduisent d'un coup. Le rapprochement avec j_{cl} est de l'édition.
La preuve vérifiée ne connaît ni coniques, ni trisections, ni base S. Le groupe $\mathfrak{S}_3$ et ses deux orbites exceptionnelles, $\{-1, 2, \frac{1}{2}\}$ au-dessus de $j = 0$ et les racines de $t^2 - t + 1$ au-dessus de $j = 1$, sont ceux du cocycle anharmonique de la section 74, où les points fixes -1 et ζ donnent l'exposant 6 ; la droite $U = \mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$ est le $U_{0,3}$ de l'épinglage de Legendre de la section 42. En termes de champs, j est l'application de U vers son quotient grossier par $\mathfrak{S}_3$, et les triplets (X, X', s) sont les points du champ quotient $[U/\mathfrak{S}_3]$; cette formulation est de l'édition et n'est pas démontrée ici.

Théorème (D'après les pages 41 à 53, trois descriptions des triplets). *Sur une base où 6 est inversible, les triplets (X, X', s) se décrivent de trois façons équivalentes : par un $\mathfrak{S}_3$-torseur T muni d'une fonction t sur T, t et $t-1$ inversibles, telle que $g \cdot t = g(t)$; par un faisceau inversible muni d'une trisection étale de somme nulle de son fibré vectoriel ; ou, par le quotient*

◊ non vérifié en Lean

53. Preuve vérifiée : `lean/Grothendieck/Folder62.lean`.

$q : X \to \mathbf{P}^1$ de degré 6, par l'invariant $j \in \Gamma(S, \mathcal{O}_S)$, qui détermine le triplet là où $j(j-1)$ est inversible.

La transcription est très lacunaire ici : l'ouverture de la page 49 et la plus grande partie des pages 51 et 53 sont illisibles ou incertaines. Mathlib n'a pas les courbes de genre 0 sur une base ni leurs trisections étales. On se reportera aux notes de Grothendieck (62, lot 3, p. 41).

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 14 et 15, Gr-champs épinglés et cohomologie relative ⧫). *Soient G un Groupe sur un topos X, non nécessairement commutatif, et N un G-Module. Les Gr-champs sur X épinglés par (G, N), qui sont pour l'essentiel des 2-gerbes sur le topos classifiant B_G liées par N et trivialisées sur X, correspondent au complexe tronqué $\tau_{\leq 2}(R\Gamma(B_G \bmod X, N)[1])$, cohomologie de B_G relative à $q_G : X \to B_G$.*

◊ non vérifié en Lean

Mathlib n'a pas les Gr-champs ni les topos classifiants. On se reportera aux notes de Grothendieck (103, lot 1, p. 14).

Théorème (Grothendieck, pages 3 à 5, suite exacte des champs de Picard épinglés ⧫). *Pour des faisceaux abéliens M, N sur un topos, il existe une suite exacte de faisceaux $0 \to \mathrm{Ext}^2(M, N) \to P(M, N) \to \mathrm{Hom}(M, {}_2N) \to 0$, où $P(M, N)$ est le faisceau des champs de Picard épinglés par M, N à équivalence près et où la dernière flèche est l'invariant de symétrie de $L \otimes L$. La page la tire, à titre heuristique, d'un triangle distingué.*

◊ non vérifié en Lean

Mathlib n'a pas les champs de Picard sur un topos. On se reportera aux notes de Grothendieck (134-1, lot 1, p. 3).

Théorème (Grothendieck, page 5, réalisation de l'invariant de symétrie ⧫). *Sur tout topos, tout homomorphisme $M \to {}_2N$ est l'invariant de symétrie d'un champ de Picard épinglé par M, N : l'obstruction, a priori dans $\mathrm{Ext}^3(M, N)$, est tuée par un argument « universel », que la page annonce « sauf erreur » sans le donner.*

◊ non vérifié en Lean

Mathlib n'a pas les champs de Picard ni leurs obstructions dans Ext^3. On se reportera aux notes de Grothendieck (134-1, lot 1, p. 5).

Partie 21

Topologie combinatoire, surfaces et cartes

Le 15 avril 1984, l'année de l'*Esquisse d'un programme*, il écrit à Lipman Bers sur l'espace de Teichmüller et l'espace de Thurston des surfaces à bord, avec des modèles en disques et en tranches d'orange (67, lot 1, p. 15). C'est la seule lettre datée du fonds sur les surfaces et leurs découpages.

51 Cote 152 : le dictionnaire des graphes circularisés et des contours [54]

La cote 152, *Catégorie des types de mots [dont arbres plans] : notes manuscrites (s.d.)*, douze pages que l'inventaire date « [à partir de 1982] », décrit un arbre plan de trois manières et montre qu'elles sont équivalentes. Les pages 4 à 12, sous sa pagination $1, 1', 2, 2', 3, 3'$, forment un texte suivi. On découpe la surface le long d'un graphe circularisé et l'on obtient un *contour*, réunion de polygones, un par face. Les pages 7 et 9 écrivent le dictionnaire entre les deux données, trois fois, et les trois formes ne s'accordent pas. La page 7 encadre des formules où seule la rotation intervient. La page 9 pose en tête « $\sigma_\Gamma = \sigma_C$, $\rho_\Gamma = \rho_C$ », puis dresse un tableau dont les deux dernières lignes associent $\rho_\Gamma\sigma_\Gamma$ à ρ_C et ρ_Γ à $\rho_C\sigma_C$. Elle encadre enfin un critère pour qu'un graphe soit un arbre, dont les deux derniers mots ne se lisent pas (152, lot 1, p. 9). La lecture retient la convention du tableau.

Définition. Soit D un ensemble, celui des arcs (arêtes orientées, ou demi-arêtes). Un *graphe circularisé sans sommet isolé* sur D est la donnée d'une involution sans point fixe σ_Γ de D (le renversement des arcs) et d'une permutation ρ_Γ de D (l'arc suivant autour de l'origine) ; ses sommets sont les orbites de ρ_Γ. Un *contour* sur D est la donnée d'une permutation ρ_C de D (l'arête suivante sur le contour orienté) et d'une involution sans point fixe σ_C de D (le recollement) ; ses polygones, ou faces, sont les cycles de ρ_C. Le graphe est *connexe* si deux arcs quelconques sont reliés par une suite de pas $x \mapsto \rho_\Gamma x$ et $x \mapsto \sigma_\Gamma x$, parcourus dans un sens ou dans l'autre. Comme la lecture, on identifie l'ensemble $A(C)$ des arêtes du contour à celui des arcs par l'application « arête droite ».

Énoncé (Équivalence, pages 7 et 9, sur les objets)**.** *Sur un même ensemble D, les applications*

$$(\sigma_\Gamma, \rho_\Gamma) \longmapsto (\rho_C, \sigma_C) = (\rho_\Gamma\sigma_\Gamma,\ \sigma_\Gamma), \qquad (\rho_C, \sigma_C) \longmapsto (\sigma_\Gamma, \rho_\Gamma) = (\sigma_C,\ \rho_C\sigma_C)$$

sont des bijections réciproques entre graphes circularisés sans sommet isolé et contours munis d'une involution de recollement sans point fixe. Les trois formules $\sigma_C = \sigma_\Gamma$, $\rho_C = \rho_\Gamma\sigma_\Gamma$, $\rho_\Gamma = \rho_C\sigma_C$ valent ensemble, et les orbites de $\rho_C\sigma_C$ sont les sommets du graphe.

Énoncé (Connexité, dans la démonstration du critère de la page 9)**.** *Si D est fini et que ρ_C n'a qu'un cycle, le graphe est connexe.*

Remarque. La tête de la page 9, $\rho_\Gamma = \rho_C$, est incompatible avec le tableau dès que D n'est pas vide : jointe à $\rho_C = \rho_\Gamma\sigma_\Gamma$, elle forcerait $\sigma_\Gamma = \mathrm{id}$.

54. Preuve vérifiée : `lean/Grothendieck/Folder152.lean`.

Démonstration de l'équivalence. Tout repose sur $\sigma^2 = \mathrm{id}$ pour une involution. Partant de $(\sigma_\Gamma, \rho_\Gamma)$, on obtient le contour $(\rho_\Gamma\sigma_\Gamma, \sigma_\Gamma)$, dont l'involution est sans point fixe puisque c'est σ_Γ, puis le graphe $(\sigma_\Gamma, \rho_\Gamma\sigma_\Gamma\sigma_\Gamma) = (\sigma_\Gamma, \rho_\Gamma)$. Partant de (ρ_C, σ_C), on obtient le graphe $(\sigma_C, \rho_C\sigma_C)$, puis le contour $(\rho_C\sigma_C\sigma_C, \sigma_C) = (\rho_C, \sigma_C)$. Les deux premières formules sont les définitions, et la troisième en résulte : $\rho_C\sigma_C = \rho_\Gamma\sigma_\Gamma\sigma_\Gamma = \rho_\Gamma$. Les permutations $\rho_C\sigma_C$ et ρ_Γ étant égales, elles ont les mêmes orbites, qui sont les sommets. □

Démonstration de la connexité. Soient $a, b \in D$. Comme ρ_C n'a qu'un cycle et que D est fini, il existe un entier $k \geq 0$ tel que $b = \rho_C^k(a)$. Raisonnons par récurrence sur k. Pour $k = 0$, $b = a$. Si $\rho_C^k(a)$ est relié à a, alors $\rho_C^{k+1}(a) = \rho_\Gamma\big(\sigma_\Gamma(\rho_C^k(a))\big)$ l'est aussi, par un pas σ_Γ suivi d'un pas ρ_Γ. □

Démonstration de la remarque. Si $\rho_\Gamma = \rho_\Gamma\sigma_\Gamma$, la composition à gauche par ρ_Γ^{-1} donne $\sigma_\Gamma = \mathrm{id}$, et tout arc serait un point fixe de σ_Γ, ce qui est exclu dès qu'il y a un arc. □

La figure 8 suit le dictionnaire sur l'arbre plan à trois arêtes issues d'un même sommet. Les six arcs sont numérotés de sorte que 1, 2, 3 partent du centre et que σ_Γ échange 1 et 4, 2 et 5, 3 et 6 ; la rotation est $\rho_\Gamma = (1\,2\,3)$, qui fixe 4, 5, 6. Alors $\rho_C = \rho_\Gamma\sigma_\Gamma$ envoie 1 sur $\rho_\Gamma(4) = 4$, 4 sur $\rho_\Gamma(1) = 2$, et ainsi de suite : $\rho_C = (1\,4\,2\,5\,3\,6)$ n'a qu'un cycle, le contour est un hexagone, et l'énoncé de connexité s'applique. Les sommets se lisent aux coins de l'hexagone : entre le côté x et le côté $\rho_C x$ se trouve l'orbite de ρ_Γ qui contient $\rho_C x$.

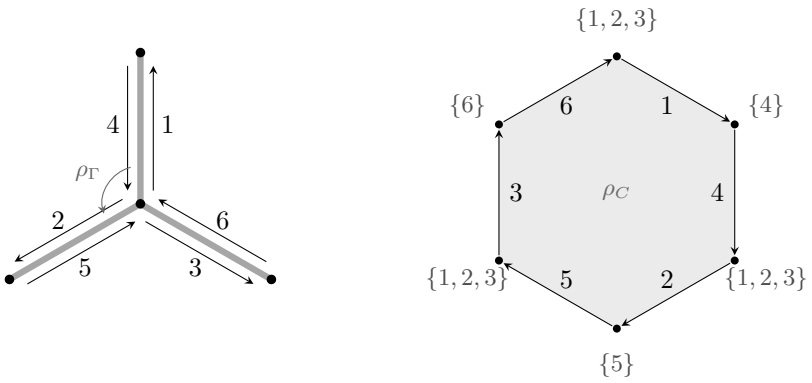


FIGURE 8 – À gauche, un arbre plan à trois arêtes et ses six arcs : σ_Γ échange les deux arcs d'une même arête, $\rho_\Gamma = (1\,2\,3)$ tourne autour du centre. À droite, le contour obtenu en découpant le plan le long de l'arbre : un seul polygone, dont les côtés se succèdent selon $\rho_C = \rho_\Gamma\sigma_\Gamma = (1\,4\,2\,5\,3\,6)$, et que $\sigma_C = \sigma_\Gamma$ recolle en identifiant les côtés 1 et 4, 2 et 5, 3 et 6. Les coins portent les sommets, orbites de $\rho_C\sigma_C = \rho_\Gamma$: le centre trois fois, chaque feuille une fois.

Remarque. L'équivalence est le dictionnaire classique des cartes combinatoires, où les faces sont les cycles du produit de la rotation et de l'involution. Il remonte aux systèmes de rotation d'Edmonds (1960) ; sa forme par une paire de permutations est celle de Jacques (1968) [76] et de Cori (1975) [36].

Remarque. L'équivalence est établie sur les objets, les deux données vivant sur le même ensemble ; les morphismes ne sont examinés ni ici ni sur la page.

Ne sont pas démontrés ici : les plongements dans une surface orientée et les circularisations (page 4) ; le critère encadré des arbres (page 9) ; la fonctorialité ; les pages 2, 3 et 10 à 12.

52 Cote 88 : l'ordre 2ν et la trichotomie des cartes standard [55]

La cote 88, *Cartes standards : notes manuscrites (s.d.)*, quinze pages sans date, appartient au groupe « Géométrie et topologie combinatoire » que l'inventaire date « 1976-[vers 1986] ». Elle contient deux textes. Le premier, sous le titre de chemise « Cartes associées aux syst. de Racines », remplace un système de racines par son groupe de Weyl, le torseur de ses bases et ses réflexions simples. Il fait opérer des involutions $\sigma_0, \dots, \sigma_{\ell-1}$ sur les drapeaux du complexe qu'il en tire, et calcule à la page 8 l'ordre du dernier produit : « ordre de $\pi = \sigma_{\ell-2}\,\sigma_{\ell-1} = 2\nu$ », ν étant « le ppcm des n_{ij} » (88, lot 1, p. 8). Le second, intitulé de sa main « Théorème (à prouver) », énonce en sept articles la théorie des cartes régulières de type (p, q). Son article (6), à la page 14, les répartit en sphériques, euclidiennes et hyperboliques par des listes de couples (88, lot 1, p. 14). Deux énoncés de la lecture sont démontrés ici : la proposition de la page 8, et l'arithmétique qui trie les cas de l'article (6).

Définition. Soient W un groupe, R un ensemble non vide sur lequel W opère librement et transitivement, I un ensemble fini de cardinal $\ell \geq 2$, et $\varphi : R \times I \to W$ une application telle que

$$\text{a)}\quad \varphi(wr, i) = w\,\varphi(r, i)\,w^{-1}, \qquad \varphi(r, i)^2 = 1 \qquad (w \in W,\ r \in R,\ i \in I).$$

Soit $\mathrm{Rep}'(I)$ l'ensemble des bijections $u : [1, \ell] \to I$, et τ la transposition de $\ell - 1$ et ℓ. On définit sur $R \times \mathrm{Rep}'(I)$

$$\sigma_{\ell-2}(r, u) = (r,\ u \circ \tau), \qquad \sigma_{\ell-1}(r, u) = \big(\varphi(r, u(\ell))\, r,\ u\big).$$

Pour $g \in W$, on note $\mathrm{ord}(g)$ le générateur positif ou nul du sous-groupe $\{k \in \mathbf{Z} \mid g^k = 1\}$, qui est nul si g est d'ordre infini, et de même pour une permutation. On pose $n_{ij} = \mathrm{ord}\big(\varphi(r, i)\varphi(r, j)\big)$ et $\nu = \mathrm{ppcm}\{n_{ij} \mid i \neq j\}$, un ppcm dont un terme est nul étant nul.

Dans la lecture, W est le groupe de Weyl, R l'ensemble des bases, $\varphi(r, i)$ la réflexion simple d'indice i relative à la base r ; seules sont retenues ici, des quatre conditions a) à d) que la lecture énonce, la condition a) et la moitié $\varphi(r, i)^2 = 1$ de c).

Énoncé (Proposition, page 8)**.** *L'ordre de $\sigma_{\ell-2}\sigma_{\ell-1}$ sur $R \times \mathrm{Rep}'(I)$ est 2ν, où ν est le plus petit commun multiple des n_{ij}, $i \neq j$.*

Énoncé (Article (6), page 14 : l'arithmétique)**.** *Soient $p, q \geq 1$ des entiers, le type (p, q) étant atteint au sens de l'article (2) : on exclut $(1, q)$ pour $q \neq 2$ et $(p, 1)$ pour $p \neq 2$. Alors*

1. *$\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$ si et seulement si $p = 2$, ou $q = 2$, ou (p, q) est l'un de $(3, 3)$, $(3, 4)$, $(4, 3)$, $(3, 5)$, $(5, 3)$;*
2. *$\frac{1}{p} + \frac{1}{q} = \frac{1}{2}$ si et seulement si (p, q) est l'un de $(4, 4)$, $(3, 6)$, $(6, 3)$;*
3. *pour $p, q \geq 3$, $\frac{1}{p} + \frac{1}{q} < \frac{1}{2}$ si et seulement si $p + q \geq 9$ et $(p, q) \neq (3, 6), (6, 3)$.*

On pose $\pi = \sigma_{\ell-1}\sigma_{\ell-2}$, le produit avec lequel calcule la page 6, et, pour (r, u) donné, $a = \varphi(r, u(\ell - 1))$ et $b = \varphi(r, u(\ell))$.

Lemme 52.1. *$\sigma_{\ell-2}$ et $\sigma_{\ell-1}$ sont des involutions ; par suite $\sigma_{\ell-2}\sigma_{\ell-1} = \pi^{-1}$.*

55. Preuve vérifiée : `lean/Grothendieck/Folder88.lean`.

Démonstration. Pour $\sigma_{\ell-2}$, c'est $\tau^2 = \mathrm{id}$. Pour $\sigma_{\ell-1}$, posons $s = \varphi(r, i)$ avec $i = u(\ell)$; par a), $\varphi(sr, i) = s\, s\, s^{-1} = s$, de sorte que $\sigma_{\ell-1}^2(r, u) = (s^2 r, u) = (r, u)$. Alors $\sigma_{\ell-2}\sigma_{\ell-1} = \sigma_{\ell-2}^{-1}\sigma_{\ell-1}^{-1} = (\sigma_{\ell-1}\sigma_{\ell-2})^{-1}$. □

Lemme 52.2. *On a $\pi(r, u) = \big(a\, r,\ u \circ \tau\big)$; pour tout $g \in W$, $\pi^2(gr, u) = (g\, ab\, r, u)$; et, pour tout entier $m \geq 0$, $\pi^{2m}(r, u) = \big((ab)^m r,\ u\big)$ et la seconde composante de $\pi^{2m+1}(r, u)$ est différente de u.*

Démonstration. Comme $(u \circ \tau)(\ell) = u(\ell - 1)$, $\pi(r, u) = \sigma_{\ell-1}(r, u \circ \tau) = (ar, u \circ \tau)$. Pour $g \in W$, a) donne $\varphi(gr, u(\ell - 1)) = gag^{-1}$, d'où $\pi(gr, u) = (gar, u \circ \tau)$; puis, $(u \circ \tau)(\ell - 1) = u(\ell)$ et $(u \circ \tau) \circ \tau = u$, et a) donne $\varphi(gar, u(\ell)) = (ga)\, b\, (ga)^{-1}$, d'où $\pi(gar, u \circ \tau) = (gabr, u)$. La formule pour π^{2m} s'en déduit par récurrence, en appliquant la précédente à $g = (ab)^m$. Enfin $\pi^{2m+1}(r, u) = \pi\big((ab)^m r, u\big)$ a pour seconde composante $u \circ \tau$, et $(u \circ \tau)(\ell) = u(\ell - 1) \neq u(\ell)$ puisque u est injective. □

Lemme 52.3. *Pour tout entier $k \geq 0$, $\pi^k(r, u) = (r, u)$ si et seulement si $2\, n_{u(\ell-1),\, u(\ell)}$ divise k.*

Démonstration. Si $k = 2m$ est pair, $\pi^k(r, u) = ((ab)^m r, u)$ par le lemme 52.2 ; l'action étant libre, c'est (r, u) si et seulement si $(ab)^m = 1$, c'est-à-dire si et seulement si $\mathrm{ord}(ab)$ divise m, soit $2\,\mathrm{ord}(ab)$ divise k. Si k est impair, $\pi^k(r, u) \neq (r, u)$ par le même lemme, et $2\,\mathrm{ord}(ab)$ ne divise pas k. Enfin $ab = \varphi(r, u(\ell - 1))\varphi(r, u(\ell))$ est d'ordre $n_{u(\ell-1),u(\ell)}$ par le lemme suivant, qui assure que cet ordre ne dépend pas de r. □

Lemme 52.4. *L'ordre de $\varphi(r, i)\varphi(r, j)$ ne dépend pas de $r \in R$. Et pour $i \neq j$ dans I, il existe $u \in \mathrm{Rep}'(I)$ avec $u(\ell - 1) = i$ et $u(\ell) = j$.*

Démonstration. Soient $r, r' \in R$; par transitivité, $r' = wr$ pour un $w \in W$, et par a), $\varphi(r', i)\varphi(r', j) = w\, \varphi(r, i)\varphi(r, j)\, w^{-1}$, qui est conjugué de $\varphi(r, i)\varphi(r, j)$ et a donc le même ordre. Pour la seconde assertion, partons d'une bijection $e : [1, \ell] \to I$, qui existe puisque I a ℓ éléments. On la compose à gauche par la transposition de $e(\ell - 1)$ et de i, pour obtenir u_1 avec $u_1(\ell - 1) = i$, puis par la transposition de $u_1(\ell)$ et de j. Comme $u_1(\ell) \neq i$ et $j \neq i$, cette seconde transposition fixe i, et la bijection obtenue envoie $\ell - 1$ sur i et ℓ sur j. □

Démonstration de la proposition. Par le lemme 52.1, $\sigma_{\ell-2}\sigma_{\ell-1}$ a le même ordre que π. Montrons que $\pi^k = \mathrm{id}$ si et seulement si $2n_{ij}$ divise k pour tous $i \neq j$. Si $\pi^k = \mathrm{id}$ et $i \neq j$, prenons u comme au lemme 52.4 et un r quelconque de R, qui n'est pas vide : le lemme 52.3 en (r, u) donne $2n_{ij} \mid k$. Réciproquement, pour tout (r, u), les indices $u(\ell - 1)$ et $u(\ell)$ sont distincts, et le lemme 52.3 donne $\pi^k(r, u) = (r, u)$. Or $2n_{ij} \mid k$ pour tous $i \neq j$ équivaut à $2\nu \mid k$: si c'est le cas pour tous, k est pair, puisqu'il existe au moins un couple $i \neq j$, et $k/2$ est un multiple commun des n_{ij}, donc de ν ; la réciproque vient de ce que chaque n_{ij} divise ν. Ainsi $\{k \mid \pi^k = \mathrm{id}\} = 2\nu\,\mathbf{Z}$, et l'ordre de π est 2ν. □

Démonstration de l'arithmétique de (6). Pour $p, q \geq 1$, $\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$, $= \frac{1}{2}$, $< \frac{1}{2}$ équivalent respectivement à $pq < 2(p + q)$, $pq = 2(p + q)$, $pq > 2(p + q)$, c'est-à-dire à $(p - 2)(q - 2) < 4$, $= 4$, > 4. Si $p \geq 7$, $pq < 2(p + q)$ entraîne $q \leq 2$, et symétriquement ; hors de ces cas, il reste un nombre fini de couples avec $p, q \leq 6$, qu'on examine un à un. Pour (1), $p = 2$ ou $q = 2$ donnent $0 < 4$; $p = 1$ n'est permis qu'avec $q = 2$, et $q = 1$ qu'avec $p = 2$; pour $p, q \geq 3$, $(p - 2)(q - 2) \in \{1, 2, 3\}$ laisse exactement $(3, 3)$, $(3, 4)$, $(4, 3)$, $(3, 5)$, $(5, 3)$. Pour (2), p ou q égal à 1 ou 2 est exclu, puisque $(p - 2)(q - 2)$ vaut alors 0, ou $2 - q$ ou $2 - p$, qui est au plus 1 ; pour $p, q \geq 3$, $(p - 2)(q - 2) = 4$ donne $(3, 6)$, $(4, 4)$, $(6, 3)$. Pour (3), les couples $p, q \geq 3$ qui

ne vérifient pas $(p-2)(q-2) > 4$ sont les huit couples obtenus en (1) et (2). Six d'entre eux, les cinq de (1) et $(4,4)$, sont exactement les couples $p, q \geq 3$ de somme au plus 8 ; les deux autres, $(3,6)$ et $(6,3)$, sont de somme 9. Un couple $p, q \geq 3$ vérifie donc $(p-2)(q-2) > 4$ si et seulement si $p+q \geq 9$ et $(p,q) \neq (3,6), (6,3)$. □

La figure 9 place les types (p,q) autour de l'hyperbole $(p-2)(q-2) = 4$, qui porte les trois types euclidiens et sépare les sphériques, en dessous, des hyperboliques, au-dessus. La droite $p+q = 9$ du point (3) passe par $(3,6)$ et $(6,3)$, sur l'hyperbole, et laisse en dessous les six autres couples $p, q \geq 3$ qui ne sont pas hyperboliques.

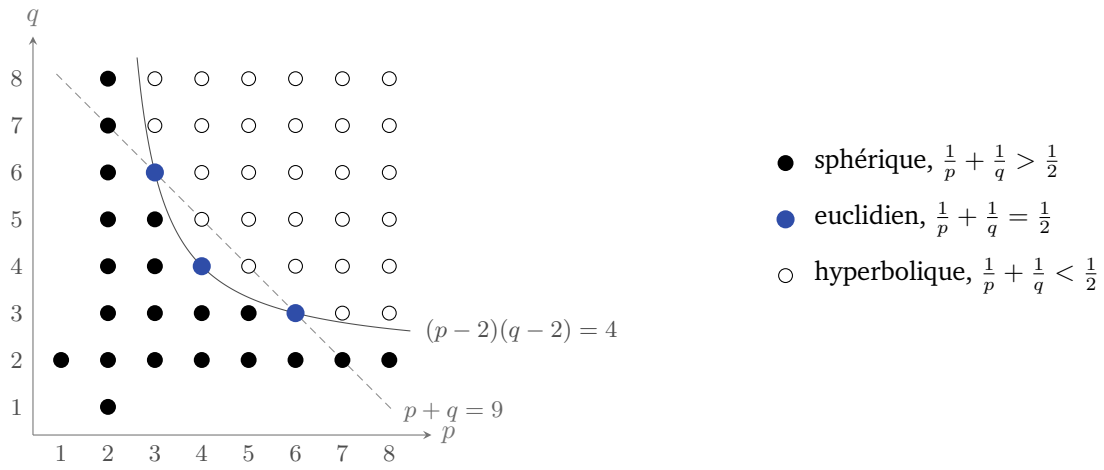


FIGURE 9 – Les types (p,q) atteints, $p, q \leq 8$. Les sphériques sont les $(2,q)$, les $(p,2)$ et les cinq types platoniciens $(3,3)$, $(3,4)$, $(4,3)$, $(3,5)$, $(5,3)$; les euclidiens, sur l'hyperbole, sont $(4,4)$, $(3,6)$, $(6,3)$. Parmi les $p, q \geq 3$, les hyperboliques sont les couples de somme au moins 9, hors de $(3,6)$ et $(6,3)$. Les types $(1,q)$, $q \neq 2$, et $(p,1)$, $p \neq 2$, sont exclus.

Remarque. La proposition demande seulement un groupe W opérant librement et transitivement sur R et une application φ vérifiant a) et $\varphi(r,i)^2 = 1$. Que W soit un groupe de Weyl, la condition b), la présentation c) et le graphe de Coxeter d) n'interviennent pas.

Remarque. La finitude de W n'intervient pas : avec la convention adoptée pour l'ordre, la formule 2ν vaut encore quand un n_{ij} est infini.

Remarque. La page 14 écrit la condition (c_2) « $p+q \geqslant 10$ ou $(p,q) \neq (3,6), (6,3)$ » ; la forme juste, que la lecture rétablit et qui est démontrée en (3), est $p+q \geq 9$ *et* $(p,q) \neq (3,6), (6,3)$.

Remarque. La répartition des types (p,q) en sphériques, euclidiens et hyperboliques selon le signe de $\frac{1}{p} + \frac{1}{q} - \frac{1}{2}$ figure au chapitre 8 de Coxeter et Moser (1957) [38]. La réalisation de toute carte de type (p,q) comme quotient de la carte universelle par un sous-groupe du groupe triangulaire, régulière si et seulement si le sous-groupe est distingué, est due à Jones et Singerman (1978) [77].

Remarque. Dans la lecture, la présentation de Coxeter du groupe cartographique, $\widehat{\Gamma} = \langle \sigma_0, \sigma_1, \sigma_2 \mid \sigma_i^2,\ (\sigma_0\sigma_2)^2 \rangle$, est une définition reprise de l'*Esquisse d'un programme*. Elle n'appelle pas de démonstration.

Ne sont pas démontrés ici : l'application $\mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Phi(\Sigma))$ (pages 3 et 4) ; les autres relations entre les σ_i ; la triangulation de la sphère ; les articles (1) à (5) et (7) ; le contenu géométrique de (6).

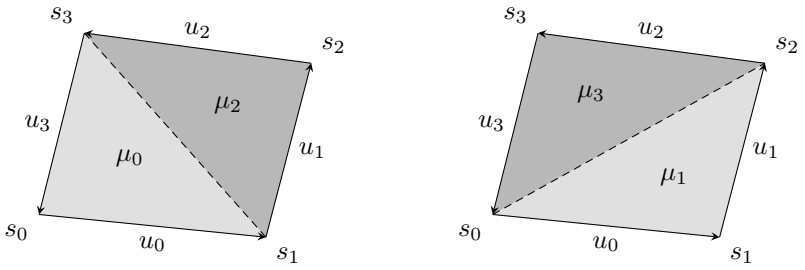
53 Cote 73 : les aires des oreilles d'un polygone plan [56]

La cote 73, *Polygones : notes manuscrites (s.d.), lettre (s.d.)*, vingt-huit pages que l'inventaire date « [à partir de 1976] », étudie l'application qui envoie un polygone plan, donné par ses côtés $u_i = s_{i+1} - s_i$, sur les aires algébriques doublées de ses « oreilles », les triangles $s_{i-1}s_is_{i+1}$: $\mu_i = u_{i-1} \wedge u_i$. La page 5, consacrée au quadrilatère fermé, établit $\mu_0 + \mu_2 = \mu_1 + \mu_3$, écrit « $\mathbf{M}_4 \to \mathbf{P}^2_{\mathbf{Z}}$ mono », puis « épi ? », donne les formules inverses et conclut « $\mathbf{M}_4 \simeq \mathbf{P}^2_{\mathbf{Z}}$ » ; elle encadre $u_2 = 0 \Leftrightarrow \mu_2 = \mu_3 = 0$ (73, lot 1, p. 5). La page 6 parle de « l'enveloppe projective de A », l'ensemble des arêtes (73, lot 1, p. 6). Les pages 14 et 15 écrivent la relation des multiplicateurs de Lagrange et encadrent la formule close $\lambda_i u_{i-1} u_i = -\lambda_0 u_{-1} u_{1i} + \lambda_1 u_1 u_{0i}$ (73, lot 1, p. 15). La page 18 pose $\lambda_0 = 0$ et dessine un ennéagone étoilé (73, lot 1, p. 18). Le bas de la page 28 énonce, pour le « cas spécial II », un critère : « a) $\sum u_i = 0$; b) $u_{i-1}, u_i \parallel u_1, u_{0i}$ », précédé d'un « il faut et il suffit » lu avec doute, et ajoute que les i tels que $\lambda_i = 0$ sont ceux pour lesquels $s_i = s_0$ (73, lot 2, p. 28).

Conventions. k est un corps et $V = k^2$, muni de la forme volume $a \wedge b = a_0 b_1 - a_1 b_0$. Une application affine agit sur les côtés par sa partie linéaire, une matrice M d'ordre 2. Pour un quadrilatère, les indices sont pris modulo 4 ; il est fermé quand $u_0 + u_1 + u_2 + u_3 = 0$, et aligné quand tous les $u_i \wedge u_j$ sont nuls. Pour un n-gone, $n \geq 3$, les côtés sont indexés par $\mathbf{Z}/n\mathbf{Z}$ et $u_{0i} = u_0 + \cdots + u_{i-1} = s_i - s_0$. Comme la lecture, on lit la juxtaposition $u\,v$ de la page comme le produit $u \cdot v$ dans le carré symétrique $\mathrm{Sym}^2 V$, identifié à k^3 par $a \cdot b = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_1 b_1)$: ce sont les coefficients de la forme quadratique $(a_0 X + a_1 Y)(b_0 X + b_1 Y)$. L'espace $N(u_*)$ des multiplicateurs est celui des $(\lambda_i) \in k^{\mathbf{Z}/n\mathbf{Z}}$ tels que

$$(*) \qquad \lambda_i u_{i-1} - \lambda_{i+1}(u_i + u_{i+1}) + \lambda_{i+2} u_{i+2} = 0 \qquad \text{pour tout } i.$$

L'oreille en s_i est le triangle $s_{i-1}s_is_{i+1}$, d'aire algébrique doublée $\mu_i = u_{i-1} \wedge u_i$. Pour un quadrilatère convexe parcouru dans le sens direct, les oreilles en s_0 et s_2 se partagent le quadrilatère le long de la diagonale s_1s_3, celles en s_1 et s_3 le long de s_0s_2 : $\mu_0 + \mu_2$ et $\mu_1 + \mu_3$ valent l'un et l'autre le double de son aire. Dans ce cas, la relation du théorème ci-dessous se lit sur la figure.



Théorème 53.1 (D'après les pages 5 et 6, forme complétée par l'édition, les quadrilatères forment un plan projectif ♦). *Soient $u = (u_0, u_1, u_2, u_3)$ et u' deux quadrilatères fermés de V.*

1. *On a $u_0 \wedge u_2 = \mu_0 - \mu_1 = \mu_3 - \mu_2$ et $u_1 \wedge u_3 = \mu_1 - \mu_2 = \mu_0 - \mu_3$; donc $\mu_0 + \mu_2 = \mu_1 + \mu_3$, et u est aligné si et seulement si tous les μ_i sont nuls. Ces identités valent sur tout anneau commutatif.*
2. *Une matrice M multiplie tous les μ_i par $\det M$. Si u n'est pas aligné, les $\mu_i(u')$ sont proportionnels aux $\mu_i(u)$, de rapport non nul, si et seulement s'il existe M inversible avec $u'_i = Mu_i$*

56. Preuve vérifiée : `lean/Grothendieck/Folder73.lean`.

pour tout i ; on peut prendre $\det M$ égal au rapport.

3. *Tout $(m_0, m_1, m_2, m_3) \neq 0$ tel que $m_0 + m_2 = m_1 + m_3$ est le vecteur (μ_i) d'un quadrilatère fermé.*
4. *Si u n'est pas aligné, $u_i = 0$ équivaut à $\mu_i = \mu_{i+1} = 0$, et alors $(\mu_j) = \mu_{i+2}\, p_i$ avec $\mu_{i+2} \neq 0$, où $p_0 = (0,0,1,1)$, $p_1 = (1,0,0,1)$, $p_2 = (1,1,0,0)$, $p_3 = (0,1,1,0)$.*
5. *La seule relation linéaire entre les p_i est $p_0 - p_1 + p_2 - p_3 = 0$: trois quelconques d'entre eux sont indépendants, et les quatre forment un repère projectif du plan $\Pi = \{m_0 + m_2 = m_1 + m_3\}$. L'application linéaire $e_i \mapsto (-1)^i p_i$ induit un isomorphisme $k^4/k \cdot (1,1,1,1) \simeq \Pi$.*

Ainsi les quadrilatères fermés non alignés, à transformation affine près, sont en bijection avec les points du plan projectif $\mathbf{P}(\Pi) \simeq \mathbf{P}\big(k^A/k \cdot (1,1,1,1)\big)$, et la droite de l'arête i y est le quadrilatère où cette arête est réduite à un point.

Démonstration. 1. On remplace u_3 par $-(u_0 + u_1 + u_2)$ et l'on développe : les quatre identités sont polynomiales en les coordonnées. Elles expriment les six produits $u_i \wedge u_j$ par les μ_i, qui sont les produits de côtés consécutifs ; si les μ_i sont nuls, tous les $u_i \wedge u_j$ le sont.

2. $Ma \wedge Mb = \det M\,(a \wedge b)$. Pour la réciproque, supposons d'abord $\mu_1(u) \neq 0$: u_0, u_1 est une base de V. La formule de Cramer $(a \wedge b)\, x = (x \wedge b)\, a + (a \wedge x)\, b$, appliquée à u_0, u_1, u_2, donne avec la première identité la carte de la page 5 :

$$\mu_1 u_2 = -\mu_2 u_0 + (\mu_3 - \mu_2) u_1.$$

Soit M l'endomorphisme qui envoie u_0, u_1 sur u'_0, u'_1. Si $\mu(u') = c\,\mu(u)$ avec $c \neq 0$, la carte de u', divisée par c, s'écrit $\mu_1 u'_2 = -\mu_2 M u_0 + (\mu_3 - \mu_2) M u_1 = \mu_1 M u_2$, d'où $u'_2 = M u_2$, puis $u'_3 = M u_3$ par fermeture. Enfin $\det M \cdot \mu_1 = \mu_1(u') = c\,\mu_1$ donne $\det M = c$. Si c'est un autre μ_i qui est non nul, on se ramène à ce cas par permutation circulaire des indices, qui préserve la fermeture et décale les μ_i.

3. Si $m_1 \neq 0$, le quadrilatère $u_0 = (m_1, 0)$, $u_1 = (0,1)$, $u_2 = (-m_2, (m_3 - m_2)/m_1)$, $u_3 = -(u_0 + u_1 + u_2)$ a $\mu_1 = m_1$, $\mu_2 = m_2$, $\mu_3 = m_3$, et $\mu_0 = m_1 + m_3 - m_2 = m_0$ par la relation. Sinon on décale les indices.

4. Si $u_i = 0$, les deux oreilles qui contiennent u_i sont plates, et la relation du point 1 donne $\mu_{i+2} = \mu_{i+3}$ ou son analogue, d'où $(\mu_j) = \mu_{i+2}\, p_i$; si μ_{i+2} était nul, tous les μ_j le seraient. Réciproquement, ramenons-nous par décalage à $i = 1$, et supposons $\mu_1 = \mu_2 = 0$ et $u_1 \neq 0$. La formule de Cramer pour u_0, u_1, u_2 se réduit à $(u_0 \wedge u_2)\, u_1 = 0$, donc $u_0 \wedge u_2 = 0$, et le point 1 donne $\mu_0 = \mu_1 = 0$ et $\mu_3 = \mu_2 = 0$: le quadrilatère est aligné.

5. $\sum c_i p_i = (c_1 + c_2,\ c_2 + c_3,\ c_0 + c_3,\ c_0 + c_1)$, qui est nul si et seulement si c est multiple de $(1,-1,1,-1)$; un tel c avec une composante nulle est nul. L'application $c \mapsto \sum (-1)^i c_i p_i = (c_2 - c_1,\ c_2 - c_3,\ c_0 - c_3,\ c_0 - c_1)$ a pour noyau les vecteurs constants, et pour image Π : un point m de Π est l'image de $(m_2,\ m_2 - m_3,\ m_2 - m_3 + m_0,\ m_2 - m_3 + m_0 - m_1)$. □

Remarque. La deuxième ligne du tableau de la page 5, $u_1 \wedge u_3 = \mu_0 - \mu_2$, que la lecture reprend, est fausse : le quadrilatère $u = (e_1, e_2, e_2, -e_1 - 2e_2)$ a $u_1 \wedge u_3 = 1$ et $\mu_0 - \mu_2 = 2$. La valeur juste, $\mu_1 - \mu_2 = \mu_0 - \mu_3$, est celle que la quatrième ligne de la même page donne pour $u_3 \wedge u_1$; à la troisième ligne, la première valeur donnée pour $u_2 \wedge u_0$, $\mu_1 - \mu_3$, est fausse aussi (il faut $\mu_2 - \mu_3$), la seconde, $\mu_1 - \mu_0$, est juste. Le reste de la lecture n'en dépend pas : la relation $\mu_0 + \mu_2 = \mu_1 + \mu_3$ ne vient que de $u_0 \wedge u_2$. L'identification canonique du point 5 demande un signe : l'application $e_i \mapsto p_i$ a pour noyau $k \cdot (1,-1,1,-1)$, et c'est $e_i \mapsto (-1)^i p_i$ qui a pour

noyau $k\cdot(1,1,1,1)$; les droites, donc les points du plan projectif, sont les mêmes. La réponse à la question « épi ? » de la page 5 (point 3), le repère projectif et l'identification canonique du point 5 sont de la lecture ; la page 6 ne nomme que trois des quatre points. Le fichier démontre l'énoncé sur un corps, les identités sur tout anneau commutatif ; l'isomorphisme de schémas sur $\operatorname{Spec}\mathbf{Z}$ que suggère l'indice de $\mathbf{P}^2_{\mathbf{Z}}$ n'est pas formalisé.

Lemme 53.2 (paire de directions)**.** *Soient a,b,c,d des vecteurs non nuls de V. Le produit $c\cdot d$ est multiple de $a\cdot b$ dans $\operatorname{Sym}^2 V$ si et seulement si $\{[a],[b]\}=\{[c],[d]\}$ comme paires de droites, c'est-à-dire si $a\wedge c=b\wedge d=0$ ou $a\wedge d=b\wedge c=0$.*

Démonstration. Si $c\cdot d=t\,a\cdot b$, alors $t\neq 0$, car un produit de vecteurs non nuls n'est pas nul. Évaluons les formes quadratiques en $x=(y_1,-y_0)$, orthogonal à y : $a\cdot b$ y vaut $(a\wedge y)(b\wedge y)$. Pour $y=a,b,c,d$ on obtient

$$(a\wedge c)(a\wedge d)=0,\quad (b\wedge c)(b\wedge d)=0,\quad (a\wedge c)(b\wedge c)=0,\quad (a\wedge d)(b\wedge d)=0.$$

Si $a\wedge c\neq 0$, la première et la troisième donnent $a\wedge d=b\wedge c=0$. Si $a\wedge c=0$ et $b\wedge d\neq 0$, la deuxième et la quatrième donnent encore $b\wedge c=a\wedge d=0$. Réciproquement, $a\wedge c=0$ avec $a\neq 0$ donne $c=\alpha a$, et de même pour les autres paires ; alors $c\cdot d=\alpha\beta\,a\cdot b$. □

Théorème 53.3 (D'après les pages 15, 18 et 28, critère du cas spécial II, forme de l'édition ♦)**.** *Soient $n\geq 3$ et $u_*=(u_i)_{i\in\mathbf{Z}/n\mathbf{Z}}$ une suite de vecteurs non nuls de V. Il existe $\lambda\in N(u_*)$ avec $\lambda_0=0$ et $\lambda_1=1$ si et seulement si*

a) $\sum u_i=0$, et

b) pour $2\leq i\leq n-1$, ou bien $s_i=s_0$, c'est-à-dire $u_{0i}=0$, ou bien la paire de directions de $\{u_{i-1},u_i\}$ est celle de $\{u_1,u_{0i}\}$.

Un tel λ est alors unique, il vérifie $\lambda_i\,u_{i-1}\cdot u_i=u_1\cdot u_{0i}$ pour tout $i\geq 1$, et $\lambda_i=0$ si et seulement si $s_i=s_0$. Enfin un multiplicateur qui a deux composantes consécutives nulles est nul ; cela permet de normaliser $\lambda_1=1$ dès que $\lambda_0=0$.

Démonstration. Posons $L_i=\lambda_i u_{i-1}-\lambda_{i+1}u_{i+1}$. La relation $(*)$ en i est $L_i-L_{i+1}=0$: $(*)$ pour tout i dit que L_i ne dépend pas de i, et, avec $\lambda_0=0$, $\lambda_1=1$, que $L_i=L_0=-u_1$ pour tout i. Notons (S_i) l'identité $\lambda_i\,u_{i-1}\cdot u_i=u_1\cdot u_{0i}$, pour $i\geq 1$ entier, les indices de u et λ étant lus modulo n. (S_1) est $u_0\cdot u_1=u_1\cdot u_0$. Si (S_i) a lieu et que $L_i=-u_1$, c'est-à-dire $\lambda_{i+1}u_{i+1}=\lambda_i u_{i-1}+u_1$, on multiplie par u_i :

$$\lambda_{i+1}\,u_i\cdot u_{i+1}=\lambda_i\,u_{i-1}\cdot u_i+u_1\cdot u_i=u_1\cdot(u_{0i}+u_i)=u_1\cdot u_{0,i+1},$$

qui est (S_{i+1}). Réciproquement, (S_i) et (S_{i+1}) donnent $u_i\cdot(\lambda_i u_{i-1}-\lambda_{i+1}u_{i+1}+u_1)=0$, d'où $L_i=-u_1$ puisque $u_i\neq 0$ et qu'un produit de deux vecteurs n'est nul que si l'un l'est. Ainsi $(*)$ équivaut à (S_i) pour tout $i\geq 1$.

Si λ existe, (S_n) s'écrit $0=\lambda_0\,u_{n-1}\cdot u_0=u_1\cdot\sum_j u_j$, d'où a) ; et pour $2\leq i\leq n-1$ avec $u_{0i}\neq 0$, (S_i) dit que $u_1\cdot u_{0i}$ est multiple de $u_{i-1}\cdot u_i$, d'où b) par le lemme 53.2. Réciproquement, sous a) et b), le lemme donne pour chaque $2\leq i\leq n-1$ un scalaire λ_i avec $\lambda_i\,u_{i-1}\cdot u_i=u_1\cdot u_{0i}$ ($\lambda_i=0$ si $u_{0i}=0$) ; avec $\lambda_0=0$ et $\lambda_1=1$, les identités $(S_1),\dots,(S_n)$ ont lieu, (S_n) par a). Comme $u_{0,i+n}=\sum_j u_j+u_{0i}=u_{0i}$, (S_{i+n}) équivaut à (S_i), et toutes ont lieu : $\lambda\in N(u_*)$.

Pour $i\geq 1$, (S_i) donne $\lambda_i=0$ si et seulement si $u_1\cdot u_{0i}=0$, si et seulement si $u_{0i}=0$, et détermine λ_i puisque $u_{i-1}\cdot u_i\neq 0$; tout indice modulo n est de la forme $i\geq 1$, d'où l'unicité.

Enfin, si $\lambda_i = \lambda_{i+1} = 0$, $(*)$ en i se réduit à $\lambda_{i+2} u_{i+2} = 0$, donc $\lambda_{i+2} = 0$, et de proche en proche $\lambda = 0$. □

Remarque. Le critère tient tel que la lecture l'énonce : le « il faut et il suffit » lu avec doute à la page 28 est juste. La démonstration, celle de la lecture, est de l'édition ; elle n'utilise aucune hypothèse sur le corps : l'hypothèse « k infini » du théorème de la page 28 ne sert qu'à l'exhaustivité des quatre cas, qui n'est pas en jeu ici. La formule $\lambda_i\, u_{i-1} \cdot u_i = u_1 \cdot u_{0i}$ vaut pour tout $i \geq 1$ et pas seulement pour $2 \leq i \leq n-1$; c'est le cas $\lambda_0 = 0$, $\lambda_1 = 1$ de la formule close encadrée de la page 15. La paire de directions est la reformulation, par la lecture, du « $u_{i-1}, u_i \parallel u_1, u_{0i}$ » de la page ; le lemme 53.2 montre qu'elle équivaut à la proportionnalité dans $\mathrm{Sym}^2 V$.

Théorème 53.4 (D'après les pages 23 à 27, Proposition, forme corrigée par l'édition ♦). *Soient k un corps et $u_* = (u_i)_{i \in \mathbf{Z}/n\mathbf{Z}}$ une suite de vecteurs non nuls de V. Alors $\lambda \mapsto (\lambda_i, \lambda_{i+1})$ est injective sur $N(u_*)$, donc $\dim N(u_*) \leqslant 2$. Si de plus les u_i ne sont pas tous sur une même droite, $\dim N(u_*) = 2$ si et seulement si $3 \mid n$, $u_{i+3} = u_i$ pour tout i et $u_0 + u_1 + u_2 = 0$: le polygone est un triangle parcouru $n/3$ fois. $N(u_*)$ est alors le plan des λ de période 3 tels que $\lambda_0 + \lambda_1 + \lambda_2 = 0$, et il contient un élément sans composante nulle dès que k a au moins trois éléments.*

Lean : `finrank_multSpace_le_two`, `finrank_multSpace_eq_two_iff`, `isMult_periodic`, `exists_mult_ne_zero`. La démonstration est celle de la lecture ; l'implication (a) ⇒ (b) ne se sert que de la surjectivité de $\lambda \mapsto (\lambda_{i+1}, \lambda_{i+2})$ quand la dimension vaut 2, et le passage de (b) à (c) propage l'indépendance de deux côtés consécutifs.

Théorème 53.5 (Grothendieck, page 28, la dichotomie, sous une hypothèse plus faible ♦). *Soient u_* comme ci-dessus et k un corps ayant plus de n éléments. Ou bien $N(u_*)$ contient un λ sans composante nulle, ou bien $N(u_*)$ est contenu dans un hyperplan de coordonnées $H_i = \{\lambda_i = 0\}$, et alors $\dim N(u_*) \leqslant 1$. Un $N(u_*)$ de dimension 2 n'est contenu dans aucun H_i.*

Démonstration. Si aucun H_i ne contient $N(u_*)$, les $N(u_*) \cap H_i$ sont n sous-espaces stricts de $N(u_*)$, et un espace vectoriel sur un corps de plus de n éléments n'est pas réunion de n sous-espaces stricts (mathlib, `Submodule.iUnion_ssubset_of_forall_ne_top_of_card_lt`) : un élément de $N(u_*)$ évite tous les H_i. Si $N(u_*) \subset H_i$, l'application $\lambda \mapsto \lambda_{i+1}$ est injective sur $N(u_*)$, puisque deux composantes consécutives nulles annulent un multiplicateur. Enfin, en dimension 2, $\lambda \mapsto (\lambda_i, \lambda_{i+1})$ est surjective et atteint $(1, 0)$. □

Remarque. La page suppose k infini ; il suffit que k ait plus de n éléments, et l'hypothèse ne sert qu'à la dichotomie. L'hypothèse de non-alignement, que la lecture ajoute, est nécessaire (le segment $(e, -e, e, -e)$), et la condition $3 \mid n$, biffée sur la page, est conséquence des autres : si $3 \nmid n$, $u_{i+3} = u_i$ rend la suite constante (Lean : `triangle_of_collinear`, `dichotomy`, `finrank_le_one_of_le_hyperplane`).

Théorème 53.6 (D'après les pages 14 et 28, $N(u_*)$ est l'espace des multiplicateurs de Lagrange, forme de l'édition ♦). *Soient k un corps, $n \geqslant 1$ et $\varphi : V^{\mathbf{Z}/n\mathbf{Z}} \to k^{\mathbf{Z}/n\mathbf{Z}}$, $\varphi(u)_i = u_{i-1} \wedge u_i$, l'application « aires des oreilles ». Elle est quadratique : $\varphi(u+v) = \varphi(u) + d\varphi_u(v) + \varphi(v)$, avec $d\varphi_u(v)_i = v_{i-1} \wedge u_i + u_{i-1} \wedge v_i$, et sur un corps valué complet, $\mathbf{R}$ par exemple, $d\varphi_u$ est sa différentielle stricte en u. Pour $\lambda \in k^{\mathbf{Z}/n\mathbf{Z}}$, les conditions suivantes sont équivalentes :*

1. *$\lambda \in N(u_*)$;*

2. *il existe* $w \in V$ *tel que* $\sum_i \lambda_i\, d\varphi_{u*}(v)_i = w \wedge \sum_i v_i$ *pour tout* v *: c'est l'égalité* $\sum \lambda_i\, df_i = \mu \sum dx_i + \nu \sum dy_i$ *de la page 14;*
3. $\sum_i \lambda_i\, d\varphi_{u*}(v)_i = 0$ *pour toute déformation fermée,* $\sum_i v_i = 0$.

En particulier $N(u_*) = 0$ *si et seulement si* $d\varphi_{u*}$ *envoie les déformations fermées sur* $k^{\mathbf{Z}/n\mathbf{Z}}$ *: le cas général (a) de la page 28 est celui où* φ*, restreinte aux polygones de* $\sum u_i$ *fixé, est une submersion en* u_*.

Démonstration. L'identité quadratique se développe ; elle fait de $d\varphi_u$ la partie linéaire de φ en u, et la différentielle stricte vient de ce que $\varphi(u) = B(u,u)$ pour une application bilinéaire B, continue en dimension finie. Une sommation par parties donne $\sum_i \lambda_i\, d\varphi_u(v)_i = \sum_i L_i \wedge v_i$, où $L_i = \lambda_i u_{i-1} - \lambda_{i+1} u_{i+1}$ est la forme de Lagrange du théorème 53.3. Si $\lambda \in N(u_*)$, L_i ne dépend pas de i, et la somme vaut $L_0 \wedge \sum_i v_i$: c'est 2, et 2 entraîne 3. Réciproquement, la déformation $v = e$ en i, $-e$ en $i+1$, nulle ailleurs, est fermée, et 3 donne $(L_i - L_{i+1}) \wedge e = 0$ pour tout $e \in V$, d'où $L_i = L_{i+1}$: c'est $(*)$. Enfin, $N(u_*)$ est, par 3, l'orthogonal pour $\sum_i \lambda_i m_i$ de l'image W des déformations fermées ; si $W \neq k^{\mathbf{Z}/n\mathbf{Z}}$, une forme linéaire non nulle nulle sur W (mathlib, `Submodule.exists_dual_map_eq_bot_of_lt_top`) est un $\lambda \neq 0$ de $N(u_*)$; si W est tout l'espace, λ est orthogonal à chaque vecteur de base, donc nul. □

Lean : `earArea_add`, `hasStrictFDerivAt_earArea`, `isMult_iff_lagrange`, `isMult_iff_closed`, `multSpace_eq_bot_iff`. Aucune page ne fait le lien entre le $N(u_*)$ de la page 28 et les multiplicateurs de la page 14 ; il est de la lecture, et l'énoncé, qui ne suppose pas le polygone fermé, de l'édition.

Théorème 53.7 (Grothendieck, page 28, le théorème des quatre cas, sous une hypothèse plus faible ♦)**.** *Soient* k *un corps ayant plus de* n *éléments et* u_* *une suite de* n *vecteurs non nuls de* V*. On est dans un et un seul des cas suivants :*

- *(a)* cas général *:* $N(u_*) = 0$*;*
- *(*b_1*)* cas spécial I *:* $N(u_*)$ *contient un* λ *sans composante nulle, et* $\dim N(u_*) = 1$*;*
- *(*b_2*)* cas hyperspécial *:* $N(u_*)$ *contient un* λ *sans composante nulle, et* $\dim N(u_*) = 2$*;*
- *(c)* cas spécial II *:* $N(u_*) \neq 0$ *et* $N(u_*) \subset H_i$ *pour un* i*; alors* $\dim N(u_*) = 1$*, et* $N(u_*)$ *est la droite engendrée par l'unique multiplicateur tel que* $\lambda_i = 0$ *et* $\lambda_{i+1} = 1$*, auquel s'applique, pour* $i = 0$*, le critère du théorème 53.3.*

Démonstration. Par la dichotomie (théorème 53.5), ou bien un $\lambda \in N(u_*)$ n'a aucune composante nulle, ou bien $N(u_*)$ est dans un H_i. Dans le premier cas $\lambda \neq 0$, et $1 \leqslant \dim N(u_*) \leqslant 2$: c'est (b_1) ou (b_2). Dans le second, ou bien $N(u_*) = 0$, c'est (a), ou bien $1 \leqslant \dim N(u_*) \leqslant 1$, c'est (c). Les cas s'excluent : (a) interdit un λ sans zéro et nie $N(u_*) \neq 0$, (b_1) et (b_2) diffèrent par la dimension, et un $\lambda \in N(u_*)$ sans composante nulle n'est dans aucun H_i. En (c), un $\lambda \neq 0$ de $N(u_*)$ a $\lambda_i = 0$, donc $\lambda_{i+1} \neq 0$ (deux composantes consécutives nulles annulent tout) ; on le normalise, et il engendre la droite $N(u_*)$. □

Lean : `four_cases`, `four_cases_exclusive`, `special_two_span`. La page suppose k infini ; plus de n éléments suffit, et cette hypothèse ne sert qu'à l'exhaustivité. Le cas hyperspécial est décrit par le théorème 53.4 quand les u_i ne sont pas alignés.

Théorème 53.8 (D'après la page 18, l'ennéagone étoilé, forme de l'édition ♦). *Soient k un corps, $\beta_1, \beta_2, \beta_3 \in k \setminus \{0,1\}$ et $y_4, y_6, y_8 \in k$ avec $y_4 \neq \beta_1$, $y_6 \neq \beta_2 y_4$, $y_8 \neq \beta_3 y_6$, et l'ennéagone de sommets*

$$s_0 = (0,0),\ s_1 = (1,0),\ s_2 = (1,1),\ s_3 = (\beta_1, \beta_1),\ s_4 = (\beta_1, y_4),$$
$$s_5 = (\beta_2\beta_1, \beta_2 y_4),\ s_6 = (\beta_2\beta_1, y_6),\ s_7 = (\beta_3\beta_2\beta_1, \beta_3 y_6),\ s_8 = (\beta_3\beta_2\beta_1, y_8).$$

Alors $N(u_*)$ est une droite, engendrée par un multiplicateur λ tel que $\lambda_0 = 0$ et $\lambda_i \neq 0$ pour $i \neq 0$.

Démonstration. Les côtés sont non nuls. Le polygone est fermé ; pour i pair, u_{i-1} est vertical comme u_1 et u_i est porté par la droite $s_0 s_i$; pour i impair, u_i est vertical et s_i est sur la droite $s_0 s_{i-1}$, qui porte u_{i-1}. Le critère du théorème 53.3 donne un $\lambda \in N(u_*)$ avec $\lambda_0 = 0$ et $\lambda_1 = 1$, et $\lambda_i \neq 0$ pour $1 \leqslant i \leqslant 8$ puisque $s_i \neq s_0$: l'abscisse de s_i, pour $i \geqslant 3$, est un produit de β_j non nuls. Comme $u_0 \wedge u_1 = 1$ et que $u_4 \neq u_1$ (l'abscisse de u_4 est $(\beta_2 - 1)\beta_1 \neq 0$), le polygone n'est pas un triangle parcouru trois fois, et $\dim N(u_*) \neq 2$ par le théorème 53.4 ; donc $\dim N(u_*) = 1$. □

Lean : `nonagon`, `nonagon_multSpace`. La lecture le vérifiait numériquement « pour des valeurs génériques des paramètres » ; il vaut pour toutes les valeurs qu'autorise la page, sur tout corps. On est dans le cas spécial II, en $i = 0$.

Ne sont pas démontrés ici : l'équation du second degré du pentagone (page 19) et la formule de Gauss ; le foncteur Polg_n de la page 1 ; l'énoncé du plan projectif sur $\mathrm{Spec}\,\mathbf{Z}$.

54 Cote 74 : complexes cubiques généralisés, la réduction à un carré latin et à ses revêtements doubles [57]

La cote 74, *Complexes cubiques : notes manuscrites (s.d.)*, cent trente-cinq pages que l'inventaire date « [à partir de 1976] », tourne autour du graphe des vingt-sept droites d'une surface cubique. La liasse qui commence page 92 porte le titre « Complexes cubiques généralisés (complexes *triadiques* ou *trilatères* ?) ». Elle pose deux axiomes sur un graphe S : toute arête est contenue dans un unique triangle (axiome 1), et tout sommet hors d'un triangle est lié à un sommet de ce triangle (axiome 2). Elle fixe un triangle $t_0 = \{a, b, c\}$ et décompose le graphe autour de lui (74, lot 5, p. 92). Les pages 93 à 96 établissent les propositions 1 à 4 et la « Scholie » : le graphe se résume à trois ensembles $\widetilde{E}_\alpha$ munis d'involutions sans point fixe et à une partie $\widetilde{T}$ de leur produit, soumise aux conditions (*) et (**). Une troisième condition, notée (***), est écrite en travers de la marge gauche, encadrée, tournée de 90°, et rattachée par une accolade à (*) et (**). La transcription en lit le début, « si $(s_\alpha)_{\alpha\in t_0} \in \prod \widetilde{E}_\alpha$ et $(t_\alpha)_{\alpha\in t_0} \in \widetilde{T}$ tels que $s_\beta = \varphi_\beta(t_\alpha) \ldots \forall\, \alpha, \beta,\ \alpha \neq \beta$ », et la fin est illisible (74, lot 5, p. 96). La page 97 affirme que des données vérifiant (*) donnent un graphe qui vérifie l'axiome 1 et l'axiome 2 pour t_0 (74, lot 5, p. 97). Les pages 98 à 100 traitent l'axiome 2 pour les autres triangles : proposition 5 pour les triangles verticaux, axiome 3 (les $\widetilde{E}_\alpha$ sont non vides), proposition 6, barrée mais lisible, pour les triangles supérieurs (74, lot 5, p. 100). La page 101 reprend la liste des données, avec en (γ) « l'axiome (Ka) plus haut », et passe aux quotients $\Gamma = \widetilde{\Gamma}/\sigma$, $E_\alpha = \widetilde{E}_\alpha/\sigma_\alpha$ (74, lot 6, p. 101). La page 102 énonce l'axiome β_Γ, « $\Gamma \to E_\alpha \times E_\beta$ est *bijectif* », et partage la classification en deux questions, I) les systèmes de trois quotients vérifiant β_Γ, II) leurs revêtements d'ordre 2, puis ceux qui satisfont (Ka) (74, lot 6, p. 102, 74, lot 6, p. 103). La page 116 étudie, sur la relation

57. Preuve vérifiée : `lean/Grothendieck/Folder74.lean`.

$xyz = 1$ d'un groupe G, les applications φ_a et conclut que tout élément est d'ordre 2 (74, lot 6, p. 116).

Conventions. Un graphe est sans boucle ni arête multiple ; un triangle est un ensemble de trois sommets deux à deux liés. On indexe t_0 par $\{0,1,2\}$, $t_0 = \{t_0(\alpha)\}$. Pour $\alpha \in t_0$, $\widetilde{E}_\alpha$ est l'ensemble des sommets hors de t_0 liés à $t_0(\alpha)$. Un triangle supérieur est un triplet $x = (x_\alpha)$ avec $x_\alpha \in \widetilde{E}_\alpha$ et les x_α deux à deux liés ; leur ensemble est $\widetilde{\Gamma}$ (le $\widetilde{T}$ de la page 96 ; figure 10). Pour des données abstraites $(\widetilde{E}_\alpha, \sigma_\alpha, \widetilde{T})$, deux points $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$, $\alpha \neq \beta$, sont *liés* s'il existe $\tau \in \widetilde{T}$ avec $\tau_\alpha = s$ et $\tau_\beta = u$. Le graphe des données a pour sommets $t_0 \amalg \coprod_\alpha \widetilde{E}_\alpha$ et pour arêtes celles de 2°) α) à δ) de la page 96 : deux sommets de t_0, $t_0(\alpha)$ et les points de $\widetilde{E}_\alpha$, s et $\sigma_\alpha s$, deux points liés. Les conditions sur les données sont :

(*) deux éléments de $\widetilde{T}$ qui ont deux coordonnées communes sont égaux ;

($\beta_{\widetilde{\Gamma}}$) pour $\alpha \neq \beta$, $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$, un et un seul des deux points s, $\sigma_\alpha s$ est lié à u (c'est la forme de la page 101, qui contient (**)) ;

(Ka) pour $\{\alpha,\beta,\gamma\} = t_0$ et $\tau, \rho_1, \rho_2 \in \widetilde{T}$ tels que $\tau_\alpha = (\rho_1)_\alpha$, $\tau_\beta = (\rho_2)_\beta$ et $(\rho_1)_\gamma = (\rho_2)_\gamma$, on a $\tau = \rho_1$.

La condition (Ka) ainsi écrite est une restitution. Elle porte sur une famille (s_α) et trois triplets de $\widetilde{T}$, chacun contenant deux des s_α, comme le début lisible de la marge. On note (Ka′) la forme qui garde la phrase de la marge et la complète par la conclusion $(s_\alpha) \in \widetilde{T}$: si $(s_\alpha) \in \prod \widetilde{E}_\alpha$ et $(t_\alpha) \in \widetilde{T}^{t_0}$ vérifient $(t_\alpha)_\beta = s_\beta$ pour $\alpha \neq \beta$, alors $(s_\alpha) \in \widetilde{T}$.

Énoncé (Pages 92 à 99, autour d'un triangle ♦). *Soit S un graphe vérifiant les axiomes 1 et 2, et t_0 un triangle de S.*

1. *(Page 92, (1)) Tout sommet hors de t_0 est lié à un et un seul sommet de t_0 ; les $\widetilde{E}_\alpha$ sont disjoints et recouvrent $S \smallsetminus t_0$.*
2. *(Prop. 1) Pour $s \in \widetilde{E}_\alpha$, le troisième sommet $\sigma_\alpha s$ du triangle de l'arête $\{t_0(\alpha), s\}$ est dans $\widetilde{E}_\alpha$, et c'est le seul point lié à la fois à $t_0(\alpha)$ et à s. L'application σ_α est une involution sans point fixe de $\widetilde{E}_\alpha$.*
3. *(Prop. 2 et 5) Pour $\beta \neq \alpha$ et $u \in \widetilde{E}_\beta$, u est lié à un et un seul des points s, $\sigma_\alpha s$.*
4. *(Prop. 3 et 4) Si $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$, $\alpha \neq \beta$, sont liés, le troisième sommet du triangle de l'arête $\{s,u\}$ est dans $\widetilde{E}_\gamma$, γ le troisième indice ; il existe donc un triangle supérieur x avec $x_\alpha = s$, $x_\beta = u$, et il est unique.*
5. *(Page 98, corollaires) Si s et u sont liés, $\sigma_\alpha s$ et $\sigma_\beta u$ le sont ; $\widetilde{\Gamma}$ est stable par $\sigma = \prod_\alpha \sigma_\alpha$, qui y est sans point fixe.*

Énoncé (Pages 99, 101 et 102, le carré latin et les revêtements doubles ♦). *Sous les mêmes hypothèses, soient $E_\alpha = \widetilde{E}_\alpha/\sigma_\alpha$, $\Gamma = \widetilde{\Gamma}/\sigma$ et $\varphi_\alpha : \Gamma \to E_\alpha$ l'application induite par $x \mapsto x_\alpha$.*

1. *(Axiome β_Γ) Pour $\alpha \neq \beta$, l'application $(\varphi_\alpha, \varphi_\beta) : \Gamma \to E_\alpha \times E_\beta$ est bijective : Γ est un carré latin sur les trois E_α.*
2. *(Page 101) Pour tout α, l'application $x \mapsto (\bar{x}, x_\alpha)$ est une bijection de $\widetilde{\Gamma}$ sur le produit fibré $\Gamma \times_{E_\alpha} \widetilde{E}_\alpha$: $\widetilde{\Gamma}$ est l'image inverse du revêtement double $\widetilde{E}_\alpha \to E_\alpha$ par φ_α.*
3. *(Page 102) Les composés $\psi_{\beta\alpha} : \Gamma \times_{E_\alpha} \widetilde{E}_\alpha \to \Gamma \times_{E_\beta} \widetilde{E}_\beta$ de ces bijections sont des isomorphismes au-dessus de Γ, et forment un système transitif : $\psi_{\gamma\beta} \circ \psi_{\beta\alpha} = \psi_{\gamma\alpha}$, $\psi_{\alpha\alpha} = \mathrm{id}$.*
4. *(Pages 99 et 104) $|\widetilde{E}_\alpha| = 2\,|E_\alpha|$, $|\widetilde{\Gamma}| = 2\,|\Gamma|$, et $|\Gamma| = |E_\alpha|\,|E_\beta|$ pour $\alpha \neq \beta$. Si $\widetilde{E}_\alpha$ est non vide, E_β et E_γ sont en bijection.*

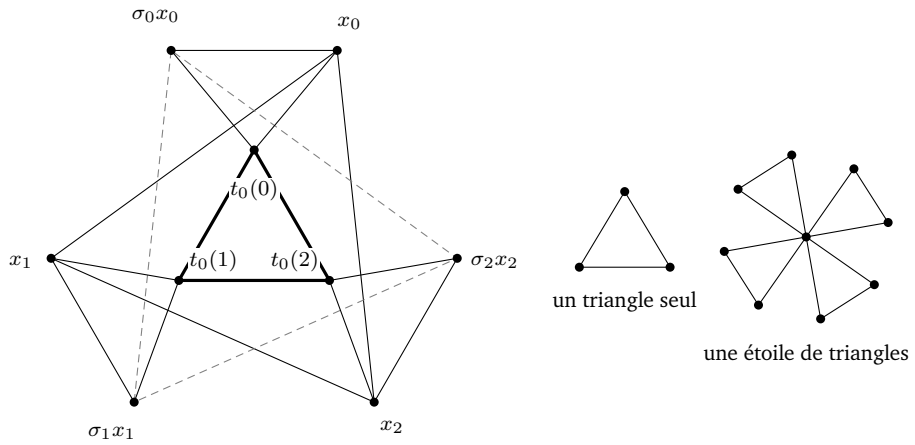


FIGURE 10 – À gauche, autour du triangle t_0 (en gras) : un triangle supérieur x et son image σx (en tirets). L'arête $\{t_0(\alpha), x_\alpha\}$ est dans l'unique triangle $\{t_0(\alpha), x_\alpha, \sigma_\alpha x_\alpha\}$ (proposition 1) ; x_α est lié à x_β et pas à $\sigma_\beta x_\beta$ (propositions 2 et 5). À droite, les deux graphes que l'axiome 3 de la page 100 écarte ; leur $\widetilde{\Gamma}$ est vide. Figure de l'édition ; Grothendieck dessine en marge de la page 100 un prisme triangulaire et une étoile de triangles (74, lot 5, p. 100).

Théorème 54.1 (Pages 96–100 corrigées par l'édition, Scholie et réciproque ♦). *1. (Scholie) Le graphe S est isomorphe au graphe de ses données $(\widetilde{E}_\alpha, \sigma_\alpha, \widetilde{\Gamma})$, et ces données vérifient (*), $\beta_{\widetilde{\Gamma}}$ et (Ka).*

2. (Réciproque) Pour des données vérifiant $\beta_{\widetilde{\Gamma}}$ et (Ka), le graphe des données vérifie les axiomes 1 et 2, et t_0 en est un triangle. Ses triangles supérieurs sont les éléments de $\widetilde{T}$: trois points deux à deux liés hors de t_0 sont les trois coordonnées d'un $\tau \in \widetilde{T}$.

3. Pour des données vérifiant (*) et $\beta_{\widetilde{\Gamma}}$, le graphe vérifie l'axiome 1 si et seulement si (Ka) est vraie.

4. (Ka) entraîne (*), et (Ka) équivaut à la conjonction de (*) et de (Ka′).

Énoncé (Pages 101 à 103, problèmes I et II ♦). *Soient Γ un ensemble, $\varphi_\alpha : \Gamma \to E_\alpha$ ($\alpha \in t_0$) trois applications vérifiant β_Γ, $p_\alpha : \widetilde{E}_\alpha \to E_\alpha$ trois revêtements doubles, c'est-à-dire des applications dont les fibres sont les orbites d'une involution sans point fixe σ_α, et $\widetilde{\Gamma}$ un ensemble muni de $\pi : \widetilde{\Gamma} \to \Gamma$ et de $\psi_\alpha : \widetilde{\Gamma} \to \widetilde{E}_\alpha$ tels que $p_\alpha \psi_\alpha = \varphi_\alpha \pi$ et que $(\pi, \psi_\alpha) : \widetilde{\Gamma} \to \Gamma \times_{E_\alpha} \widetilde{E}_\alpha$ soit bijective pour tout α. Alors les données $(\widetilde{E}_\alpha, \sigma_\alpha, \widetilde{T})$, $\widetilde{T}$ l'image de $(\psi_\alpha)_\alpha$, vérifient (*) et $\beta_{\widetilde{\Gamma}}$. Si elles vérifient (Ka), leur graphe vérifie les axiomes 1 et 2 ; il vérifie l'axiome 1 si et seulement si elles vérifient (Ka). Un graphe muni d'un triangle t_0 fournit de telles données par l'énoncé précédent.*

Contre-exemple (Pages 96 et 97, contre-exemple de l'édition : la condition (Ka) est nécessaire). *Soient $E_\alpha = \mathbb{Z}/2$, $\widetilde{E}_\alpha = \mathbb{Z}/2 \times \mathbb{Z}/2$, $\sigma_\alpha(u, e) = (u, e + 1)$, et $\widetilde{T}$ l'ensemble des triplets $((u, e), (v, e), (u + v, e))$. Ce sont les données du carré latin d'ordre 2, table de $\mathbb{Z}/2$, avec trois revêtements triviaux. Elles vérifient (*) et $\beta_{\widetilde{\Gamma}}$, et ne vérifient pas (Ka). Leur graphe ne vérifie pas l'axiome 1 : l'arête qui joint $(0, 0) \in \widetilde{E}_a$ à $(0, 0) \in \widetilde{E}_b$ est contenue dans deux triangles, fermés par $(0, 0)$ et par $(1, 0) \in \widetilde{E}_c$.*

Énoncé (Page 116 ♦). *Soit G un groupe. Les applications $\varphi_a : (x, y, z) \mapsto (x, a^{-1}z^{-1}, a^{-1}y^{-1})$ préservent la relation $xyz = 1$ pour tout $a \in G$ si et seulement si $g^2 = 1$ pour tout $g \in G$. Le groupe G est alors commutatif.*

Démonstration des pages 92 à 99. (1) Soit s hors de t_0. L'axiome 2 pour t_0 donne un sommet de t_0 lié à s. S'il y en avait deux, $t_0(\alpha)$ et $t_0(\beta)$, l'arête $\{t_0(\alpha), t_0(\beta)\}$ serait contenue dans le triangle t_0 et dans le triangle qu'elle forme avec s ; l'axiome 1 donnerait $s = t_0(\gamma)$, contre l'hypothèse.

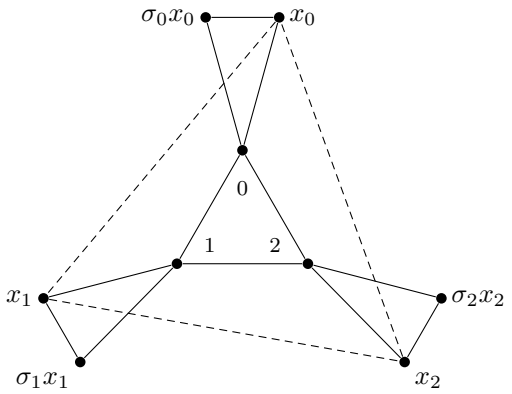
(2) Soit $s \in \widetilde{E}_\alpha$ et z le troisième sommet du triangle de $\{t_0(\alpha), s\}$. Si z était un sommet $t_0(\beta)$ de t_0, on aurait $\beta \neq \alpha$ et s serait lié à $t_0(\alpha)$ et à $t_0(\beta)$, contrairement à (1) ; donc $z \in \widetilde{E}_\alpha$. Tout point lié à $t_0(\alpha)$ et à s est égal à z par l'axiome 1. Le point s est lié à $t_0(\alpha)$ et à $\sigma_\alpha s$, donc $\sigma_\alpha \sigma_\alpha s = s$, et $\sigma_\alpha s \neq s$ puisque s et $\sigma_\alpha s$ sont liés.

(3) Si u était lié à s et à $\sigma_\alpha s$, l'arête $\{s, \sigma_\alpha s\}$ serait contenue dans le triangle qu'elle forme avec $t_0(\alpha)$ et dans celui qu'elle forme avec u, d'où $u = t_0(\alpha)$, absurde (proposition 2 ; l'hypothèse $\beta \neq \alpha$ n'y sert pas). L'axiome 2 pour le triangle vertical $\{t_0(\alpha), s, \sigma_\alpha s\}$ lie u à l'un de ses trois sommets ; ce n'est pas $t_0(\alpha)$ par (1), puisque u est lié à $t_0(\beta)$; c'est donc s ou $\sigma_\alpha s$ (proposition 5).

(4) Soit z le troisième sommet du triangle de $\{s, u\}$. Si z était un sommet $t_0(\delta)$, (1) donnerait $\delta = \alpha$ et $\delta = \beta$. Par (1), z est dans un $\widetilde{E}_\delta$. Si $\delta = \alpha$, z est lié à $t_0(\alpha)$ et à s, donc $z = \sigma_\alpha s$ par (2), et u est lié à s et à $\sigma_\alpha s$, contrairement à (3) ; de même $\delta \neq \beta$. Donc $\delta = \gamma$, et (s, u, z), rangé selon les indices, est un triangle supérieur. Deux triangles supérieurs x, y avec $x_\alpha = y_\alpha$ et $x_\beta = y_\beta$ ont x_γ et y_γ liés à x_α et à x_β, donc égaux par l'axiome 1.

(5) Si s et u sont liés, $\sigma_\beta u$ n'est pas lié à s par (3) appliqué au triangle vertical de u ; il est donc lié à $\sigma_\alpha s$ par (3) appliqué au triangle vertical de s. Les coordonnées de σx sont donc deux à deux liées, et $\sigma x \neq x$ puisque σ_α est sans point fixe. □

La décomposition autour de t_0, dont les sommets sont marqués $\alpha = 0, 1, 2$: à chaque sommet $t_0(\alpha)$, un triangle vertical, formé de $t_0(\alpha)$, d'un point x_α de $\widetilde{E}_\alpha$ et de $\sigma_\alpha x_\alpha$; en tirets, un triangle supérieur $x = (x_0, x_1, x_2)$; son image σx relie de même les trois points $\sigma_\alpha x_\alpha$ (point 5). Chacun des points x_β, $\beta \neq \alpha$, est lié à un seul des deux points x_α, $\sigma_\alpha x_\alpha$ (point 3).



Lemme 54.2. *Soit X un ensemble muni d'une involution sans point fixe f. Le choix d'un représentant dans chaque orbite donne une bijection $X \simeq X/f \times \{0, 1\}$; en particulier $|X| = 2\,|X/f|$.*

Démonstration. Soit $r(q)$ le représentant de l'orbite q. On envoie x sur $(\bar{x}, 0)$ si $x = r(\bar{x})$ et sur $(\bar{x}, 1)$ sinon, et $(q, 0)$ sur $r(q)$, $(q, 1)$ sur $f(r(q))$. Comme l'orbite de x est $\{r(\bar{x}), f(r(\bar{x}))\}$ et que f est sans point fixe, ces deux applications sont réciproques. □

Lemme 54.3. *Soient $f : \Gamma \to A$, $g : \Gamma \to B$, $h : \Gamma \to D$ telles que (f, g) et (f, h) soient bijectives. Pour tout $a \in A$, l'application $b \mapsto h\big((f, g)^{-1}(a, b)\big)$ est une bijection de B sur D.*

Démonstration. Si deux valeurs b_1, b_2 ont même image, les éléments $(f, g)^{-1}(a, b_i)$ ont même f et même h ; ils sont égaux par l'injectivité de (f, h), d'où $b_1 = b_2$. Pour $d \in D$, soit $x = (f, h)^{-1}(a, d)$; alors $(f, g)^{-1}(a, g(x)) = x$, et $b = g(x)$ a pour image d. □

Démonstration des pages 99, 101 et 102. Les applications φ_α sont bien définies, car $(\sigma x)_\alpha = \sigma_\alpha(x_\alpha)$ a même classe que x_α.

(1) *Injectivité.* Montrons d'abord que deux triangles supérieurs x, y avec $y_\alpha = x_\alpha$ et $y_\beta \in \{x_\beta, \sigma_\beta x_\beta\}$ sont égaux. Si $y_\beta = \sigma_\beta x_\beta$, le point $x_\alpha = y_\alpha$ serait lié à x_β et à $\sigma_\beta x_\beta$, contrairement à la proposition 2 ; donc $y_\beta = x_\beta$, et $y = x$ par l'unicité de (4). Soient alors x, y de mêmes images dans E_α et E_β. Si $y_\alpha = x_\alpha$, on conclut. Si $y_\alpha = \sigma_\alpha x_\alpha$, on remplace y par σy, qui a même classe : $(\sigma y)_\alpha = x_\alpha$ et $(\sigma y)_\beta$ est dans l'orbite de x_β, donc $\sigma y = x$. *Surjectivité.* Soient $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$. Par la proposition 5, u est lié à s ou à $\sigma_\alpha s$, et (4) donne un triangle supérieur dont les coordonnées d'indices α et β sont ce point et u ; sa classe a pour images les classes de s et de u.

(2) Si $\bar{x} = \bar{y}$ et $x_\alpha = y_\alpha$, alors $y = x$ ou $y = \sigma x$, et le second cas donnerait $\sigma_\alpha x_\alpha = x_\alpha$. Si (g, s) est dans le produit fibré, avec $g = \bar{x}$, la classe de x_α est celle de s, donc $s = x_\alpha$ ou $s = (\sigma x)_\alpha$; dans les deux cas (g, s) est l'image d'un triangle supérieur.

(3) Par construction, $\psi_{\beta\alpha}$ envoie l'image de x dans le premier produit fibré sur l'image de x dans le second ; les deux ont pour première composante $\bar{x}$, et les relations de transitivité se lisent sur cette description.

(4) Les deux premières égalités sont le lemme 54.2 pour σ_α et pour σ, la troisième est (1). Pour la dernière, on applique le lemme 54.3 à $f = \varphi_\alpha$, $g = \varphi_\beta$, $h = \varphi_\gamma$ et à la classe d'un point de $\widetilde{E}_\alpha$. □

Démonstration de la Scholie et de sa réciproque. (1) L'application qui envoie $\alpha \in t_0$ sur $t_0(\alpha)$ et $s \in \widetilde{E}_\alpha$ sur s est bijective par (1) des pages 92 à 99. Elle respecte les arêtes : deux sommets de t_0 sont liés ; $t_0(\alpha)$ est lié à $s \in \widetilde{E}_\beta$ si et seulement si $\beta = \alpha$, par (1) ; deux points d'un même $\widetilde{E}_\alpha$ sont liés si et seulement si l'un est l'image de l'autre par σ_α, par (2) ; deux points de $\widetilde{E}_\alpha$ et de $\widetilde{E}_\beta$, $\alpha \neq \beta$, sont liés dans S si et seulement s'ils sont deux coordonnées d'un triangle supérieur, par (4). Les conditions (*) et $\beta_{\widetilde{\Gamma}}$ sont (4) et (3). Pour (Ka), soient x, y, z trois triangles supérieurs avec $x_\alpha = y_\alpha$, $x_\beta = z_\beta$, $y_\gamma = z_\gamma$. Le point y_γ est lié à $y_\alpha = x_\alpha$, et, comme z_γ, à $z_\beta = x_\beta$. L'axiome 1 pour l'arête $\{x_\alpha, x_\beta\}$ donne $x_\gamma = y_\gamma$, et (*) donne $x = y$.

(2) *Axiome 1.* On examine les arêtes une à une. L'arête $\{t_0(\alpha), t_0(\beta)\}$ a pour seul troisième sommet $t_0(\gamma)$: un point de $\widetilde{E}_\delta$ n'est lié qu'au sommet $t_0(\delta)$. L'arête $\{t_0(\alpha), s\}$ a pour seul troisième sommet $\sigma_\alpha s$: un sommet lié à $t_0(\alpha)$ et à s est dans $\widetilde{E}_\alpha$, et le seul point de $\widetilde{E}_\alpha$ lié à s est $\sigma_\alpha s$. L'arête $\{s, \sigma_\alpha s\}$ a pour seul troisième sommet $t_0(\alpha)$: un point r lié à s et à $\sigma_\alpha s$ qui ne serait pas dans t_0 ne pourrait être dans $\widetilde{E}_\alpha$, où il serait égal à $\sigma_\alpha s$ et à s, ni dans un autre $\widetilde{E}_\beta$, où $\beta_{\widetilde{\Gamma}}$ l'interdit. Enfin, soient $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$ liés par $\tau \in \widetilde{T}$. Le point τ_γ est lié à s et à u. Soit r un autre sommet lié à s et à u. Il n'est pas dans t_0, car il serait lié à $t_0(\alpha)$ et à $t_0(\beta)$. S'il était dans $\widetilde{E}_\alpha$, il serait égal à $\sigma_\alpha s$, et u serait lié à s et à $\sigma_\alpha s$, contre $\beta_{\widetilde{\Gamma}}$; de même il n'est pas dans $\widetilde{E}_\beta$. Il est donc dans $\widetilde{E}_\gamma$, lié à s par un $\rho_1 \in \widetilde{T}$ et à u par un $\rho_2 \in \widetilde{T}$. Alors $\tau_\alpha = (\rho_1)_\alpha = s$, $\tau_\beta = (\rho_2)_\beta = u$ et $(\rho_1)_\gamma = (\rho_2)_\gamma = r$, et (Ka) donne $\tau = \rho_1$, d'où $r = \tau_\gamma$.

Ce dernier argument montre aussi que trois points deux à deux liés hors de t_0 sont les coordonnées d'un même τ : deux d'entre eux ne sont pas dans une même orbite, car un point lié à s et à $\sigma_\alpha s$ est dans t_0, et le troisième est le troisième sommet de l'arête des deux premiers.

Axiome 2. Un triangle du graphe est de l'un des trois types suivants : t_0 ; un triangle vertical $\{t_0(\alpha), s, \sigma_\alpha s\}$; un triangle supérieur $\{\tau_\alpha\}$, $\tau \in \widetilde{T}$. Un triangle qui contient deux sommets de t_0 et un point de $\widetilde{E}_\alpha$ demanderait que ce point soit dans deux $\widetilde{E}$; un triangle formé de $t_0(\alpha)$ et de deux points est vertical, puisque ces points sont dans $\widetilde{E}_\alpha$; un triangle formé de trois points est supérieur par ce qui précède. Pour t_0, tout point de $\widetilde{E}_\alpha$ est lié à $t_0(\alpha)$. Pour un triangle vertical, un sommet de t_0 autre que $t_0(\alpha)$ est lié à $t_0(\alpha)$, ainsi qu'un point de $\widetilde{E}_\alpha$; un point $w \in \widetilde{E}_\beta$,

$\beta \neq \alpha$, est lié à s ou à $\sigma_\alpha s$ par $\beta_{\widetilde{\Gamma}}$. Pour un triangle supérieur τ, un sommet $t_0(\delta)$ est lié à τ_δ. Soit $w \in \widetilde{E}_\delta$. Si $w = \sigma_\delta \tau_\delta$, il est lié à τ_δ. Sinon, notons β, γ les deux autres indices, et supposons w lié ni à τ_β ni à τ_γ. Par $\beta_{\widetilde{\Gamma}}$, $\sigma_\delta w$ est lié à τ_β par un ρ_1 et à τ_γ par un ρ_2. La condition (Ka) pour les indices (β, γ, δ) et les triplets τ, ρ_1, ρ_2 donne $\tau = \rho_1$, d'où $\tau_\delta = \sigma_\delta w$ et $w = \sigma_\delta \tau_\delta$, contre l'hypothèse. C'est l'argument de la proposition 6.

(3) Le sens réciproque est (2). Supposons l'axiome 1, et soient τ, ρ_1, ρ_2 comme dans (Ka). Les points τ_γ et $(\rho_1)_\gamma$ sont liés à τ_α (par τ et par ρ_1) et à τ_β (par τ et par ρ_2). L'axiome 1 pour l'arête $\{\tau_\alpha, \tau_\beta\}$ donne $\tau_\gamma = (\rho_1)_\gamma$, et (*) pour les indices α, γ donne $\tau = \rho_1$.

(4) Si τ et ρ ont mêmes coordonnées d'indices α et β, (Ka) pour les indices (α, γ, β) et les triplets τ, ρ, τ donne $\tau = \rho$. (Ka) entraîne (Ka′) : pour (s_α) et (t_α) comme dans (Ka′), (Ka) appliquée à t_c, t_b, t_a donne $t_c = t_b$, et (s_α) a les coordonnées de t_c. Inversement, sous (*) et (Ka′), soient τ, ρ_1, ρ_2 comme dans (Ka). La famille s égale à τ hors de γ et à $(\rho_1)_\gamma$ en γ, avec $t_\gamma = \tau$, $t_\beta = \rho_1$, $t_\alpha = \rho_2$, vérifie les hypothèses de (Ka′) ; donc $s \in \widetilde{T}$, puis $s = \tau$ par (*), d'où $\tau_\gamma = (\rho_1)_\gamma$ et $\tau = \rho_1$ par (*). □

Démonstration des problèmes I et II. (*). Si $\psi_\alpha(x) = \psi_\alpha(y)$ et $\psi_\beta(x) = \psi_\beta(y)$, alors $\varphi_\alpha \pi(x) = p_\alpha \psi_\alpha(x) = \varphi_\alpha \pi(y)$, et de même pour β ; β_Γ donne $\pi(x) = \pi(y)$, et l'injectivité de (π, ψ_α) donne $x = y$.

$\beta_{\widetilde{\Gamma}}$. Soient $s \in \widetilde{E}_\alpha$ et $u \in \widetilde{E}_\beta$. Deux éléments x, y de $\widetilde{\Gamma}$ avec $\psi_\beta(x) = \psi_\beta(y) = u$ et $p_\alpha \psi_\alpha(x) = p_\alpha \psi_\alpha(y) = p_\alpha(s)$ ont la même image dans $E_\alpha \times E_\beta$, donc la même image dans Γ par β_Γ, et sont égaux par l'injectivité de (π, ψ_β). Si s et $\sigma_\alpha s$ étaient tous deux liés à u, par x et par y, on aurait donc $x = y$ et $s = \sigma_\alpha s$. Pour l'existence, soit $g \in \Gamma$ d'image $(p_\alpha(s), p_\beta(u))$, et x au-dessus de g avec $\psi_\beta(x) = u$; alors $p_\alpha \psi_\alpha(x) = \varphi_\alpha(g) = p_\alpha(s)$, donc $\psi_\alpha(x) \in \{s, \sigma_\alpha s\}$.

La suite résulte de la réciproque de la Scholie. Pour un graphe, les données de l'énoncé sont Γ, les E_α, les classes $\widetilde{E}_\alpha \to E_\alpha$, $\widetilde{\Gamma}$, $x \mapsto \bar{x}$ et $x \mapsto x_\alpha$; les hypothèses sont (1) et (2) de l'énoncé des pages 99, 101 et 102. □

Démonstration de la nécessité de (Ka). Les conditions (*) et $\beta_{\widetilde{\Gamma}}$ portent sur un nombre fini de cas et sont vérifiées par énumération. Les triplets $\tau = ((0,0),(0,0),(0,0))$, $\rho_1 = ((0,0),(1,0),(1,0))$ et $\rho_2 = ((1,0),(0,0),(1,0))$ de $\widetilde{T}$ vérifient $\tau_a = (\rho_1)_a$, $\tau_b = (\rho_2)_b$ et $(\rho_1)_c = (\rho_2)_c$, et $\tau \neq \rho_1$. La condition (Ka) est donc fausse, et l'axiome 1 aussi par (3) de la Scholie. □

Démonstration de la page 116. Si les φ_a préservent la relation, on l'applique à $(1,1,1)$ et à $a = g^{-1}$: il vient $g \cdot g = 1$. Inversement, si $g^2 = 1$ pour tout g, alors $g^{-1} = g$, et $gk = (gk)^{-1} = k^{-1} g^{-1} = kg$: le groupe est commutatif. Pour $xyz = 1$, on a $x \cdot a^{-1} z^{-1} \cdot a^{-1} y^{-1} = x \cdot az \cdot ay = a^2 \cdot xyz = 1$. □

Remarque. La direction directe n'emploie l'axiome 2 que pour t_0 et pour les triangles verticaux. Elle n'emploie pas l'axiome 3 de la page 100 ; celui-ci ne sert qu'aux dénombrements. Les cas exclus par l'axiome 3, un triangle seul ou une étoile de triangles en un sommet (figure 10, à droite), ont $\widetilde{\Gamma} = \varnothing$, et leur Γ vide vérifie β_Γ puisque deux des E_α au moins sont vides. La page 101, qui demande $\widetilde{\Gamma} \neq \varnothing$, les écarte.

Remarque. Le contre-exemple de la nécessité de (Ka) vérifie (*), (**) et $\beta_{\widetilde{\Gamma}}$, et son graphe ne vérifie pas l'axiome 1. L'énoncé de la page 97, qui tire l'axiome 1 de (*) seule, demande donc la condition de la marge, que l'accolade rattache à (*) et (**). Sous (*), l'axiome 1 du graphe des données équivaut à (Ka), et cette équivalence permet de restituer la condition. La conclusion de la marge est illisible : les formes (Ka) et (Ka′) sont les deux lectures, équivalentes sous (*),

qui rendent la Scholie juste. La condition (*) n'est pas utilisée pour la réciproque ; elle découle de (Ka). Les points 3 et 4 de l'énoncé encadré sont de l'édition.

Remarque. Pour l'axiome 2 aux triangles supérieurs, la page 100 (proposition 6) invoque la proposition 2, qui vient de l'axiome 1 dans un graphe donné. Dans la réciproque, la démonstration utilise (Ka) à cet endroit.

Remarque. L'énoncé de la page 116 suppose dès le départ que le carré latin est la table d'un groupe. La lecture écrit qu'il explique pourquoi le carré latin du problème I « doit être la table d'un $\mathbb{F}_2$-espace vectoriel ». L'énoncé démontré ici est plus étroit : si Γ est la table de $xyz = 1$ dans un groupe et si les φ_a la préservent, le groupe est un 2-groupe abélien élémentaire. La page applique la relation à $y = z = 1$; la démonstration prend $x = y = z = 1$; les deux choix reviennent au même puisque x est déterminé par y et z.

Remarque. Le groupe des autotopies de la table de Klein est d'ordre 96. Soit $V = (\mathbb{Z}/2)^2$. Trois permutations f, g, h de V vérifient $f(x)+g(y) = h(x+y)$ pour tous x, y si et seulement s'il existe un automorphisme φ de V et $c_f, c_g \in V$ tels que $f = \varphi+c_f$, $g = \varphi+c_g$ et $h = \varphi+c_f+c_g$. En effet, $y = 0$ et $x = 0$ donnent $h(z) = f(z) + g(0) = f(0) + g(z)$: les normalisées $f + f(0)$, $g + g(0)$ et $h + f(0) + g(0)$ coïncident, et l'égalité de départ dit que cette application commune est additive. L'énoncé vaut pour tout groupe commutatif, avec $f - f(0)$. Comme V a six automorphismes, les autotopies sont au nombre de $6 \cdot 4 \cdot 4 = 96$; une énumération des 24^3 triplets de permutations le confirme. Ce nombre redonne l'ordre $1152 = 32 \cdot 36$ que la cote 69 trouve pour le stabilisateur d'un triangle dans le graphe des vingt-sept droites : 96 autotopies, deux relèvements chacune et les 6 permutations du triangle donnent $1152 = |W(F_4)|$. Cette décomposition et le nom $W(F_4)$ sont de l'édition ; le relèvement n'est pas formalisé.

Ne sont pas démontrés ici : la classification des graphes vérifiant les axiomes 1 à 3 et leur identification aux quadrangles généralisés d'ordre $(2, c)$, la description des carrés latins du problème I et la classification des revêtements doubles du problème II, leur lien avec les extensions centrales des pages 32 à 39, l'affirmation de la lecture que le carré latin est en général la table d'un $\mathbb{F}_2$-espace vectoriel, et les nombres de la page 104 pour $|S|$, $|A|$ et $|T|$. L'identification des $\widetilde{E}_\alpha$ du graphe des données aux ensembles de départ, qui achèverait l'équivalence dans le sens réciproque, n'est démontrée que pour les triangles supérieurs. La fin de la marge (Ka) reste à lire sur le fac-similé.

55 Cote 76 : l'ordre des sommets ; drapeaux de type H, le lemme de surjectivité [58]

La cote 76, *n-cartes cellulaires : notes manuscrites (s.d.)*, soixante-deux pages que l'inventaire date « [vers 1977] », cherche une description combinatoire des complexes cellulaires et des cartes de dimension n. Les pages 20 à 24 relient les ensembles semi-simpliciaux aux ensembles ordonnés munis d'un ordre sur les sommets ; la relation lue sur les arêtes, $x \prec y$, doit être transitive. La page 26 donne un second exemple (« Ex 2 ») : un groupe G, des éléments $\sigma_0, \dots, \sigma_n$ tels que σ_i et σ_j commutent pour $j \geq i + 2$, le sous-groupe N_H engendré par les σ_i, $i \notin H$, un G-ensemble X et ses « drapeaux de type H », $D(H) = X/N_H$ (76, lot 2, p. 26). La page 27 pose $x_i \prec y_j$ si $i < j$ et si x_i, y_j ont un majorant commun, ramène la transitivité à la surjectivité de $D(\{i,j,k\}) \to D(\{i,j\}) \times_{D(\{j\})} D(\{j,k\})$ et énonce un lemme plus général, sous l'hypothèse

58. Preuve vérifiée : `lean/Grothendieck/Folder76.lean`.

« $H \cap H'$ … segment final de l'ens tot. ordonné H, un segment initial de l'ens tot ordonné H' » (76, lot 2, p. 27). La page 28 le démontre par la décomposition $G_{K\cup K'} \subset G_{K_0} \cdot G_{K'_0}$, et une note oblique dans la marge gauche dit n'avoir utilisé que « a) le dernier él. de H est dans H' ; b) $H \cap H'$ est un segment initial de H' » (76, lot 2, p. 28).
Conventions. On note $\Delta_n = \{0, \dots, n\}$, G_K le sous-groupe de G engendré par les σ_i, $i \in K$, pour $K \subset \Delta_n$, et $N_H = G_{\Delta_n \smallsetminus H}$. Pour $H \subset H'$, on a $N_{H'} \subset N_H$, d'où la restriction $D(H') \to D(H)$, $N_{H'}x \mapsto N_H x$; elle est transitive. Aucune autre hypothèse n'est faite sur les σ_i : ce ne sont pas nécessairement des involutions.

Lemme 55.1. *Soient $K, K' \subset \Delta_n$ et $i \in \Delta_n \smallsetminus (K \cup K')$ tels que tout $j \in K \cup K'$ avec $j < i$ soit dans K' et tout $j \in K \cup K'$ avec $j > i$ soit dans K. Alors tout élément de $G_{K\cup K'}$ s'écrit $k'k$ avec $k' \in G_{K'}$ et $k \in G_K$.*

Démonstration. Soient $A = G_{K'_0}$ et $B = G_{K_0}$, où $K'_0 = \{j \in K \cup K' : j < i\}$ et $K_0 = \{j \in K \cup K' : j > i\}$. Par hypothèse $A \subset G_{K'}$ et $B \subset G_K$. Un indice de K'_0 et un indice de K_0 diffèrent d'au moins 2, donc leurs générateurs commutent ; tout générateur de B est alors dans le centralisateur de A, puis B tout entier, et tout élément de A commute à tout élément de B. L'ensemble AB contient donc 1, les générateurs σ_j, $j \in K \cup K'$ (qui sont dans K'_0 ou K_0 puisque $i \notin K \cup K'$), et il est stable par produit, $(ab)(a'b') = (aa')(bb')$, et par inverse, $(ab)^{-1} = a^{-1}b^{-1}$. Il contient le sous-groupe $G_{K\cup K'}$ qu'ils engendrent. □

Théorème 55.2 (Grothendieck, pages 27 et 28, lemme ♦). *Soient G un groupe, $\sigma_0, \dots, \sigma_n \in G$ tels que σ_i et σ_j commutent pour $j \geq i+2$, et X un G-ensemble. Soient $H, H' \subset \Delta_n$ tels que le plus grand élément de H soit dans H' et que $H \cap H'$ soit un segment initial de H'. Alors l'application*

$$D(H \cup H') \longrightarrow D(H) \times_{D(H\cap H')} D(H')$$

est surjective : deux drapeaux de types H et H' de même restriction à $H \cap H'$ sont les restrictions d'un même drapeau de type $H \cup H'$.

Démonstration. Soient $a = N_H x$ et $b = N_{H'} y$ de même image dans $D(H \cap H')$: il existe $g \in N_{H\cap H'}$ avec $gy = x$. Posons $K = \Delta_n \smallsetminus H$ et $K' = \Delta_n \smallsetminus H'$, de sorte que $N_{H\cap H'} = G_{K\cup K'}$, et soit i le plus grand élément de H. Il est dans $H \cap H'$, donc hors de $K \cup K'$. Un $j > i$ n'est pas dans H, donc est dans K. Un $j < i$ de $K \cup K'$ n'est pas dans H' : sinon, $j \leq i$ avec $i \in H \cap H'$ et le segment initial le mettraient dans H, donc dans $H \cap H'$, ce qui contredit $j \in K \cup K'$. Le lemme 55.1 écrit $g^{-1} = k'k$ avec $k' \in N_{H'}$ et $k \in N_H$. Le drapeau c, classe de kx dans $D(H \cup H')$, a pour image $N_H kx = N_H x = a$ dans $D(H)$, et, puisque $y = g^{-1}x = k'(kx)$, pour image $N_{H'}kx = N_{H'}y = b$ dans $D(H')$. □

Corollaire 55.3 (page 27). *Pour $x \in D(\{i\})$ et $y \in D(\{j\})$, posons $x \prec y$ si $i < j$ et si x et y sont les restrictions d'un même drapeau d'un type $H \supset \{i, j\}$. Cette relation est transitive, pour tout G-ensemble X. Un majorant commun peut toujours être pris dans $D(\{i, j\})$, les sommets $i < j$ d'un même drapeau vérifient $\prec$, et $x \prec y$ n'a jamais lieu pour x et y de même type.*

Démonstration. La restriction d'un majorant de type H à $\{i, j\}$ est un majorant de type $\{i, j\}$. Soient $i < j < k$, $x \prec y$ par $u \in D(\{i, j\})$ et $y \prec w$ par $v \in D(\{j, k\})$. On a $\{i, j\} \cap \{j, k\} = \{j\}$, qui est le plus grand élément de $\{i, j\}$ et un segment initial de $\{j, k\}$. Les restrictions de u et v à $\{j\}$ valent y, et le théorème 55.2 donne $c \in D(\{i, j, k\})$ qui restreint à u et à v, donc à x et à w : sa restriction à $\{i, k\}$ est un majorant commun de x et w, et $i < k$. □

Remarque. Le lemme tient tel que la lecture l'énonce, sous les deux hypothèses de la note marginale, plus faibles que celles de l'énoncé de la page 27 : la non-vacuité de $H \cap H'$ découle de a), et le segment final de H ne sert pas. La démonstration est celle de la page 28 ; la page écrit $G_{K\cup K'} = G_K \cdot G_{K'}$, le fichier en démontre l'inclusion sous la forme $G_{K'} \cdot G_K$, la seule dont la démonstration se sert. Comme la lecture le dit, le groupe, l'ensemble X et l'action sont quelconques : la page n'utilise que la commutation des σ_i éloignés. Le fichier formalise l'ordre des sommets sur $D_0 = \coprod_i D(\{i\})$, sa transitivité, et l'ensemble semi-simplicial qui en résulte (corollaire 55.4 ci-dessous). La piste demande si cette surjectivité, pour des G-ensembles quelconques, figure dans la théorie des géométries de classes de Tits ou des systèmes de chambres.

Corollaire 55.4 (page 27, « ainsi »). *Soit $D_m = \coprod_{\operatorname{card} H = m+1} D(H)$, et, pour $u\colon \Delta_k \to \Delta_m$ strictement croissante et $d \in D(H)$, $H = \{h_0 < \cdots < h_m\}$, soit u^*d la restriction de d au type $\{h_{u(0)} < \cdots < h_{u(k)}\}$. C'est un ensemble semi-simplicial satisfaisant (1). Son ensemble ordonné de simplexes est $D_* = \coprod_H D(H)$, avec $d \le d'$ si et seulement si $H \subset H'$ et d est la restriction de d' ; il satisfait (a). Sa relation d'arête sur D_0 est la relation $\prec$ du corollaire 55.3 ; elle est donc transitive, et les ordres des simplexes sont tous induits par un même ordre sur D_0 satisfaisant (b) et (c). Cela vaut pour tout G-ensemble X.*

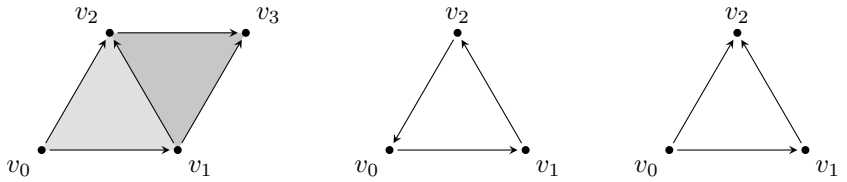
Esquisse. Les identités semi-simpliciales viennent de la transitivité des restrictions et de ce que la face de type $u(\Delta_k) \subset H$ d'une face de type $v(\Delta_m)$ est celle de type $(v\circ u)(\Delta_k)$, l'énumération croissante d'une partie étant unique. Deux faces $u^*d = v^*d$ ont même type, donc $u = v$: c'est (1). Si $H \subset H'$, l'application croissante u qui envoie le i-ième élément de H sur son rang dans H' donne pour u^*d' la restriction de d' à H, d'où la description de l'ordre ; (a) vient alors de (1) par le théorème des pages 22 à 24 ci-dessous. Une arête de type $\{i < j\}$ a pour sommets ses restrictions à $\{i\}$ et $\{j\}$, ce qui identifie la relation d'arête à $\prec$; le corollaire 55.3 donne la transitivité et le théorème des pages 22 à 24 l'ordre sur D_0. □

L'ordre des sommets (pages 20 à 24). Un ensemble semi-simplicial D satisfait (1) si les faces d'un simplexe sont deux à deux distinctes ; $D_* = \coprod D_m$, ordonné par « est face de », satisfait alors (a). Sur D_0, $x \prec y$ s'il existe une arête de x à y ; (2 bis) demande que deux arêtes composables bordent un 2-simplexe. La proposition des pages 23 et 24 met en correspondance les ensembles semi-simpliciaux satisfaisant (1) et « (2) », chiffre incertain que la lecture lit comme la transitivité (2°), et les ensembles ordonnés satisfaisant (a) munis d'un ordre sur D_0 satisfaisant (b) et (c) (76, lot 2, p. 22, 76, lot 2, p. 24).

Théorème 55.5 (D'après les pages 22 à 24, avec (2°) ♦). *Soit D un ensemble semi-simplicial satisfaisant (1). Alors D_* satisfait (a), les ordres de ses simplexes sont compatibles, et leur relation d'arête est $\prec$; la relation $\prec$ est transitive si et seulement si ces ordres sont tous induits par un même ordre sur D_0 satisfaisant (b) et (c), et cet ordre est alors $\prec$. Sur tout ensemble ordonné satisfaisant (a), les ordres sur D_0 satisfaisant (b) et (c) correspondent bijectivement, par restriction et par la relation d'arête, aux familles d'ordres totaux compatibles sur les simplexes dont la relation d'arête est transitive. Enfin (2 bis) entraîne (2°), et le bord d'un triangle satisfait (1) et (2°) sans satisfaire (2 bis).*

La figure 11 donne trois cas, une flèche de x vers y figurant une arête de x à y, donc $x \prec y$. Dans le premier, deux triangles pleins partagent une arête, et les ordres de leurs sommets sont induits par $v_0 < v_1 < v_2 < v_3$. Dans le deuxième, trois arêtes tournent : (1) tient, mais

$v_0 \prec v_1 \prec v_2$ sans $v_0 \prec v_2$, et aucun ordre sur D_0 n'induit les ordres des arêtes. Le troisième est le bord d'un triangle orienté sans cycle.



(1) et (2 bis) (1), sans (2°) (1) et (2°), sans (2 bis)

FIGURE 11 – L'ordre des sommets. À gauche, deux 2-simplexes (en gris) d'arête commune v_1v_2 : la relation d'arête est l'ordre $v_0 < v_1 < v_2 < v_3$, qui induit celui de chaque simplexe. Au milieu, trois arêtes en cycle, sans 2-simplexe : $\prec$ n'est pas transitive. À droite, le bord du triangle : $\prec$ est l'ordre $v_0 < v_1 < v_2$, mais les arêtes composables v_0v_1 et v_1v_2 ne bordent aucun 2-simplexe.

L'énoncé tient avec (2°), comme la lecture le lit : voir `trans_iff_vertexOrder`, `vertexOrder_unique`, `vertexOrderEquiv`, `isFlagGeom`, `trans_of_hornFill` et `triangleBoundary_not_hornFill` dans `Folder76.lean`. Du côté des ensembles ordonnés, la correspondance n'utilise de (a) que l'existence, sous un simplexe, de l'arête qui joint deux de ses sommets. Le retour des ordres compatibles à l'ensemble semi-simplicial (pages 17 et 18) n'est pas refait ici : c'est le cas $M = \Delta_{\text{inj}}$ de l'équivalence de la cote 104 (§ 70).

La condition (a) pour $D_* = \coprod_H D(H)$ et l'ensemble semi-simplicial qu'elle définit, avec $D_m = \coprod_{\operatorname{card} H = m+1} X/N_H$, sont démontrés (corollaire 55.4) : voir `flagSS`, `flagSS_le_iff`, `flagSS_isFlagGeom`, `flagSS_prec_iff`, `flagSS_prec_trans` et `flagSS_vertexOrder`. N'est pas démontré ici : le programme de la page 29.

56 Cote 77 : le discriminant universel modulo 2 et modulo 4, la sphère, la symétrie canonique [59]

La cote 77, *Quadriques affines, extensions quadratiques : notes manuscrites (s.d.)*, compte cent cinquante-sept pages, que l'inventaire place après 1977. La partie IV, dont la couverture de la page 64 porte « discriminant des formes quadratiques », prend la forme quadratique universelle $\sum_i Y_i x_i^2 + \sum_{i<j} Y_{ij} x_i x_j$ sur l'anneau $\mathbf{Z}[Y]$ et le déterminant Δ de sa forme polaire, matrice qui porte $2Y_i$ sur la diagonale et Y_{ij} ailleurs. Les pages 65 à 67 développent Δ en une somme sur des graphes : sommets isolés pour les points fixes, arêtes doubles pour les transpositions, polygones pour les autres cycles. La page 68 réduit cette somme modulo 2 : il n'y reste que les involutions sans point fixe, et la page conclut « On voit donc que $\Delta \bmod 2 = 0$ si $\operatorname{card} I$ est impair » (77, lot 4, p. 68). En rang pair $m = 2n$, elle pose B, somme sur les couplages parfaits de I des produits des Y_{ij}, cherche $\varepsilon = \pm 1$ tel que $B^2 - \varepsilon\Delta \equiv 0 \pmod 4$, et « prévoit » $\varepsilon = (-1)^n$. Les pages 69 et 71 comparent B^2 et Δ modulo 4 par les paires de couplages, avec une fausse alarme à l'encre brune corrigée deux lignes plus bas. La page 87, barrée, contrôle les coefficients du développement en rang 4 (77, lot 5, p. 87), et la page 127 prend le discriminant divisé $\delta' = \delta/2$ du rang impair comme critère de régularité (77, lot 7, p. 127). La partie V, aux pages 117 à 125, étudie les quadriques affines « birégulières », lisses et lisses à l'infini : elle les ramène à un triplet (T, q, a) avec $q(a) = 1$, pose $\pi = \varphi(a, \cdot)$ et, page 123, définit la symétrie

59. Preuve vérifiée : `lean/Grothendieck/Folder77.lean`.

canonique $\sigma = \mathrm{id} - \pi \otimes a$; une note en marge affirme qu'elle est la seule réflexion qui fixe l'hyperplan à l'infini et laisse la quadrique invariante (77, lot 7, p. 123). Le feuillet découpé de la page 124 traite l'exemple $T = M_2$, $q = \det$, $a = 1$.
Conventions. Pour $n \geq 0$, les indéterminées sont indexées par les parties $J \subset \{1, \dots, n\}$ de cardinal 1 ou 2, notées Y_i et Y_{ij} ; on note $\mathbf{Z}[Y]$ l'anneau de polynômes correspondant. La matrice polaire universelle P_n a pour coefficients $2Y_i$ en (i,i) et Y_{ij} en (i,j) et (j,i) pour $i \neq j$. Sur un anneau commutatif R, une famille $y = (y_i, y_{ij})$ d'éléments de R définit la forme $\sum y_i x_i^2 + \sum_{i<j} y_{ij} x_i x_j$, de matrice polaire $P(y)$, image de P_n par le morphisme $Y \mapsto y$.

Énoncé (Page 68, rang impair ♦). *Si n est impair, $\det P_n$ est divisible par 2 dans $\mathbf{Z}[Y]$. Le quotient $\delta'_n = \det P_n / 2$ est l'unique polynôme tel que $\det P_n = 2\delta'_n$, et pour tout anneau commutatif R et toute famille y d'éléments de R, $\det P(y) = 2\,\delta'_n(y)$.*

Démonstration. Soit K_n la matrice de $\mathbf{Z}[Y]$ qui porte Y_{ij} en (i,j) pour $i < j$, $-Y_{ij}$ en (i,j) pour $i > j$ et 0 sur la diagonale. Elle est antisymétrique : ${}^t K_n = -K_n$. On a donc $\det K_n = \det {}^t K_n = \det(-K_n) = (-1)^n \det K_n = -\det K_n$, d'où $2 \det K_n = 0$; comme $\mathbf{Z}[Y]$ est intègre de caractéristique nulle, $\det K_n = 0$.

Soit $\rho : \mathbf{Z}[Y] \to \mathbf{F}_2[Y]$ la réduction des coefficients modulo 2. Les matrices P_n et K_n ont même image par ρ : sur la diagonale, $\rho(2Y_i) = 0$; au-dessus, les coefficients sont égaux ; au-dessous, $\rho(-Y_{ij}) = \rho(Y_{ij})$ en caractéristique 2. Le déterminant commutant aux morphismes d'anneaux, $\rho(\det P_n) = \det \rho(P_n) = \det \rho(K_n) = \rho(\det K_n) = 0$. Le noyau de ρ est formé des polynômes dont tous les coefficients sont pairs, c'est-à-dire de l'idéal engendré par 2 ; donc 2 divise $\det P_n$.

L'unicité du quotient vient de ce que 2 n'est pas diviseur de zéro dans $\mathbf{Z}[Y]$. Pour R et y donnés, le morphisme $Y \mapsto y$ envoie P_n sur $P(y)$ et commute au déterminant ; il envoie $2\delta'_n$ sur $2\,\delta'_n(y)$. □

Remarque. Le discriminant divisé du rang impair figure chez Conrad (2014, proposition C.1.4) [35], qui le présente comme découvert indépendamment par M. Kneser et par Grothendieck. L'énoncé tient pour tout n impair. La démonstration ne suit pas le développement en graphes de la page : elle remplace, modulo 2, la matrice symétrique par la matrice antisymétrique K_n, dont le déterminant est nul sur $\mathbf{Z}[Y]$ en taille impaire. Sur $\mathbf{F}_2[Y]$, l'argument $\det = -\det$ ne donne rien : il faut donc relever $\rho(P_n)$ en une matrice antisymétrique sur $\mathbf{Z}[Y]$. La seconde partie de la piste, « q est régulière si et seulement si $\delta'(q)$ est inversible », est la définition de la régularité que la lecture adopte (page 127). Les équivalences de la page 127 avec la lissité de $V(q)$ et l'isomorphie locale à la forme standard ne sont pas formalisées.

Énoncé (Pages 68 à 71 et 87, rangs 2 et 4 ♦). *Soit R un anneau commutatif.*

1. *(Rang 2, $n = 1$.) Pour $a_1, a_2, b_{12} \in R$, $-\det \begin{pmatrix} 2a_1 & b_{12} \\ b_{12} & 2a_2 \end{pmatrix} = B^2 - 4C$ avec $B = b_{12}$ et $C = a_1 a_2$.*
2. *(Rang 4, $n = 2$.) Soit P la matrice polaire de la forme $\sum_{i \leq 4} a_i x_i^2 + \sum_{i<j} b_{ij} x_i x_j$ et $B = b_{12}b_{34} + b_{13}b_{24} + b_{14}b_{23}$, somme sur les trois couplages parfaits de $\{1,2,3,4\}$. Alors $\det P = B^2 - 4C$ avec*

$$\begin{aligned} C = {} & -4a_1a_2a_3a_4 + a_1a_2b_{34}^2 + a_1a_3b_{24}^2 + a_1a_4b_{23}^2 + a_2a_3b_{14}^2 + a_2a_4b_{13}^2 + a_3a_4b_{12}^2 \\ & - a_1b_{23}b_{24}b_{34} - a_2b_{13}b_{14}b_{34} - a_3b_{12}b_{14}b_{24} - a_4b_{12}b_{13}b_{23} \\ & + b_{12}b_{13}b_{24}b_{34} + b_{12}b_{14}b_{23}b_{34} + b_{13}b_{14}b_{23}b_{24}. \end{aligned}$$

3. *Le signe $\varepsilon = -(-1)^n$ ne convient dans aucun des deux rangs : sur $\mathbf{Z}$, pour $a_1 = a_2 = 0$ et $b_{12} = 1$, $B^2 - \det P = 2$; pour $b_{12} = b_{34} = 1$ et les autres coefficients nuls, $B^2 + \det P = 2$. Aucun des deux n'est divisible par 4.*

Démonstration. En rang 2, $\det = 4a_1a_2 - b_{12}^2$. En rang 4, on développe $\det P$ selon la première ligne, puis chaque mineur d'ordre 3 par la règle de Sarrus. On obtient

$$\begin{aligned}\det P = {} & 16a_1a_2a_3a_4 - 4\,(a_1a_2b_{34}^2 + a_1a_3b_{24}^2 + a_1a_4b_{23}^2 + a_2a_3b_{14}^2 + a_2a_4b_{13}^2 + a_3a_4b_{12}^2) \\ & + 4\,(a_1b_{23}b_{24}b_{34} + a_2b_{13}b_{14}b_{34} + a_3b_{12}b_{14}b_{24} + a_4b_{12}b_{13}b_{23}) + b_{12}^2b_{34}^2 + b_{13}^2b_{24}^2 + b_{14}^2b_{23}^2 \\ & - 2\,(b_{12}b_{13}b_{24}b_{34} + b_{12}b_{14}b_{23}b_{34} + b_{13}b_{14}b_{23}b_{24}).\end{aligned}$$

Ce sont les coefficients de la page 87 : 2^4 pour les quatre sommets isolés, -2^2 pour une arête double et deux sommets isolés, 2^2 pour un triangle et un sommet isolé, 1 pour deux arêtes doubles, -2 pour un carré. Le carré B^2 a pour termes carrés les $b_{12}^2b_{34}^2$, $b_{13}^2b_{24}^2$, $b_{14}^2b_{23}^2$ et pour termes croisés $2\,(b_{12}b_{13}b_{24}b_{34} + b_{12}b_{14}b_{23}b_{34} + b_{13}b_{14}b_{23}b_{24})$; la différence $B^2 - \det P$ est donc $4C$, terme à terme. Les deux contre-exemples se calculent sur ces formules : en rang 2, $B^2 - \det P = 1 - (-1)$; en rang 4, $\det P = b_{12}^2b_{34}^2 = 1$ et $B^2 + \det P = 2$. □

Remarque. L'identité est démontrée sur tout anneau commutatif, donc en particulier sur $\mathbf{Z}[Y]$, avec un C écrit en entier. Elle confirme en rangs 2 et 4 le signe $(-1)^n$ que la page « prévoit », et le choix opposé échoue dans ces deux rangs ; la lecture l'avait déjà contrôlé par machine pour $m = 2, 4, 6$. En rang 4, la vérification confirme les coefficients et les nombres de graphes de la page 87. Le rang pair quelconque fait l'objet de l'énoncé suivant, sans expression de C.

Théorème 56.1 (Grothendieck, pages 68 à 71, rang pair quelconque ♦). *Soient $n \geq 0$ et $B_{2n} = \sum_M \prod_{\{i,j\}\in M} Y_{ij}$, la somme portant sur les couplages parfaits M de $\{1, \ldots, 2n\}$. Alors 4 divise $(-1)^n \det P_{2n} - B_{2n}^2$ dans $\mathbf{Z}[Y]$. Il existe donc $C_{2n} \in \mathbf{Z}[Y]$ tel que, pour tout anneau commutatif R et toute famille y d'éléments de R, $(-1)^n \det P(y) = B_{2n}(y)^2 - 4\,C_{2n}(y)$.*

Démonstration. Soit U la matrice qui porte Y_i en (i,i), Y_{ij} en (i,j) pour $i < j$, et 0 sous la diagonale. Alors $P_{2n} = U + {}^tU$, et la matrice antisymétrique K_{2n} de l'énoncé du rang impair est $U - {}^tU = P_{2n} - 2\,{}^tU$. On écrit P, K et B pour P_{2n}, K_{2n} et B_{2n}.

Premier pas : $\det K \equiv (1-2n)\det P \pmod 4$. Soit $f(t) = \det(P - t\,{}^tU) \in \mathbf{Z}[Y][t]$, que l'on écrit $f(t) = f_0 + f_1t + t^2g(t)$. On a $f_0 = f(0) = \det P$ et $\det K = f(2) = \det P + 2f_1 + 4g(2)$; il reste à voir que $2f_1 = -2n\det P$. Le déterminant $\det P$ n'est pas nul : pour $Y_i = 1$ et $Y_{ij} = 0$ il vaut 2^{2n}. La matrice P est donc inversible sur le corps des fractions L de $\mathbf{Z}[Y]$, et sur L, $f(t) = \det P \cdot \det(1 - t\,P^{-1}\,{}^tU)$, dont le coefficient de t est $-\det P \cdot \operatorname{tr}(P^{-1}\,{}^tU)$. Comme P est symétrique, P^{-1} l'est aussi, et $\operatorname{tr}(P^{-1}\,{}^tU) = \operatorname{tr}\big({}^t(P^{-1}\,{}^tU)\big) = \operatorname{tr}(UP^{-1}) = \operatorname{tr}(P^{-1}U)$. La somme de ces deux traces est $\operatorname{tr}(P^{-1}(U + {}^tU)) = \operatorname{tr}(1) = 2n$. Donc $2f_1 = -2n\det P$ dans L, et dans $\mathbf{Z}[Y]$, qui s'injecte dans L.

Deuxième pas : $\det K$ *est un carré dans* $\mathbf{Z}[Y]$. Sur un corps k de caractéristique différente de 2, une matrice antisymétrique A de taille paire a pour déterminant un carré. On raisonne par récurrence sur la taille ; la diagonale de A est nulle. Si la première ligne est nulle, $\det A = 0$. Sinon, soit $c = A_{1j} \neq 0$, avec $j \neq 1$; la permutation qui échange 2 et j, appliquée aux lignes et aux colonnes, ne change pas le déterminant et amène c en position $(1,2)$. On découpe alors A en blocs $\begin{pmatrix} E & F \\ G & D \end{pmatrix}$, avec $E = \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}$ inversible de déterminant c^2 ; on a $\det A = c^2 \det S$

avec $S = D - GE^{-1}F$. Comme $G = -{}^tF$, ${}^tD = -D$ et ${}^t(E^{-1}) = -E^{-1}$, la matrice S est antisymétrique, de taille deux de moins. Par récurrence $\det S = s^2$, d'où $\det A = (cs)^2$. Appliqué à l'image de K sur L, cela donne $\det K = s^2$ avec $s \in L$. L'élément s est racine du polynôme unitaire $T^2 - \det K$ de $\mathbf{Z}[Y][T]$; l'anneau $\mathbf{Z}[Y]$ est factoriel, donc intégralement clos, et s est l'image d'un $r \in \mathbf{Z}[Y]$, avec $\det K = r^2$.

Troisième pas : réduction modulo 2. Soit M une matrice symétrique à diagonale nulle sur un anneau de caractéristique 2. Dans $\det M = \sum_\sigma \varepsilon(\sigma) \prod_i M_{\sigma(i)i}$, les signes valent 1, et σ et σ^{-1} donnent le même produit, par symétrie de M. Les termes des σ distinctes de σ^{-1} s'annulent donc deux à deux ; ceux des involutions qui ont un point fixe sont nuls, car la diagonale est nulle. Il reste les involutions sans point fixe, c'est-à-dire les couplages parfaits, et pour un couplage le produit est le carré du produit des M_{ij} sur ses arêtes. En caractéristique 2 une somme de carrés est le carré de la somme, d'où $\det M = \left(\sum_{M'} \prod_{\{i,j\}\in M'} M_{ij}\right)^2$. La matrice $\rho(K)$ est symétrique, car $-1 = 1$ dans $\mathbf{F}_2[Y]$, à diagonale nulle, et ses coefficients au-dessus de la diagonale sont les $\rho(Y_{ij})$; on obtient $\rho(r)^2 = \rho(\det K) = \rho(B)^2$. En caractéristique 2, $\rho(r-B)^2 = \rho(r)^2 - \rho(B)^2 = 0$, et comme $\mathbf{F}_2[Y]$ est intègre, $\rho(r-B) = 0$. Comme dans l'énoncé du rang impair, $r = B + 2h$ avec $h \in \mathbf{Z}[Y]$, et $\det K = r^2 = B^2 + 4(Bh + h^2)$.

Conclusion. Par récurrence sur n, $(-1)^n \equiv 1 - 2n \pmod 4$. Donc $(-1)^n \det P \equiv (1 - 2n)\det P \equiv \det K \equiv B^2 \pmod 4$. Si $(-1)^n \det P - B^2 = 4Q$, on prend $C_{2n} = -Q$; le morphisme $Y \mapsto y$ envoie P_{2n} sur $P(y)$ et commute au déterminant. □

Remarque. L'énoncé tient en tout rang pair, avec le signe $(-1)^n$ que la page « prévoit ». La démonstration ne suit pas les pages 69 et 71, qui comparent B^2 et Δ par les paires de couplages : elle passe par la matrice antisymétrique $K = U - {}^tU$. Le signe $(-1)^n$ vient du terme du premier ordre, $\det K \equiv (1 - 2n)\det P \pmod 4$; la congruence $\det K \equiv B^2$ vient de ce que $\det K$ est le carré d'un polynôme r qui se réduit sur B modulo 2. Ce polynôme r est, au signe près, le pfaffien de K, qui manque à mathlib ; il n'est pas construit ici, et son existence découle de la clôture intégrale de $\mathbf{Z}[Y]$. Le polynôme C_{2n} n'est écrit qu'en rangs 2 et 4.

La sphère comme restriction de Weil d'une conique (pages 89 à 98). Le module spécial quadratique E de rang 3 est la partie pure d'une algèbre de quaternions M, avec $q(u) = u^2$; la loi $[x, y] = xy - yx$ y est le crochet. Pour un $x + \mathbf{i}y$ isotrope, $q(x) = q(y)$ et $\varphi(x, y) = 0$, la page 95 pose $\tilde{f}(x + \mathbf{i}y) = [x, y]/2q(x)$, les pages 94 à 97 démontrent que $\tilde{f}$ induit un isomorphisme de U sur la quadrique affine $\Sigma : q = -1$, et la page 98 encadre $\Sigma \simeq X^{S[\mathbf{i}]} \smallsetminus X$ (77, lot 5, p. 94, 77, lot 5, p. 98).

Théorème 56.2 (Grothendieck, pages 94 à 98, en coordonnées sur un corps ♦). *Soient K un corps de caractéristique différente de 2, $a, b \in K^\times$, E la partie pure de l'algèbre de quaternions (a, b), $q(u) = u^2$ et φ sa polaire. Soient $\tilde{U}$ l'ensemble des couples $(x, y) \in E^2$ tels que $q(x) = q(y) \neq 0$ et $\varphi(x, y) = 0$, et $\Sigma = \{t \in E : q(t) = -1\}$.*

1. *$q([x, y]) = -4\,q(x)\,q(y) + \varphi(x, y)^2$ (formule (21 bis)).*
2. *L'application $(x, y) \mapsto [x, y]/2q(x)$ envoie $\tilde{U}$ sur Σ, et deux couples ont la même image si et seulement s'ils se déduisent l'un de l'autre par l'action d'un $c + \mathbf{i}d$, $c^2 + d^2 \neq 0$.*
3. *Si $x + \mathbf{i}y$ est isotrope, non nul, et $q(x) = 0$, alors $x = c\,x_0$ et $y = d\,x_0$ avec $q(x_0) = 0$: un point réel.*

L'énoncé tient tel que la page l'écrit, sur un corps (Lean : `qf_commutator`, `sphere_quotient`,

`hors_de_U`).

Sur $\mathbf{R}$, avec $a = b = -1$, l'algèbre est celle des quaternions de Hamilton et l'énoncé se voit (figure 12). E est l'espace euclidien des quaternions purs, $q(u) = u^2 = -\|u\|^2$, $\varphi(x, y) = -2\,x \cdot y$ et $[x, y] = 2\,x \times y$. Un couple de $\tilde{U}$ est un couple de vecteurs orthogonaux de même norme, son image $[x, y]/2q(x) = -x \times y/\|x\|^2$ est le vecteur unitaire normal à leur plan, et Σ est la sphère unité. Comme q est définie, le cas du point 3 ne se présente pas : la conique n'a pas de point réel.

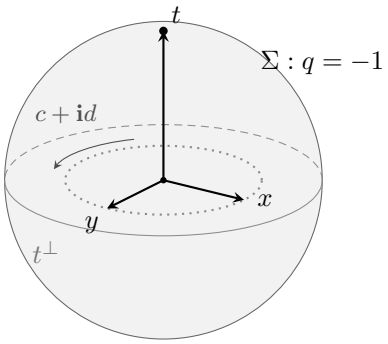


FIGURE 12 – La sphère comme quotient des couples isotropes, sur $\mathbf{R}$ et pour les quaternions de Hamilton. Le couple (x, y), orthogonal et de même norme, a pour image le point $t = [x, y]/2q(x)$ de la sphère unité Σ, normal au plan $t^\perp$ de x et y, avec (y, x, t) direct. Les couples de même image, dont l'un est $(x, -tx)$ pour chaque $x \in t^\perp$ non nul, se déduisent de (x, y) par les $c + \mathbf{i}d$, qui les font tourner et les dilatent dans $t^\perp$; le cercle pointillé en figure les extrémités, à norme fixée.

Remarque. L'inverse est explicite et ne demande aucune localisation étale : pour $t \in \Sigma$ et tout x orthogonal à t avec $q(x) \neq 0$, $\tilde{f}(x - \mathbf{i}\,tx) = t$, et tout $(x, y) \in \tilde{U}$ d'image t vérifie $y = -tx$. L'injectivité modulo l'action vient de ce que t, x et tx forment une base orthogonale de E. La version schématique et la version tordue des pages 102 à 116 ne sont pas formalisées.

Énoncé (Pages 117 à 124, la symétrie canonique ♦). *Soient R un anneau commutatif, T un R-module, q une forme quadratique sur T, $\varphi(x, y) = q(x + y) - q(x) - q(y)$ sa forme polaire, $a \in T$ avec $q(a) = 1$, $\pi = \varphi(a, \cdot)$, $V = \ker \pi$, $E = \pi^{-1}(1)$ et $\sigma(x) = x - \pi(x)\,a$.*

1. *On a $\pi(a) = 2$, $q \circ \sigma = q$ et $\sigma^2 = \mathrm{id}$, et σ fixe V point par point.*
2. *Supposons φ non dégénérée, au sens où $\varphi(y, \cdot) = 0$ entraîne $y = 0$, et π surjective. Une application linéaire $u : T \to T$ qui fixe V point par point et vérifie $q \circ u = q$ est de la forme $u(x) = x - e\,\pi(x)\,a$ avec $e \in R$ idempotent. Réciproquement, pour tout idempotent e, cette application préserve q et fixe V. Si 0 et 1 sont les seuls idempotents de R, alors $u = \mathrm{id}$ ou $u = \sigma$.*
3. *Si 2 est inversible dans R, alors $\pi(a/2) = 1$, et pour $x \in E$, $-\sigma(x) \in E$ et $-\sigma(x) - a/2 = -(x - a/2)$. Sur E, la transformation projective définie par σ est la symétrie de centre $a/2$.*
4. *Si $2 = 0$ dans R, alors $\pi(a) = 0$, donc $a \in V$, $\pi \circ \sigma = \pi$, et $\sigma(x) = x - a$ pour $x \in E$: $\sigma = \mathrm{id} - \pi \otimes a$ est une transvection.*
5. *(Page 124.) Pour $T = M_2(R)$, $q = \det$ et $a = 1$, $\varphi(x, 1) = \det(x + 1) - \det x - 1 = \mathrm{tr}\,x$.*

Démonstration. On a $\varphi(a, a) = 2q(a) = 2$. Pour $t \in R$, $q(x + ta) = q(x) + t\,\varphi(a, x) + t^2 q(a)$; avec $t = -\pi(x)$, $q(\sigma x) = q(x) - \pi(x)^2 + \pi(x)^2 = q(x)$. Ensuite $\pi(\sigma x) = \pi(x) - 2\pi(x) = -\pi(x)$, d'où $\sigma(\sigma x) = \sigma x + \pi(x)\,a = x$. Si $\pi(v) = 0$, $\sigma v = v$.

Pour le point 2, soient b tel que $\pi(b) = 1$ et $c = u(b) - b$. Pour tout x, $x - \pi(x)b$ est dans V, donc $u(x) = x + \pi(x)\,c$. Alors $q(ux) = q(x) + \pi(x)f(x)$ avec $f(x) = \pi(x)q(c) + \varphi(x, c)$, forme linéaire, et l'hypothèse donne $\pi(x)f(x) = 0$ pour tout x. En $x = b$, $f(b) = 0$. En $x + b$, $0 = (\pi(x) + 1)\big(f(x) + f(b)\big) = \pi(x)f(x) + f(x) = f(x)$. Donc $\varphi(c + q(c)\,a, \cdot) = f = 0$, et $c = -q(c)\,a$ par non-dégénérescence. Posons $e = q(c)$; alors $e = q(-ea) = e^2$, et $u(x) = x - e\,\pi(x)\,a$. Réciproquement, $q(x - e\,\pi(x)\,a) = q(x) - e\,\pi(x)^2 + e^2\pi(x)^2 = q(x)$. Si $e = 0$, $u = \mathrm{id}$; si $e = 1$, $u = \sigma$.

Pour le point 3, $\pi(a/2) = \pi(a)/2 = 1$; si $\pi(x) = 1$, $\sigma(x) = x - a$, $\pi(-\sigma x) = -(1 - 2) = 1$ et $-\sigma(x) - a/2 = a/2 - x$. Pour le point 4, $\pi(a) = 2 = 0$, $\pi(\sigma x) = \pi(x) - \pi(x)\,\pi(a) = \pi(x)$, et $\sigma(x) = x - a$ si $\pi(x) = 1$. Pour le point 5, $\det(x + 1) = \det x + \operatorname{tr} x + 1$ pour une matrice 2×2. □

Remarque. La lecture adopte la normalisation $\pi = \varphi(a, \cdot)$, que la page 117 biffe. Elle donne $\pi(a) = 2$ et $\sigma^2 = \mathrm{id}$, alors que la page justifie (21) par « $\pi(a) = 1$ », qui donnerait $\sigma^2 = \sigma$. L'unicité utilise l'absence d'idempotent non trivial et deux hypothèses que la page tire de sa situation : φ non dégénérée (« comme ψ est iso ») et π surjective, qui découle de la structure d'extension (1). La page conclut de $\lambda(\lambda + 1) = 0$ que $\lambda = -1$ hors de l'identité ; sur un anneau quelconque les solutions sont les $\lambda = -e$, e idempotent. Sur $R = R_1 \times R_2$ et pour $e = (1, 0)$, le point 2 donne une isométrie qui fixe V et qui vaut σ au-dessus de la première composante et l'identité au-dessus de la seconde. La Proposition de la marge vaut donc sur une base connexe, ou fibre à fibre. L'énoncé formalisé traite l'invariance $q \circ u = q$; l'invariance à une unité près, $q \circ u = \lambda q$, dont la page déduit $\lambda = 1$ en rang au moins 3, n'est pas formalisée. Sur la page 124 la polaire de $\det$ est écrite avec le signe opposé, d'où $\pi = -\operatorname{tr}$ et la remarque « attention au signe ! » ; avec la convention $\varphi(x, y) = q(x + y) - q(x) - q(y)$, π est la trace et $\pi(1) = 2$.

Ne sont pas démontrés ici : une expression de C en rang pair $2n \geq 6$; le développement de Δ en graphes des pages 65 à 67 ; les équivalences de la page 127 entre l'inversibilité de $\delta'(q)$, la lissité de $V(q)$ et l'isomorphie locale à la forme standard ; l'invariance de q à une unité près et $\lambda = 1$ en rang au moins 3 (page 123) ; l'équivalence du Scholie (page 120) entre les (P, Q, H) et les (T, q, a) ; la version schématique et la version tordue de la sphère (pages 98 à 116) ; la symétrie (22) du rang impair et la structure $G \simeq G^0 \times \mathbf{Z}/2$ annoncée page 125 ; les parties I à III et V du dossier : revêtements quadratiques, extension à travers 2 (hors la proposition de la page 85, ci-dessous), groupes orthogonaux.

Contre-exemple 56.3 (page 85, extension à travers 2 ♦). *La proposition de la page 85 porte sur A noethérien où 2 est régulier, $A/2A$ intègre et normal, $\Delta \notin 2A$; sa condition c) demande que $A_{2\Delta}[U]/(U^2 - \Delta)$ se prolonge en une extension finie de A_Δ, le mot « étale » étant biffé. Ainsi écrite, c) n'entraîne pas a). Pour $A = \mathbf{Z}$ et $\Delta = 3$, l'algèbre $\mathbf{Z}[1/3][\sqrt{3}]$ est finie sur $\mathbf{Z}[1/3]$ et redonne $\mathbf{Z}[1/6][\sqrt{3}]$ quand on inverse 2, mais 3 n'est pas de la forme $b^2 - 4c$ avec $b, c \in \mathbf{Z}$, puisque $b^2 - 4c \equiv 0$ ou $1 \pmod 4$.*

Démonstration. Posons $A_\Delta = \mathbf{Z}[1/3]$ et $B_\Delta = A_\Delta[U]/(U^2 - 3)$. Le polynôme $U^2 - 3$ est unitaire de degré 2, donc B_Δ est libre de base $1, U$ sur A_Δ : c'est une extension finie, et même quadratique. Inverser 2 dans B_Δ revient à inverser 2 dans les coefficients : les deux morphismes évidents, $(B_\Delta)_2 \to A_{2\Delta}[U]/(U^2 - 3)$, qui envoie U sur U et existe parce que 2 y est inversible, et $A_{2\Delta}[U]/(U^2 - 3) \to (B_\Delta)_2$, qui envoie U sur l'image de U, sont inverses l'un de l'autre, comme on le vérifie sur les coefficients et sur U. Enfin, si $b^2 - 4c = 3$, on réduit modulo 4 : $b^2 \equiv 3$, alors que les carrés modulo 4 sont 0 et 1. □

Le contre-exemple est formalisé tel que la page écrit c), avec $\mathbf{Z}[1/6]$ réalisé comme $\mathbf{Z}[1/3][1/2]$; le lemme `quadAlg_away` établit, sur un anneau commutatif quelconque R, l'isomorphisme $(R[U]/(U^2-d))_s \simeq R_s[U]/(U^2-d)$ (Lean : `extension_across_two_counterexample`, `quadAlg_away`, `sq_sub_four_mul_ne_three`). Ici B_Δ n'est pas étale sur $\mathbf{Z}[1/3]$, puisque son discriminant 12 n'y est pas inversible : le contre-exemple ne contredit donc pas la proposition lue avec « finie étale », démontrée ci-dessous, dont ce fait est d'ailleurs une conséquence (corollaire 56.5).

Théorème 56.4 (page 85, c) ⇒ a) avec « finie étale » ♦). *Soient A un anneau commutatif où 2 est régulier, tel que $A_0 = A/2A$ soit intègre et intégralement clos, et $\Delta \in A$ avec $\Delta \notin 2A$. S'il existe une A_Δ-algèbre finie étale B_Δ et un isomorphisme de A_Δ-algèbres $(B_\Delta)_2 \simeq A_{2\Delta}[U]/(U^2-\Delta)$, alors il existe $b, c \in A$ avec $b^2 - 4c = \Delta$. De plus, deux morphismes de A_Δ-algèbres $B_\Delta \to B'_\Delta$ compatibles avec de tels isomorphismes pour B_Δ et B'_Δ sont égaux.*

Esquisse. Soit $P = 2A_\Delta$, premier puisque $\Delta \notin 2A$, et $R = (A_\Delta)_P$: c'est un anneau local d'idéal maximal $2R$, et aussi le localisé de A en $2A$. Soit $C = R \otimes_{A_\Delta} B_\Delta$, réalisé comme localisé de B_Δ ; C est fini et non ramifié sur R, sans 2-torsion (B_Δ est plat et 2 régulier), non nul (puisque $A_\Delta \to B_\Delta$ est injectif, ce que donne l'isomorphisme après inversion de 2). Une racine de $U^2 = \Delta$ dans $(B_\Delta)_2$ fournit $v \in C$ avec $v^2 = 4^n\Delta$.

L'étape locale n'utilise pas de présentation monogène. Le quotient $C/2C$ est fini et non ramifié sur le corps $R/2R$, donc réduit ; de $v^2 \in 4C$ on tire $v \in 2C$, et, 2 étant régulier, on descend jusqu'à $u \in C$ avec $u^2 = \Delta$. Pour un idéal maximal Q de C au-dessus de $2R$ (montée), C/Q est une extension finie séparable de $R/2R$, de caractéristique 2 ; l'image de u y est séparable et de carré dans $R/2R$, donc dans $R/2R$: $\Delta \equiv c^2 \pmod{2R}$. Alors $(u-c)^2 \in 2C$, donc $u = c + 2s$ par réduction, et $\Delta - c^2 = 4(cs + s^2)$; écrivant $\Delta - c^2 = 2y$, on obtient $y \in 2C \cap R = 2R$, d'où $\Delta = c^2 - 4d$ dans R.

Retour à A : on écrit $c = \alpha/\tau$ avec $\tau \notin 2A$ et l'on chasse les dénominateurs, d'où $\alpha^2 - \tau^2\Delta \in 4A$. Dans le corps des fractions de A_0, $(\bar\alpha/\bar\tau)^2 = \bar\Delta$; cet élément est entier, donc égal à un $\bar b \in A_0$, et $\alpha = b\tau + 2x$. Alors $\tau^2(b^2 - \Delta) \in 4A$, et, $2A$ étant premier et 2 régulier, $\tau y \in 4A$ avec $\tau \notin 2A$ entraîne $y \in 4A$: $b^2 - \Delta = 4c'$. Pour l'unicité, B'_Δ est plat, donc sans 2-torsion, et $B'_\Delta \to (B'_\Delta)_2$ est injectif. (Lean : `prop85_c_imp_a`, `prop85_local`, `exists_of_sq_sub`, `dvd_four_of_mul`, `prop85_iso_unique`.) □

Corollaire 56.5. *L'algèbre $B_\Delta = \mathbf{Z}[1/3][U]/(U^2-3)$ du contre-exemple n'est pas étale sur $\mathbf{Z}[1/3]$.*

Démonstration. Sinon le théorème 56.4, appliqué à $A = \mathbf{Z}$, $\Delta = 3$ et à l'isomorphisme du contre-exemple (qui est automatiquement $\mathbf{Z}[1/3]$-linéaire), donnerait $3 = b^2 - 4c$ dans $\mathbf{Z}$. (Lean : `B3_not_etale`.) □

Remarque. L'hypothèse noethérienne de la page est inutile. La démonstration de l'édition passe par une présentation monogène de $B_\Delta \otimes A_\mathfrak{p}$ et son discriminant ; celle-ci la remplace par la réduction de $C/2C$ et la séparabilité de ses corps résiduels, ce qui évite le calcul du rang. L'existence d'un isomorphisme entre deux extensions B_Δ (l'unicité de B_Δ à isomorphisme près), les implications a) ⇒ b) ⇒ c) et le corollaire 3 (page 63) ne sont pas formalisés.

57 Cote 79 : graphes à homothéties, commutant et étoiles sur $(\mathbf{Z}/n)^2$ [60]

La cote 79, *Géométrie et topologie combinatoire*, compte deux cent quatre-vingt-quinze pages. Elle part des triangles d'un module libre M de rang 2 sur un anneau commutatif Λ : les sommets sont les éléments de M^*, vecteurs qui font partie d'une base, pris au signe près, et une arête de type $\pm e$ joint $\dot{x}$ et $\dot{y}$ quand $x \wedge y = \pm e$. Pour $\Lambda = \mathbf{Z}/n$ on obtient les polyèdres $P_{M,i}$, un par type $i \in \Lambda^*/\pm 1$. La page 19 relie deux sommets par $z = \lambda x + \lambda y$ quand $e = \lambda\, x \wedge y$; la page 20 cite comme connu que deux éléments de M^* ont sur un anneau semi-local un partenaire de base commun, et en tire la distance au plus 3, « atteinte pour l'icosaèdre » (79, lot 1, p. 19, 79, lot 1, p. 20). Pages 92 à 95, elle calcule le commutant de $\mathrm{SL}(M)$ et de $\mathrm{SL}(M)/\pm 1$ par le normalisateur du stabilisateur d'un point ; elle trouve l'exception $2\Lambda = \{0,2\} \neq \{0\}$, un élément σ induit par la matrice de lignes $(1,0)$ et $(2,1)$, un produit « direct (pas seulement ½direct !) », et pour $\Lambda = \mathbf{Z}/4$ l'antipodie de l'octaèdre ; une formule biffée y donne $\sigma(\dot{x}) = (x+2y)^{\cdot}$ (79, lot 5, p. 93, 79, lot 5, p. 94, 79, lot 5, p. 95). Pages 136 à 140, le « fait mirifique » : $(\mathbf{Z}/n)^*/\pm 1$ opère sur les structures de polygone d'un ensemble à n éléments, et l'axiome To 6 demande qu'une homothétie redessine chaque étoile en polygone étoilé (79, lot 7, p. 138, 79, lot 7, p. 139). Pages 187 et 188, elle examine si une homothétie λ d'un 2-polyèdre régulier tord la triangulation en une autre ; la condition (32) a″) demande que $\lambda^{-1}s$ soit à distance au plus 3 de s, « et en fait, égale à 3 », sauf pour l'identité et pour l'antipodie de l'octaèdre (distance 2) ; la distance 1 est exclue par les stabilisateurs, et la distance 2 donnerait deux sommets de même étoile. La phrase porte un mot illisible et deux lectures incertaines (79, lot 10, p. 188). Les pages 242 à 247 traduisent un graphe homogène muni d'un groupe d'homothéties en données de théorie des groupes (H, U_0, σ, T_H) et énoncent l'équivalence (88), avec en marge « [ ] résulte des autres » ; la réciproque, page 247, porte plusieurs mots illisibles (79, lot 13, p. 242, 79, lot 13, p. 245, 79, lot 13, p. 247). Pages 275 à 279, elle demande si un sommet est déterminé par son étoile, répond sur un anneau semi-local par la même exception, et construit l'involution a, de déterminant -1 (79, lot 14, p. 276, 79, lot 14, p. 277, 79, lot 14, p. 278).

Conventions. Pour un groupe H, un sous-groupe U_0 et $\sigma \in H$, le graphe de classes a pour sommets $S = H/U_0$, pour origine $s_0 = U_0$ et $t_0 = \sigma U_0$; les arcs sont les (hs_0, ht_0), $h \in H$. On note $U_1 = \sigma U_0 \sigma^{-1}$, stabilisateur de t_0. Les hypothèses $\sigma^2 \in U_0$ (l'élément σ échange s_0 et t_0) et $U_0 \cap U_1 = 1$ disent que H est simplement transitif sur les arcs. Un *groupe d'homothéties* est un sous-groupe Z du groupe des permutations de S dont les éléments commutent à H, envoient chaque arc (s,t) sur un arc $(\lambda s, \lambda^{-1} t)$, et vérifient la fidélité (72) : si $u \in H$ fixe s_0 et envoie t_0 sur λt_0, alors $\lambda = 1$. Pour le rang 2, R est un anneau commutatif quelconque, $M = R^2$, $x \wedge y = x_0 y_1 - x_1 y_0$, et $S_M = M^*/\pm 1$, où $x \in M^*$ s'il existe y avec $x \wedge y = 1$. Le groupe $\mathrm{SL}(2,R)$ opère sur S_M, et $c \in R^*$ par $\dot{x} \mapsto (cx)^{\cdot}$. On dit que R est *exceptionnel* si $2s \in \{0,2\}$ pour tout $s \in R$, c'est-à-dire $2R \subset \{0,2\}$; avec $2 \neq 0$, c'est $2R = \{0,2\} \neq \{0\}$.

Énoncé (Pages 242 à 247, (88) et (89) ♦). *Soient H, U_0, σ comme ci-dessus, avec $\sigma^2 \in U_0$ et $U_0 \cap U_1 = 1$. Appelons* tore *un sous-groupe $T \subset H$ tel que (a) $\sigma t \sigma^{-1} = t^{-1}$ pour $t \in T$, (b) T normalise U_0, (c) l'application $U_0 \times T \times U_1 \to H$, $(u_0, t, u_1) \mapsto u_0 t u_1$, est injective.*

1. *Pour un groupe d'homothéties Z, $T_H = \{u \in H \mid \exists \lambda \in Z,\ us_0 = \lambda s_0,\ ut_0 = \lambda^{-1} t_0\}$ est un sous-groupe, et c'est un tore.*

60. Preuve vérifiée : `lean/Grothendieck/Folder79.lean`.

2. *Pour un tore T, les permutations λ de S qui commutent à H et vérifient $\lambda s_0 = ts_0$ pour un $t \in T$, c'est-à-dire $hU_0 \mapsto htU_0$, forment un groupe d'homothéties Z_T.*
3. *Les applications $Z \mapsto T_H$ et $T \mapsto Z_T$ sont des bijections réciproques entre groupes d'homothéties et tores.*
4. *Un groupe d'homothéties est commutatif, et cela sans l'hypothèse $U_0 \cap U_1 = 1$.*

Démonstration. Une permutation qui commute à H est déterminée par l'image de s_0, puisque $\lambda(hs_0) = h\lambda(s_0)$. Deux éléments de H qui coïncident sur s_0 et sur t_0 sont égaux, puisque $U_0 \cap U_1 = 1$. Comme σ^2 est dans U_0 et dans U_1, $\sigma^2 = 1$.

Commutativité. Soient $\lambda, \mu \in Z$ et $u, v, w \in H$ tels que $u(s_0, t_0) = (\lambda s_0, \lambda^{-1} t_0)$, $v(s_0, t_0) = (\mu s_0, \mu^{-1} t_0)$, $w(s_0, t_0) = (\mu\lambda s_0, (\mu\lambda)^{-1} t_0)$; ils existent par la condition d'homothétie appliquée à l'arc (s_0, t_0). L'élément $w^{-1}uv$ fixe s_0 et envoie t_0 sur $c\,t_0$, avec $c = \mu^{-1}\lambda^{-1}\mu\lambda$. La fidélité donne $c = 1$.

Point 1. Si u correspond à λ et v à μ, uv correspond à $\mu\lambda$, grâce à la commutativité ; u^{-1} correspond à λ^{-1}. Pour (a), $\sigma u \sigma^{-1}$ et u^{-1} envoient tous deux s_0 sur $\lambda^{-1}s_0$ et t_0 sur λt_0, donc sont égaux. Pour (b), si $u \in U_0$ et t correspond à λ, $tut^{-1}s_0 = t\lambda^{-1}us_0 = \lambda^{-1}ts_0 = s_0$. Pour (c), soit $atb = a't'b'$. On pose $c' = t'^{-1}a'^{-1}at' \in U_0$, $r = t'^{-1}t \in T_H$ et $d = bb'^{-1} \in U_1$; alors $c'rd = 1$. Si r correspond à λ, $c'^{-1} = rd$ fixe s_0 et envoie t_0 sur $rt_0 = \lambda^{-1}t_0$; la fidélité donne $\lambda = 1$, donc r fixe s_0 et t_0 et $r = 1$. Il reste $c'd = 1$, avec $d \in U_0 \cap U_1$, d'où $d = 1$, $c' = 1$, et $(a, t, b) = (a', t', b')$.

Point 2. L'ensemble Z_T est un sous-groupe : si $\lambda s_0 = ts_0$ et $\mu s_0 = t's_0$, alors $\lambda\mu s_0 = t'ts_0$ et $\lambda^{-1}s_0 = t^{-1}s_0$. De (a) on tire $\sigma t^{-1} = t\sigma$, d'où $\lambda^{-1}t_0 = \sigma\lambda^{-1}s_0 = \sigma t^{-1}s_0 = tt_0$: l'arc $(\lambda hs_0, \lambda^{-1}ht_0)$ est l'image par ht de (s_0, t_0). Pour la fidélité, soit $u \in U_0$ avec $ut_0 = \lambda t_0 = \sigma ts_0$. Alors $a = t^{-1}\sigma^{-1}u\sigma \in U_0$, et $b = \sigma^{-1}u\sigma$ est dans U_1 puisque $\sigma^{-1}b\sigma = u$. L'égalité $(tat^{-1})\,t \cdot 1 = 1 \cdot 1 \cdot b$ et l'injectivité (c) donnent $t = 1$, donc $\lambda s_0 = s_0$ et $\lambda = 1$.

Point 3. Si $\lambda \in Z$, un u associé à λ par la condition d'homothétie est dans T_H et $\lambda s_0 = us_0$, donc $\lambda \in Z_{T_H}$; réciproquement, si $\lambda \in Z_{T_H}$, $\lambda s_0 = ts_0 = \mu s_0$ pour un $\mu \in Z$, et $\lambda = \mu$. Si $t \in T$, la permutation $hU_0 \mapsto htU_0$, bien définie parce que t et t^{-1} normalisent U_0, est dans Z_T et lui associe t, donc $t \in T_{Z_T}$; réciproquement, si u est associé à $\lambda \in Z_T$ avec $\lambda s_0 = ts_0$, u et t coïncident sur s_0 et sur t_0, donc $u = t$. □

Remarque. Les deux sens de l'équivalence tiennent, y compris la réciproque que la page 247 vérifie sur des lignes en partie illisibles. La commutativité de Z, que la piste suppose et que la page met entre crochets, découle de la condition d'homothétie et de la fidélité (72), comme le dit la marge « [ ] résulte des autres » ; la démonstration n'utilise pas la simple transitivité. La fidélité de H sur H/U_0, condition (77), n'intervient nulle part, ni $s_0 \neq t_0$. La condition d'homothétie est prise sous la forme corrigée par la lecture, $u(s_0, t_0) = (\lambda s_0, \lambda^{-1}t_0)$. L'isomorphisme $T_H \simeq Z$ de (81') n'est pas formalisé comme morphisme de groupes, seulement la bijection entre les deux familles.

Théorème 57.1 (Grothendieck, pages 92 à 95, le commutant ♦). *Soit R un anneau commutatif.*

1. *Si R est exceptionnel, l'application $\sigma(\dot{x}) = (x+2y)\dot{}$, pour un y tel que $x \wedge y = 1$, est bien définie sur S_M. Elle commute à $\mathrm{SL}(2, R)$ et aux scalaires, et $\sigma^2 = 1$. Si de plus $2 \neq 0$, $\sigma(v) \neq cv$ pour tout $c \in R^*$ et tout v ; en particulier σ n'a pas de point fixe.*
2. *Les scalaires commutent à $\mathrm{SL}(2, R)$, et c, c' agissent de même si et seulement si $c' = \pm c$.*

3. *Toute application $f : S_M \to S_M$ qui commute à $\mathrm{SL}(2,R)$ est un scalaire, ou bien R est exceptionnel et $f = c\,\sigma$ pour un $c \in R^*$.*
4. *Sur $\mathbf{Z}/n$, $2R = \{0,2\} \neq \{0\}$ si et seulement si $n = 4$; pour $n \neq 4$ le commutant est formé des scalaires.*
5. *Sur $\mathbf{Z}/4$, si $x \wedge y = 1$, les $z \in M^*$ tels que $x \wedge z$ ne soit pas inversible sont $\pm x$ et $\pm(x+2y)$: $\sigma(\dot{x})$ est le seul sommet autre que $\dot{x}$ qui ne lui soit pas adjacent, l'antipode sur l'octaèdre.*

Démonstration. Si $x \wedge y = 1$, tout z s'écrit $z = (z \wedge y)\,x + (x \wedge z)\,y$. Dans un anneau exceptionnel, $4 = 0$ (car $2 \cdot 2 \in \{0,2\}$) et $2c = 2$ pour tout c inversible.

Point 1. Deux partenaires de x diffèrent d'un multiple tx ; comme $2t \in \{0,2\}$ et $4 = 0$, $x + 2y' = x + 2y$ ou $x + 2y' = -(x+2y)$. Le passage de x à $-x$ change y en un partenaire de $-x$ et donne de même $\pm(x+2y)$; σ est donc bien définie. Si $g \in \mathrm{SL}(2,R)$, gy est un partenaire de gx, d'où $\sigma g = g\sigma$. Comme $(x+2y) \wedge y = 1$, $\sigma^2(\dot{x}) = (x+4y)^{\cdot} = \dot{x}$. Pour $c \in R^*$, $c^{-1}y$ est un partenaire de cx et $2c^{-1} = 2c = 2$, d'où $\sigma(c\dot{x}) = c\,\sigma(\dot{x})$. Si $x + 2y = \pm cx$, on applique $x \wedge \cdot$: $2 = 0$.

Point 3. Soit $v = (p,q)$ un représentant de $f(\dot{e}_1)$, avec $e_1 = (1,0)$. Les matrices de lignes $(1,t)$ et $(0,1)$ fixent $\dot{e}_1$, donc $(p+tq, q) = \pm(p,q)$ pour tout t. Pour $t = 1$: ou bien $q = 0$, et p est inversible puisque $v \in M^*$; ou bien $2q = 0$ et $q = -2p$. Dans ce second cas $p(s+2r) = 1$ si $v \wedge (r,s) = 1$, donc p est inversible. Pour $a \in R$ et $t = ap^{-1}$, $tq = -2a$, et la condition donne $2a = 0$ ou $2a = 2p$. Avec $a = 1$, $2p = 2$; donc $2a \in \{0,2\}$ pour tout a, R est exceptionnel, et $q = -2p = 2$. Pour $\dot{x}$ quelconque, soit g la matrice de colonnes x et y, avec $x \wedge y = 1$; alors $g\dot{e}_1 = \dot{x}$ et $f(\dot{x}) = gf(\dot{e}_1) = (px+qy)^{\cdot}$. Si $q = 0$, c'est $p\dot{x}$. Sinon c'est $(px+2y)^{\cdot} = (p(x+2y))^{\cdot} = p\,\sigma(\dot{x})$, puisque $2p = 2$.

Point 4. Si $2 \cdot 2 \in \{0,2\}$ dans $\mathbf{Z}/n$, n divise 4 ou 2 ; on écarte $n = 1, 2$ par $2 \neq 0$ et l'on vérifie $n = 4$ par calcul. Si R n'est pas exceptionnel, le point 3 donne un scalaire ; si $2 = 0$, σ est l'identité. Point 5. On écrit $z = ax + by$ avec $b = x \wedge z$ non inversible, donc $b \in \{0,2\}$. Comme $z \in M^*$, a est inversible, donc $a = \pm 1$, et $-x + 2y = -(x+2y)$. □

Remarque. L'énoncé tient sur tout anneau commutatif, sans l'hypothèse $2 \neq 0$: quand $2 = 0$, R est exceptionnel au sens adopté ici mais σ est l'identité, et le commutant se réduit aux scalaires. L'application f n'a pas à être supposée bijective. Le produit direct de la page est confirmé : σ commute aux scalaires, $\sigma^2 = 1$, et $\sigma \neq c$ pour tout c, de sorte que le commutant est $R^*/\pm 1 \times \{1, \sigma\}$. La démonstration ne passe pas par le normalisateur $N_{G'}(H')$: elle fixe l'image de $\dot{e}_1$, et le calcul est le même. La formule biffée de la page 95, $\sigma(\dot{x}) = (x+2y)^{\cdot}$, est celle que l'on démontre ; l'élément σ envoie $\dot{e}_1$ sur la classe de $(1,2)$, image de e_1 par la matrice de lignes $(1,0)$ et $(2,1)$.

Énoncé (Pages 275 à 279, un sommet et son étoile ♦). *Soient R un anneau commutatif, $x, y \in M$ avec $x \wedge y = 1$, et $x' \in M$.*

1. *On a l'équivalence : pour tout z tel que $x \wedge z$ soit inversible, $x' \wedge z = \pm\, x \wedge z$, si et seulement si $x' = \pm x$, ou bien R est exceptionnel et $x' = \pm(x+2y)$, c'est-à-dire $\dot{x}' = \sigma(\dot{x})$.*
2. *Si R est exceptionnel, la matrice A de lignes $(1,2)$ et $(2,-1)$ vérifie $Ax = \pm(x+2y)$; elle a pour déterminant -1 et $A^2 = 1$.*

Démonstration. On écrit $x' = \alpha x + \beta y$, avec $\alpha = x' \wedge y$ et $\beta = x \wedge x'$. Pour $s \in R$, $z = y + sx$ vérifie $x \wedge z = 1$ et $x' \wedge z = \alpha - s\beta$. L'hypothèse donne $\alpha - s\beta = \pm 1$ pour tout s. Avec $s = 0$,

$\alpha = \pm 1$. Si $\alpha = 1$, $s = 1$ donne $\beta = 0$, d'où $x' = x$, ou $\beta = 2$; dans ce dernier cas, $1 - 2s = \pm 1$ donne $2s \in \{0, 2\}$ pour tout s, et $x' = x + 2y$. Le cas $\alpha = -1$ donne de même $x' = -x$, ou $\beta = -2$ et $x' = -(x + 2y)$. Réciproquement, $(x + 2y) \wedge z = x \wedge z - 2(z \wedge y)$; si $2(z \wedge y) = 0$ c'est $x \wedge z$, et si $2(z \wedge y) = 2$ c'est $x \wedge z - 2 = -x \wedge z$, puisque $2(x \wedge z) = 2$ pour $x \wedge z$ inversible.

Pour le point 2, on note $x = (p, q)$, $y = (r, s)$, avec $ps - qr = 1$. Chacun de $2p, 2q, 2r, 2s$ vaut 0 ou 2, et $2(ps) = (2p)s$ vaut 0 si $2p = 0$, $2s$ si $2p = 2$. On examine les seize cas ; l'égalité $2(ps) - 2(qr) = 2$ en écarte une partie, et dans les autres on a $2q = 2r$ et $2p = 2q + 2s$, ce qui donne $Ax = x + 2y$, ou bien $2p + 2q + 2r = 0$ et $2p = 2s$, ce qui donne $Ax = -(x + 2y)$. Enfin $\det A = -1 - 4 = -1$ et $A^2 = 5 \cdot 1 = 1$. □

Remarque. L'hypothèse « semi-local » de la page n'est pas nécessaire : l'énoncé tient sur tout anneau commutatif, et la démonstration n'utilise ni les corps résiduels ni le lemme de colinéarité de la page 276. Il suffit des voisins $y + sx$ d'un seul type, ceux pour lesquels $x \wedge z = 1$. L'énoncé dit aussi que, dans le cas exceptionnel, le seul sommet autre que $\dot{x}$ qui ait la même étoile est $\sigma(\dot{x})$: la question que la page laisse ouverte (« il n'est pas vrai nécessairement … ») est donc tranchée dans ce cadre algébrique, où l'étoile est prise type par type. La transcription signale à la page 277 la conclusion $\alpha - \beta \in \pm(\alpha - \beta)$, qui doit se lire $\alpha + \beta \in \pm(\alpha - \beta)$; la démonstration ci-dessus ne passe pas par elle. L'involution a de la page 278 est l'élément σ de l'énoncé précédent, et la matrice A réalise le déterminant -1 annoncé, sur tout anneau exceptionnel ; pour $\mathbf{Z}/4$ c'est la matrice que la lecture vérifie. Le lemme combinatoire de la page 275 (deux sommets distincts de même étoile forment un double cône, figure 13) n'est pas formalisé.

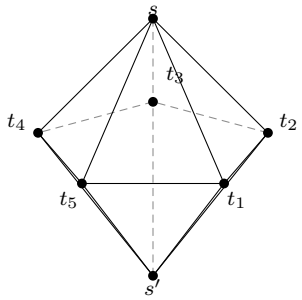


FIGURE 13 – Le lemme du double cône de la page 275 : sur une surface triangulée fermée, deux sommets distincts s et s' qui ont la même étoile, ici le cycle $t_1 \cdots t_5$ de leurs voisins, sont les deux pointes d'une bipyramide sur ce cycle, qui est alors toute la surface (si elle est connexe) ; avec un cycle de quatre sommets, c'est l'octaèdre. Ce lemme n'est pas formalisé ici. Figure de l'édition ; Grothendieck dessine à la page 275 une bipyramide sur un pentagone (79, lot 14, p. 275).

Énoncé (Pages 19 et 20, distance au plus 3 ♦). *Soit R un anneau commutatif qui n'a qu'un nombre fini d'idéaux maximaux.*

1. *Si $a_0 d + b_0 d' = 1$, il existe $a \in R$ tel que $ad + d'$ soit inversible.*
2. *Pour tout $e \in R^*$ et tous $x, y \in M^*$, il existe $z_1, z_2 \in M^*$ avec $x \wedge z_1 = z_1 \wedge z_2 = z_2 \wedge y = e$: deux sommets de SP_M sont à distance au plus 3.*

Cela vaut en particulier pour un anneau local, un corps, et $\mathbf{Z}/n$ pour $n \geq 1$.

Le point 2 donne un chemin de trois arêtes de type e entre deux sommets quelconques :

$$\dot{x} \overset{e}{\text{———}} \dot{z}_1 \overset{e}{\text{———}} \dot{z}_2 \overset{e}{\text{———}} \dot{y} \qquad x \wedge z_1 = z_1 \wedge z_2 = z_2 \wedge y = e.$$

Démonstration. Point 1. L'égalité $a_0 d + b_0 d' = 1$ dit que d' et d sont étrangers ; par le rang stable 1 des anneaux semi-locaux, énoncé général rappelé à la suite de la démonstration, $d' + ad$ est inversible pour un $a \in R$.

Point 2. Soient w et y' avec $x \wedge w = 1$ et $y \wedge y' = 1$. L'identité $(x \wedge y)(w \wedge y') - (x \wedge y')(w \wedge y) = (x \wedge w)(y \wedge y')$ donne $(w \wedge y')\, d - (x \wedge y')\, d' = 1$ pour $d = x \wedge y$ et $d' = w \wedge y$. Par le point 1, $u = ad + d'$ est inversible pour un a. Le vecteur $z = ax + w$ vérifie $x \wedge z = 1$ et $z \wedge y = u$. On pose $z_1 = ez$, d'où $x \wedge z_1 = e$ et $z_1 \wedge y = eu$, puis, suivant la page 19, $z_2 = u^{-1}(z_1 + y)$: $z_1 \wedge z_2 = u^{-1}eu = e$ et $z_2 \wedge y = e$. Les vecteurs z_1 et z_2 sont dans M^*, puisque $z_1 \wedge y$ et $z_2 \wedge y$ sont inversibles. Un anneau local n'a qu'un idéal maximal ; un anneau fini n'a qu'un nombre fini d'idéaux. □

Résultat général, démontré en Lean dans
`Upstream/SemilocalStableRange.lean` *; la démonstration n'est pas reprise ici.*

Remarque. L'énoncé tient sur tout anneau semi-local, au sens où l'ensemble des idéaux maximaux est fini. Pour $\Lambda = \mathbf{Z}/n$ et $n \geq 5$, le diamètre 3 du graphe est le théorème 11 de Singerman et Strudwick, mis en ligne en 2018 et publié en 2020 [114] (numérotation de la version arXiv). La page cite comme connu (« on sait que ») le rang stable 1 des anneaux semi-locaux, dû à Bass (1964, § 4 et lemme 6.4) [11] ; le fichier général le démontre par le théorème chinois. La démonstration ne construit pas un partenaire commun dans chaque corps résiduel comme le propose la lecture : elle cherche ce partenaire sur la droite $ax + w$, où $x \wedge z = 1$ est automatique. La borne est atteinte sur $\mathbf{Z}/n$ dès que $(\mathbf{Z}/n)^*$ contient un $\mu \neq \pm 1$, c'est-à-dire pour $n \notin \{1, 2, 3, 4, 6\}$, en particulier pour l'icosaèdre ($n = 5$) : c'est le point 4 de l'énoncé de la page 188 ci-dessous. Le cas $n = 6$, que couvre le théorème de Singerman et Strudwick pour $n \geq 5$, n'est pas formalisé. Le cas $\Lambda = \mathbf{Z}$, qui n'est pas semi-local, n'est pas traité.

Énoncé (Pages 96 à 101 et 136 à 140, la torsion dans le modèle ♦). *Soient R un anneau commutatif, $e, \mu \in R^*$ et $x, y \in M$ avec $x \wedge y = e$.*

1. *(Torsion d'une extrémité.) $x \wedge \mu y = \pm \mu e$ si et seulement si $x \wedge y = \pm e$: les arêtes $\{\dot{x}, \mu\dot{y}\}$, pour $\{\dot{x}, \dot{y}\}$ arête de type $\pm e$, sont les arêtes de type $\pm \mu e$. De même $\mu x \wedge z = \pm \mu e$ si et seulement si $x \wedge z = \pm e$: l'étoile de $\dot{x}$ dans $P_{M,\pm e}$ est, comme partie de S_M, l'étoile de $\mu\dot{x}$ dans $P_{M,\pm \mu e}$.*
2. *(L'étoile est une droite.) Si $x \wedge z = e$, alors $z = y + kx$ avec $k = z \wedge e^{-1}y$.*
3. *(Formule (178), page 67, 79, lot 4, p. 67.) Si $x \wedge z = \pm e$ et $z \wedge y = \pm e$, alors $z = ax + by$ avec $a, b \in \{1, -1\}$.*
4. *(Le polygone étoilé.) Pour $k, k' \in R$, $(y + kx) \wedge (y + k'x) = (k - k')\, e$; ces deux points sont joints par une arête de type $\pm \mu e$ si et seulement si $k - k' = \pm \mu$.*
5. *(L'indice.) $\mu(y + kx) = \mu y + (\mu k)x$, et $x \wedge \mu y = \mu\, (x \wedge y)$.*

Démonstration. Les points 1 et 5 viennent de la bilinéarité : $x \wedge \mu y = \mu\, x \wedge y$, et l'on simplifie par μ inversible. Pour le point 2, $(x, e^{-1}y)$ est une base de déterminant 1 et $z = (z \wedge e^{-1}y)\, x + (x \wedge z)\, e^{-1}y$. Le point 3 se lit sur la même décomposition : les coefficients sont $e^{-1}(z \wedge y)$ et $(x \wedge z)e^{-1}$, égaux à ± 1. Pour le point 4, $(y + kx) \wedge (y + k'x) = k'(y \wedge x) + k(x \wedge y) = (k - k')e$, et $(k - k')e = \pm \mu e$ équivaut à $k - k' = \pm \mu$. □

Remarque. Ces identités vérifient le calcul de la lecture dans le modèle, et non l'énoncé abstrait de la piste. Sur l'étoile de $\dot{x}$, indexée par $k \mapsto (y+kx)^{\cdot}$, le polyèdre $P_{M,\pm e}$ induit le polygone $k \sim k \pm 1$ et $P_{M,\pm\mu e}$ le polygone $k \sim k \pm \mu$, sa puissance μ-ième. La multiplication par μ envoie l'indice k sur μk : l'exposant est μ lui-même, sans la puissance illisible des formules (65) et (66), comme la lecture l'avait calculé. Les identités tiennent sur tout anneau commutatif, et pas seulement sur $\mathbf{Z}/n$. L'action de $(\mathbf{Z}/n)^*/\pm 1$ sur les structures de polygone, l'axiome To 6 dans le cadre abstrait et l'injection $Z \hookrightarrow Z'_n$ font l'objet de l'énoncé des pages 136 à 140 plus bas ; la comparaison avec les opérateurs de Wilson n'est pas formalisée.

Théorème 57.2 (Page 188, forme de l'édition, distance à l'image ⧫). *1. (Cadre abstrait.) Soient H, U_0, σ comme ci-dessus, avec $\sigma^2 \in U_0$, et $\lambda \neq 1$ une permutation de $S = H/U_0$ qui commute à H. Alors λ n'a pas de point fixe ; si λs est voisin de s, c'est le seul voisin de s ; si s et λs ont un voisin commun, ils ont les mêmes voisins. En particulier, si s a au moins deux voisins et si aucun autre sommet n'a les voisins de s, alors λs n'est ni s, ni un voisin de s, ni à distance 2 de s ; s'il est à distance au plus 3, il est à distance 3.*

2. *(Modèle, sur un anneau commutatif R non nul.) Soient $e \in R^*$ et, sur S_M, le graphe des arêtes de type $\pm e$: $\dot{x}$ et $\dot{z}$ sont adjacents si $x \wedge z = \pm e$. Soit $f \neq \mathrm{id}$ une application de S_M dans lui-même qui commute à $\mathrm{SL}(2,R)$. Pour tout sommet v, $f(v) \neq v$, $f(v)$ n'est pas adjacent à v, et v et $f(v)$ ont un voisin commun si et seulement si R est exceptionnel et $f = \sigma$. Pour $f = \sigma$, un voisin commun de $\dot{x}$ et $\sigma(\dot{x})$ est $(ey)^{\cdot}$, si $x \wedge y = 1$.*
3. *Si de plus R n'a qu'un nombre fini d'idéaux maximaux et si $f \neq \sigma$, chaque sommet v est à distance 3 de $f(v)$.*
4. *Sur $\mathbf{Z}/n$, $n \geq 2$, pour $\mu \in (\mathbf{Z}/n)^*$ avec $\mu \neq \pm 1$ et tout type $\pm e$, chaque sommet $\dot{x}$ est à distance 3 de $\mu\dot{x}$.*

Démonstration. Point 1. Une permutation qui commute à H et fixe un sommet hs_0 fixe s_0, donc est l'identité. Les arcs sont permutés par H, et $\sigma^2 \in U_0$ rend le graphe non orienté : $h\sigma$ envoie (s_0,t_0) sur (ht_0,hs_0). Si (s,t) et (s,t') sont des arcs, images de (s_0,t_0) par k et k', alors $g = k'k^{-1}$ fixe s et envoie t sur t' : le stabilisateur de s est transitif sur les voisins de s. Il fixe aussi λs, puisque $\lambda(gs) = g\lambda s$. Si λs est voisin de s et t' un autre voisin, on prend g fixant s avec $g\lambda s = t'$, d'où $t' = \lambda s$. Si t est voisin de s et de λs, et t' voisin de s, on prend g fixant s avec $gt = t'$; l'arête $\{t, \lambda s\}$ a pour image $\{t', \lambda s\}$. Dans l'autre sens, si t' est voisin de λs, on prend g fixant λs avec $gt = t'$; alors $\lambda(gs) = \lambda s$, donc $gs = s$ par injectivité de λ, et l'arête $\{s,t\}$ a pour image $\{s,t'\}$. Les deux hypothèses du point 1 excluent alors les distances 0, 1 et 2.

Point 2. Par l'énoncé du commutant, f est un scalaire c, ou bien R est exceptionnel et $f = c\sigma$. Si $f = c$, $f \neq \mathrm{id}$ donne $c \neq \pm 1$. Si $cx = \pm x$, on applique $\cdot \wedge y$: $c = \pm 1$, exclu. On a $x \wedge cx = 0 \neq \pm e$, puisque R est non nul. Si $x \wedge z = \varepsilon_1 e$ et $z \wedge cx = \varepsilon_2 e$, avec $\varepsilon_i = \pm 1$, alors $-c\varepsilon_1 e = \varepsilon_2 e$, et $c = \pm 1$ en simplifiant par e. Si $f = c\sigma$ et $2 = 0$, σ est l'identité et l'on est dans le cas précédent. Supposons $2 \neq 0$, de sorte que $f(\dot{x}) = (c(x+2y))^{\cdot}$ avec $2c = 2$. Si $c(x+2y) = \pm x$, on applique $x \wedge \cdot$: $2 = 0$, exclu. On a $x \wedge c(x+2y) = 2c = 2$; si $2 = \pm e$, 2 est inversible, et $2 \cdot 2^{-1} \in \{0,2\}$ donne $1 = 0$ ou $1 = 2$, impossible dans un anneau non nul. Soit enfin z voisin de $\dot{x}$ et de $f(\dot{x})$, avec $x \wedge z = \varepsilon_1 e$ et $b = z \wedge y$. Alors $z \wedge c(x+2y) = c(-\varepsilon_1 e + 2b)$, avec $2b \in \{0,2\}$ et $2 = 2e$; comme $4 = 0$, $-\varepsilon_1 e + 2b = \pm e$ dans tous les cas, et l'égalité $c(\pm e) = \varepsilon_2 e$ donne $c = \pm 1$, donc $f = \sigma$. Réciproquement, $x \wedge ey = e$ et $ey \wedge (x+2y) = -e$.

Points 3 et 4. Sur un anneau semi-local, deux sommets quelconques sont joints par un chemin de longueur 3 formé d'arêtes de type e (énoncé des pages 19 et 20). Sur $\mathbf{Z}/n$, $n \geq 2$,

l'anneau est fini et non nul, et l'on applique le point 2 aux scalaires. □

Remarque. La partie abstraite de la piste est démontrée dans le cadre du graphe de classes, sous la forme : pas de point fixe, pas de voisin, et un voisin commun force l'égalité des étoiles. Elle n'utilise que la transitivité de H sur les arcs et la commutation de λ à H ; ni la simple transitivité, ni la condition d'homothétie, ni la structure de surface n'interviennent. L'exclusion de la distance 1, que la page attribue aux stabilisateurs (lecture incertaine), demande que s ait au moins deux voisins. Le passage de « même étoile » à « octaèdre » est le lemme du double cône de la page 275 ; le point 1 le remplace par l'hypothèse qu'aucun autre sommet n'a l'étoile de s, et l'encadré suivant le démontre, ce qui donne l'énoncé de la page sous sa forme propre. La page parle de $\lambda^{-1}s$; comme λ^{-1} commute aussi à H, cela revient au même, et l'énoncé vaut pour un sommet comme pour tous (« c'est kif-kif »).

L'énoncé de la page est celui de l'encadré non vérifié ci-dessous ; le cadre abstrait du point 1 et l'application au modèle des points 2 à 4 sont de l'édition. Dans le modèle, l'énoncé tient sur tout anneau commutatif non nul pour les distances 0, 1 et 2, pour toute application qui commute à $\mathrm{SL}(2,R)$ et pour tout type $\pm e$; pour les scalaires le calcul est direct ($x \wedge \mu x = 0$, et $\mu e = \pm e$ force $\mu = \pm 1$), sans argument de stabilisateur. L'exception de la distance 2 est σ, et elle seule. Sur $\mathbf{Z}/n$ elle ne se produit que pour $n = 4$, où σ est l'antipodie de l'octaèdre et où les scalaires sont triviaux. Sur un autre anneau exceptionnel avec $2 \neq 0$, par exemple $\mathbf{Z}/4 \times \mathbf{F}_2$, σ est aussi à distance 2 ; un calcul hors de Lean, à partir du polygone de l'étoile $k \sim k \pm 1$ indexé par R, montre que l'étoile y est formée de deux cycles de longueur 4 ; le polyèdre n'est donc pas une surface, et l'exemple ne contredit pas la page. Pour $e = 1$ et $n \geq 5$, le point 4 est le théorème 9 de Singerman et Strudwick sur les pôles de la carte de Farey modulo n [114].

Ne sont pas démontrés ici : l'isomorphisme de groupes $T_H \simeq Z$ de (81') et le cas $\mathfrak{z}_H \neq 1$ de (88) ; l'optimalité de la borne 3 pour $\mathbf{Z}/6$ et pour un anneau semi-local quelconque ; la connexité de SP_M pour $\Lambda = \mathbf{Z}$; le caractère de morphisme de groupes de $Z \to Z'_n$ dans le cadre abstrait (pages 139 et 140), et l'existence de ν en un sommet à partir de la seule structure de $G_{0s} \simeq \mathbf{D}_n$ (pages 184 à 187) ; la question de la page 141 sur les triangulations dont les sommets sont d'ordre 7 ; la distance exactement 3 de la page 188 hors des anneaux semi-locaux.

Théorème 57.3 (Grothendieck, pages 187 et 188, homothéties à distance trois ⧫). *Dans un 2-polyèdre régulier triangulé abstrait, deux sommets distincts n'ont la même étoile que dans l'octaèdre (lemme du double cône, page 275). Une homothétie $\lambda \neq \mathrm{id}$ n'envoie donc aucun sommet à distance 1 ou 2, l'antipodie de l'octaèdre exceptée, et quand $\lambda^{-1}s$ est à distance au plus 3 de s, cette distance vaut exactement 3.*

Forme démontrée. On prend un 2-polyèdre triangulé régulier sous la forme la plus faible que l'argument utilise : une relation symétrique A sur un ensemble S, connexe, telle que l'étoile de chaque sommet porte, pour les arêtes de A qu'elle contient, une structure de polygone d'un même ordre $n \geq 3$ (condition (A2) de la lecture, tous les sommets ayant le même ordre ; (A1) en découle). L'*octaèdre* est le graphe $K_{2,2,2}$: les sommets $\{0,1,2\} \times \{\pm\}$, joints quand leurs premières coordonnées diffèrent.

Théorème 57.4 (Pages 187, 188 et 275, forme de l'édition ⧫).

1. *(Le double cône, page 275.) Dans un tel polyèdre, si deux sommets distincts $s \neq s'$ ont la même étoile E, alors $n = 4$, $S = \{s, s'\} \cup E$, et A est isomorphe à l'octaèdre.*
2. *(Page 188.) Soient H, U_0, σ comme ci-dessus, avec $\sigma^2 \in U_0$, tels que le graphe de classes*

H/U_0 soit un tel polyèdre (il est alors régulier : H est transitif sur ses arcs), et $\lambda \neq 1$ une permutation de S qui commute à H. Si λ envoie un sommet s à distance au plus 2 de s, alors $n = 4$, le polyèdre est l'octaèdre, et λ est son antipodie : pour tout sommet y, $\lambda y \neq y$ et λy a l'étoile de y.

3. *Hors de l'octaèdre ($n \neq 4$), λs n'est ni s, ni un voisin de s, ni à distance 2 de s : quand λs, ou $\lambda^{-1} s$, est à distance au plus 3 de s, cette distance vaut exactement 3.*

Démonstration. Point 1 (`double_cone`). Un polygone n'a pas de boucle, donc aucun sommet n'est dans sa propre étoile (`not_adj_self`) ; en particulier $s' \notin E$, sinon s' serait dans l'étoile de s'. Soit $u \in E$. Par symétrie, s et s' sont dans l'étoile de u, qui est un polygone $k \sim k \pm 1$ indexé par $\mathbf{Z}/n$; soient i et j leurs indices. Un sommet de l'étoile de u est voisin de s si et seulement s'il est dans E, donc si et seulement s'il est voisin de s' : dans le polygone, i et j ont les mêmes voisins. Le voisin $i+1$ de i est voisin de j et $i \neq j$, donc $j = i+2$; le voisin $i-1$ est alors à l'écart -3 de j, et $-3 = \pm 1$ donne $4 = 0$ ou $2 = 0$; comme $n \geq 3$, n divise 4 et $n = 4$ (`cyc_same_nbrs`, `eq_four_of_four_eq_zero`). L'étoile de u a donc quatre sommets, d'indices i, $i+1$, $i+2$, $i+3$: s, s', et deux voisins de s, c'est-à-dire deux points de E. L'ensemble $\{s, s'\} \cup E$ est ainsi stable par passage à un voisin, et la connexité donne $S = \{s, s'\} \cup E$. Enfin E est un carré $k \sim k \pm 1$ sur $\mathbf{Z}/4$, dont les sommets non adjacents sont k et $k+2$; on envoie s, s' sur $(0, \pm)$ et les indices $0, 2$ sur $(1, \pm)$, $1, 3$ sur $(2, \pm)$. Les sommets de E sont adjacents à s et à s', et s, s' ne le sont pas entre eux : l'adjacence est celle de $K_{2,2,2}$.

Point 2 (`homothety_dist_le_two`). Par l'énoncé précédent, λ n'a pas de point fixe. L'étoile de s a au moins deux sommets, $\varphi(0) \neq \varphi(1)$, de sorte que λs n'est pas voisin de s. Il reste le cas d'un voisin commun, où s et λs ont la même étoile ; le point 1 donne $n = 4$ et l'octaèdre. Pour un autre sommet $y = gs$, $g \in H$, on a $\lambda y = g \lambda s$, et g envoie l'étoile de s sur celle de gs et celle de λs sur celle de $g \lambda s$ (`isArc_smul_iff`) : λy a l'étoile de y. Point 3 (`homothety_dist_three`) : c'est la contraposée ; pour λ^{-1}, qui commute aussi à H, on applique le même énoncé. □

Remarque. L'énoncé de la page tient, dans un cadre plus large qu'elle ne le dit : le double cône n'utilise ni l'orientation, ni la régularité au sens des drapeaux, seulement la connexité et l'égalité des ordres des sommets ; sans cette égalité, la même démonstration donne seulement que les sommets de E sont d'ordre 4, et le double cône sur un n-gone est un contre-exemple pour tout $n \geq 3$, ce qui est la « double pyramide » de la page 275. Dans le point 2, seule la transitivité de H sur les arcs sert ; la condition d'homothétie (70 b) et la fidélité (72) n'interviennent pas. Que l'antipodie de l'octaèdre soit effectivement une homothétie, à distance 2, est vu dans le modèle sur $\mathbf{Z}/4$ (`zmod4_non_neighbours`, `commutant_dist`), et dans le cadre abstrait par l'encadré suivant. La page dit « 2-polyèdre régulier triangulé » sans fixer d'axiomes ; la forme retenue ici (étoiles polygonales d'un même ordre, connexité) est celle de l'édition. Le point 3 ne dit pas que la distance est au plus 3 : c'est la condition a) de la page, qu'elle pose comme hypothèse, et qui n'est démontrée que sur un anneau semi-local (encadré précédent, point 3).

Théorème 57.5 (Pages 188 et 275, l'antipodie de l'octaèdre, forme de l'édition ♦). *Soit A une relation sur S et $e : S \simeq \{0,1,2\} \times \{\pm\}$ un isomorphisme sur l'octaèdre $K_{2,2,2}$. Soit α l'antipodie, $e\,\alpha\,e^{-1}(i, \varepsilon) = (i, -\varepsilon)$.*

1. *Les sommets non adjacents à y sont y et αy ; α est une involution sans point fixe, αy a l'étoile de y, et y, αy sont à distance 2. La condition (H1) vaut : $\{s, t\} \in A \iff \{\alpha s, \alpha^{-1} t\} \in A$. Toute application injective de S dans lui-même qui respecte A commute*

à α, et toute permutation qui envoie chaque sommet sur un autre sommet de même étoile est α.

2. *Si le graphe de classes H/U_0 est l'octaèdre (sans hypothèse sur σ), α commute à H, vérifie la condition d'homothétie (70 b), est distincte de l'identité et stricte ($A_\alpha = A$). Elle ne vérifie pas la fidélité (72) : un élément de H fixe s_0 et envoie t_0 sur αt_0 ; elle n'appartient donc à aucun groupe d'homothéties au sens de (88).*
3. *Dans le cadre de l'encadré précédent (point 2), une permutation $\lambda \neq 1$ qui commute à H et envoie un sommet à distance au plus 2 est l'antipodie de l'octaèdre.*

Démonstration. Point 1 (`not_adj_iff_octAnti`, `star_octAnti`, `octAnti_homothety`, `octAnti_common_nbr`, `octAnti_comm`, `eq_octAnti`). Dans $K_{2,2,2}$, (j,η) n'est pas adjacent à (i,ε) si et seulement si $j = i$, c'est-à-dire si c'est $(i,\pm\varepsilon)$; l'adjacence ne dépend que de la première coordonnée, que α conserve, d'où l'égalité des étoiles et (H1), puisque $\alpha^{-1} = \alpha$. Le sommet $(i+1,+)$ est un voisin commun de y et αy. Si g est injective et respecte A, $g\alpha y$ n'est pas adjacent à gy et en est distinct, donc c'est $\alpha(gy)$. Si $\lambda y \neq y$ a l'étoile de y, λy n'est pas adjacent à y, sinon il serait dans sa propre étoile, et c'est αy. Point 2 (`octAnti_isHomothety`). Les éléments de H respectent les arcs (`isArc_smul_iff`) et agissent injectivement ; $A_\alpha = A$ parce que α préserve chaque étoile (`twistGraph_eq_self`). Les sommets t_0 et αt_0 sont voisins de s_0, et le stabilisateur de s_0 est transitif sur ses voisins (`IsArc.stab_trans`) ; la fidélité forcerait alors $\alpha = 1$. Point 3 (`homothety_dist_le_two_eq`) : l'encadré précédent donne l'octaèdre et que $\lambda y \neq y$ a l'étoile de y pour tout y ; on conclut par le point 1. □

Remarque. La page excepte « l'octaèdre et λ = l'antipodisme » sans dire que l'antipodie est une homothétie ; c'est vrai au sens de la condition (H1) des pages 187 et 188, et l'homothétie est même stricte. Mais elle échappe au cadre des pages 242 à 247 : dès que H est transitif sur les arcs de l'octaèdre, la fidélité (72) tombe, et la bijection (88) entre groupes d'homothéties et sous-groupes T_H ne la voit pas. L'existence d'un graphe de classes isomorphe à l'octaèdre (par exemple sous son groupe de rotations, d'ordre 24) n'est pas formalisée ; dans le modèle, le cas $\mathbf{Z}/4$ en tient lieu (`zmod4_non_neighbours`, `star_sigma`).

Théorème 57.6 (Grothendieck, pages 136 à 140 et 184 à 187, polygones étoilés ♦). *Le groupe $(\mathbf{Z}/n)^*/\pm 1$ opère sur les structures de polygone d'un ensemble à n éléments. Sous l'axiome To 6, une homothétie agit sur une triangulation en redessinant chaque étoile comme le polygone étoilé d'indice $\nu \in (\mathbf{Z}/n)^*/\pm 1$, recentré au sommet image, avec ν indépendant du sommet, et l'on a une injection $Z \hookrightarrow Z'_n$, sauf pour l'octaèdre.*

Conventions. Pour $n \geq 1$ et un ensemble E, une *structure de polygone* sur E est une relation de la forme $a \sim b \iff \varphi^{-1}(b) - \varphi^{-1}(a) = \pm 1$, pour une bijection $\varphi : \mathbf{Z}/n \to E$; son *polygone étoilé d'indice* ν est la relation $\varphi^{-1}(b) - \varphi^{-1}(a) = \pm\nu$. Pour un graphe A sur un ensemble S, l'étoile $\mathrm{Et}(s)$ est l'ensemble des voisins de s, et pour une permutation λ de S le graphe tordu A_λ joint u et t quand A joint $\lambda^{-1}u$ et t : l'étoile de λs pour A_λ est, comme partie de S, l'étoile de s pour A. L'axiome To 6 pour (λ,ν) demande que A induise un polygone sur chaque étoile et que A_λ induise sur $\mathrm{Et}(s)$ le polygone étoilé d'indice ν de celui de A, pour tout s.

Théorème 57.7 (Pages 136 à 140 et 184 à 187, forme de l'édition ♦). *Soit $n \geq 3$.*

1. *(Le « fait mirifique ».) Le polygone étoilé d'indice ν ne dépend que du polygone, et non de la bijection φ ; pour $\nu \in (\mathbf{Z}/n)^*$ c'est encore un polygone. On obtient une action de*

$(\mathbf{Z}/n)^*$ *sur les structures de polygone de* E*, dans laquelle* ν *et* ν' *agissent de même sur un polygone si et seulement si* $\nu' = \pm\nu$ *: l'action passe à* $Z'_n = (\mathbf{Z}/n)^*/\pm 1$ *et y est libre.*

2. *(Pages 184 à 187.) Deux structures de polygone de* E *dont les rotations* $\varphi(k) \mapsto \varphi(k+1)$ *engendrent le même groupe se déduisent l'une de l'autre par un* $\nu \in (\mathbf{Z}/n)^*$*; réciproquement, les polygones étoilés d'un polygone ont son groupe de rotations.*
3. *(To 6.) Si To 6 vaut pour* (λ, ν) *et pour* (λ, ν')*, et si* S *n'est pas vide, alors* $\nu' = \pm\nu$*. Si To 6 vaut pour* (λ, ν) *et* $(\lambda', \pm\nu)$*, et si toute arête de* A_λ *et de* $A_{\lambda'}$ *est dans un triangle, alors* $A_\lambda = A_{\lambda'}$*; si de plus deux sommets distincts de* A *n'ont jamais la même étoile, alors* $\lambda = \lambda'$*.*
4. *(L'indice ne dépend pas du sommet, (29).) Si un automorphisme* g *de* A *commute à* λ *et si* A_λ *induit sur* $\mathrm{Et}(s)$ *le polygone étoilé d'indice* ν*, il induit sur* $\mathrm{Et}(gs)$ *celui de même indice. Si ces automorphismes sont transitifs sur* S*, To 6 en un sommet entraîne To 6.*
5. *(Le modèle.) Sur* $\mathbf{Z}/n$*, pour* $e, \mu \in (\mathbf{Z}/n)^*$*, le polyèdre* $P_{M,\pm e}$ *induit un polygone sur chaque étoile, et l'homothétie* T_μ *vérifie To 6 avec* $\nu = \mu$*; son graphe tordu est* $P_{M,\pm\mu e}$*.*
6. *(Sauf pour l'octaèdre, pages 139, 140 et 275.) Supposons* A *symétrique et connexe, ses étoiles étant des polygones d'ordre* n*. Si To 6 vaut pour* (λ, ν) *et* $(\lambda', \pm\nu)$ *et si toute arête de* A_λ *et de* $A_{\lambda'}$ *est dans un triangle, alors* $\lambda = \lambda'$ *ou* A *est l'octaèdre (*$n = 4$*,* $A \simeq K_{2,2,2}$*); en particulier* $\lambda = \lambda'$ *dès que* $n \neq 4$*. L'exception est effective : sur* $\mathbf{Z}/4$*, dans* $P_{M,\pm e}$*, l'antipodie* σ *et l'identité vérifient toutes deux To 6 avec* $\nu = 1$*, leurs graphes tordus sont triangulés, et* $\sigma \neq 1$*.*

Démonstration. Point 1. Si deux bijections φ et ψ définissent le même polygone, $f = \psi^{-1}\varphi$ est une permutation de $\mathbf{Z}/n$ qui envoie k et $k+1$ sur deux éléments d'écart ± 1. Posons $d = f(1) - f(0) = \pm 1$; par récurrence $f(k) = dk + f(0)$: si $f(k) = dk + f(0)$ et $f(k+1) = d(k+1) + f(0)$, alors $f(k+2)$ vaut $f(k+1) \pm d$, et la valeur $f(k+1) - d = f(k)$ est exclue par l'injectivité, puisque $2 \neq 0$ dans $\mathbf{Z}/n$ pour $n \geq 3$. Les automorphismes du n-gone sont donc les $k \mapsto \pm k + c$ (`affine_of_adj`), et la condition $\psi^{-1}(b) - \psi^{-1}(a) = \pm\nu$, multipliée par $d = \pm 1$, équivaut à la même pour φ (`cyc_congr`). Pour ν inversible, le polygone étoilé d'indice ν de φ est le polygone de $k \mapsto \varphi(\nu k)$ (`cyc_reindex`), d'où l'action (`twist_twist`, `twist_one`, `polygonAction`). Le changement de ν en $-\nu$ ne change rien (`twist_neg`). Si l'indice ν fixe le polygone de φ, l'arête $\{\varphi(0), \varphi(\nu)\}$ du polygone étoilé est une arête du polygone, donc $\nu = \pm 1$ (`twist_eq_self_iff`), et l'on conclut par l'action (`twist_eq_twist_iff`).

Point 2. Si la rotation ρ_ψ est une puissance ρ_φ^m (dans un groupe fini, les puissances entières sont des puissances naturelles), alors $\psi(k) = \rho_\psi^k \psi(0) = \varphi(c + mk)$ avec $c = \varphi^{-1}\psi(0)$; la bijectivité de $k \mapsto c + mk$ rend m inversible, et $\varphi^{-1}(b) - \varphi^{-1}(a) = m(\psi^{-1}(b) - \psi^{-1}(a))$ donne le polygone de ψ comme polygone étoilé d'indice m de celui de φ (`exists_twist_of_zpowers_rot`). Réciproquement la rotation de $k \mapsto \varphi(\nu k)$ est ρ_φ^ν, et ρ_φ en est la puissance ν^{-1} (`zpowers_rot_reindex`).

Point 3. L'unicité au signe près vient du point 1 appliqué à l'étoile d'un sommet (`toSix_unique`). Une arête $\{u, t\}$ de A_λ est dans un triangle $\{w, u, t\}$, donc u et t sont dans l'étoile de w pour A_λ, c'est-à-dire dans $\mathrm{Et}(\lambda^{-1}w)$; sur cette étoile A_λ et $A_{\lambda'}$ induisent le même polygone étoilé, donc $\{u, t\}$ est une arête de $A_{\lambda'}$, et inversement (`twistGraph_eq_of_toSix`) : c'est $A_\lambda = A_0^{(\nu)}$. Enfin $A_\lambda = A_{\lambda'}$ dit que $\lambda^{-1}u$ et $\lambda'^{-1}u$ ont la même étoile pour tout u, d'où $\lambda = \lambda'$ (`eq_of_toSix`).

Point 4. L'automorphisme g envoie $\mathrm{Et}(s)$ sur $\mathrm{Et}(gs)$; comme il commute à λ, il préserve

aussi A_λ. Il transporte donc la bijection φ de l'étoile de s en une bijection $g\varphi$ de l'étoile de gs, le polygone de A en celui de A et celui de A_λ en celui de A_λ (`toSix_at_smul`, `toSix_of_transitive`).

Point 5. Écrivons $\dot{x}$ avec $x \wedge y_0 = 1$ et posons $y = ey_0$. L'application $k \mapsto (y + kx)^{\cdot}$ est une bijection de $\mathbf{Z}/n$ sur l'étoile de $\dot{x}$: elle est surjective parce que l'étoile est la droite $y + Rx$, à un signe près, et injective parce que $y + kx = -(y + k'x)$ donnerait $2e = 0$ (`starIndex`). Le graphe tordu A_{T_μ} joint $\dot{u}$ et $\dot{t}$ quand $\mu^{-1}u \wedge t = \pm e$, c'est-à-dire $u \wedge t = \pm\mu e$: c'est $P_{M,\pm\mu e}$ (`twistGraph_scal`). Par le calcul $(y+kx)\wedge(y+k'x) = (k-k')e$ de l'énoncé précédent, $P_{M,\pm\mu e}$ induit sur l'étoile le polygone $k \sim k \pm \mu$ (`onStar_adj`) : pour $\mu = 1$, c'est le polygone de $P_{M,\pm e}$ (`isPolygon_adj`), et en général son polygone étoilé d'indice μ (`toSix_scal`).

Point 6. Si deux sommets distincts n'ont jamais la même étoile, le point 3 conclut (`eq_of_toSix`) ; sinon le lemme du double cône (`double_cone`) donne $n = 4$ et l'octaèdre (`eq_of_toSix_or_octahedron`, `eq_of_toSix_of_ne_four`). Pour l'exception, une permutation qui préserve chaque étoile ne tord pas le graphe, $A_\lambda = A$ (`twistGraph_eq_self`), et vérifie donc To 6 avec $\nu = 1$ (`toSix_one_of_star_eq`). Dans un graphe symétrique à étoiles polygonales, toute arête $\{u, t\}$ est dans un triangle : si t a l'indice k dans l'étoile de u, le sommet d'indice $k + 1$ convient (`triangulated_of_pol`). Sur un anneau exceptionnel, $\sigma(\dot{x})$ a, type par type, les voisins de $\dot{x}$ (`same_star_iff`), d'où l'égalité des étoiles dans $P_{M,\pm e}$ (`star_sigma`) ; enfin σ n'a pas de point fixe sur $\mathbf{Z}/4$, où $2 \neq 0$ (`sigma_ne_scal`), d'où $\sigma \neq 1$ (`octahedron_toSix`). □

Remarque. Les points 1, 3 et 5 démontrent l'énoncé de la page sous la forme suivante : l'action de Z'_n est fidèle, et même libre ; To 6 détermine ν au signe près ; deux homothéties de même ν ont le même graphe tordu, et sont égales dès que deux sommets distincts n'ont jamais la même étoile. Deux hypothèses restent explicites. D'abord que toute arête de A_λ soit dans un triangle, ce que la page suppose en parlant de triangulation et qu'elle discute aux pages 187 et 188 (condition a)). Ensuite que deux sommets distincts n'aient pas la même étoile, qui remplace « sauf pour l'octaèdre » : le point 6 fait ce passage par le lemme du double cône de la page 275 (`double_cone`), sous la seule hypothèse de connexité, et montre que l'exception de l'octaèdre est nécessaire. La page dit « homomorphisme injectif » ; dans le cadre abstrait, Lean ne démontre que l'injectivité de $\lambda \mapsto \nu$; que $\nu(\lambda\lambda') = \nu(\lambda)\nu(\lambda')$ ne découle pas de To 6 par cet argument, car $A_{\lambda\lambda'}$ mêle les étoiles de s et de λs. Dans le modèle, $T_\mu \mapsto \mu$ est évidemment multiplicative, et injective modulo ± 1 par `scal_eq_scal_iff`. Le point 4 démontre l'indépendance par rapport au sommet de la page 187 sous l'hypothèse de transitivité ; l'existence de ν en un sommet, que la page tire de l'unicité du sous-groupe cyclique d'ordre n dans $G_{0s} \simeq \mathbf{D}_n$, se ramène par le point 2 à l'égalité des groupes de rotations, que Lean prend comme hypothèse sans la déduire de G_{0s}. La question de la page 141, pour les triangulations à sommets d'ordre 7, reste ouverte.

58 Cote 85 : représentations de G_2 et de $\mathbb{D}_\infty$ dans PGL_2, rotation d'ordre 5 [61]

La cote 85, *2-polyèdres et 1-polygônes : notes manuscrites (s.d.)*, du groupe « Géométrie et topologie combinatoire », étudie les polygones et polyèdres réguliers réalisés dans une forme de PGL_2 sur une base quelconque, au moyen d'un seul invariant A. Pour PGL_2, la lecture le donne par $A(v) = (\operatorname{Tr} v)^2/\det v - 2$ pour un relèvement $v \in \mathrm{GL}_2$ (pages 23 et 27, 85, lot 2, p. 23, 85, lot 2, p. 27). La page 30 dit qu'un élément est d'ordre 5 en tout point si et seulement si

61. Preuve vérifiée : `lean/Grothendieck/Folder85.lean`.

$\alpha^2+\alpha-1=0$, hors caractéristique 5 (85, lot 2, p. 30). La page 10 énonce le cas de l'icosaèdre avec un facteur $\mathbf{Z}/2$ et la marge « laisser tomber $\mathbf{Z}/2$ dans l'énoncé » (85, lot 1, p. 10) ; la page 40 énonce le théorème sans ce facteur : pour une forme G de PGL_2 sur un schéma S et un monomorphisme $\varphi:\mathfrak{A}_5\to G$, $\alpha(\varphi)=A(\varphi(\pi))$, π un 5-cycle, satisfait $\alpha^2+\alpha-1=0$, la catégorie des (G,φ) est rigide, et le foncteur des classes d'isomorphisme est « représentable par $M=\operatorname{Spec}\mathbf{Z}[T]/(T^2+T-1)$ » (85, lot 2, p. 40). Le calcul qui porte ce théorème est démontré ici, sur tout anneau commutatif, ainsi qu'un modèle explicite des relations de l'icosaèdre.

Le théorème de la page 4 (85, lot 1, p. 4) porte sur le groupe $G_2=\langle\tau_0,\tau_1,\tau_2\mid\tau_i^2,(\tau_0\tau_2)^2\rangle$, avec $\rho_0=\tau_0\tau_1$ et $\rho_1=\tau_1\tau_2$. Pour un homomorphisme φ de G_2 dans une forme de PGL_2 sur S tel qu'en tout point $\rho_0^2\neq1$, $\rho_1^2\neq1$ et $\rho_0\rho_1\neq\rho_1\rho_0$, la page énonce trois choses : 1) les invariants $\alpha_0=A(\varphi(\rho_0))$, $\alpha_1=A(\varphi(\rho_1))$ sont tels que $(\alpha_0+2)(\alpha_1+2)(\alpha_0+\alpha_1)$ est inversible ; 2) le foncteur $\varphi\mapsto(\alpha_0,\alpha_1)$ est pleinement fidèle, c'est-à-dire que le centralisateur de l'image est trivial et que deux objets de mêmes invariants sont isomorphes ; 3) tout couple admissible provient d'un φ. La lecture en tire que l'espace de modules est l'ouvert de $\mathbb{A}^2_{\mathbf{Z}}$ complémentaire des trois droites $\alpha_0=-2$, $\alpha_1=-2$, $\alpha_0+\alpha_1=0$. La démonstration des pages 5 et 6 renvoie à des « généralités » absentes du dossier (85, lot 1, p. 5, 85, lot 1, p. 6). Le corollaire des pages 6 et 7 prescrit les ordres de ρ_0 et ρ_1 par $\Psi_{\nu_i}(\alpha_i)=0$, avec ν_i inversible si ν_i n'est pas premier (85, lot 1, p. 7). Les pages 8 à 10 traitent les trois cas finis (85, lot 1, p. 8). On démontre ici les calculs de traces et la rigidité sur tout anneau, la conjugaison sur un corps qui contient une racine de $T^2-\alpha_0T+1$, une forme normale explicite après adjonction d'une telle racine et la traduction des ordres 3, 4, 5 et 6.

Conventions. R est un anneau commutatif et $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ une matrice de $M_2(R)$ de déterminant δ inversible ; on note $t=\operatorname{Tr}g$ et $A(g)=t^2\delta^{-1}-2$. On dit que g est *nulle part scalaire* si b, c et $a-d$ engendrent l'idéal unité. Un idéal est l'idéal unité si et seulement s'il n'est contenu dans aucun idéal premier ; la condition dit donc que l'image de g dans $\mathrm{PGL}_2(k(s))$ est différente de 1 en tout point s de $\operatorname{Spec}R$. Comme 5 est premier, l'image de g est alors d'ordre 5 en tout point si et seulement si g^5 est scalaire.

Conventions pour G_2. Un homomorphisme $G_2\to\mathrm{PGL}_2(R)$ est donné par trois matrices τ_0,τ_1,τ_2 de déterminants d_0,d_1,d_2 inversibles, telles que τ_0^2, τ_1^2, τ_2^2 et $(\tau_0\tau_2)^2$ soient scalaires. On note $\rho_0=\tau_0\tau_1$, $\rho_1=\tau_1\tau_2$, $\alpha_0=A(\rho_0)$, $\alpha_1=A(\rho_1)$, $t_{01}=\operatorname{Tr}(\tau_0\tau_1)$, $t_{12}=\operatorname{Tr}(\tau_1\tau_2)$, $t_{02}=\operatorname{Tr}(\tau_0\tau_2)$, $T=\operatorname{Tr}(\tau_0\tau_1\tau_2)$ et $\Delta=(\alpha_0+2)(\alpha_1+2)(\alpha_0+\alpha_1)$. Sur un corps k, la condition $(*)$ de la page 4 s'écrit : ρ_0^2 et ρ_1^2 ne sont pas scalaires, et il n'existe pas de $\mu\in k$ tel que $\rho_0\rho_1=\mu\,\rho_1\rho_0$. « $(*)$ en tout point » signifie que $(*)$ vaut pour les images des τ_i dans $M_2(R/\mathfrak{m})$, pour tout idéal maximal $\mathfrak{m}$. Pour $\nu\geq2$, on dit que g est d'ordre ν en tout point si g^ν est scalaire et si g^m est nulle part scalaire pour tout diviseur m de ν avec $1\leq m<\nu$.

Lemme 58.1. *Soient $\tau_0,\tau_1,\tau_2\in M_2(R)$ de trace nulle et de déterminants inversibles.*

1. $\alpha_0+2=t_{01}^2(d_0d_1)^{-1}$ *et* $\alpha_1+2=t_{12}^2(d_1d_2)^{-1}$.
2. $\rho_0\rho_1-\rho_1\rho_0=-T\,\tau_1$.
3. *Si* $t_{02}=0$, *alors* $T^2=4d_0d_1d_2-t_{01}^2d_2-t_{12}^2d_0$, *donc* $\alpha_0+\alpha_1=-T^2(d_0d_1d_2)^{-1}$.
4. *Si* $t_{02}=0$, Δ *est inversible si et seulement si* t_{01}, t_{12} *et* T *le sont.*

Démonstration. (1) $\det\rho_0=d_0d_1$ et $A(\rho_0)=t_{01}^2(d_0d_1)^{-1}-2$ par définition. (2) et (3) sont des identités polynomiales entre les coefficients, une fois $\tau_i=\begin{pmatrix}a_i&b_i\\c_i&-a_i\end{pmatrix}$; pour (3), la différence

des deux membres est t_{02} multiplié par un polynôme explicite, et Lean la vérifie sous cette forme. Le membre de droite de (3) est, au signe près, le déterminant de Gram des τ_i pour la forme $\mathrm{Tr}(XY)$, avec $t_{02}=0$. En reportant (3) dans $\alpha_0+\alpha_1 = t_{01}^2(d_0d_1)^{-1}+t_{12}^2(d_1d_2)^{-1}-4$, on obtient $-T^2(d_0d_1d_2)^{-1}$. (4) Par (1) et (3), $\Delta = -t_{01}^2t_{12}^2T^2\cdot d_0^{-2}d_1^{-3}d_2^{-2}$, et un produit est inversible si et seulement si chaque facteur l'est. □

Énoncé (Page 4, partie 1), les invariants ♦). *Soient $\tau_0,\tau_1,\tau_2\in M_2(R)$ de déterminants inversibles, avec τ_i^2 et $(\tau_0\tau_2)^2$ scalaires.*

1. *Si $(*)$ vaut en tout point, alors τ_0, τ_1, τ_2 et $\tau_0\tau_2$ sont de trace nulle, et $\Delta=(\alpha_0+2)(\alpha_1+2)(\alpha_0+\alpha_1)$ est inversible.*
2. *Réciproquement, si τ_0, τ_1, τ_2 et $\tau_0\tau_2$ sont de trace nulle et Δ inversible, alors $(*)$ vaut en tout point.*

Démonstration. (1) Fixons un idéal maximal $\mathfrak{m}$ et travaillons dans $k=R/\mathfrak{m}$. Si τ_0 y était scalaire, $\rho_0^2=c^2\tau_1^2$ serait scalaire ; de même pour τ_1 (avec τ_0^2) et pour τ_2 (avec $\rho_1^2=c^2\tau_1^2$). Si $\tau_0\tau_2=c$ était scalaire, c serait non nul, $\tau_2\tau_0=c$ aussi, et $\rho_0\rho_1=\tau_0\tau_1^2\tau_2$ et $\rho_1\rho_0=\tau_1(\tau_2\tau_0)\tau_1$ vaudraient tous deux $c\,s$, où $\tau_1^2=s$; cela contredit $(*)$ avec $\mu=1$. Les quatre matrices sont donc nulle part scalaires sur R, car un idéal qui n'est contenu dans aucun idéal maximal est l'idéal unité. Pour une matrice g nulle part scalaire avec g^2 scalaire, Cayley–Hamilton donne $g^2=(\mathrm{Tr}\,g)\,g-\det g$; les coefficients hors diagonale de $(\mathrm{Tr}\,g)\,g$ et la différence de ses coefficients diagonaux sont nuls, donc $\mathrm{Tr}\,g$ annule un idéal égal à l'idéal unité, et $\mathrm{Tr}\,g=0$. Les quatre traces sont nulles. Revenons dans k. Si $t_{01}=0$, ρ_0 est de trace nulle et $\rho_0^2=-\det\rho_0$ est scalaire ; de même $t_{12}\neq 0$. Si $T=0$, le lemme 58.1 (2) donne $\rho_0\rho_1=\rho_1\rho_0$. Les images de t_{01}, t_{12} et T sont donc non nulles en tout point, ces trois éléments sont inversibles, et Δ l'est par le lemme 58.1 (4).

(2) Par le lemme 58.1 (4), t_{01}, t_{12} et T sont inversibles, et le restent dans chaque $R/\mathfrak{m}$. Il suffit donc de montrer $(*)$ sur un anneau non nul où ces trois éléments sont inversibles. On a $T=\mathrm{Tr}(\rho_0\tau_2)=(\rho_{0,00}-\rho_{0,11})\,\tau_{2,00}+\rho_{0,01}\,\tau_{2,10}+\rho_{0,10}\,\tau_{2,01}$, car τ_2 est de trace nulle ; T appartient donc à l'idéal engendré par les coefficients hors diagonale de ρ_0 et la différence de ses coefficients diagonaux, et ρ_0 est nulle part scalaire. Si ρ_0^2 était scalaire, on aurait $t_{01}=\mathrm{Tr}\,\rho_0=0$. Même raisonnement pour ρ_1, avec $T=\mathrm{Tr}(\rho_1\tau_0)$. Si enfin $\rho_0\rho_1=\mu\,\rho_1\rho_0$, multiplions à gauche par τ_0 et prenons la trace : $\mathrm{Tr}(\tau_0\rho_0\rho_1)=d_0d_1\mathrm{Tr}\,\tau_2=0$, et $\mathrm{Tr}(\tau_0\rho_1\rho_0)=t_{01}T$ (identité polynomiale pour des matrices de trace nulle). Donc $\mu\,t_{01}T=0$, $\mu=0$, et $\rho_0\rho_1=0$, ce qui contredit $\det(\rho_0\rho_1)=d_0d_1^2d_2$ inversible. □

Remarque. Chaque facteur de Δ répond à une condition de $(*)$: α_0+2 inversible équivaut à t_{01} inversible, c'est-à-dire $\rho_0^2\neq 1$; α_1+2 à $\rho_1^2\neq 1$; et $\alpha_0+\alpha_1$, au vu de $\rho_0\rho_1-\rho_1\rho_0=-T\tau_1$, à la non-commutation. L'énoncé vaut sur tout anneau, sans hypothèse sur 2 : en caractéristique 2 les involutions sont unipotentes, et τ_0, τ_2 commutent au lieu d'anticommuter, sans que les calculs changent. L'hypothèse « $(\tau_0\tau_2)^2$ scalaire » sert à obtenir $t_{02}=0$; sans elle, l'identité (3) du lemme a un terme en t_{02}.

Lemme 58.2. *Si $X\in M_2(R)$ est nulle part scalaire et $gX=Xg$, il existe $p,q\in R$ avec $g=p+qX$.*

Démonstration. Écrivons $X=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $g=\begin{pmatrix}e & f\\ h & k\end{pmatrix}$. La commutation donne $fc=bh$, $b(e-k)=f(a-d)$ et $h(a-d)=c(e-k)$: les vecteurs $(f,h,e-k)$ et $(b,c,a-d)$ sont proportionnels au sens où leurs mineurs d'ordre 2 sont nuls. Soit $r_1b+r_2c+r_3(a-d)=1$. Posons $q=r_1f+r_2h+r_3(e-k)$ et $p=e-qa$. Alors $f=f(r_1b+r_2c+r_3(a-d))=qb$ par les relations, de même $h=qc$ et $e-k=q(a-d)$, d'où $g=p+qX$. □

Énoncé (Page 4, partie 2), rigidité). *Soient $\tau_0, \tau_1, \tau_2 \in M_2(R)$ de déterminants inversibles, de trace nulle, avec $t_{02} = 0$ et Δ inversible. Si $g \in \mathrm{GL}_2(R)$ et $\mu_0, \mu_1, \mu_2 \in R$ vérifient $g\tau_i = \mu_i\, \tau_i g$ pour $i = 0, 1, 2$, alors g est scalaire.*

Démonstration. On a $g\rho_0 = \mu_0\mu_1\, \rho_0 g$, d'où $t_{01} = \mathrm{Tr}(g^{-1}g\rho_0) = \mu_0\mu_1\, \mathrm{Tr}(g^{-1}\rho_0 g) = \mu_0\mu_1 t_{01}$, et $\mu_0\mu_1 = 1$ puisque t_{01} est inversible. De même $\mu_1\mu_2 = 1$: g commute à ρ_0 et à ρ_1. Comme T est inversible, ρ_0 est nulle part scalaire (démonstration de l'énoncé précédent), et le lemme 58.2 donne $g = p + q\rho_0$. La commutation avec ρ_1 donne $q(\rho_0\rho_1 - \rho_1\rho_0) = 0$, soit $qT\tau_1 = 0$; en multipliant par τ_1, $qTd_1 = 0$, donc $q = 0$ et $g = p$. □

La forme normale. Pour $\ell, b \in R$, posons

$$\rho_0^\circ = \begin{pmatrix} \ell & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_1^\circ = \begin{pmatrix} 0 & 1 \\ -b & b \end{pmatrix}, \quad \tau_1^\circ = \begin{pmatrix} b & 1-\ell-b \\ b(1-\ell) & -b \end{pmatrix}, \quad \tau_0^\circ = \rho_0^\circ\tau_1^\circ, \quad \tau_2^\circ = \tau_1^\circ\rho_1^\circ.$$

La matrice ρ_0° a pour trace $\ell + 1$ et pour déterminant ℓ, et $A(\rho_0^\circ) = \ell + \ell^{-1}$; ρ_1° a pour trace et pour déterminant b, et $A(\rho_1^\circ) = b - 2$. La matrice τ_1° est, à un scalaire près, l'unique matrice de trace nulle orthogonale à ρ_0° et à ρ_1° pour la forme $\mathrm{Tr}(XY)$.

Énoncé (Page 4, partie 3), une forme normale). *Soient $\alpha_0, \alpha_1 \in R$ avec $\Delta = (\alpha_0 + 2)(\alpha_1 + 2)(\alpha_0 + \alpha_1)$ inversible, $\ell \in R$ une racine de $T^2 - \alpha_0 T + 1$ et $b = \alpha_1 + 2$. Alors τ_0°, τ_1°, τ_2° sont de déterminants inversibles, de trace nulle, avec $\mathrm{Tr}(\tau_0^\circ\tau_2^\circ) = 0$ (de sorte que $(\tau_i^\circ)^2$ et $(\tau_0^\circ\tau_2^\circ)^2$ sont scalaires), $A(\tau_0^\circ\tau_1^\circ) = \alpha_0$, $A(\tau_1^\circ\tau_2^\circ) = \alpha_1$, et $(*)$ vaut en tout point. Pour tout anneau R et tout tel couple, cela s'applique sur $R[\ell] = R[T]/(T^2 - \alpha_0 T + 1)$, libre de rang 2 sur R.*

Démonstration. On a $\ell(\alpha_0 - \ell) = 1$, donc ℓ est inversible. Les traces de τ_1°, τ_0°, τ_2° et $\tau_0^\circ\tau_2^\circ$ sont nulles par calcul direct. Ensuite $\det\tau_1^\circ = -b\big((1-\ell)^2 + \ell b\big)$ et, comme $\ell^2 + 1 = \alpha_0\ell$, $(1-\ell)^2 + \ell b = \ell(\alpha_0 + \alpha_1)$; ce déterminant est inversible, et $\det\tau_0^\circ = \ell\det\tau_1^\circ$, $\det\tau_2^\circ = b\det\tau_1^\circ$. Comme τ_1° est de trace nulle, $(\tau_1^\circ)^2 = s$ avec $s = -\det\tau_1^\circ$ inversible, d'où $\tau_0^\circ\tau_1^\circ = s\rho_0^\circ$ et $\tau_1^\circ\tau_2^\circ = s\rho_1^\circ$. L'invariant ne dépend pas du relèvement : $A(\tau_0^\circ\tau_1^\circ) = (\ell+1)^2\ell^{-1} - 2 = \alpha_0$, car $(\ell+1)^2 = (\alpha_0 + 2)\ell$, et $A(\tau_1^\circ\tau_2^\circ) = b^2b^{-1} - 2 = \alpha_1$. Enfin Δ est inversible, et la partie (2) de l'énoncé des invariants donne $(*)$ en tout point. Dans $R[T]/(T^2 - \alpha_0 T + 1)$, la classe de T est racine par construction. □

Remarque. La forme normale demande une racine ℓ de $T^2 - \alpha_0 T + 1$. Sur R lui-même, une réalisation dans le PGL_2 déployé n'existe pas toujours : pour $R = \mathbf{R}$ et $(\alpha_0, \alpha_1) = (-1, c_5)$, elle donnerait un $\mathfrak{A}_5$ dans $\mathrm{PGL}_2(\mathbf{R})$, qui n'en contient pas (cas du critère de Beauville rappelé plus bas, non formalisé ici). D'où les formes de PGL_2 dans l'énoncé de la page 4. Le passage de $R[\ell]$ à une forme sur R, par descente le long de $R \to R[\ell]$ en s'appuyant sur la rigidité, n'est pas formalisé.

Énoncé (Page 4, partie 2), conjugaison sur un corps). *Soient K un corps et $\tau_0, \tau_1, \tau_2 \in \mathrm{GL}_2(K)$ de trace nulle, avec $t_{02} = 0$ et $\Delta \neq 0$. Soit $\ell \in K$ une racine de $T^2 - \alpha_0 T + 1$ et $b = \alpha_1 + 2$. Il existe $g \in \mathrm{GL}_2(K)$ et $c_0, c_1, c_2 \in K$ tels que $\tau_i g = c_i\, g\tau_i^\circ$ pour $i = 0, 1, 2$. En particulier, deux tels triplets de mêmes invariants (α_0, α_1) sont conjugués dans $\mathrm{PGL}_2(K)$.*

Démonstration. Le lemme 58.1 donne t_{01}, t_{12}, T non nuls. Posons $X = (\ell+1)t_{01}^{-1}\rho_0$ et $Y = b\, t_{12}^{-1}\rho_1$. On a $\ell \neq 0$, $\ell + 1 \neq 0$ car $(\ell+1)^2 = (\alpha_0 + 2)\ell$, et $b \neq 0$. Alors $\mathrm{Tr}\, X = \ell + 1$, $\det X = (\ell+1)^2 t_{01}^{-2} d_0 d_1 = \ell$, $\mathrm{Tr}\, Y = \det Y = b$, $\mathrm{Tr}(XY)$ est un multiple de $\mathrm{Tr}(\tau_0\tau_1^2\tau_2) = -d_1 t_{02} = 0$, et $\det(XY - YX)$ est un multiple non nul de $\det(T\tau_1) = T^2 d_1$.

Comme $\det(X-\ell) = \ell^2-\ell(\ell+1)+\ell = 0$, il existe $v \neq 0$ avec $Xv = \ell v$. Posons $w = -b^{-1}Yv$ et soit g la matrice de colonnes v, w. Par définition $Yv = -bw$; par Cayley–Hamilton, $Y^2 = bY - b$, d'où $Yw = v + bw$. L'identité $XY + YX = (\operatorname{Tr} X)Y + (\operatorname{Tr} Y)X + \operatorname{Tr}(XY) - \operatorname{Tr} X \operatorname{Tr} Y$ donne $XYv = Yv - bv$, soit $Xw = v + w$. Ces quatre égalités disent $Xg = g\rho_0^\circ$ et $Yg = g\rho_1^\circ$. Si $\det g = 0$, w est proportionnel à v, qui est alors vecteur propre commun de X et Y ; $(XY - YX)v = 0$ et $\det(XY - YX) = 0$, ce qui est exclu. En Lean, cette étape passe par les identités $b\,v_i \left((XY - YX)v\right)_j \in (\det g)$ modulo les relations, et le choix d'une coordonnée $v_i \neq 0$.

Soit $M = g^{-1}\tau_1 g$. Sa trace est nulle ; $\operatorname{Tr}(M\rho_0^\circ) = \operatorname{Tr}(\tau_1 X)$ est un multiple de $\operatorname{Tr}(\tau_1\tau_0\tau_1) = -d_1 \operatorname{Tr}\tau_0 = 0$, et de même $\operatorname{Tr}(M\rho_1^\circ) = 0$. Ces trois équations linéaires imposent $M = M_{00} b^{-1}\,\tau_1^\circ$. Enfin $\tau_0 = (-d_1)^{-1}(\ell+1)^{-1}t_{01}\,X\tau_1$ et $\tau_2 = (-d_1)^{-1}b^{-1}t_{12}\,\tau_1 Y$, d'où $\tau_0 g \in K\,g\rho_0^\circ\tau_1^\circ = K\,g\tau_0^\circ$ et $\tau_2 g \in K\,g\tau_1^\circ\rho_1^\circ = K\,g\tau_2^\circ$. Pour deux triplets τ, σ de mêmes invariants, avec g, g' ainsi obtenus, $h = gg'^{-1}$ vérifie $\tau_i h = c_i c_i'^{-1}\, h\sigma_i$. □

Remarque. La conjugaison est démontrée sur un corps qui contient ℓ, par exemple algébriquement clos. Sur un corps quelconque, la rigidité et un argument de descente galoisienne la donneraient aussi ; ce passage n'est pas formalisé, ni la conjugaison sur un anneau local ou une base quelconque. La matrice ρ_0° couvre d'un seul coup le cas semi-simple ($\ell \neq 1$) et le cas unipotent ($\ell = 1$, $\alpha_0 = 2$, possible hors caractéristique 2).

Énoncé (Pages 6 et 7, 29 à 31, les ordres)**.** *Soit $g \in M_2(R)$ nulle part scalaire, de trace t et de déterminant d inversible, et $\alpha = A(g)$. Définissons $x_0 = 0$, $x_1 = 1$, $x_{n+2} = tx_{n+1} - dx_n$, et $P_0 = 0$, $P_1 = 1$, $P_{n+2} = P_{n+1} - P_n$ pour n pair, $P_{n+2} = (\alpha+2)P_{n+1} - P_n$ pour n impair.*

1. *$g^{n+1} = x_{n+1}\,g - d\,x_n$; g^{n+1} est scalaire si et seulement si $x_{n+1} = 0$, et nulle part scalaire si et seulement si x_{n+1} est inversible.*
2. *$x_{2k+1} = d^k P_{2k+1}(\alpha)$ et $x_{2k+2} = t\,d^k P_{2k+2}(\alpha)$. Donc g^{2k+1} est scalaire si et seulement si $P_{2k+1}(\alpha) = 0$, et, si t est inversible, g^{2k+2} est scalaire si et seulement si $P_{2k+2}(\alpha) = 0$.*
3. *$P_3 = \alpha + 1$, $P_4 = \alpha$, $P_5 = \alpha^2 + \alpha - 1$, $P_6 = \alpha^2 - 1$, $P_7 = \alpha^3 + \alpha^2 - 2\alpha - 1$.*
4. *g est d'ordre 3 en tout point si et seulement si $\alpha = -1$; d'ordre 4 en tout point si et seulement si $\alpha = 0$ et 2 est inversible ; d'ordre 6 en tout point si et seulement si $\alpha = 1$ et 6 est inversible.*

Démonstration. (1) Par récurrence, avec $g^2 = tg - d$: $g^{n+2} = (x_{n+1}g - dx_n)g = (tx_{n+1} - dx_n)g - dx_{n+1}$. Pour g nulle part scalaire, $xg + y$ est scalaire si et seulement si $x = 0$ (argument d'idéal), et nulle part scalaire si et seulement si x est inversible : ses coefficients hors diagonale et la différence diagonale sont x fois ceux de g, et un idéal maximal contient xb, xc, $x(a-d)$ si et seulement s'il contient x, ou b, c et $a - d$. (2) Par récurrence sur k, avec $t^2 = (\alpha+2)d$: $x_{2k+3} = t \cdot td^k P_{2k+2} - d \cdot d^k P_{2k+1} = d^{k+1}\big((\alpha+2)P_{2k+2} - P_{2k+1}\big)$ et $x_{2k+4} = td^{k+1}P_{2k+3} - d \cdot td^k P_{2k+2} = td^{k+1}(P_{2k+3} - P_{2k+2})$. (3) Calcul direct. (4) Ordre 3 : g^3 scalaire équivaut à $P_3(\alpha) = 0$. Ordre 4 : g^2 nulle part scalaire équivaut à $x_2 = t$ inversible, et g^4 scalaire à $t\,d\,\alpha = 0$, soit $\alpha = 0$; alors $t^2 = 2d$, donc 2 est inversible ; réciproquement $\alpha = 0$ et 2 inversible donnent $t^2 = 2d$ inversible. Ordre 6 : il faut t inversible, $x_3 = d(\alpha+1)$ inversible et $td^2(\alpha-1)(\alpha+1) = 0$, soit $\alpha = 1$; alors $2 = \alpha + 1$ est inversible et $t^2 = 3d$ donne 3 inversible ; la réciproque est le même calcul. □

Remarque. La suite x_n est celle du lemme 58.3, et $P_5 = \Psi_5$ redonne le calcul de l'ordre 5. Les valeurs de (3) sont Ψ_3, Ψ_4, Ψ_5, $\Psi_3\Psi_6$ et Ψ_7 : ce sont les F_n de la page 29 pour $n \leq 7$. L'identification $P_n = F_n = \prod_{d|n,\, d\geq 3} \Psi_d$ pour tout n n'est pas formalisée. Le point (4) confirme la condition c) du corollaire des pages 6 et 7 pour $\nu = 4$ et $\nu = 6$: dans PGL_2, l'ordre 6

demande 6 inversible, alors que, dans SL_2, le cas B) de la page 31 ne demande que 2 ; un élément de $\mathrm{PGL}_2(k)$ d'invariant 1 en caractéristique 3 a une trace nulle et est une involution. Pour les cas finis des pages 8 à 10, $\Delta(-1,-1) = -2$, $\Delta(0,-1) = -2$ et, si $\alpha^2 + \alpha - 1 = 0$, $\Delta(-1,\alpha) = -1$: les deux premiers demandent 2 inversible, le troisième est inversible sur toute base, comme le dit la lecture.

Énoncé (Pages 10, 30 et 40, l'invariant d'une rotation d'ordre 5 ♦). *Soit $g \in M_2(R)$ de déterminant inversible.*

1. *$A(\mu g) = A(g)$ pour tout $\mu \in R^\times$: A ne dépend que de l'image de g dans $\mathrm{PGL}_2(R)$.*
2. *Si g est nulle part scalaire et g^5 scalaire, alors $A(g)^2 + A(g) - 1 = 0$.*
3. *Réciproquement, si $A(g)^2 + A(g) - 1 = 0$, alors g^5 est scalaire.*
4. *$A(g^2) = A(g)^2 - 2$; en particulier, si $A(g)^2 + A(g) - 1 = 0$, alors $A(g^2) = -1 - A(g)$ (corollaire de la page 40).*

Lemme 58.3. *Pour toute matrice $g \in M_2(R)$, $g^5 = x_5\, g + y_5$, avec $x_5 = t^4 - 3\delta t^2 + \delta^2$ et $y_5 = -\delta(t^3 - 2\delta t)$. Si δ est inversible, $x_5 = \delta^2\,(A(g)^2 + A(g) - 1)$.*

Démonstration. Par Cayley–Hamilton, $g^2 = tg - \delta$. Si $g^n = x_n g + y_n$, alors $g^{n+1} = (tx_n + y_n)g - \delta x_n$. Partant de $x_1 = 1$, $y_1 = 0$, on trouve $x_2 = t$, $x_3 = t^2 - \delta$, $x_4 = t^3 - 2\delta t$, $y_4 = -\delta(t^2 - \delta)$, puis $x_5 = t^4 - 3\delta t^2 + \delta^2$ et $y_5 = -\delta x_4$. La vérification en Lean se fait coefficient par coefficient. Posons $u = t^2\delta^{-1}$, de sorte que $A(g) = u - 2$. Alors $A(g)^2 + A(g) - 1 = u^2 - 3u + 1$, et $\delta^2(u^2 - 3u + 1) = t^4 - 3\delta t^2 + \delta^2$. □

Démonstration de l'énoncé. (1) $\mathrm{Tr}(\mu g) = \mu t$ et $\det(\mu g) = \mu^2\delta$, donc $(\mu t)^2(\mu^2\delta)^{-1} = t^2\delta^{-1}$.

(2) Écrivons $g^5 = \gamma \cdot 1$. Par le lemme 58.3, $x_5 g = (\gamma - y_5)\cdot 1$. En lisant les coefficients hors diagonale et la différence des coefficients diagonaux, $x_5 b = x_5 c = x_5(a-d) = 0$. L'ensemble des $r \in R$ tels que $x_5 r = 0$ est un idéal ; il contient b, c, $a - d$, donc l'idéal unité, et $x_5 = 0$. Comme δ^2 est inversible, le lemme donne $A(g)^2 + A(g) - 1 = 0$.

(3) Si $A(g)^2 + A(g) - 1 = 0$, le lemme donne $x_5 = 0$ et $g^5 = y_5$.

(4) $\mathrm{Tr}(g^2) = t^2 - 2\delta$ et $\det(g^2) = \delta^2$, d'où $A(g^2) = (t^2-2\delta)^2\delta^{-2} - 2 = (u-2)^2 - 2 = A(g)^2 - 2$. Si $A(g)^2 = 1 - A(g)$, cela vaut $-1 - A(g)$. □

Énoncé (Page 40, un modèle des relations de l'icosaèdre). *Soit $\zeta \in R$ tel que $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$, et posons*

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad p = \begin{pmatrix} \zeta & 1 \\ 0 & \zeta^4 \end{pmatrix}.$$

Alors $s^2 = -1$, $(sp)^3 = -1$ et p^5 est scalaire ; s, p et sp sont nulle part scalaires ; $\det p = 1$ et $A(p) = \zeta^2 + \zeta^3$ est racine de $T^2 + T - 1$. C'est le cas en particulier pour $R = \mathbf{Z}[\zeta_5] = \mathbf{Z}[X]/(X^4 + X^3 + X^2 + X + 1)$ et ζ la classe de X.

Démonstration. On a $\zeta^5 - 1 = (\zeta - 1)(\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) = 0$, donc ζ est inversible d'inverse ζ^4, et $\det p = \zeta^5 = 1$. Le calcul direct donne $s^2 = -1$. Le produit $sp = \begin{pmatrix} 0 & -\zeta^4 \\ \zeta & 1 \end{pmatrix}$ a pour trace 1 et pour déterminant $\zeta^5 = 1$, donc $(sp)^2 = sp - 1$, puis $(sp)^3 = sp(sp-1) = (sp-1) - sp = -1$. Ensuite $\mathrm{Tr}\, p = \zeta + \zeta^4$ et $A(p) = (\zeta + \zeta^4)^2 - 2 = \zeta^2 + 2\zeta^5 + \zeta^8 - 2 = \zeta^2 + \zeta^3$. On a $(\zeta^2+\zeta^3)^2 + \zeta^2 + \zeta^3 - 1 = \zeta^4 + 2\zeta^5 + \zeta^6 + \zeta^2 + \zeta^3 - 1 = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, et le point (3) de l'énoncé précédent donne p^5 scalaire. Le coefficient $(0,1)$ vaut -1 pour s, 1 pour p et $-\zeta^4$

pour sp ; c'est chaque fois un inversible, et les trois matrices sont nulle part scalaires. Dans $\mathbf{Z}[X]/(X^4+X^3+X^2+X+1)$, la classe de X est racine du polynôme par construction. □

Remarque. Le point (2) vaut sur tout anneau commutatif, sans hypothèse sur 2, 3 ou 5, ni de réduction. L'exclusion de la caractéristique 5 à la page 30 concerne le sens réciproque, l'ordre exact 5 : en caractéristique 5, $T^2+T-1=(T-2)^2$, et $A(g)=2$ vaut aussi pour $g=1$. Avec l'hypothèse « nulle part scalaire » et 5 premier, les points (2) et (3) disent qu'un élément nulle part scalaire de déterminant inversible est d'ordre 5 en tout point si et seulement si $A(g)^2+A(g)-1=0$, en toute caractéristique. Dans le modèle, en caractéristique 5, $\zeta=1$ convient, p est unipotent et $A(p)=2$: c'est la rotation unipotente que la lecture signale pour $\mathfrak{A}_5\simeq\mathrm{PSL}_2(\mathbf{F}_5)$.

Remarque. Les relations s^2, $(sp)^3$, p^5 scalaires sont celles du groupe triangulaire de type $(2,3,5)$, qui est $\mathfrak{A}_5$. En tout point, le sous-groupe de $\mathrm{PGL}_2(k(s))$ engendré par les images de s et p est un quotient de $\mathfrak{A}_5$ différent de 1, donc isomorphe à $\mathfrak{A}_5$, ce groupe étant simple. Ce passage n'est pas formalisé. Le modèle est dans le PGL_2 déployé sur $\mathbf{Z}[\zeta_5]$, et non sur $\mathbf{Z}[T]/(T^2+T-1)$. Sur $\mathbf{Q}(\sqrt{5})$, corps réel où -1 n'est pas somme de deux carrés, le PGL_2 déployé ne contient pas $\mathfrak{A}_5$ d'après le critère de Beauville (2010) [13], que la lecture cite de mémoire (note des pages 36 et 37) : sur un corps K de caractéristique première à l'ordre du groupe, $\mathrm{PGL}_2(K)$ contient $\mathfrak{A}_5$ si et seulement si -1 est somme de deux carrés et 5 un carré dans K ; un modèle sur $\mathbf{Z}[\varphi]$ demande donc une forme non déployée, et le théorème de la page 40 porte pour cette raison sur les formes de PGL_2.

Les représentations de $\mathbb{D}_\infty$ (pages 16 à 20). D'après la lecture, la page 17 (85, lot 1, p. 17) énonce : la catégorie C des (G,φ), G forme de PGL_2 sur S et $\varphi:\mathbb{D}_\infty=\langle\tau_0,\tau_1\mid\tau_0^2,\tau_1^2\rangle\to G(S)$ avec $u_s^2\neq1$ en tout point, $u=\varphi(\tau_0\tau_1)$, est équivalente à celle des couples (α,R), $\alpha+2$ inversible et R torseur sous $\mathcal{U}_{2-\alpha}$, groupe des λ avec $1+\lambda\rho$ inversible et la loi $\lambda+\lambda'+\rho\lambda\lambda'$. La page 19 donne $\underline{\mathrm{Aut}}(G,\varphi)\simeq{}_2\mathcal{U}_{2-\alpha}$ (85, lot 1, p. 19). On traite le groupe déployé sur un corps K : une représentation est un couple $t_0,t_1\in\mathrm{GL}_2(K)$ avec t_0^2, t_1^2 scalaires et u^2 non scalaire, $u=t_0t_1$. Alors t_0 et t_1 sont de trace nulle et $\tau=\operatorname{Tr}u\neq0$. On note $d=\det u$ et $\alpha=A(u)=\tau^2/d-2$.

Énoncé (Pages 16 à 20, sur un corps, énoncé de l'édition ♦). *Soit K un corps.*

1. *Deux représentations (t_0,t_1) et (s_0,s_1) sont conjuguées dans $\mathrm{PGL}_2(K)$ si et seulement si elles ont le même invariant, $A(t_0t_1)=A(s_0s_1)$, et si le quotient $\det t_0/\det s_0$ est un carré de $K^\times$.*
2. *Il existe une représentation d'invariant α avec $-\det t_0=\delta$ si et seulement si $\alpha+2\neq0$, $\delta\neq0$ et δ est une valeur de la forme $p^2+(\alpha+2)pr+(\alpha+2)r^2$.*
3. *Si $2\neq0$ dans K, le centralisateur de $\{t_0,t_1\}$ dans $\mathrm{PGL}_2(K)$ est formé de 1 et de la classe du commutateur $c=t_0t_1-t_1t_0$, qui n'est pas scalaire et a pour déterminant $d(2-\alpha)$. Il a deux éléments si $\alpha\neq2$, un seul si $\alpha=2$.*
4. *Sur $\mathbf{Q}$, $\left(\mathrm{diag}(1,-1),\left(\begin{smallmatrix}1&1\\-2&-1\end{smallmatrix}\right)\right)$ et $\left(\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\2&-1\end{smallmatrix}\right)\right)$ ont toutes deux $\alpha=-6$ et ne sont pas conjuguées dans $\mathrm{PGL}_2(\mathbf{Q})$.*

Démonstration. Pour des matrices de trace nulle, $t_0t_1+t_1t_0=\tau$, d'où $t_0u=(\tau-u)t_0$. Comme u n'est pas scalaire, il a un vecteur cyclique v. Dans la base (v,uv), u est la matrice compagnon C de $T^2-\tau T+d$, et t_0, de trace nulle avec $t_0C=(\tau-C)t_0$, s'écrit $X(p,r)=\left(\begin{smallmatrix}p&\tau p+dr\\r&-p\end{smallmatrix}\right)$. On a $-\det t_0=N(p,r)=p^2+\tau pr+dr^2$, norme de $w=(p+r\tau)-rC$ dans $K[C]$, et

$X(p,r) = X(1,0)\,w$ avec $X(1,0)\,z = \bar{z}\,X(1,0)$ pour $z \in K[C]$. La conjugaison par $\mathrm{diag}(1, c^{-1})$ remplace (τ, d) par $(c\tau, c^2 d)$ et r par cr : seul α compte.

(1) La trace et le déterminant donnent l'invariance de A, et $t_0 g = c_0\, g s_0$ donne $\det t_0 = c_0^2 \det s_0$. Réciproquement, on est ramené à $X(p,r)$ et $X(p',r')$ pour le même C, avec $N(p,r) = e^2 N(p',r')$. Posons $y = w\bar{w}'$ et $f = eN(w')$, de sorte que $N(y) = f^2$. Pour $\theta \in K[C]$, $z = f\theta + \bar{y}\bar{\theta}$ vérifie $yz = f\bar{z}$, d'où $X(p,r)\,z = e\,z\,X(p',r')$: c'est Hilbert 90 pour $K[C]$, qui peut être un corps, $K \times K$ ou $K[\varepsilon]$. Il reste à trouver un tel z inversible, parmi $\theta = 1$ avec $\pm f$ et $\theta = C$. Pour $\theta = 1$, $\det z = N(w')\,N(w \pm ew')$, et la somme des deux normes est $4e^2 N(w')$. Si les deux sont nulles, $2 = 0$ dans K ; alors $N(w+ew') = 0$ donne $pr' = p'r$, $\det z_C = 0$ donne $Q = pp' + \tau pr' + drr' = 0$, et l'identité $Q^2 - N(p,r)N(p',r') = (pr' - p'r)(\cdots)$ donne $e^2 N(w')^2 = 0$, ce qui est exclu. On compose enfin les conjugaisons de t_0 et de u, et celle de $t_1 = t_0^{-1} u$ s'en déduit.

(2) Par la forme normale, $-\det t_0 = N(p,r)$, et la mise à l'échelle $(\tau, d) \mapsto (\alpha+2, \alpha+2)$ remplace r par rd/τ. Réciproquement, $t_0 = X(p,r)$ et $t_1 = \delta^{-1} t_0 C$, avec $\tau = d = \alpha + 2$, conviennent.

(3) Si $gt_i = c_i t_i g$, alors $gug^{-1} = c_0 c_1 u$, et la trace donne $c_0 c_1 = 1$ puisque $\tau \neq 0$. Donc g commute à u et s'écrit $p + qu$. Avec $ut_0 = \tau t_0 - t_0 u$, la relation $gt_0 = c_0 t_0 g$ devient $(p + q\tau - c_0 p)\,t_0 - (q + c_0 q)\,t_0 u = 0$, et t_0, $t_0 u$ sont libres. Si $q \neq 0$, alors $c_0 = -1$, $2p + q\tau = 0$ et $g = \frac{q}{2}(2u - \tau) = \frac{q}{2}\,c$. Inversement, c anticommute à t_0 et à t_1, et $\det c = 4d - \tau^2 = d(2-\alpha)$.

(4) On a $\mathrm{Tr}(t_0 t_1) = \mathrm{Tr}(s_0 s_1) = 2$ et $\det(t_0 t_1) = \det(s_0 s_1) = -1$. Mais $\det t_0 = -1$, $\det s_0 = 1$, et -1 n'est pas un carré dans $\mathbf{Q}$. □

Remarque. L'équivalence de la page 17, telle que la lecture la donne, est fausse. Pour $\alpha = -6$, $\rho = 2 - \alpha = 8$ est inversible, $\mathcal{U}_\rho \simeq \mathbb{G}_m$ et $H^1(\mathbf{Q}, \mathbb{G}_m) = 0$: C' n'a qu'une classe d'invariant -6 sur $\mathbf{Q}$. Les automorphismes de PGL_2 sur un corps sont intérieurs, et le point (4) donne deux classes dans C. De même, le groupe des automorphismes d'un objet (α, R) de C' est $\mathcal{U}_\rho(S)$, infini ici, quand la page 19, confirmée par le point (3), donne ${}_2\mathcal{U}_\rho \simeq \mu_2$. Les classes du groupe déployé sont repérées par un élément de $K^\times / K^{\times 2} = H^1(K, \mu_2)$, comme on l'attend de torseurs sous ${}_2\mathcal{U}_\rho$. Enfin « $u_s^2 \neq 1$, c'est-à-dire $\alpha + 2$ inversible » n'est pas une équivalence : $t_1 = t_0$ donne $u = 1$ et $\alpha = 2$. Les formes de PGL_2, les bases autres qu'un corps et les torseurs sur S ne sont pas formalisés.

Ne sont pas démontrés ici : la rigidité de la catégorie des (G, φ) et la représentabilité de son foncteur des classes d'isomorphisme par $\mathrm{Spec}\,\mathbf{Z}[T]/(T^2 + T - 1)$ (page 40), ni l'existence d'un plongement de $\mathfrak{A}_5$ dans une forme de PGL_2 sur cette base ; pour le théorème de la page 4, le passage des formes de PGL_2 aux matrices de GL_2, qui n'a lieu que localement, la descente de la forme normale de $R[\ell]$ à une forme sur R, la conjugaison sur un corps qui ne contient pas ℓ et sur une base quelconque, et donc la représentabilité par l'ouvert de $\mathbb{A}^2_{\mathbf{Z}}$; l'identification $P_n = F_n$ pour tout n et le théorème de la page 31 pour n quelconque ; l'équivalence entre « nulle part scalaire » et « différent de 1 en tout point » pour une forme quelconque, et la description de son invariant A comme quotient adjoint (pages 23 à 26) ; l'homomorphisme $\mathfrak{A}_5 \to \mathrm{PGL}_2(\mathbf{Z}[\zeta_5])$ défini par le modèle et son injectivité sur les fibres ; les représentations de $\mathbb{D}_\infty$ sur une base quelconque et dans les formes de PGL_2 (pages 12 à 21), les systèmes de Schwarz (pages 42 à 56), les hyperpolygônes (pages 58 à 73), les polyèdres de caractéristique 0 (pages 75 à 80) et les pages 82 à 97.

Théorème 58.4 (D'après les pages 4 à 7, modules des représentations de G_2, reformulation de l'édition ♦). *Sur un schéma quelconque, les homomorphismes de G_2 dans une forme de*

♢ non vérifié en Lean

PGL_2 *qui vérifient* $(*)$ *en toute fibre sont rigides et classés par le couple* (α_0, α_1) *: leur foncteur des classes d'isomorphisme est représentable par l'ouvert de* $\mathbb{A}^2_{\mathbf{Z}}$ *où* $(\alpha_0+2)(\alpha_1+2)(\alpha_0+\alpha_1)$ *est inversible, complément de trois droites. Imposer les ordres exacts* ν_0*,* ν_1 *le découpe par* $\Psi_{\nu_i}(\alpha_i) = 0$*.*

Corollaire 58.5 (Grothendieck, pages 10 et 40, sous-groupes icosaédraux ♦)**.** *Pour tout schéma* S*, le groupoïde des couples* (G, φ)*,* G *forme de* PGL_2 *sur* S *et* $\varphi : \mathfrak{A}_5 \to G$ *un monomorphisme, est rigide, et* $\varphi \mapsto A(\varphi(\pi))$*,* π *un* 5*-cycle standard, rend son foncteur des classes d'isomorphisme représentable par* $\operatorname{Spec} \mathbf{Z}[T]/(T^2+T-1)$*. Il se déduit du théorème de la page 4 pour* $(\nu_0, \nu_1) = (3, 5)$*, où le discriminant est inversible.*

◊ non vérifié en Lean

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 1 à 3, groupoïde fondamental d'un produit fibré ♦)**.** *Pour une fibration de Serre* $f : X \to S$ *et une application* $g : Y \to S$*, le foncteur* $\Pi_1(X \times_S Y) \to \Pi_1(X) \times^2_{\Pi_1(S)} \Pi_1(Y)$ *est bijectif sur* π_0 *et surjectif sur* π_1*, de noyau* $\operatorname{Coker}(\pi_2 X \times \pi_2 Y \to \pi_2 S)$ *en la composante de base. C'est donc une équivalence quand* X*,* Y *et* S *sont asphériques.*

◊ non vérifié en Lean

Le dernier mot de la page 3, « asphériques », est illisible et restitué par la lecture, qui restreint aussi à la composante de base le calcul du noyau, énoncé sans restriction par la page. Mathlib n'a pas les fibrations de Serre ni le groupe π_2 à ce niveau. On se reportera aux notes de Grothendieck (132, lot 1, p. 1).

Théorème (Grothendieck, pages 16 à 20, extensions d'un groupe non connexe ; voir aussi Brown–Mucuk 1994 ♦)**.** *Soient* H *un groupe topologique dont* $\pi_0(H) = \mathfrak{G}$ *est discret, et* $\tilde{H}$ *une extension de* H *par* $\pi = \pi_1(H^0)$ *qui prolonge le revêtement universel de* H^0*. Pour tout groupe discret* N*, non nécessairement abélien, la catégorie des extensions de* H *par* N *est équivalente à celle des couples* $(\tilde{G}_0, \varphi)$ *formés d'une extension* $\tilde{G}_0$ *de* $\mathfrak{G}$ *par* N *et d'un morphisme* $\mathfrak{G}$*-équivariant* $\varphi : \pi \to \mathfrak{z}(N)$*. L'extension* G *s'obtient par produit contracté, et* $\pi_0(G) \simeq \tilde{G}_0/\varphi(\pi)$*.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 16 à 20) : seules les réductions et la construction explicite sont écrites, et les hypothèses de connexité locale sont de l'édition. Brown et Mucuk classent les revêtements des groupes topologiques non connexes par des modules croisés, non ces extensions. Mathlib n'a pas les revêtements universels des groupes topologiques. On se reportera aux notes de Grothendieck (132, lot 1, p. 16).

Exemple (D'après les pages 5 à 8, forme complétée par l'édition, Gr-catégorie périphérique d'une surface ♦)**.** Pour une surface compacte orientable à $n \geq 1$ composantes de bord, le 2-groupe des autoéquivalences du modèle formé de π_1, des lacets de bord ℓ_i et de leurs attaches $\alpha(i)$ a pour π_0 le groupe des classes d'applications à bord libre, et pour π_1 zéro, sauf pour le disque ($\mathbf{Z}$, canoniquement) et le cylindre ($\mathbf{Z}$, non canoniquement). Sa version à bord fixé a pour π_0 le groupe des classes d'applications relatif au bord, et un π_1 toujours nul.

◊ non vérifié en Lean

La page calcule ces groupes sans les identifier aux groupes de classes d'applications. Cette identification, une forme de Dehn–Nielsen–Baer à plusieurs composantes de bord, est de la lecture et n'est vérifiée que pour $n = 1$. Mathlib n'a pas les groupes de classes d'applications des surfaces. On se reportera aux notes de Grothendieck (132, lot 1, p. 5).

Les deux énoncés suivants viennent de la cote 147, *Structure à l'infini des* $M_{g,\nu}$: quatre-vingt-dix pages numérotées de sa main et annoncées par une table en treize paragraphes, que l'édition date de l'hiver 1982–1983. C'est un texte suivi, jamais édité. Il énonce à sa page 29 le principe des deux étages de la tour de Teichmüller, un an avant l'*Esquisse d'un programme*.

Théorème (Grothendieck, pages 148 à 151, voisinage épointé et codimension deux ♦). *Soient X un espace analytique complexe lisse et Θ un diviseur à croisements normaux. Le voisinage tubulaire épointé $V^*_{\Theta,X}$ est la colimite homotopique du système semi-simplicial des voisinages tubulaires épointés des strates déployées. Son groupoïde fondamental est donc la somme amalgamée $\tilde{\Pi}_1 \leftarrow \tilde{\Pi}_{2,1} \rightarrow \tilde{\Pi}_2$ des groupoïdes des fibrés en tores multinormaux au-dessus des strates ouvertes de codimension 1 et 2. Il en va de même de $\Pi_1(X \setminus \Theta)$ quand $X \setminus \Theta$ et son bout ont des groupoïdes fondamentaux équivalents.*

◊ non vérifié en Lean

La page 149 énonce le théorème de recollement comme une équivalence de topos et le corrige aussitôt en équivalence d'homotopie ; aucune démonstration n'est donnée. La lecture lit « limite inductive » comme colimite homotopique, corrige le $\Pi_1 X$ du corollaire 3 en $\Pi_1 X^*$ et rapproche le cas $X^* = M_{g,\nu}$, où le groupe modulaire serait décrit par les strates de codimension 1 et 2 du bord, du principe des deux niveaux ; ce rapprochement n'est pas sur la page. Hatcher, Lochak et Schneps ajoutent aux relations de $\widehat{GT}$, avec $\lambda = 1$, une relation dans le groupe modulaire profini de genre 1 à deux composantes de bord. Le sous-groupe Λ qu'elle définit agit sur toute la tour de Teichmüller profinie et s'injecte dans ses automorphismes extérieurs spéciaux (2000, théorèmes A à C [70]). Les relations qui définissent Λ relèvent des dimensions modulaires 1 et 2 : des relations sur les deux premiers niveaux donnent déjà une action sur toute la tour, en tout genre. L'énoncé général de la page n'a pas été cherché dans la littérature sur l'éclatement réel orienté. Voir les groupoïdes de Teichmüller de la cote 146 (section 74). Mathlib n'a pas les voisinages tubulaires ni les colimites homotopiques d'espaces. On se reportera aux notes de Grothendieck (147, lot 8, p. 148).

Exemple (D'après les pages 62 à 64, forme complétée par l'édition, classe stratifiée de $M_{1,1}$ sur $\mathbf{Z}$ ♦). Dans l'invariant additif qui compte chaque pièce localement fermée d'un champ de Deligne–Mumford à groupe d'automorphismes constant H comme la classe de son espace grossier divisée par $\operatorname{card} H$, le champ des courbes elliptiques sur $\operatorname{Spec}\mathbf{Z}$ a pour classe $\frac{1}{2}(L-1)-\frac{1}{12}+\frac{1}{8}\zeta_2+\frac{1}{6}\zeta_3$, où $\zeta_p = [\operatorname{Spec}\mathbf{F}_p]$, et sa compactification $\frac{1}{2}L-\frac{1}{12}+\frac{1}{8}\zeta_2+\frac{1}{6}\zeta_3$. Sur $\mathbf{Z}[1/6]$, ces classes se réduisent à $\frac{1}{2}(L-1)-\frac{1}{12}$ et $\frac{1}{2}(L-1)+\frac{5}{12}$.

◊ non vérifié en Lean

La page dit seulement « dans un groupe de Grothendieck convenable » ; la règle de l'invariant est reconstituée par la lecture, qui étend aussi à $\mathbf{Z}[1/6]$ la formule que la page donne sur $\mathbf{Z}[1/2]$, et l'arithmétique a été refaite. Cet invariant n'est ni le nombre de points pondéré, qui vaut q pour $M_{1,1}$ sur $\mathbf{F}_q$, ni la classe dans le groupe de Grothendieck des champs. Les termes en ζ_2 et ζ_3 portent sur les fibres de caractéristique 2 et 3, où le point $j = 0 = 1728$ a un groupe d'automorphismes d'ordre 24, resp. 12 ; sur $\mathbf{Z}[1/6]$, les points à automorphismes exceptionnels sont ceux que la section 50 repère par $j(j-1) = 0$ dans sa normalisation. Mathlib n'a pas les champs de Deligne–Mumford. On se reportera aux notes de Grothendieck (147, lot 4, p. 62).

Énoncé (Grothendieck, pages 63 et 64, l'arithmétique de la formule (80)). [a] *Dans un corps de caractéristique nulle, pour tous éléments L, ζ_2, ζ_3,*

$$\tfrac{1}{2}(L-2+\zeta_2+\zeta_3)+\tfrac{1}{4}(1-\zeta_2-\zeta_3)+\tfrac{1}{6}(1-\zeta_2-\zeta_3)+\tfrac{1}{24}\zeta_2+\tfrac{1}{12}\zeta_3 = \tfrac{1}{2}(L-1)-\tfrac{1}{12}+\tfrac{1}{8}\zeta_2+\tfrac{1}{6}\zeta_3,$$

et l'ajout de $\frac{1}{2}$ donne $\frac{1}{2}L-\frac{1}{12}+\frac{1}{8}\zeta_2+\frac{1}{6}\zeta_3$.

a. Preuve vérifiée : `lean/Grothendieck/Folder147.lean`.

Démonstration. La page 63 découpe la droite des j selon les deux sections S_0 et S_1 des courbes à automorphismes $\mathbf{Z}/4$ et $\mathbf{Z}/6$, qui ne se coupent qu'en un point a_2 de caractéristique 2 et un point a_3 de caractéristique 3, où les groupes d'automorphismes sont d'ordre 24 et 12. Le reste U a pour groupe générique $\{\pm 1\}$. Chaque pièce compte pour l'inverse de l'ordre de son groupe : $\frac{1}{2}$ pour U, $\frac{1}{4}$ et $\frac{1}{6}$ pour $S_0' = S_0 \smallsetminus \{a_2, a_3\}$ et S_1', $\frac{1}{24}$ et $\frac{1}{12}$ pour a_2 et a_3. La page 64 calcule les classes des pièces : la droite moins deux sections, auxquelles on rend les deux points ôtés deux fois, donne $[U] = L - 2 + \zeta_2 + \zeta_3$, et $[S_0'] = [S_1'] = 1 - \zeta_2 - \zeta_3$. Le membre de gauche vaut alors $\frac{1}{2}L - \frac{7}{12} + \frac{1}{8}\zeta_2 + \frac{1}{6}\zeta_3$, car $\frac{1}{2} - \frac{5}{12} + \frac{1}{24} = \frac{1}{8}$ et $\frac{1}{2} - \frac{5}{12} + \frac{1}{12} = \frac{1}{6}$: c'est la formule (80) (`class_M11`). La pointe, de poids $\frac{1}{2}$, donne la classe de la compactification (`class_M11_bar`). En annulant ζ_2 et ζ_3, c'est-à-dire au-dessus de $\mathbf{Z}[1/6]$, on retrouve la formule (79) (`class_M11_away_from_6`). Au-dessus de $\mathbf{Z}[1/2]$, où la page 63 écrit (79), il reste le terme $\frac{1}{6}\zeta_3$; la lecture le relève. Lean vérifie l'algèbre, avec L, ζ_2, ζ_3 indéterminés. Il ne vérifie ni la stratification, ni les groupes d'automorphismes, ni l'invariant lui-même, et l'encadré précédent reste non vérifié. Les noms sont ceux de `Folder147.lean`.

Conjecture (Grothendieck, page 18, l'ordre cyclique détermine la position ♦). *Une position relative d'une pseudo-droite ajoutée, autre que les D_i eux-mêmes, est déterminée par l'ordre cyclique, compatible à l'antipodie, dans lequel son revêtement double rencontre les pseudo-droites orientées de Σ.*

La page écrit « il ne devrait pas être difficile de montrer » et ne le démontre pas. Mathlib n'a pas les arrangements de pseudo-droites. On se reportera aux notes de Grothendieck (154, lot 1, p. 18).

Théorème (Grothendieck, pages 55 à 63, 85 et 86, monodromie diédrale ♦). *Soit Σ un système de n pseudo-droites d'un plan projectif réel. Les $2n$-gones $\mathrm{Pol}(D)$ découpés sur le revêtement double d'une pseudo-droite ajoutée D forment un système local sur la surface cellulaire des positions relatives. Le transport le long d'un demi-tour autour d'une position $D = D_i$ est la rotation $t \mapsto t - (n-1)$ de $\mathbf{Z}/2n\mathbf{Z}$, et la monodromie $\pi_1 \to \mathbb{D}_{2n}$, à valeurs dans le groupe diédral d'ordre $4n$, est surjective sur la surface où la traversée des D_i est permise.*

◊ non vérifié en Lean

L'édition corrige deux fois $\mathbf{Z}/n\mathbf{Z}$ en $\mathbf{Z}/2n\mathbf{Z}$ (pages 57 et 85), et note que pour n impair la surjectivité demande une réflexion latérale. La surjectivité sans traversée des D_i (pages 85 et 86) n'est pas reprise. Mathlib n'a pas les arrangements de pseudo-droites ni les systèmes locaux sur un complexe cellulaire. On se reportera aux notes de Grothendieck (154, lot 3, p. 55).

Théorème (Grothendieck, page 153, cube des générisations, sous la forme précisée par l'édition ♦). *Soit Σ un arrangement de pseudo-droites, vu comme matroïde orienté de rang 3, et appelons* position *d'une pseudo-droite ajoutée une signature σ des cocircuits (les sommets de Σ, au signe près) valide sur chaque droite de Σ au sens de Las Vergnas : le long de chaque droite, lue sur son revêtement double, les signes sont de la forme $+\cdots+\ (0)\ -\cdots-$ au renversement près, avec au plus un 0, et pas tous nuls. Disons que σ est une générisation de σ_D si $\sigma = \sigma_D$ partout où $\sigma_D \neq 0$. Si σ_D s'annule en exactement ν sommets, les générisations de D sont exactement les 3^ν choix de signes, 0 compris, en ces sommets ; ordonnées par la spécialisation, elles forment l'ensemble ordonné des faces du cube $[-1,1]^\nu$. Les 2^ν générisations stables (sans zéro) en sont les sommets, les $\nu\, 2^{\nu-1}$ générisations sous-stables (un seul zéro) les arêtes, l'incidence étant la spécialisation.*

Démonstration. Le point est que la condition de Las Vergnas se vérifie droite par droite, et qu'une droite ne porte jamais deux zéros de σ_D : deux sommets de D ne sont jamais sur une même droite de Σ. Sur une droite qui porte un zéro de σ_D, la suite des signes est $a \cdots a\, 0\, (-a) \cdots (-a)$; remplacer ce 0 par a, par $-a$

ou le garder donne encore une suite valide. Sur une droite qui n'en porte pas, rien ne change. Tout choix de signes aux ν zéros de σ_D est donc une position, et les choix aux différents sommets sont indépendants : c'est le « décollement » de la page, de chaque côté, en chaque sommet (figure 14). La restriction aux zéros de σ_D est alors une bijection des générisations de D sur $\{-,0,+\}^\nu$, qui respecte la spécialisation (0 en dessous de $+$ et de $-$). Le vecteur de signes w correspond à la face du cube où la coordonnée z vaut w_z si $w_z \neq 0$ et parcourt $[-1,1]$ sinon ; une face est contenue dans une autre exactement quand le vecteur de la seconde est une spécialisation de celui de la première, et les vecteurs sans zéro donnent les sommets. Il reste à compter : 2^ν vecteurs sans zéro, et, pour chacun des ν emplacements du zéro unique, $2^{\nu-1}$ choix de signes ailleurs. L'hypothèse $\nu \geq 2$ n'est pas utile, ni les axiomes d'un arrangement (deux droites se coupent en un sommet, …) : l'énoncé vaut pour toute donnée de droites portant des suites de sommets. Lean (`Folder154.lean`) définit les arrangements (`Arrangement`), la condition sur une droite (`ValidSeq`), les positions (`IsPosition`) et la spécialisation (`Spec`), et démontre qu'une droite porte au plus un zéro (`IsPosition.eq_of_zero_on_line`), l'indépendance (`IsPosition.of_spec`, `isPosition_and_spec_iff`), la bijection et l'incidence (`genEquiv`, `genEquiv_spec_iff`), le cube (`cubeFace_subset_iff`, `cubeFace_eq_singleton`) et les comptes (`card_gen`, `card_gen_stable`, `card_gen_substable`). La page énonce le résultat sans justification ; l'indépendance est celle que proposait la lecture. Ne sont pas démontrés : le même énoncé pour des pseudo-droites topologiques, qui demanderait le théorème de représentation de Folkman–Lawrence ; la tension avec la page 150 pour $\nu \geq 3$ (les 2ν positions sous-stables incidentes à un sommet de la surface X^* contre les $\nu\,2^{\nu-1}$ arêtes du cube) ; le contraste avec une droite passant par ν sommets d'un arrangement de droites, qui n'a que 2ν perturbations stables ; la question de la même page. On se reportera aux notes de Grothendieck (154, lot 8, p. 153).

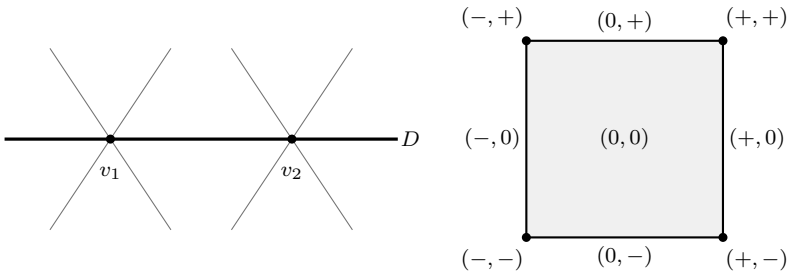


FIGURE 14 – Le cas $\nu = 2$. La pseudo-droite ajoutée D passe par deux sommets v_1, v_2 de Σ. La décoller d'un côté ou de l'autre en chacun d'eux donne les quatre générisations stables, sommets du carré ; la décoller en un seul sommet donne ses quatre arêtes, et D elle-même, de vecteur $(0,0)$, est le carré entier (grisé). Figure de l'édition ; à la page 153 Grothendieck dessine un fuseau dont le sommet est traversé par $\Delta_1, \ldots, \Delta_\nu$ (154, lot 8, p. 153).

Théorème (Grothendieck, pages 132 à 143 et 155 à 157, revêtement d'Arf par factorisation de Stein ; voir aussi Conrad [35] ♦). *Sur toute base, caractéristique 2 comprise, les schémas de drapeaux isotropes $\Delta_H(E,q)$ d'un module quadratique régulier sont lisses et projectifs, à fibres géométriquement connexes sauf quand $N = 2n$ et $n \in H$. La factorisation de Stein de la grassmannienne isotrope maximale définit le revêtement double d'Arf, $\mathrm{Arf}' \simeq \mathrm{Arf}\,\wedge^{\mathbf{Z}/2}\,\mu_2$, et l'homomorphisme de Dickson est l'action de $O(q)$ sur ce revêtement, sans algèbres de Clifford.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 133 à 143) : la lissité et la connexité sont démontrées sur un corps, et le passage à une base quelconque « par spécialisation et factorisation de Stein » tient en une ligne. La section de la cote 77 ne traite pas cet énoncé. Conrad construit l'invariant de Dickson par l'algèbre de Clifford paire. Mathlib n'a pas les schémas de drapeaux isotropes ni la factorisation de Stein. On se reportera aux notes de Grothendieck (77, lot 7, p. 132).

Partie 22

Jeux et combinatoire

59 Cote 68 : les théories de l'orientation et leurs applications de Stokes [62]

La cote 68 réunit des notes sur les jeux positionnels, les réarrangements, l'exponentielle et, aux pages 49 à 55, l'orientation des espaces vectoriels réels et les déterminants. La page 49 (68, lot 3, p. 49) énonce deux lemmes sur les ensembles à deux éléments, puis les données d'une « théorie de l'orientation » sur le groupoïde des espaces vectoriels réels de dimension finie : un foncteur Ω vers les ensembles à deux éléments, une identification $\Omega(0) \simeq \{\pm 1\}$, et pour tout hyperplan $W \subset V$ et tout demi-espace V' bordé par W une application de Stokes $\mathrm{St}_{V'} : \Omega(V) \to \Omega(W)$, naturelle en (V, V'), bijective, qui change par l'involution de $\Omega(W)$ quand on passe au demi-espace opposé. Le théorème de la page dit : a) tout morphisme de théories est un isomorphisme ; b) entre deux théories il existe un et un seul isomorphisme ; c) il existe une théorie. La page démontre a) et l'unicité dans b) par récurrence sur la dimension. La page 51 (68, lot 3, p. 51) ramène une théorie en dimension n à un caractère ε_n de $\mathrm{GL}(n, \mathbf{R})$ et à une bijection de Stokes $\omega_n \to \omega_{n-1}$ pour le demi-espace $\mathbf{R}^{n-1} \times \mathbf{R}_+$, écrit la compatibilité au stabilisateur $\varepsilon_n(u_n) = \mathrm{sg}(\lambda)\, \varepsilon_{n-1}(u_{n-1})$ et conclut « de proche en proche » $\varepsilon_n = \mathrm{sg} \circ \det$. On démontre ici a), b) et la valeur $\mathrm{sg} \circ \det$ de l'action, c'est-à-dire tout l'énoncé de la piste ; l'existence c) n'en fait pas partie.

Conventions. Les espaces sont les espaces vectoriels réels de dimension finie (dans l'univers `Type`) et leurs isomorphismes linéaires. Un demi-espace fermé bordé par W est un ensemble $H = \{f \geq 0\}$, où f est une forme linéaire non nulle de noyau W ; le demi-espace opposé est $-H = \{f \leq 0\}$. Une théorie de l'orientation est la donnée d'un ensemble $\Omega(V)$ à deux éléments pour chaque V, d'une action fonctorielle des isomorphismes $e : V \to V_2$, d'une bijection $\Omega(\mathbf{R}^0) \simeq \{\pm 1\}$ et, pour chaque couple (W, H), d'une application $\mathrm{St}_H : \Omega(V) \to \Omega(W)$, soumise aux conditions suivantes. Naturalité : si $e : V \to V_2$ envoie W sur W_2 et H sur H_2, alors $\mathrm{St}_{H_2} \circ e = e|_W \circ \mathrm{St}_H$. Bijectivité de St_H. Opposé : $\mathrm{St}_{-H}(\omega) \neq \mathrm{St}_H(\omega)$ pour tout ω, ce qui, dans un ensemble à deux éléments, revient à $\mathrm{St}_{-H} = \tau \circ \mathrm{St}_H$, où τ est l'involution sans point fixe. Un morphisme de théories est une transformation naturelle $\varphi_V : \Omega(V) \to \Omega'(V)$ compatible à l'identification de $\Omega(0)$ et aux applications de Stokes. On note $\mathbf{R}^n_+ = \mathbf{R}^{n-1} \times \mathbf{R}_+$ le demi-espace standard de $\mathbf{R}^n$, bordé par $\mathbf{R}^{n-1} \times 0$.

Lemme 59.1. *Soient P, Q des ensembles à deux éléments. (1) Deux éléments distincts d'un même troisième sont égaux. (2) Deux applications injectives $P \to Q$ qui coïncident en un point sont égales. (3) Une bijection de P fixe tous les points ou n'en fixe aucun ; la composée de deux bijections fixe tous les points si et seulement si les deux fixent tous les points ou aucune n'en fixe ; le carré d'une bijection fixe tous les points.*

Démonstration. (1) est la définition du cardinal 2. Pour (2), si $y \neq x_0$, $f(y)$ et $g(y)$ sont distincts de $f(x_0) = g(x_0)$, donc égaux par (1). Pour (3), si $\sigma(x) \neq x$ et $\sigma(y) = y$, alors $x \neq y$ et

62. Preuve vérifiée : `lean/Grothendieck/Folder68.lean`.

$\sigma(x) \neq \sigma(y) = y$, donc $\sigma(x) = x$ par (1), contradiction. Si ni σ ni ρ ne fixent de point, $\sigma(\rho x)$ et x sont distincts de ρx, donc égaux ; les autres cas sont immédiats. □

Énoncé (Page 51, l'action de $\mathrm{GL}(n, \mathbf{R})$ ♦). *Soit* (Ω, St) *une théorie de l'orientation et* $g \in \mathrm{GL}(n, \mathbf{R})$. *Pour tout* $\omega \in \Omega(\mathbf{R}^n)$, $g\omega = \omega$ *si* $\det g > 0$ *et* $g\omega = \tau\omega$ *si* $\det g < 0$ *: l'action de* $\mathrm{GL}(n, \mathbf{R})$ *sur* $\Omega(\mathbf{R}^n)$ *est* $\mathrm{sg} \circ \det$. *Il en est de même pour un automorphisme de tout espace* V.

Démonstration. Disons qu'une matrice inversible M est *bonne* si l'automorphisme de matrice M fixe $\Omega(\mathbf{R}^n)$ si et seulement si $\det M > 0$. Par le lemme 59.1 (3), un produit de deux matrices bonnes est bon, car $\det(AB) > 0$ si et seulement si $\det A$ et $\det B$ sont de même signe, et un carré A^2 est bon, car il fixe $\Omega(\mathbf{R}^n)$ et $\det A^2 > 0$. Une transvection $1 + c\,E_{ij}$ est le carré de $1 + \frac{c}{2}E_{ij}$; elle est bonne. Une matrice diagonale $\mathrm{diag}(1, \dots, d, \dots, 1)$ avec $d > 0$ est le carré de $\mathrm{diag}(1, \dots, \sqrt{d}, \dots, 1)$; elle est bonne.

Reste $r_i = \mathrm{diag}(1, \dots, -1, \dots, 1)$, avec -1 en place i, dont le déterminant est -1 : il faut voir qu'elle ne fixe pas $\Omega(\mathbf{R}^n)$. Pour $i = n$, r_n fixe l'hyperplan $\mathbf{R}^{n-1} \times 0$ point par point et envoie $\mathbf{R}^n_+$ sur le demi-espace opposé. La naturalité donne $\mathrm{St}_{-\mathbf{R}^n_+}(r_n\omega) = \mathrm{St}_{\mathbf{R}^n_+}(\omega)$; si $r_n\omega = \omega$, cela contredit l'axiome de l'opposé. Pour i quelconque, r_i est conjuguée de r_n par la matrice de la transposition de i et n, et un conjugué fixe Ω si et seulement si l'élément conjugué le fait. Une matrice diagonale inversible est un produit de matrices $\mathrm{diag}(1, \dots, d_i, \dots, 1)$, et pour $d_i < 0$ on écrit $\mathrm{diag}(\dots, d_i, \dots) = \mathrm{diag}(\dots, -d_i, \dots)\, r_i$: toute matrice diagonale inversible est bonne.

Toute matrice inversible est produit de matrices diagonales inversibles et de transvections (par un principe de récurrence de mathlib) ; elle est donc bonne. Si g ne fixe pas $\Omega(\mathbf{R}^n)$, il n'en fixe aucun point (lemme 59.1 (3)), et $g\omega = \tau\omega$. Pour un espace V et un isomorphisme $c : V \to \mathbf{R}^n$, g fixe $\Omega(V)$ si et seulement si cgc^{-1} fixe $\Omega(\mathbf{R}^n)$, et $\det(cgc^{-1}) = \det g$. □

Théorème 59.2 (Grothendieck, page 49, théorème, a) et unicité dans b) ♦). *Soient* (Ω, St) *et* (Ω', St') *deux théories de l'orientation. (1) Toutes les composantes d'un morphisme* φ *sont bijectives, et* φ *a un inverse qui est un morphisme de théories. (2) Deux morphismes* $\varphi, \psi : \Omega \to \Omega'$ *sont égaux.*

Démonstration. Par récurrence sur $n = \dim V$, on montre que φ_V est injective et que $\varphi_V = \psi_V$. Si $n = 0$, on choisit un isomorphisme $c : V \to \mathbf{R}^0$. Par naturalité et compatibilité à $\Omega(0) \simeq \{\pm 1\}$, φ_V et ψ_V s'écrivent toutes deux $c^{-1} \circ \iota'^{-1} \circ \iota \circ c$, où ι et ι' sont les deux identifications ; elles sont égales et injectives. Si $n = m + 1$, on choisit une forme linéaire non nulle f ; son noyau W est de dimension m, et $H = \{f \geq 0\}$ est un demi-espace bordé par W. La compatibilité aux applications de Stokes donne $\mathrm{St}'_H \circ \varphi_V = \varphi_W \circ \mathrm{St}_H$, et de même pour ψ. Comme $\varphi_W = \psi_W$ est injective par hypothèse de récurrence et que St_H et St'_H sont bijectives, φ_V est injective et $\mathrm{St}'_H \circ \varphi_V = \mathrm{St}'_H \circ \psi_V$, d'où $\varphi_V = \psi_V$. Une injection entre deux ensembles à deux éléments est bijective. Pour l'inverse, on prend le morphisme $\Omega' \to \Omega$ de l'énoncé suivant ; ses composées avec φ sont des morphismes d'une théorie dans elle-même, donc égales à l'identité par (2). □

Énoncé (Page 49, théorème, existence dans b) ♦). *Entre deux théories de l'orientation* (Ω, St) *et* (Ω', St'), *il existe un morphisme ; c'est donc l'unique isomorphisme entre elles.*

Démonstration. On suit la réduction de la page 51. Notons $\omega_n = \Omega(\mathbf{R}^n)$ et $s_n : \omega_n \to \omega_{n-1}$ la bijection composée de $\mathrm{St}_{\mathbf{R}^n_+}$ et de l'identification $\mathbf{R}^{n-1} \times 0 \simeq \mathbf{R}^{n-1}$. On définit des éléments de référence $r_0 \in \omega_0$, image réciproque de 1, et $r_n = s_n^{-1}(r_{n-1})$; de même $r'_n \in \omega'_n$. Soit $\psi_n : \omega_n \to \omega'_n$ la bijection qui envoie r_n sur r'_n et l'autre élément sur l'autre. Elle commute à

l'action de $\mathrm{GL}(n,\mathbf{R})$: par l'énoncé de la page 51, g agit trivialement des deux côtés si $\det g > 0$, et par τ des deux côtés si $\det g < 0$, et une bijection commute à τ (lemme 59.1 (1)). Par le lemme 59.1 (2), elle vérifie $s'_n \circ \psi_n = \psi_{n-1} \circ s_n$, puisque les deux membres sont injectifs et envoient r_n sur r'_{n-1}, et elle est compatible à l'identification de $\Omega(0)$.

Pour un espace V de dimension n et un isomorphisme $c : V \to \mathbf{R}^n$, on pose $\varphi_V = c^{-1} \circ \psi_n \circ c$. Cela ne dépend pas de c : si $c_2 = gc$ avec $g \in \mathrm{GL}(n,\mathbf{R})$, ψ_n commute à g. La naturalité de φ s'en déduit, en calculant φ_{V_2} avec la carte $c \circ e^{-1}$. Pour la compatibilité à St_H, $H = \{f \geq 0\}$ bordé par W dans V de dimension $m+1$, on construit un isomorphisme $c : V \to \mathbf{R}^{m+1}$ dont la dernière coordonnée est f : avec v_0 tel que $f(v_0) = 1$ et un isomorphisme $j : W \to \mathbf{R}^m$, l'application $u \mapsto j^{-1}(u_1, \ldots, u_m) + u_{m+1} v_0$ est injective entre espaces de même dimension, et c est son inverse. Alors c envoie W sur $\mathbf{R}^m \times 0$ et H sur $\mathbf{R}^{m+1}_+$. La naturalité des applications de Stokes pour c et pour c^{-1} ramène $\mathrm{St}'_H \circ \varphi_V = \varphi_W \circ \mathrm{St}_H$ à la relation $s'_{m+1} \circ \psi_{m+1} = \psi_m \circ s_{m+1}$, φ_W étant calculé avec la carte $j' \circ c|_W$, où j' identifie $\mathbf{R}^m \times 0$ à $\mathbf{R}^m$. □

Remarque. La vérification suit la lecture, qui pose la bijectivité des applications de Stokes en axiome : l'argument de cardinal de la page 49 ne la donne pas, et elle sert à chaque pas de la récurrence. La partie a) et l'unicité dans b) n'utilisent ni l'axiome de l'opposé ni la naturalité des applications de Stokes : elles n'utilisent que leur bijectivité, la compatibilité des morphismes et l'identification de $\Omega(0)$. L'axiome de l'opposé ne sert qu'à l'existence, par l'action de $\mathrm{diag}(1, \ldots, 1, -1)$; sans lui, la théorie où $\Omega(V) = \{\pm 1\}$, avec action triviale et applications de Stokes identiques, satisferait aux autres axiomes sans être isomorphe aux orientations usuelles (observation non formalisée). Le passage « de proche en proche » de la page 51 repose, d'après la note de la lecture, sur la factorisation par le déterminant de tout caractère de $\mathrm{GL}(n,\mathbf{R})$ à valeurs dans $\{\pm 1\}$; la démonstration tire cette factorisation de la décomposition des matrices inversibles en transvections et matrices diagonales, les transvections et les matrices diagonales positives étant des carrés. La forme « $\Omega(W,V) \wedge \Omega(V) \simeq \Omega(W)$ » des axiomes et le lemme 2 de la page 49 ne sont pas formalisés : on énonce directement l'axiome de l'opposé.

Ne sont pas démontrés ici : l'existence c) d'une théorie de l'orientation, c'est-à-dire la construction des applications de Stokes sur les orientations usuelles et la vérification des axiomes ; la reformulation par le produit contracté $D(W,V) \wedge \Omega(V) \simeq \Omega(W)$ et le lemme 2 de la page 49 ; la comparaison de la normalisation de la page (normale rentrante en dernier) avec celle des géomètres, au signe $(-1)^{\dim V}$; le produit, la règle de Koszul et la compatibilité de Stokes et des produits de la page 53 ; les déterminants de la page 55.

Partie 23

Groupes fondamentaux et théorie de Galois

60 Cote 29 : le critère du déterminant sur l'inertie modérée [63]

La cote 29 réunit, entre 1959 et 1969, les notes de Grothendieck sur le groupe fondamental modéré, dont l'échange de 1967 avec Murre. Le tapuscrit « Comportement fonctoriel des groupes d'inertie » (pages 116 à 122) calcule, pour un morphisme f de schémas strictement locaux réguliers munis de diviseurs à croisements normaux de branches indexées par C et C', l'application induite sur l'inertie modérée : c'est l'application $N : \prod_{\ell\neq p} \mathbf{Z}_\ell(1)^C \to \prod_{\ell\neq p} \mathbf{Z}_\ell(1)^{C'}$ de la matrice $(n_{c,c'})$ des multiplicités, $f^*(\bar{E}_{c'}) = \sum_c n_{c,c'} \bar{D}_c$ (29, lot 6, p. 120). L'identification de cette application à N demande l'inertie modérée des schémas réguliers, que mathlib n'a pas ; elle n'est pas démontrée ici. Le critère que la page en tire porte sur la seule matrice, $\mathbf{Z}_\ell(1)$ étant libre de rang 1 sur $\mathbf{Z}_\ell$.

Ramification modérée. Le cadre est celui de SGA 1, exposé XIII, et de son appendice I : pour X strictement local régulier et D à croisements normaux de branches indexées par C, le groupe fondamental modéré de $X \smallsetminus D$ est $\prod_{\ell\neq p} \mathbf{Z}_\ell(1)^C$ (corollaire 5.3 de l'appendice, dans l'édition de 2003 [63]), et l'on cherche ici sa fonctorialité. Le groupe fondamental modéré d'un voisinage formel d'un diviseur à croisements normaux, objet des pages 87 à 97 et de l'échange avec Murre, est aussi le sujet du livre de Grothendieck et Murre (1971) [64]. Les pages 190 à 200 cherchent un cadre axiomatique, les « domaines de ramification », et réalisent les revêtements modérés comme revêtements étales d'un champ (ci-dessous). La monodromie modérée à plusieurs paramètres de la cote 34 et la dimension cohomologique de la cote 31, de la même période, sont encadrées dans les parties « Groupes fondamentaux et théorie de Galois » et « Cohomologie étale et ℓ-adique ».

Théorème 60.1 (Grothendieck, page 120, le critère ♦)**.** *Soient C, C' des ensembles finis, N une matrice entière de lignes indexées par C' et de colonnes par C, et p un nombre premier ou $p = 1$ (l'exposant caractéristique). L'application $\mathbf{Z}_\ell^C \to \mathbf{Z}_\ell^{C'}$ de matrice N est bijective pour tout nombre premier $\ell \neq p$ si et seulement si $\operatorname{card} C = \operatorname{card} C'$ et, les colonnes étant mises en bijection avec les lignes, l'entier $\det N$ vaut $\pm p^k$ pour un $k \geq 0$.*

L'énoncé tient tel que la page le donne, par l'argument d'une ligne de la lecture (`criterion`, dans `Folder29.lean`). L'égalité des cardinaux vient d'une seule valeur de ℓ ; le choix de la bijection entre colonnes et lignes ne change le déterminant que d'un signe.

La preuve vérifiée établit aussi les deux pas : la bijectivité pour un ℓ donné force $\operatorname{card} C = \operatorname{card} C'$ (`card_eq_of_bijective`), et une matrice carrée entière est bijective sur $\mathbf{Z}_\ell$ si et seulement si $\ell \nmid \det$ (`bijective_iff_not_dvd_det`). Elle ne définit ni l'inertie modérée ni $\mathbf{Z}_\ell(1)$: le passage de la géométrie à la matrice est l'énoncé encadré ci-dessous, non vérifié.

Théorème (Grothendieck, page 120, inertie modérée et matrice des multiplicités)**.** *Dans la situation ci-dessus, l'application induite sur l'inertie modérée est l'application N de matrice $(n_{c,c'})$; lorsque N est un isomorphisme, les sous-groupes d'inertie de H en y sont exactement*

◊ non vérifié en Lean

63. Preuve vérifiée : `lean/Grothendieck/Folder29.lean`.

les conjugués des images de ceux de G en x.

Mathlib n'a pas l'inertie modérée des schémas réguliers. On se reportera aux notes de Grothendieck (29, lot 6, p. 120).

Le degré comme donnée primitive (pages 212 et 214). Deux feuillets insérés, « 1 bis » et « 1 ter », axiomatisent directement la notion de morphisme de degré n, sans foncteur fibre ni points à compter (29, lot 11, p. 212). Sur une catégorie C, on se donne pour chaque $n \in \mathbf{N}$ une classe $\deg_n$ de morphismes telle que : a) elle est stable par changement de base ; b) elle est additive pour les sommes finies ($\varnothing \to Y$ est de degré 0, et si $X = X_1 \sqcup X_2$ avec $X_i \to Y$ de degré n_i, alors $X \to Y$ est de degré $n_1 + n_2$) ; c) un isomorphisme est de degré 1 ; d′) pour tout $f : X \to Y$, $Y = \coprod_{n\in\mathbf{N}} Y_n$ avec $X \times_Y Y_n \to Y_n$ de degré n ; d) un morphisme de degré $n \geq 1$ est de descente effective universelle ; e) un morphisme de degré 0 a une source vide et est l'inclusion d'un sommande direct. La « Conclusion » de la page 214 affirme que, sous ces conditions et les conditions (0) à (2) de la page 212 (limites projectives finies, monomorphismes inclusions de sommandes directs), la notion est uniquement déterminée, et qu'un morphisme est de degré n si et seulement s'il devient $[1, n]$, la somme de n copies de la base, après un changement de base de descente effective universelle.

Dans la vérification, la classe des morphismes trivialisants est un paramètre E, puisque mathlib n'a pas les morphismes de descente effective universelle ; on n'en utilise que les propriétés que la page utilise. On note $\mathrm{Triv}_n(E)$ la classe des $f : X \to Y$ pour lesquels il existe $g : Y' \to Y$ dans E avec $X \times_Y Y' \simeq [1, n]_{Y'}$ au-dessus de Y'.

Contre-exemple 60.2 (Grothendieck, page 214, la Conclusion telle qu'elle est écrite ♦)**.** *Les conditions a) à e) ne déterminent pas la notion de degré. Si $\deg$ les vérifie, la classe $\deg^{\leq}$, où $\deg^{\leq}_0 = \deg_0$ et où f est de degré $n \geq 1$ s'il est de degré k pour un $1 \leq k \leq n$, les vérifie aussi. Dans la catégorie des ensembles finis, avec pour E les surjections, le degré usuel (toutes les fibres ont n éléments) et son $\deg^{\leq}$ sont deux notions distinctes : l'identité d'un point y est de degré 1 et 2.*

Démonstration. Pour $\deg^{\leq}$, a), c), d′) et e) se lisent sur $\deg$, d) vient de ce qu'un degré $k \geq 1$ est encore ≥ 1, et b) de ce que $1 \leq k_1 \leq n_1$ et $1 \leq k_2 \leq n_2$ donnent $k_1 + k_2 \leq n_1 + n_2$. Dans les ensembles finis, le degré usuel vérifie a) à e) : les fibres se conservent par changement de base et s'additionnent sur une somme, Y_n est l'ensemble des points dont la fibre a n éléments, une fibre non vide donne la surjectivité. L'identité d'un point n'y est pas de degré 2. □

Le pas de la page 214 qui cède est « donc par additivité, $X'_1 \to Y'$ est de degré $n - 1$ » : de $X' = Y' \sqcup X'_1$ de degré n et $Y' \to Y'$ de degré 1, la condition b) ne permet pas de soustraire. C'est une simplification, et elle suppose qu'un morphisme n'a qu'un degré. On ajoute donc la condition

(u) si $f : X \to Y$ est à la fois de degré m et de degré n, avec $m \neq n$, alors Y est vide (initial),

que le degré usuel des ensembles finis vérifie, et que $\deg^{\leq}$ ne vérifie pas.

Théorème 60.3 (d'après les pages 212 et 214, avec la condition (u) ♦)**.** *Soit C une catégorie à produits fibrés, finitairement extensive (sommes finies disjointes et universelles), dans laquelle tout monomorphisme est l'inclusion d'un sommande direct. Soit E une classe de morphismes contenant les identités, stable par composition, et dont tout changement de base d'un élément est un épimorphisme. Si $\deg$ vérifie a) à e) pour E et la condition (u), alors pour tout n, $\deg_n = \mathrm{Triv}_n(E)$. En particulier deux telles notions de degré coïncident.*

Démonstration. *Sens direct*, par récurrence sur n, en suivant la page 214. Pour $n = 0$, X est vide par e), et $g = \mathrm{id}_Y$ convient. Pour $n \geq 1$, f est dans E par d) ; on change de base par f lui-même : $q : X' = X \times_Y X \to X$ est de degré n par a). La diagonale est un monomorphisme, donc $X' = X \sqcup X'_1$, la diagonale étant une section de q. *Simplification* : on décompose $X = \coprod_j Z_j$ par d′) pour $r : X'_1 \to X$. Au-dessus de Z_j, la somme universelle donne $X' \times_X Z_j = Z_j \sqcup (X'_1 \times_X Z_j)$, de degré $1+j$ par b) et c), et de degré n par a) ; par (u), Z_j est vide pour $j \neq n-1$, donc $Z_{n-1} = X$ et r est de degré $n-1$. La récurrence fournit $h : W \to X$ dans E avec $X'_1 \times_X W \simeq [1, n-1]_W$; alors hf est dans E, et $X \times_Y W = X' \times_X W = W \sqcup (X'_1 \times_X W) \simeq [1, n]_W$.

Réciproque, que la page n'écrit pas. Soient $g : Y' \to Y$ dans E et $X \times_Y Y' \simeq [1, n]_{Y'}$, qui est de degré n par b) et c). On décompose $Y = \coprod_k Y_k$ par d′) pour f, et l'on pose $R_k = Y' \times_Y Y_k$. Au-dessus de R_k, le changement de base de f est de degré n (par Y') et de degré k (par Y_k) ; par (u), R_k est vide pour $k \neq n$. Alors $R_k \to Y_k$, changement de base de g, est un épimorphisme de source vide, et Y_k est vide dans une catégorie extensive. Donc $Y = Y_n$ et f est de degré n. □

Lean : `DegreeAxioms`, `DegreeAxioms.atMost`, `atMost_ne`, `Finite.degree_not_unique` pour le contre-exemple ; `cancel` (la simplification), `deg_imp_triv` (la récurrence de la page 214), `triv_imp_deg` (la réciproque), `deg_iff_triv` et `unique` pour le théorème. Le contre-exemple reste vrai si l'on ajoute les conditions (0) à (2), que les ensembles finis vérifient (corollaire ci-dessous) ; la réciproque n'utilise de E que l'universalité des épimorphismes, la récurrence que les identités et la composition. Ne sont pas formalisés : que les morphismes de descente effective universelle ont ces propriétés (leur stabilité par composition est un théorème de la théorie de la descente), et l'énoncé A(iii) qu'en tire la page pour les catégories multigaloisiennes.

Corollaire 60.4 (les ensembles finis, d'après les pages 212 et 214 ♦). *La catégorie des ensembles finis vérifie les conditions (0) à (2) de la page 212 : ses classes d'isomorphie forment un ensemble, elle a les limites projectives finies, et tout monomorphisme y est l'inclusion d'un sommande direct. Elle est finitairement extensive, et, E étant la classe des surjections, tout changement de base d'un élément de E est un épimorphisme. Par suite, une notion de degré qui vérifie a) à e) pour les surjections et la condition (u) est le degré usuel, et f est de degré n si et seulement si un changement de base surjectif le rend isomorphe à $[1, n]$. La notion $\deg^{\leq}$ du contre-exemple vérifie a) à e) et (0) à (2), mais pas (u).*

Démonstration. (0) : la catégorie est équivalente à son squelette, indexé par $\mathbf{N}$. (1) : les limites finies se calculent dans les ensembles. (2) : un monomorphisme $m : A \to B$ est injectif, et B est la somme de l'image de m et de son complémentaire. L'extensivité se lit dans les ensembles, le foncteur d'oubli préservant les produits fibrés et les sommes binaires et reflétant les isomorphismes. Si $g : Y' \to Y$ est surjectif, son changement de base $B \times_Y Y' \to B$ est surjectif, donc épimorphe. Le théorème s'applique au degré usuel, qui vérifie (u), et à toute autre notion vérifiant (u), d'où l'unicité ; si $\deg^{\leq}$ vérifiait (u), il serait égal au degré usuel, ce que le contre-exemple exclut. □

Lean : `Finite.conditions`, `Finite.mono_complement`, `Finite.surj_pullback_epi`, `Finite.deg_iff_triv`, `Finite.unique`, `Finite.not_uniqueDegree_atMost`. Les surjections sont ici les morphismes de descente effective universelle des ensembles finis ; cette identification n'est pas formalisée.

Les autres pistes de la cote, hors de portée de Lean pour l'instant :

Théorème (Grothendieck, pages 190 à 193, axiome R2 des domaines de ramification ♦). *Soit (R, r) un domaine de ramification sur S : un champ de catégories multigaloisiennes sur le site étale de S muni d'une réalisation géométrique continue r vers les schémas relatifs. Sous les axiomes R1, R3 et R4, l'axiome R2 (les sous-objets directs de X correspondent bijectivement aux parties ouvertes et fermées de $r(X)$) équivaut à la fidélité de r.*

◊ non vérifié en Lean

La proposition est énoncée page 193, une page rayée. La page n'en argumente que le sens « r fidèle $\Rightarrow$ R2 », en se ramenant à $X'' = X' \sqcup X_1$ et jusqu'à $r(X_1) = \emptyset$; la réciproque n'est démontrée ni sur la page ni ici. Les catégories multigaloisiennes sont les sommes finies de catégories galoisiennes au sens de SGA 1, exposé V [63] ; un domaine de ramification en fait un champ sur le site étale de S, et la réalisation r joue le rôle du foncteur fibre.

Énoncé (Grothendieck, page 197, proposition 6, homomorphismes de domaines de ramification, énoncée sans démonstration ♦). *Pour (R, r) défini par un schéma Z muni d'un groupe fini d'opérateurs G, $\mathrm{Hom}((R, r), (R', r'))$ est équivalente à la catégorie des couples (P', α), P' objet galoisien de R'_S de groupe G et α un G-isomorphisme $r'(P') \simeq Z$. En particulier, dans tout homomorphisme (φ, λ) de domaines de ramification, φ est pleinement fidèle.*

◊ non vérifié en Lean

Théorème (Grothendieck, pages 87 à 97, π_1 modéré et auto-intersection ♦). *Soit $\mathfrak{X}$ un schéma formel régulier dont la fibre spéciale X_o est une composante d'un diviseur à croisements normaux D. Le groupe fondamental modéré $\pi_1^t(\mathfrak{X}/D)$ est une extension centrale de $\pi_1^t(X_o/D'_o)$ par un quotient de μ^∞, dont la classe est la classe de Chern de l'auto-intersection de X_o dans $\mathfrak{X}$; pour $X_o = \mathbf{P}^1_k$ et D'_o vide, l'extension est $\mu_n(k)$, où n est la partie première à p du degré de $X_o \cdot X_o$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète : les lemmes 1 et 2 et l'argument de Kummer de la page 95 sont donnés, mais la page 91 porte « il faut prouver » et « à vérifier », et la raison de la divisibilité, page 93, est omise. Le cas local, au-dessus d'un schéma strictement local, est le corollaire 5.3 cité plus haut ; l'énoncé global, avec la classe d'extension égale à la classe de Chern du fibré normal $\mathcal{O}_{X_o}(X_o)$, n'a été trouvé ni dans SGA 1 ni dans la description logarithmique de l'inertie. En termes de champs, on peut la rapprocher de la μ_n-gerbe des racines n-ièmes du fibré normal (ci-dessous), dont la classe dans $H^2(X_o, \mu_n)$ est l'image de Kummer de la classe de ce fibré ; ce rapprochement est de l'édition.

Gerbes de Kummer et champs des racines (pages 199 et 200). Les revêtements modérés de (S, D) y sont construits comme les revêtements étales finis du champ associé à la gerbe dont les objets au-dessus de S' sont les familles d'équations a_i des D_i et les morphismes les familles ξ d'unités telles que $b_i = a_i \xi_i^{n_i}$; l'obstruction à une section globale est la classe des D_i. C'est aujourd'hui le champ des racines n_i-ièmes le long des D_i : Cadman (2007) [26] définit, dans la numérotation de la version arXiv, le champ des racines r-ièmes d'un couple (L, s) (définition 2.1), la racine r-ième de X le long d'un diviseur de Cartier effectif D (définition 2.3) et la μ_r-gerbe au-dessus de D que contient ce champ (définition 3.5). La correspondance entre revêtements modérés et revêtements étales de ce champ, que la page affirme, n'est pas démontrée ici.

Théorème (Grothendieck, pages 170 et 171, torseurs sous un groupe discret infini ♦). *Soit G un groupe discret, éventuellement infini, et soient C_1 à C_5 les classes de familles couvrantes fppf quasi-compactes, de type fini, quasi-finies, principales finies et principales finies étales. On a $H^1_{C_3} \simeq H^1_{C_2}$ en général ; $H^1_{C_2} \simeq H^1_{C_1}$ sur un anneau de Dedekind ; $H^1_{C_i} \simeq H^1(\hat{V}/V, -)$ pour $i = 1, 2, 3$ sur un anneau de valuation discrète complet V à corps résiduel algébriquement*

◊ non vérifié en Lean

clos ; $H^1_{C_5} \simeq H^1_{C_4} \simeq H^1_{C_3}$ et $H^1_{C_i}(V,-) \simeq H^1_{C_i}(k,-)$ sur un anneau local complet V de corps résiduel k.

Mathlib n'a pas les torseurs fppf ni le H^1 pour ces topologies. On se reportera aux notes de Grothendieck (29, lot 9, p. 170).

61 Cote 145 : l'exposant unité dans le groupe profini libre [64]

La cote 145 étudie les automorphismes du groupe profini libre $\hat\pi$ sur l_0, l_1, avec $l_\infty l_1 l_0 = 1$, qui préservent les sous-groupes de lacets L_0, L_1, L_∞ à des « rectificateurs » près. Les pages 34 et 35 caractérisent dans le cas discret, où l'exposant p vaut ± 1, les systèmes $(p, \sigma, 1, 1, 1)$ à rectificateurs triviaux : ce sont les six $(\operatorname{sg}\sigma, \sigma)$ du groupe Γ_P. La page conjecture (« Sans doute ») qu'il en va de même dans le cas profini, ramène la question à l'énoncé (14) ci-dessous et le laisse en « Exercice ! » (145, lot 2, p. 34). La lecture modernisée en donne une solution, qui est de l'édition, par un quotient diédral.

L'axe galoisien de ce texte. Les cotes 142, 145, 146 et 149 étudient l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur le groupe fondamental profini de $\mathbf{P}^1 \smallsetminus \{0,1,\infty\}$ et des espaces de modules $M_{g,\nu}$, que l'on décrit aujourd'hui par le groupe de Grothendieck–Teichmüller $\widehat{GT}$ (Drinfeld 1990, § 4 [44] ; Ihara 1991 [73]). Le groupe $\hat\pi$ de la page est le groupe profini libre $\hat F_2$, complété de $\pi_1(\mathbf{P}^1(\mathbf{C}) \smallsetminus \{0,1,\infty\})$; les sous-groupes L_0, L_1, L_∞ sont les sous-groupes d'inertie des trois pointes, et les « rectificateurs » sont les éléments par lesquels on conjugue l'image de chacun d'eux pour retrouver un $L_{\sigma(i)}$. Les droites tangentes aux points marqués de la section 74 sont les points base tangentiels de Deligne [41]. Le groupe $\mathfrak{S}_3$ des six substitutions anharmoniques, qui permute les trois pointes, revient aux sections 74, 50 et 42. Les énoncés de la cote 142 (catégorie de Teichmüller–Galois, image de Galois sur une seule courbe) et de la cote 149, non démontrés, sont encadrés à la fin de cette partie ; ceux de la cote 147 dans la partie « Topologie combinatoire, surfaces et cartes ».

Deux ensembles inédits de la même époque prolongent cet axe vers les espaces de modules : les *Teichmülleries* (cote 144, 1981–1983), avec une « Rétrospection sur les cartes cellulaires » de 1982 et les présentations du groupe des tresses B_3, et la *Structure à l'infini des $M_{g,\nu}$* (cote 147). Ce sont des textes suivis, jamais édités. Aucun énoncé de 144 n'est formalisé ici ; ceux de 147 sont dans la partie « Topologie combinatoire, surfaces et cartes ».

Conventions. Mathlib n'a ni le groupe profini libre ni les puissances d'exposant dans $\hat{\mathbf{Z}}$. Une relation vaut dans $\hat\pi$ si et seulement si elle vaut pour toute image de (l_0, l_1) dans tout groupe fini, et $p \in \hat{\mathbf{Z}}$ agit sur un groupe fini G par son résidu modulo $\operatorname{card} G$. On représente donc p par une famille compatible de résidus $p_n \in \mathbf{Z}/n$, $n \geq 1$, et l'on pose $x^p = x^{p_{\operatorname{card} G}}$ dans un groupe fini G. La relation (14) pour p signifie : pour tout groupe fini G et tous $x, y, z \in G$ tels que $zyx = 1$, on a $z^p y^p x^p = 1$.

Théorème 61.1 (Grothendieck, pages 34 et 35, l'exercice ♦). *Soit $p \in \hat{\mathbf{Z}}^*$. Si $l_\infty^p\, l_1^p\, l_0^p = 1$ dans le groupe profini libre sur l_0, l_1, avec $l_\infty l_1 l_0 = 1$, alors $p = 1$. Autrement dit, la relation (14) vaut pour p si et seulement si $p_n = 1$ pour tout $n \geq 1$.*

Démonstration. La réciproque est claire. Soit $N \geq 1$. Comme p_2 est inversible dans $\mathbf{Z}/2$, $p_2 = 1$, et par compatibilité le représentant $m \in [0, 2N[$ de p_{2N} est impair. Dans le groupe diédral D_N, d'ordre $2N$, soient x et y deux réflexions dont le produit $r = yx$ est une rotation d'ordre

64. Preuve vérifiée : `lean/Grothendieck/Folder145.lean`.

N, et $z = r^{-1}$, de sorte que $zyx = 1$. Comme m est impair, $x^m = x$ et $y^m = y$, donc $z^m y^m x^m = r^{-m} r = r^{1-m}$, qui vaut 1 si et seulement si $m \equiv 1 \pmod N$. La relation (14) dans D_N donne donc $p_N = 1$, image de p_{2N}. □

Remarque. L'énoncé tient sous une hypothèse plus faible : seule sert l'imparité de p, c'est-à-dire $p_2 = 1$, et non l'inversibilité de p aux nombres premiers impairs. L'imparité ne peut être omise, car $p = 0$ vérifie (14). La compatibilité de la famille ne sert qu'à passer de p_{2N} à p_N et à p_2.

La preuve vérifiée établit l'équivalence pour toute famille compatible impaire (`rel14_iff`), en déduit la forme de la page pour $p \in \hat{\mathbf{Z}}^*$ (`rel14_unit_iff`) et montre que $p = 0$ vérifie (14) (`rel14_zero`). Elle ne construit pas $\hat{F}_2$: la relation y est lue dans tous les groupes finis, ce qui revient au même par définition de la complétion profinie.

Remarque. La relation (14) a la forme de la relation hexagonale de $\widehat{GT}$ pour $f = 1$. Un élément de $\widehat{GT}$ est un couple (λ, f), $\lambda \in \hat{\mathbf{Z}}^*$, f dans l'adhérence du groupe dérivé de $\hat{F}_2$, soumis entre autres à $f(z,x)\, z^m f(y,z)\, y^m f(x,y)\, x^m = 1$ pour $xyz = 1$ et $m = (\lambda - 1)/2$ (relation (5) chez Furusho 2010 [53], d'après Drinfeld [44]). Pour $f = 1$, elle devient $z^m y^m x^m = 1$ sous $xyz = 1$: l'ordre des facteurs est renversé par rapport à (14). Le même quotient diédral montre que ses seules solutions sont $m = 0$ et $m = -1$, c'est-à-dire $\lambda = \pm 1$: pour m impair, deux réflexions x, y et $z = (xy)^{-1}$ donnent $(yx)^{m+1} = 1$, d'où $m \equiv -1$ modulo tout N ; pour m pair, $z^m = 1$ donne $m \equiv 0$; et $m = -1$ convient, $z^{-1} y^{-1} x^{-1} = (xyz)^{-1}$. Cet argument est de l'édition et n'est pas vérifié en Lean. Il rejoint le cas discret de la page 35, où $p = \pm 1$.

Ne sont pas démontrés ici : la conséquence pour $S\hat{\hat{\mathcal{E}}}$ (les systèmes à rectificateurs triviaux sont les six $(\operatorname{sg}\sigma, \sigma)$ de Γ_P), qui demande le groupe Γ_P et la réduction de la page aux σ paires, ni le cas discret de la page 35. Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Définition (Grothendieck, pages 2 à 16, catégorie de Teichmüller–Galois ♦). La catégorie de Teichmüller–Galois a pour objets les courbes anabéliennes de tous types (g, ν) et pour flèches les complétés profinis des classes d'isotopie d'applications étales finies ; elle est obtenue par une complétion profinie des catégories dont les groupes d'automorphismes vérifient la condition de finitude $(*)$, l'image du stabilisateur de chaque flèche $u : X \to Y$ étant d'indice fini dans $\mathrm{Aut}(Y)$. Chaque groupe d'automorphismes y est le groupe de Teichmüller profini ; la construction est algébrique, invariante par extension de corps algébriquement clos de caractéristique 0, et $\mathrm{Aut}(k)$ y opère.

Les flèches de cette catégorie relient des types (g, ν) différents par des applications étales finies, et non par les inclusions de sous-surfaces et les recollements de la tour de Teichmüller. Sur cette tour, Hatcher, Lochak et Schneps font agir le sous-groupe Λ de $\widehat{GT}$ défini par une relation de plus, et montrent que Λ s'injecte dans les automorphismes extérieurs spéciaux de la tour (2000, théorèmes A à C [70]). Dans la catégorie de la page, l'action de $\mathrm{Aut}(k)$ est l'analogue, pour tous les types, de l'action de Galois sur $\hat{\pi}_1(M_{0,4}) = \hat{F}_2$ de la section 61. Mathlib n'a pas la complétion profinie des catégories ni les groupes de Teichmüller. On se reportera aux notes de Grothendieck (142, lot 1, p. 2).

Théorème (Grothendieck, pages 167 et 175 à 180, monodromie modérée à plusieurs paramètres ♦). *Soient S un schéma strictement local de dimension quelconque et $\bar{X}$ un S-schéma projectif et plat, de fibre fermée à croisements normaux hors de la codimension 2, lisse à bord à croisements normaux relatifs au-dessus d'un ouvert $U \subset S$. L'image de $\pi_1(U)$ dans $\mathrm{Out}(\pi_1^{(p')})$ d'une fibre géométrique est un groupe abélien d'ordre premier à p, de rang au plus*

◊ non vérifié en Lean

le nombre ν de points doubles en dimension relative 1.

Les feuillets en esquissent une démonstration incomplète (pages 175 à 180), où le lemme 3.1, sur la courbe nodale verselle, n'est pas démontré. Les hypothèses (a) à (d) reposent sur des lectures incertaines de la page 167. Sur une base de dimension 1, la finitude de l'image de l'inertie sauvage dans $\mathrm{Out}(\pi_1^{(p')})$ d'une fibre géométrique, pour toute variété sur un corps complet de valuation discrète, est le théorème 2.1 de Kisin (2000) [83], démontré par les altérations et non par réduction aux courbes. En dimension relative 1, la lecture y voit la description de la monodromie le long d'une courbe stable dégénérée par les twists de Dehn des points doubles, élevés aux multiplicités n_i des équations locales $xy = t^{n_i}$; en dimension relative ≥ 2, l'énoncé encadré reste ouvert ici. Quand $S \smallsetminus U$ est un diviseur à r branches à croisements normaux, le groupe fondamental modéré de U au voisinage du point fermé est $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)^r$ (SGA 1, exposé XIII, appendice I, corollaire 5.3 [63]), abélien d'ordre premier à p ; la section 60 en calcule la fonctorialité. Mathlib n'a pas la monodromie modérée. On se reportera aux notes de Grothendieck (34, lot 9, p. 167).

Contre-exemple (pages 36 à 39, le lemme du Complément ♦). *Le lemme de la page 36, qui omet l'hypothèse de $(*)$ sur les groupes fondamentaux, est faux pour les courbes hyperboliques de types $(1,1)$ et $(1,2)$, et réduire l'ouvert V n'écarte pas le cas exceptionnel $\operatorname{card} I = 1$. L'extension que la page annonce aux polycourbes hyperboliques de toute dimension repose sur un plongement dans une variété semi-abélienne, qui manque en dimension 2 : la courbe elliptique universelle privée de sa section nulle, au-dessus de $Y(N)$, n'en a pas.*

◊ non vérifié en Lean

Pour les courbes, l'énoncé de la piste, en caractéristique 0 sur un corps algébriquement clos (deux morphismes $f, g : X \to Y$ vers une courbe hyperbolique, f dominant, qui induisent le même homomorphisme extérieur des groupes fondamentaux étales profinis, sont égaux), n'est pas démontré ici ; l'édition ferme les types $(1,1)$ et $(1,2)$ par l'hypothèse de $(*)$. Mathlib n'a pas le groupe fondamental étale des courbes hyperboliques. On se reportera aux notes de Grothendieck (149, lot 2, p. 21).

Théorème (Grothendieck, pages 153 à 155, 1-asphéricité locale ♦). *Soit $f : X \to S$ plat sur un trait strictement local, de fibre fermée X_0 localement d'intersection complète, dont le lieu non lisse est de codimension ≥ 2 dans X_0. Alors f est localement 1-asphérique pour les premiers $\neq p$; si f est propre, la spécialisation $H^1(X_0, G) \to H^1(X_{\bar\eta}, G)$ est bijective pour tout groupe fini G d'ordre premier à p.*

◊ non vérifié en Lean

Démonstration de la page (pages 153 à 155). Au n° 5.5, f étant localement 1-acyclique aux générisations strictes de x, la 1-asphéricité locale en x pour un groupe fini G d'ordre premier à p se ramène à (5.5.1), $H^i(\bar V, G) \simeq H^i(V_{\bar\eta}, G)$ pour $i \leq 1$ (p. 153), puis à (5.5.2), $H^i(V(h), G) = 0$ pour $i \leq 1$ (p. 154). La page affirme sans démonstration (« On sait ») que (5.5.2) vaut aux points d'intersection complète de dimension ≥ 3, et la lecture le rapporte à la pureté de SGA 2. Pour f plat, cela revient à X_0 d'intersection complète de dimension ≥ 2 en x, et le cas lisse traite les autres points, d'où le théorème 5.6 et, sans autre argument, l'assertion sur H^1.

◊ non vérifiée en Lean

Conjecture (D'après les pages 94, 95 et 98 à 101, forme regroupée par l'édition, image de Galois sur une seule courbe ♦). *Soient X une courbe algébrique anabélienne sur un corps K de type fini sur $\mathbf{Q}$ et Θ un automorphisme du groupoïde fondamental profini $\hat\Pi_1(X, I)$ qui fixe les points base. Si Θ se relève à $\hat\Pi_1(X', I')$ pour tout revêtement étale fini X' de X défini sur K, respecte les noyaux de $\hat\pi_1(X', x') \to \hat\pi_1(Y, f(x'))$ pour tout K-morphisme $f : X' \to Y$, est compatible aux morphismes entre revêtements et vérifie la condition des lacets avec un seul multiplicateur, alors Θ provient de $\mathrm{Gal}(\bar K / K)$. Ces conditions sont nécessaires.*

La page 95 conjecture suffisantes les conditions de relèvement et de noyaux ; leur regroupement avec les conditions des pages 98 à 101 est de l'édition. En termes actuels, c'est une forme de la question d'Ihara et de la conjecture d'Oda–Matsumoto (I/OM) attachée à une seule courbe et à ses revêtements : I/OM demande si $\mathrm{Gal}(\overline{K}/K)$ est le groupe des automorphismes du foncteur groupe fondamental géométrique sur une catégorie de K-variétés. Topaz (2018) [119] en démontre une forme renforcée, pour le quotient modulo ℓ abélien-par-central de ce groupe, sur un corps parfait infini de caractéristique $\neq \ell$ et pour toute catégorie de variétés assez grosse au sens de son § 1.7 ; cette forme porte sur une catégorie de variétés, non sur une courbe et ses revêtements, et ne fait pas intervenir de condition d'inertie. Les variantes tripodes finies de Pop (2019) [107] supposent une base de dimension au moins deux, munie d'un nombre fini d'applications rationnelles dominantes vers $\mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$; elles ne couvrent donc pas les revêtements d'une seule courbe, et c'est la condition des lacets de la page qui devrait en tenir lieu. Pour $X = \mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$, la condition des lacets est celle des sous-groupes L_0, L_1, L_∞ de la section 61. Mathlib n'a pas les groupoïdes fondamentaux profinis des courbes. On se reportera aux notes de Grothendieck (142, lot 5, p. 94).

Conjecture (Grothendieck, pages 72 à 77 et 84 à 93, spécialisation vers une pointe ♦). *Soient $U = X \setminus T$ une courbe hyperbolique relative sur un trait et f une section rationnelle qui rencontre la section de pointe g_{i_0} dans la fibre spéciale avec la multiplicité n. L'inertie s'envoie sur n fois le sous-groupe de lacet L_{i_0} de cette pointe, et elle agit trivialement exactement quand f se prolonge.*

Mathlib n'a pas la spécialisation des sections des courbes hyperboliques relatives. On se reportera aux notes de Grothendieck (149, lot 4, p. 72).

Partie 24

Polyèdres et géométrie convexe

62 Cote 70 : l'icosaèdre sur $\mathbf{Z}[\alpha]$, fidèle en toute caractéristique, et sa conique modulo 5 [65]

La cote 70, *Réalisations géométriques de structures combinatoires (vieilles rédactions)*, compte cent vingt-cinq pages. Sa section VII, sous la chemise de la page 73, écrit l'icosaèdre régulier sur l'anneau $\mathbf{Z}[\alpha] = \mathbf{Z}[x]/(x^2+x-1)$ par trois réflexions dans le repère des sommets $(s_0, s_1 - s_0, s_2 - s_0, s_3 - s_0)$. Les pages 74 et 75 donnent les générateurs et les douze sommets (70, lot 4, p. 74, 70, lot 4, p. 75), les pages 89 à 92 le centre et l'antipodisme ι, avec sa forme en caractéristique 2 (70, lot 5, p. 91). Les pages 93 et 94 veulent établir, « sur un corps de base quelconque », que trois sommets distincts ne sont jamais alignés et qu'aucun sommet n'est dans le plan d'une face qui ne le contient pas ; elles traitent les droites issues de s_0 et le plan $z = 0$ de la face (s_0, s_1, s_2), et invoquent l'homogénéité pour le reste (70, lot 5, p. 93, 70, lot 5, p. 94). La page 95 donne la fonction quadratique invariante q, les pages 101 et 102 sa partie quadratique q_0 et ses discriminants (70, lot 6, p. 101). Le tableau « Directions remarquables » de la page 78 compte 6 directions de sommets, 15 d'arêtes et 10 de plans de faces, $31 = 5^2 + 5 + 1$, dit que « les 6 directions de sommets correspondent à la conique » et écrit $125 = 1 + 24 + 60 + 40$, avec « deux icos. » (70, lot 4, p. 78). On démontre ici l'énoncé de la page 78 sur $\mathbf{F}_5$, les incidences des pages 93 et 94 sur tout anneau non nul où $\alpha^2 + \alpha = 1$, donc en toute caractéristique, 2 et 5 comprises, et, en fin de section, les formules universelles des pages 9 à 25 avec le critère d'ordre de la page 67 pour les ordres 3, 4 et 5.

Conventions. R est un anneau commutatif, $\alpha \in R$, $\alpha' = -1 - \alpha$, et l'on écrit les points de R^3 en coordonnées (x, y, z). Les générateurs sont

$$\sigma_0(x,y,z) = \big(1-(x+y+z), y, z\big), \quad \sigma_1(x,y,z) = (y+\alpha' z, x-\alpha' z, z), \quad \sigma_2(x,y,z) = (x,z,y),$$

et $\iota(x,y,z) = (\alpha' - x, 1-\alpha'-y, 1-\alpha'-z)$. Les douze sommets sont, dans cet ordre, $s_0 = 0$, $s_1 = e_1$, $s_2 = e_2$, $s_3 = e_3$, $s_3' = (\alpha', -\alpha', 1)$, $s_3'' = (0, -\alpha', 1)$ et leurs images par ι (figure 15). On pose

$$q_0 = x^2 + y^2 + z^2 - \alpha yz + zx + xy, \qquad q = q_0 - (x+y+z),$$

et φ la forme polaire de q_0, de matrice $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & -\alpha \\ 1 & -\alpha & 2 \end{pmatrix}$. Les trente arêtes sont les paires de sommets à distance $q_0 = 1$ sur $\mathbf{Q}(\sqrt{5})$, listées dans le fichier ; les vingt faces sont les triangles d'arêtes. Sur R, on dit que p est sur la droite (r,u) s'il existe $a \in R$ avec $p - r = a(u-r)$, et dans le plan (r,u,w) s'il existe $s, t \in R$ avec $p - r = s(u-r) + t(w-r)$; sur un corps, et pour $r \neq u$, c'est l'alignement et la coplanarité usuels. Sur $\mathbf{F}_5$, la seule racine de $x^2 + x - 1$ est 2, de sorte que la réduction modulo 5 de la réalisation est celle de $\alpha = 2$, $\alpha' = 2$; on note alors $o = (1,2,2)$ et $\bar{s} = s - o$ pour un sommet s.

65. Preuve vérifiée : `lean/Grothendieck/Folder70.lean`.

Énoncé (Pages 74, 75, 91, 94 et 101, sur un anneau quelconque)**.** *Supposons* $\alpha^2+\alpha-1=0$ *dans* R*.*

1. *Les douze sommets annulent* q*.*
2. σ_0*,* σ_1*,* σ_2 *permutent les douze sommets, par des permutations de* $\{0,\dots,11\}$ *qui ne dépendent pas de* R*.*
3. *Pour chacune des trente arêtes* $\{s,s'\}$*,* $q_0(s'-s)=1$*.*
4. *Les neuf sommets autres que* s_0*,* s_1*,* s_2 *ont une coordonnée* z *inversible :* 1*,* $1-\alpha'=2+\alpha$ *ou* $-\alpha'=1+\alpha$*.*
5. *Sans hypothèse sur* α*, si* $2=0$ *dans* R*,* ι *est la translation de vecteur* (α',α,α)*.*

Démonstration. Chaque point est une identité polynomiale en α et en les coordonnées, vraie modulo $\alpha^2+\alpha-1$: on l'écrit comme combinaison de la relation $\alpha^2+\alpha-1=0$, de coefficient $-2-\alpha$ ou $-1-\alpha$ pour $q(\iota s_0)$, $q(\iota s_1)$, $q(\iota s_2)$, $q(\iota s_3)$, ±1 pour σ_1, $-\alpha$ ou $1+\alpha$ pour quatre des arêtes, nul ailleurs. Pour le point 4, $(2+\alpha)(1-\alpha)=1$ et $(1+\alpha)\alpha=1$. Pour le point 5, la première coordonnée de $\iota(p)-p-(\alpha',\alpha,\alpha)$ vaut $-2x$, les deux autres $2(1-y)$ et $2(1-z)$. □

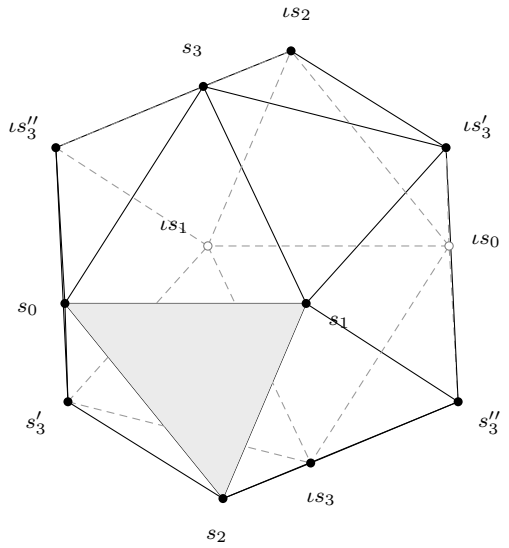


FIGURE 15 – Les douze sommets des pages 74 et 75 sur $\mathbf{R}$, pour $\alpha=(\sqrt{5}-1)/2$, dessinés par l'édition dans la métrique de q_0 : la face (s_0,s_1,s_2) est grisée, les arêtes cachées sont en tirets. Les trente arêtes sont les paires à distance $q_0=1$, et ι envoie chaque sommet sur le sommet opposé. Grothendieck dessine l'icosaèdre en perspective, puis projeté dans un triangle, à la page 74 (70, lot 4, p. 74).

Énoncé (Pages 93 et 94, fidélité en toute caractéristique ♦)**.** *Soit* R *un anneau commutatif non nul où* $\alpha^2+\alpha-1=0$*. Alors*

1. *les douze sommets sont distincts ;*
2. *pour trois sommets distincts* s,s',s''*, le point* s'' *n'est pas sur la droite* (s,s')*;*
3. *pour une face* (a,b,c) *et un sommet* m *distinct de* a*,* b*,* c*, le point* m *n'est pas dans le plan* (a,b,c)*.*

Démonstration. Les applications σ_k sont affines : si $p-r = s(u-r)+t(w-r)$, alors $\sigma_k p-\sigma_k r = s(\sigma_k u-\sigma_k r)+t(\sigma_k w-\sigma_k r)$, coordonnée par coordonnée. D'après l'énoncé précédent, un mot w en les σ_k envoie le sommet d'indice i sur le sommet d'indice $\pi_w(i)$, où π_w est le mot correspondant en les trois permutations, qui est une permutation de $\{0,\dots,11\}$. Un mot transporte donc l'égalité de deux sommets, l'appartenance d'un sommet à la droite de deux autres, et à un plan de trois autres.

C'est l'homogénéité que la page invoque, rendue explicite par deux tables. Pour toute paire (i,j) d'indices distincts, la table `pairWord` donne un mot w tel que $\pi_w(i)=0$ et $\pi_w(j)\in\{1,5,6\}$, c'est-à-dire qui envoie (s_i,s_j) sur (s_0,s_1), (s_0,s_3'') ou $(s_0,\iota s_0)$; pour toute face (a,b,c), la table `faceWord` donne un mot qui l'envoie, dans l'ordre, sur (s_0,s_1,s_2). Ces $132+20$ propriétés portent sur des permutations de $\{0,\dots,11\}$ et sont vérifiées par le noyau de Lean (`decide +kernel`).

Il reste les cas de base. Comme $s_0=0$, le sommet s_k est sur la droite (s_0,s_j) si et seulement si $s_k = a\,s_j$ pour un $a\in R$, ce qui annule les trois mineurs d'ordre 2 de la matrice de colonnes s_k, s_j. Pour $j\in\{1,5,6\}$ et chacun des trente $k\neq 0,j$, l'un de ces mineurs est une unité de $\mathbf{Z}[\alpha]$, à savoir ±1, $\pm(1+\alpha)$, $\pm(2+\alpha)$ ou $\pm(3+2\alpha)$, d'inverses $\pm\alpha$, $\pm(1-\alpha)$ et $\pm(2\alpha-1)$. Pour chaque cas, une identité $1 = u\,(m_{rs}) + c\,(\alpha^2+\alpha-1)$, où m_{rs} s'écrit à partir des égalités de coordonnées, donne $1=0$, ce qui est exclu dans un anneau non nul. Le point 2 s'en déduit : si s'' est sur la droite (s,s'), le mot de la paire (s,s') amène s'' sur un sommet s_k de la droite (s_0,s_j), avec $k\neq 0,j$ puisque π_w est injective. Pour le point 1, le même mot ramène une égalité $s_i=s_j$ à $s_{j'}=0$ pour $j'\in\{1,5,6\}$; or s_1 a pour première coordonnée 1, s_3'' pour troisième coordonnée 1, et ιs_0 pour troisième coordonnée l'unité $2+\alpha$. Pour le point 3, le mot de la face amène m sur un sommet d'indice au moins 3 dans le plan (s_0,s_1,s_2), c'est-à-dire de coordonnée z nulle, contre le point 4 de l'énoncé précédent. □

Théorème 62.1 (D'après la page 78, forme complétée par l'édition, la conique de $\mathbf{P}^2(\mathbf{F}_5)$ ♦). *Sur $\mathbf{F}_5$, avec $\alpha=2$:*

1. *$2o=(\alpha',1-\alpha',1-\alpha')$, o est fixe par σ_0, σ_1, σ_2 et ι, et $q(o)=0$;*
2. *les douze sommets sont isotropes pour q_0 centrée en o : $q_0(\bar s)=0$;*
3. *les vecteurs non nuls isotropes de q_0 sont les douze $\bar s$ et leurs doubles $2\bar s$; ces vingt-quatre vecteurs sont distincts ;*
4. *un point de $\mathbf{P}^2(\mathbf{F}_5)$ est sur la conique $q_0=0$ si et seulement si c'est l'une des six directions $\bar s_0,\dots,\bar s_3''$;*
5. *les six directions de sommets, les quinze directions $s'-s$ d'arêtes choisies et les dix directions $\bar a+\bar b+\bar c$ des faces 0 à 9 sont les trente et un points de $\mathbf{P}^2(\mathbf{F}_5)$, chacun une fois ; toute arête et toute face donne l'une de ces directions, tout sommet l'une des six ;*
6. *la direction $\bar a+\bar b+\bar c$ d'une face (a,b,c) est φ-orthogonale à $b-a$ et à $c-a$, c'est-à-dire au plan de la face ;*
7. *par une direction d'arête passent exactement deux tangentes à la conique, par une direction de face aucune ; q_0 prend la valeur 1 ou 4 sur 60 vecteurs, la valeur 2 ou 3 sur 40.*

Démonstration. L'unicité de la racine 2 se vérifie sur les cinq éléments de $\mathbf{F}_5$. Le reste porte sur les 125 vecteurs de $\mathbf{F}_5^3$ et sur des listes finies de sommets, d'arêtes et de faces, et chaque point est vérifié par le noyau de Lean. Pour le point 5, l'application qui envoie chacun des trente et un représentants sur son point de $\mathbf{P}^2(\mathbf{F}_5)$ est injective, car aucun représentant n'est multiple d'un

autre, et surjective, car tout vecteur non nul est multiple de l'un d'eux ; on en tire aussi que $\mathbf{P}^2(\mathbf{F}_5)$ a 31 points. Le point 4 est l'énoncé, vérifié sur les 124 vecteurs non nuls, que $q_0(v) = 0$ si et seulement si v est multiple d'un des six représentants de sommets. Au point 7, la tangente à la conique au point $\bar{s}$ est la droite $\varphi(\bar{s}, \cdot) = 0$, et l'on compte, pour chaque représentant, les six sommets dont la tangente le contient. □

Remarque. La page 78 donne le tableau des points 4 et 5 et le décompte $125 = 1 + 24 + 60 + 40$; les points 6 et 7 sont de l'édition. La vérification confirme ce tableau et la lecture : la réduction modulo 5 place les sommets sur le cône isotrope de sommet o, les six directions de sommets remplissent la conique, et les $6 + 15 + 10$ directions sont les 31 points du plan. L'explication des quinze directions d'arêtes par les points extérieurs et des dix directions de faces par les points intérieurs, que la piste laissait à l'édition parce que les mots de la page y sont incertains, est démontrée au point 7, avec la définition par les tangentes ; les classes $\{1, 4\}$ et $\{2, 3\}$ des valeurs de q_0 en sont la forme arithmétique, et donnent le décompte $60 + 40$. Les vingt-quatre vecteurs isotropes non nuls sont les sommets de l'icosaèdre et de son homothétique de rapport 2 : ce sont les « deux icos. » de la page. Pour la fidélité, la démonstration n'utilise ni corps ni calcul de normes au-delà de trente mineurs inversibles : elle vaut sur tout anneau non nul où $\alpha^2 + \alpha = 1$, donc en caractéristique 2 (sur une $\mathbf{F}_4$-algèbre) et 5. L'argument d'homogénéité de la page suffit, une fois les deux tables de mots vérifiées, et la marge « c'est en fait faux en car. 2 ! » ne vise donc ni le non-alignement ni le plan de la face. Le vecteur de translation de ι en caractéristique 2 est $(\alpha', \alpha, \alpha)$, et non le $(\alpha', 1, 1)$ lu sur la page 91.

Énoncé (Pages 75 et 87, l'ordre du groupe ♦). *Soit R un anneau commutatif non nul où $\alpha^2 + \alpha - 1 = 0$. Le groupe G des permutations de R^3 engendré par σ_0, σ_1, σ_2 est d'ordre 120 ; il agit fidèlement sur les douze sommets, et le groupe des permutations de $\{0, \ldots, 11\}$ engendré par les trois permutations du premier énoncé est lui aussi d'ordre 120.*

Démonstration. Pour les permutations, une table de 120 mots en π_0, π_1, π_2, de longueur au plus 15, obtenue par un parcours en largeur, donne 120 permutations distinctes, et une seconde table dit sur quel mot de la première la multiplication à gauche par chaque π_k envoie chacun d'eux. Comme les π_k sont des involutions, l'ensemble de ces 120 permutations contient 1 et est stable par multiplication à gauche par les générateurs et leurs inverses : il contient le groupe engendré, qui le contient. Ces vérifications sont faites par le noyau de Lean (`decide +kernel`). Pour G, on compare les deux morphismes du groupe libre à trois générateurs, vers G et vers le groupe des permutations des indices. Par récurrence sur les mots, l'image g d'un mot dans G envoie le sommet d'indice i sur celui d'indice $\pi(i)$, où π est l'image du même mot, et g est affine, $g(x, y, z) = g(0) + x\,(g(e_1) - g(0)) + y\,(g(e_2) - g(0)) + z\,(g(e_3) - g(0))$, propriété stable par composition. Si $g = 1$, π fixe tous les indices, puisque les sommets sont distincts ; si $\pi = 1$, g fixe $s_0 = 0$, $s_1 = e_1$, $s_2 = e_2$, $s_3 = e_3$, donc $g = 1$. Les deux noyaux coïncident, et G est isomorphe au groupe des permutations. □

Voir `card_icoPermGroup` et `card_icoGroup` dans `Folder70.lean`. La page 87 admet l'ordre 120 (« si nous admettons que G est d'ordre 120 ») ; il vaut sur tout anneau non nul où $\alpha^2 + \alpha = 1$, caractéristiques 2 et 5 comprises. Ne sont pas démontrés ici : que G soit le groupe de Coxeter $H_3 \simeq \mathfrak{A}_5 \times \mathbf{Z}/2$, et que les trente paires listées soient l'orbite de l'arête $\{s_0, s_1\}$ (le fichier montre seulement que les générateurs permutent les sommets et que ces paires sont à distance $q_0 = 1$) ; la quadrique des pages 101 et 102 fait l'objet de l'énoncé suivant ; les relations $\Delta = \alpha\Delta'$ et $\Phi' = (2\alpha - 1)\Phi$ de la page 76 ; la proposition « régulière ⇒ fidèle » de la page 109.

Exemple 62.2 (Grothendieck, pages 101, 102 et 106, la quadrique de l'icosaèdre ♦). Soit R un anneau commutatif où $\alpha^2+\alpha-1=0$, et $q=x^2+y^2+z^2-\alpha yz+zx+xy-(x+y+z)$.

1. q est invariante par σ_0, σ_1, σ_2 et s'annule aux douze sommets ; toute fonction quadratique $F=ax^2+\cdots+k$ qui s'annule en $s_0, s_1, s_2, s_3, s'_3, s''_3, \iota s_0, \iota s_1, \iota s_2$ est égale à $a\,q$. La quadrique passant par les sommets est donc unique.
2. Sa partie quadratique q_0 a pour demi-discriminant $\delta'(q_0)=1$; sa matrice polaire $\left(\begin{smallmatrix} 2 & 1 & 1 \\ 1 & 2 & -\alpha \\ 1 & -\alpha & 2 \end{smallmatrix}\right)$ a pour déterminant 2.
3. La quadrique projective $Q(x,y,z,t)=q_0(x,y,z)-(x+y+z)\,t$ a pour discriminant $-\alpha-3$, de norme $(-\alpha-3)(-\alpha'-3)=5$; il est inversible si et seulement si 5 l'est, et alors le seul zéro commun des quatre dérivées partielles de Q est 0 : Q est lisse.
4. Si $5=0$ et $\alpha=2$, les zéros communs des dérivées partielles sont les multiples de $(1,2,2,1)$, qui est sur Q : la quadrique est un cône de sommet le centre $o=(1,2,2)$. Sur un corps, Q a un point singulier si et seulement si la caractéristique est 5.

Démonstration. L'invariance se vérifie en développant $q\circ\sigma_k$, pour tout α. Pour l'unicité, une fonction quadratique a dix coefficients, et ses valeurs aux sommets sont des formes linéaires en ces coefficients. Sur les neuf sommets cités, le mineur d'ordre 9 pris hors de la colonne de x^2 vaut $13\alpha+21$, unité de $\mathbf{Z}[\alpha]$ d'inverse $13\alpha-8$ (de norme -1) : chacun des neuf coefficients restants, diminué de a fois le coefficient correspondant de q, est une combinaison à coefficients dans $\mathbf{Z}[\alpha]$ des neuf valeurs, par exemple, pour la fonction F, $d+a=F(s_1)-F(s_0)$ et $k=F(s_0)$. La page fait le même calcul par l'invariance (« c'est clair ») ; ici l'invariance n'est pas même nécessaire, et l'énoncé vaut sur tout anneau, sans diviser par rien.

Le demi-discriminant de $ax^2+by^2+cz^2+uyz+vzx+wxy$ est le polynôme $4abc+uvw-au^2-bv^2-cw^2$, dont le double est le déterminant de la matrice polaire. Pour q_0, il vaut $4-\alpha-\alpha^2-1-1=2-(\alpha^2+\alpha)=1$: c'est la « merveille » de la page 101, et elle vaut aussi en caractéristique 2. Le déterminant d'ordre 4 de la matrice (22), développé selon la première ligne, vaut $\alpha^2-4=-\alpha-3$. Comme $(-\alpha-3)(\alpha-2)=5$ et $(-\alpha-3)^2=5(\alpha+2)$, le discriminant divise 5 et 5 divise son carré, de sorte que l'un est inversible si et seulement si l'autre l'est. Les lignes de la matrice sont les dérivées partielles de Q (et $v\cdot Mv=2Q(v)$) ; une matrice de déterminant inversible n'a pas de noyau, d'où la lissité. En caractéristique 5, $\alpha^2+\alpha-1=(\alpha-2)^2$, donc $\alpha=2$ sur un corps ; le système $Mv=0$ se réduit alors, modulo 5, à $x=t$, $y=z=2t$, et $Q(1,2,2,1)=1+4+4-8+2+2-5=0$. □

Remarque. Voir `q_sigma`, `quadric_unique`, `halfDisc_q`, `det_qMat4`, `norm_disc`, `isUnit_det_qMat4_iff`, `qHom_smooth`, `qMat4_ker_char_five` et `qHom_singular_iff` dans `Folder70.lean`. La lissité est formalisée par l'absence de zéro commun non nul des dérivées partielles, lues sur la matrice polaire ; on n'a pas construit le schéma projectif ni utilisé le critère jacobien de Mathlib. L'unicité est démontrée parmi les fonctions quadratiques affines, non parmi les quadriques projectives, ce qui revient au même ici puisque Q est l'homogénéisée de q. Que le cône de caractéristique 5 soit un cône sur une conique lisse découle de $\delta'(q_0)=1$ et de `conic_iff` plus haut, mais n'est pas énoncé comme un théorème séparé.

Les pages 9 à 25 écrivent toute réalisation affine régulière par réflexions du polytope $\{p_1,\dots,p_n\}$ dans le repère des sommets $(s_0,\dots,s_{n+1})$, avec n paramètres $\alpha_0,\dots,\alpha_{n-1}$ (70, lot 1, p. 15, 70, lot 2, p. 23) ; la page 67 énonce pour $n=2$, sans démonstration, « $\rho_s^p=\mathrm{id}\iff F_p(\alpha)=0$ » (70, lot 4, p. 67). En coordonnées barycentriques $(t_0,\dots,t_{n+1})$ relatives

à ce repère, sur un anneau commutatif R, on pose $\ell_i = t_i - t_{i+1} + (1+\alpha_i)(t_{i+2} + \cdots + t_{n+1})$, $\sigma_i = \mathrm{id} + \ell_i \otimes (s_{i+1} - s_i)$ pour $0 \le i \le n$, et $w_k = s_{k+1} - s_k$.

Théorème 62.3 (D'après les pages 19, 23 à 25 et 67, forme générale de l'édition, formules universelles ♦). *Soit R un anneau commutatif, $n \ge 1$ et $\alpha_0, \dots, \alpha_{n-1} \in R$.*

1. *Quels que soient les α_i, $\sigma_i^2 = 1$ et $\sigma_i\sigma_j = \sigma_j\sigma_i$ pour $i+2 \le j \le n$; σ_i conserve $t_0 + \cdots + t_{n+1}$, $\sigma_i s_i = s_{i+1}$, $\sigma_i s_j = s_j$ pour $j < i$, et $\sigma_i s_j = s_j + (1+\alpha_i)w_i$ pour $i+2 \le j \le n+1$.*
2. *Pour $k \le n-1$, l'image de $\sigma_k\sigma_{k+1} - 1$ est contenue dans le plan $\langle w_k, w_{k+1}\rangle$, et $(t-1)(t^2 - \alpha_k t + 1)$ annule $\sigma_k\sigma_{k+1}$.*
3. *Si R est non nul, $\sigma_k\sigma_{k+1}$ est d'ordre exactement 3, 4 ou 5 si et seulement si, respectivement, $\alpha_k = -1$, $\alpha_k = 0$ ou $\alpha_k^2 + \alpha_k - 1 = 0$.*

Démonstration. Comme $\ell_i(w_i) = -2$, $\ell_i(\sigma_i x) = -\ell_i(x)$, d'où $\sigma_i^2 = 1$. Pour $i+2 \le j \le n$, $\ell_i(w_j) = (1+\alpha_i)(1-1) = 0$ et $\ell_j(w_i) = 0$, de sorte que $\sigma_i\sigma_j x = x + \ell_i(x)w_i + \ell_j(x)w_j = \sigma_j\sigma_i x$. Les coordonnées de w_i sont de somme nulle, et le tableau se lit sur les valeurs $\ell_i(s_j)$.

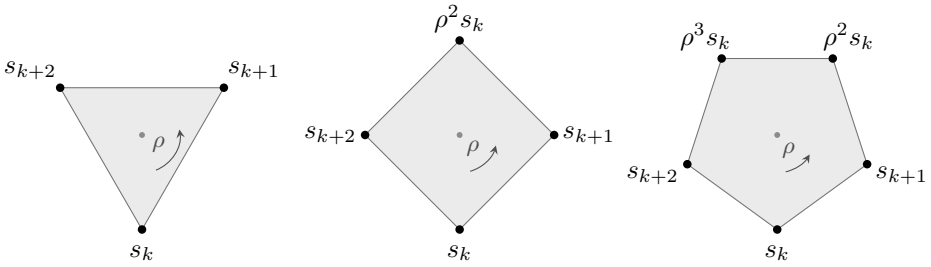
Soit $\rho = \sigma_k\sigma_{k+1}$. On a $\rho x = x + \ell_k(\sigma_{k+1}x)\, w_k + \ell_{k+1}(x)\, w_{k+1}$, et, puisque $\ell_{k+1}(w_k) = 1$ et $\ell_k(w_{k+1}) = 2 + \alpha_k$,

$$\rho w_k = (1+\alpha_k)w_k + w_{k+1}, \qquad \rho w_{k+1} = -(2+\alpha_k)w_k - w_{k+1}.$$

Sur $W = \langle w_k, w_{k+1}\rangle$, ρ a pour trace α_k et pour déterminant 1 : $\rho^2 - \alpha_k\rho + 1$ est nul sur W, qui contient l'image de $\rho - 1$, d'où le point 2. Pour le point 3, $\rho^m x = x + \sum_{j<m} \rho^j(\rho x - x)$; sur W, $\sum_{j<3}\rho^j = (1+\alpha_k)\rho$, $\sum_{j<4}\rho^j = \alpha_k\big((1+\alpha_k)\rho - 1\big)$ et $\sum_{j<5}\rho^j = (\alpha_k^2 + \alpha_k - 1)(\alpha_k\rho - 1)$, nuls sous l'hypothèse correspondante, de sorte que $\rho^p = 1$. Réciproquement, $\rho s_k = s_{k+1}$, $\rho s_{k+1} = s_{k+2} + (1+\alpha_k)w_k$, $\rho s_{k+2} = s_k$: sur $\langle s_k, s_{k+1}, s_{k+2}\rangle$, $\rho(a,b,c) = \big(c - (1+\alpha)b, a + (1+\alpha)b, b\big)$, $\alpha = \alpha_k$. Les itérés de $s_k = (1,0,0)$ sont $(0,1,0)$, $(-1-\alpha, 1+\alpha, 1)$, $(-2\alpha - \alpha^2, \alpha + \alpha^2, 1+\alpha)$, puis des vecteurs de dernières coordonnées $(\alpha^3 + \alpha^2 - \alpha, \alpha + \alpha^2)$ et, avec $P = \alpha^2 + \alpha - 1$, $\big((\alpha^2-1)P, \alpha P\big)$. Ainsi $\rho^3 s_k = s_k$ force $1 + \alpha = 0$; $\rho^4 s_k = s_k$ force $\alpha + \alpha^2 = 0 = \alpha^3 + \alpha^2 - \alpha$, d'où $\alpha = \alpha(\alpha + \alpha^2) - (\alpha^3 + \alpha^2 - \alpha) = 0$; $\rho^5 s_k = s_k$ force $\alpha P = 0 = (\alpha^2 - 1)P$, d'où $P = \alpha \cdot \alpha P - (\alpha^2 - 1)P = 0$. Sous chaque hypothèse, les itérés d'ordre $m < p$ ont une coordonnée égale à 1 (ou à $\alpha + \alpha^2 = 1$) là où s_k a 0, de sorte que $\rho^m \ne 1$ dès que R est non nul. □

La figure 16 montre le point 3 sur $\mathbf{R}$. Le plan affine $s_k + W$ contient s_k, $s_{k+1} = s_k + w_k$ et $s_{k+2} = s_{k+1} + w_{k+1}$, et ρ le conserve, puisque $\rho x - x \in W$. Sa partie linéaire, de trace α_k et de déterminant 1, est conjuguée à la rotation d'angle $2\pi/p$ quand $\alpha_k = 2\cos(2\pi/p)$: les valeurs -1, 0 et $(\sqrt{5}-1)/2$, racine de $\alpha^2 + \alpha - 1$, donnent $p = 3, 4, 5$. L'orbite de s_k est alors un polygone régulier à p sommets, sur lequel $s_{k+1} = \rho s_k$ suit s_k et $s_{k+2} = \rho^{-1}s_k$ le précède.

Remarque. Voir `usig_mul_self`, `usig_comm`, `sum_usig`, `rho_cubic`, `orderOf_rho_eq_three`, `orderOf_rho_eq_four` et `orderOf_rho_eq_five` dans `Folder70.lean`. La lecture démontre le critère sur un corps où p est inversible ; pour $p = 3, 4, 5$, les seules valeurs des polytopes réguliers finis, il vaut sur tout anneau, en toute dimension, caractéristiques 2, 3 et 5 comprises. Les générateurs des pages 74 et 75 sont le cas $n = 2$, $(\alpha_0, \alpha_1) = (-1, \alpha)$ (`usig_emb`, `ico_orderOf`) ; tétraèdre $(-1,-1)$, cube $(0,-1)$, octaèdre $(-1,0)$ et dodécaèdre $(\alpha,-1)$ sont les autres solides de Platon, et l'autre racine de $\alpha^2 + \alpha - 1$, celle des polyèdres étoilés de la page 69,



$p = 3,\ \alpha_k = -1$ $\qquad$ $p = 4,\ \alpha_k = 0$ $\qquad$ $p = 5,\ \alpha_k^2 + \alpha_k = 1$

FIGURE 16 – L'orbite de s_k sous $\rho = \sigma_k\sigma_{k+1}$ dans le plan affine $s_k + W$, sur $\mathbf{R}$, dans une coordonnée affine où la partie linéaire de ρ est une rotation. Le centre est le point fixe de ρ dans ce plan. Pour $p = 3$, $\rho^2 s_k = s_{k+2}$. L'autre racine de $\alpha^2 + \alpha - 1$, $-(1+\sqrt{5})/2 = 2\cos(4\pi/5)$, donne la rotation d'angle $4\pi/5$ et le pentagone étoilé.

vérifie les mêmes identités. Le critère pour p quelconque fait l'objet de l'énoncé suivant ; n'est pas démontré le passage de la définition d'une réalisation régulière à la forme normale (pages 7 à 18).

Théorème 62.4 (D'après la page 67, forme de l'édition, le critère pour tout p ♦). *Soit $n \geq 1$, $k \leq n-1$ et $\rho = \sigma_k\sigma_{k+1}$.*

1. *Si R est non nul, pour tout $m \geq 0$, $\rho^m = 1$ si et seulement si $\chi = (t-1)(t^2 - \alpha_k t + 1)$ divise $t^m - 1$ dans $R[t]$.*
2. *Pour $p \geq 3$, soit $\Psi_p \in \mathbf{Z}[x]$ le polynôme minimal de $2\cos(2\pi/p)$, de degré d. Alors $x^d\,\Psi_p(x + x^{-1}) = \Phi_p(x)$, le p-ième polynôme cyclotomique ; en particulier $2d = \deg\Phi_p$, l'indicatrice d'Euler de p.*
3. *Si $R = K$ est un corps de caractéristique 0 et $p \geq 3$, ρ est d'ordre exactement p si et seulement si $\Psi_p(\alpha_k) = 0$.*

Démonstration. Pour le point 1, $\chi(\rho) = 0$ par le point 2 du théorème précédent, d'où une implication. Réciproquement, si $\rho^m = 1$, le reste $r = r_0 + r_1 t + r_2 t^2$ de la division de $t^m - 1$ par χ, unitaire, vérifie $r(\rho) = 0$; appliqué à s_k, il donne $r_0 s_k + r_1 s_{k+1} + r_2\big(s_{k+2} + (1+\alpha_k)w_k\big) = 0$, et les coordonnées $k+2$, $k+1$, k donnent $r_2 = r_1 = r_0 = 0$: le vecteur s_k est cyclique.

Pour le point 2, soit $\zeta = e^{2i\pi/p}$, de sorte que $c = \zeta + \zeta^{-1} = 2\cos(2\pi/p)$. Le polynôme $T = \sum_{i\leq d} c_i\, x^{d-i}(x^2+1)^i$, où $\Psi_p = \sum c_i x^i$, est à coefficients entiers, de degré au plus $2d$, de terme constant $c_d = 1$, et vaut $z^d\,\Psi_p(z+z^{-1})$ en tout $z \neq 0$; il s'annule en ζ, donc Φ_p, polynôme minimal de ζ sur $\mathbf{Z}$, le divise : $T = \Phi_p\, g$. Le corps $\mathbf{Q}(c)$ est réel et ne contient pas ζ, dont la partie imaginaire $\sin(2\pi/p)$ n'est pas nulle ; comme $\mathbf{Q}(c) \subset \mathbf{Q}(\zeta)$, $\deg\Phi_p = [\mathbf{Q}(\zeta) : \mathbf{Q}] = d\,[\mathbf{Q}(\zeta) : \mathbf{Q}(c)] \geq 2d$. Ainsi g est constant, et $g = T(0)/\Phi_p(0) = 1$.

Pour le point 3, soit ζ une racine de $t^2 - \alpha_k t + 1$ dans une clôture algébrique L de K ; $\zeta \neq 0$ et $\alpha_k = \zeta + \zeta^{-1}$. La divisibilité du point 1 se lit dans $L[t]$, où $\chi = (t-1)(t-\zeta)(t-\zeta^{-1})$ et où $t^m - 1$, pour $m \geq 1$, est à racines simples : $\rho^m = 1$ si et seulement si $\zeta^m = 1$ et $\zeta^2 \neq 1$. Si $\zeta^2 = 1$, ρ est d'ordre infini et ζ n'est pas racine primitive p-ième de l'unité ; sinon ρ et ζ ont le même ordre. Donc ρ est d'ordre p si et seulement si ζ est racine primitive p-ième, c'est-à-dire $\Phi_p(\zeta) = 0$, soit, par le point 2, $\zeta^d\,\Psi_p(\alpha_k) = 0$. □

Remarque. Voir `rho_pow_eq_one_iff`, `chi_dvd_iff`, `recip_minpoly_cos` et `orderOf_rho_eq_iff` dans `Folder70.lean`. C'est le « $\rho_s^p = \mathrm{id} \iff F_p(\alpha) = 0$ » de la page 67, en toute dimension,

avec $F_p = \Psi_p$; $\Psi_3 = x + 1$, $\Psi_4 = x$, $\Psi_5 = x^2 + x - 1$ redonnent le théorème précédent sur $\mathbf{Q}$. La caractéristique 0 sert deux fois : $t^m - 1$ est à racines simples, et les racines de Φ_p sont exactement les racines primitives p-ièmes. Pour $p = 3, 4, 5$, le théorème précédent vaut en toute caractéristique ; en caractéristique positive, le critère pour p quelconque n'est pas démontré ici.

63 Cote 86 : les cinq trièdres de l'icosaèdre et l'icosaèdre gauche [66]

La cote 86, *[Polyèdres réguliers] : notes manuscrites (s.d.)*, trente-deux pages, reprend l'icosaèdre comme un objet purement combinatoire. Sous la chemise « Cours », la page 18 définit une permutation ρ des quinze directions d'arêtes par le côté du pentagone d'un sommet opposé à l'arête, et la page 19 affirme $\rho^3 = \mathrm{id}$ (86, lot 1, p. 18, 86, lot 1, p. 19). Ses orbites sont les cinq « trièdres distingués ». La page 20 montre que deux arêtes orthogonales n'ont pas de sommet commun et que les cinq arêtes d'un sommet ont des trièdres distincts (86, lot 1, p. 20). Les pages 21 et 22 en tirent que le groupe G des automorphismes opère sur les trièdres par permutations paires et munissent l'ensemble T des trièdres d'une orientation canonique (86, lot 2, p. 21, 86, lot 2, p. 22). La conclusion des pages 23 à 25 est que $G \to \mathfrak{S}_T$ a pour image Alt_T et pour noyau le sous-groupe engendré par l'antipodisme (86, lot 2, p. 23, 86, lot 2, p. 25). Les pages 26 à 30 reconstruisent l'icosaèdre gauche $\bar{\Pi} = \Pi/\iota$, aujourd'hui l'hémi-icosaèdre, à partir de l'ensemble orienté T, et les pages 31 et 32, d'une autre encre, donnent le tableau des ensembles de drapeaux et les trois involutions sur les numérotations $(a_1, \dots, a_5)$ (86, lot 2, p. 26, 86, lot 2, p. 30, 86, lot 2, p. 31, 86, lot 2, p. 32).

Conventions. Les sommets sont $\{0, \dots, 11\}$: 0 et 11 sont deux sommets opposés, $1, \dots, 5$ et $6, \dots, 10$ les deux pentagones de leurs voisins ; la liste des voisins est donnée une fois pour toutes, et tout le reste est calculé à partir de l'adjacence. Pour une face $\{x, y, z\}$, $\mathrm{o}(x, y, z)$ est le troisième sommet de l'autre face qui borde $\{x, y\}$; l'antipode ιx est l'unique sommet qui n'est ni x, ni un voisin de x, ni un voisin d'un voisin de x. G est le groupe des bijections de l'ensemble des sommets qui conservent l'adjacence dans les deux sens. Un drapeau est un triangle orienté (s, t, u) : le sommet s, l'arête $\{s, t\}$, la face $\{s, t, u\}$; il y en a 120. Une arête est un couple de sommets adjacents, considéré à l'ordre près ; deux arêtes ont même direction si elles sont égales ou antipodales. Pour une arête $\{s, t\}$ de faces $\{s, t, u\}$ et $\{s, t, v\}$, on pose $\rho_0(s, t) = \{\mathrm{o}(s, u, t), \mathrm{o}(s, v, t)\}$, le côté $\{\Pi_{s,u}, \Pi_{s,v}\}$ de la page 18 (figure 17). Les numérotations de T sont les bijections $\{1, \dots, 5\} \to T$, composées à droite par les permutations des places : $(a \circ \tau)(k) = a(\tau(k))$.

Énoncé (Pages 18 à 20 et 23, les trièdres distingués ♦).

1. *$\rho_0(s, t)$ est une arête et ne dépend pas de celle des deux faces que l'on appelle u ; $\rho_0(t, s)$ est l'antipode de $\rho_0(s, t)$; si deux arêtes ont même direction, leurs images aussi. On obtient une permutation ρ des quinze directions, avec $\rho^3 = \mathrm{id}$, sans point fixe, et $\rho^2\overline{\{s, t\}} = \overline{\{u, \iota v\}}$.*
2. *Il y a cinq orbites, les trièdres ; deux arêtes de même trièdre et de directions différentes n'ont aucun sommet commun ; en chaque sommet, les cinq arêtes ont des trièdres deux à deux distincts, et chaque trièdre est représenté. Chaque trièdre est donc une partition des douze sommets en six arêtes.*
3. *(Page 23) Pour une face $\{u, v, w\}$, avec $u_1 = \mathrm{o}(v, w, u)$, $v_1 = \mathrm{o}(w, u, v)$, $w_1 = \mathrm{o}(u, v, w)$, les directions $\overline{\{u, v_1\}}$, $\overline{\{v, w_1\}}$, $\overline{\{w, u_1\}}$ sont dans un même trièdre, $\overline{\{u, w_1\}}$, $\overline{\{v, u_1\}}$, $\overline{\{w, v_1\}}$*

66. Preuve vérifiée : `lean/Grothendieck/Folder86.lean`.

dans un autre, et ces deux trièdres et ceux des trois côtés de la face sont les cinq trièdres. Les arêtes $\{u, v\}$ et $\{v, w_1\}$ ne sont jamais dans le même trièdre.

Démonstration. Ce sont des énoncés finis sur l'icosaèdre, vérifiés par le noyau de Lean (`decide`), sans évaluation compilée. Pour (2), on étiquette les trente arêtes par $\{0, \dots, 4\}$ et l'on vérifie que deux arêtes ont la même étiquette si et seulement si la direction de l'une est celle de l'autre, de son image par ρ ou de son image par ρ^2 : les étiquettes sont alors les orbites, et l'étiquetage n'est qu'un nom donné à chacune. □

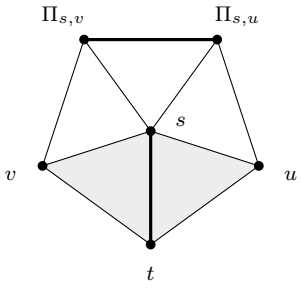
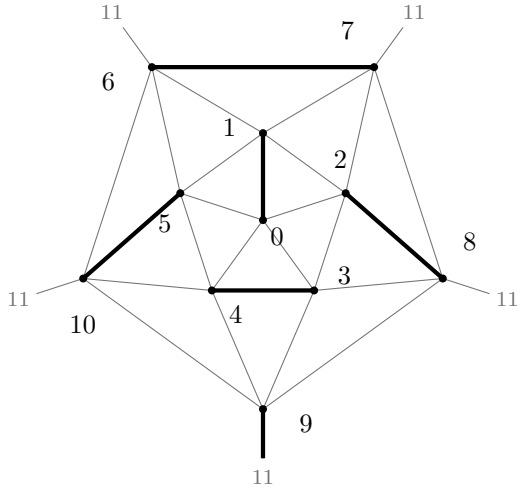


FIGURE 17 – L'étoile du sommet s et la règle ρ_0 de la page 18. Les faces grisées sont $\{s, t, u\}$ et $\{s, t, v\}$; $\Pi_{s,u} = \mathrm{o}(s, u, t)$ est le troisième sommet de l'autre face qui borde $\{s, u\}$, et de même pour $\Pi_{s,v}$. L'arête $\rho_0(s, t) = \{\Pi_{s,u}, \Pi_{s,v}\}$ (en gras) est le côté du pentagone de s opposé à t. Figure de l'édition ; Grothendieck dessine en marge de la page 18 le voisinage de l'arête $\{s, t\}$ (86, lot 1, p. 18).

L'icosaèdre des conventions, projeté depuis le sommet $11 : 0$ au centre, le pentagone $1, \dots, 5$ autour, le pentagone $6, \dots, 10$ à l'extérieur, et 11 à l'infini, joint à $6, \dots, 10$ par les segments radiaux. En trait épais, l'un des cinq trièdres : les six arêtes $\{0, 1\}$, $\{9, 11\}$, $\{3, 4\}$, $\{6, 7\}$, $\{2, 8\}$, $\{5, 10\}$, deux à deux sans sommet commun, en trois directions formées chacune de deux arêtes antipodales.



Théorème 63.1 (Grothendieck, pages 20 à 25, l'action sur les trièdres ♦). *1. Un automorphisme est déterminé par l'image du drapeau $(0, 1, 2)$, et tout drapeau est l'image de $(0, 1, 2)$ par un automorphisme : G a 120 éléments.*

2. Tout automorphisme g commute à ι et à ρ, et l'application qui envoie le trièdre d'une arête a sur celui de $g(a)$ définit un homomorphisme $G \to \mathfrak{S}_T$.

3. *Son image est contenue dans* Alt_T *et lui est égale.*
4. *Son noyau est* $\{1, \iota\}$.

Démonstration. (1) Si g conserve l'adjacence, $g(\mathrm{o}(x,y,z)) = \mathrm{o}(gx, gy, gz)$, car $\mathrm{o}(x,y,z)$ est l'unique voisin commun de x et y distinct de z. Les douze sommets s'obtiennent à partir de 0, 1, 2 par neuf applications de o ; g est donc déterminé par $(g0, g1, g2)$. Réciproquement, pour chaque drapeau (x,y,z), la même suite d'applications de o définit une application dont on vérifie qu'elle est bijective et conserve l'adjacence. (2) ιx est caractérisé par l'adjacence, donc $g\iota = \iota g$. Comme $\rho_0(s,t)$ est formé de deux valeurs de o et ne dépend pas du choix de u, g envoie $\rho_0(s,t)$ sur $\rho_0(gs, gt)$; g conserve donc la relation « même trièdre », et l'action sur les cinq étiquettes est bien définie et multiplicative. (3) et (4) Par (1), tout g est l'automorphisme associé à un drapeau, et la permutation de T qu'il induit se calcule à partir de ce drapeau. On vérifie sur les 120 drapeaux que ces permutations sont paires, qu'elles sont au nombre de 60, ce qui est l'ordre de Alt_T, et que seuls les drapeaux $(0,1,2)$ et $(\iota 0, \iota 1, \iota 2)$ donnent l'identité. □

Remarque. La démonstration de la page suit un autre chemin : la parité par les générateurs $\bar\sigma_0$, $\bar\sigma_1$, $\bar\sigma_2$ et le cas $n \equiv 1 \pmod 4$ du polygone, l'image par les ordres 6, 10 et 4 des images des stabilisateurs d'une face, d'un sommet et d'une arête. Ici l'énoncé est établi par le décompte des drapeaux ; seule la parité des symétries d'un pentagone, vues comme permutations de ses sommets, est vérifiée pour elle-même (énoncé suivant). La vérification confirme le calcul de ρ^2 et de ρ^3, que la page ne détaille pas, et la correction de la lecture à la page 23 : avec $\{u, v\}$, la page met dans un même triple deux arêtes de trièdres différents. Les deux choix de u dans la définition de ρ_0 donnent la même arête, et le passage de s à t donne l'arête antipodale : ρ est bien défini sur les directions, comme la page l'affirme.

Théorème 63.2 (D'après les pages 21 et 26 à 32, forme complétée par l'édition, l'icosaèdre gauche par l'ensemble orienté T ♦). *À un drapeau* (s,t,u)*, avec* $v = \mathrm{o}(s,t,u)$*, associons la numérotation* $\nu(s,t,u)$ *de* T *formée des trièdres des arêtes* $\{s,t\}$*,* $\{s,v\}$*,* $\{s, \Pi_{s,v}\}$*,* $\{s, \Pi_{s,u}\}$*,* $\{s,u\}$ *: les cinq arêtes de* s *dans l'ordre du pentagone, à partir de* t*, dans le sens qui s'éloigne de* u *(page 30).*

1. *Pour* $g \in G$*,* $\nu(gs, gt, gu)$ *est* $\nu(s,t,u)$ *composée à gauche par la permutation de* T *induite par* g*.*
2. *Toutes les numérotations* $\nu(s,t,u)$ *ont la même parité ; elles définissent donc une orientation* ϖ *de* T *qui ne dépend d'aucun choix. Toute numérotation compatible avec* ϖ *est de la forme* $\nu(s,t,u)$*, et* $\nu(s,t,u) = \nu(s',t',u')$ *si et seulement si* (s',t',u') *est* (s,t,u) *ou* $(\iota s, \iota t, \iota u)$*. Les* 60 *drapeaux de* $\bar\Pi$ *sont ainsi les* 60 *numérotations compatibles avec* ϖ*.*
3. *Changer le sommet, l'arête ou la face d'un drapeau, c'est-à-dire* $(s,t,u) \mapsto (t,s,u)$*,* (s,u,t)*,* (s,t,v)*, revient à composer* ν *à droite par*

$$\tau_0 = (2\,4)(3\,5), \qquad \tau_1 = (1\,5)(2\,4), \qquad \tau_2 = (2\,5)(3\,4)$$

   (permutations des places) : $\sigma_0(a) = (a_1, a_4, a_5, a_2, a_3)$*,* $\sigma_1(a) = (a_5, a_4, a_3, a_2, a_1)$*,* $\sigma_2(a) = (a_1, a_5, a_4, a_3, a_2)$*.*
4. *Le* σ_1 *de la page 31,* $(a_2, a_1, a_5, a_4, a_3)$*, est* $\tau_1' = (1\,2)(3\,5) = \tau_2\tau_1\tau_2$*, et* τ_2 *commute à* τ_0*. Le triple de la page est donc l'action des trois mêmes changements sur la numérotation* $(s,t,u) \mapsto \nu(s,t,v)$*.*

5. *Avec le triple de la page,* $\sigma_1\sigma_0 : a \mapsto (a_4, a_1, a_3, a_2, a_5)$*,* $\sigma_2\sigma_1 : a \mapsto (a_2, a_3, a_4, a_5, a_1)$ *et* $\sigma_0\sigma_2 : a \mapsto (a_1, a_3, a_2, a_5, a_4)$ *sont d'ordres* 3*,* 5 *et* 2*, et* $\sigma_0\sigma_1$ *est d'ordre* 3*.*
6. *Deux drapeaux ont le même sommet dans* $\bar{\Pi}$ *si et seulement si leurs numérotations tracent le même pentagone sur* T*; la même arête si et seulement si elles donnent la même partition* $\{a_1\} \sqcup \{a_2, a_3\} \sqcup \{a_4, a_5\}$ *de type* $(2, 2, 1)$*; la même face si et seulement si elles donnent la même partie* $\{a_1, a_3, a_5\}$*.*
7. *Les symétries du pentagone* $1\,2\,3\,4\,5$ *sont des permutations paires des places. Par suite une numérotation de* T *trace le pentagone d'un sommet de* $\bar{\Pi}$ *si et seulement si elle est compatible avec* ϖ*. On obtient* 6 *pentagones,* 15 *partitions de type* $(2, 2, 1)$*, c'est-à-dire toutes, et les* 10 *parties à trois éléments.*

Démonstration. (1) Les cinq arêtes de s s'écrivent avec o, que g respecte, et g opère sur les trièdres par l'énoncé précédent. (2) Par (1), $\nu(g0, g1, g2)$ est la permutation de T induite par g, composée avec $\nu(0, 1, 2)$; avec l'étiquetage choisi, $\nu(0, 1, 2)$ est la permutation des places $\tau_2 = (2\,5)(3\,4)$, qui est paire, et toute permutation paire s'obtient ainsi par la surjectivité sur Alt_T. Deux drapeaux $g(0, 1, 2)$ et $h(0, 1, 2)$ ont la même numérotation si et seulement si $g^{-1}h$ est dans le noyau $\{1, \iota\}$, c'est-à-dire $h = g$ ou $h = g\iota$, et $g\iota(0, 1, 2) = \iota g(0, 1, 2)$. (3) Les changements de drapeau sont $g \mapsto gs_i$, où s_0, s_1, s_2 sont les automorphismes qui envoient $(0, 1, 2)$ sur $(1, 0, 2)$, $(0, 2, 1)$, $(0, 1, 5)$; par (2), il suffit de vérifier les trois égalités de permutations $\pi(s_i)\,\nu(0, 1, 2) = \nu(0, 1, 2)\,\tau_i$, où $\pi(s_i)$ est la permutation de T induite. (4) et (5) sont des calculs de permutations ; par (3), $\nu(\sigma_2(\sigma_1 r)) = \nu(r)\tau_1\tau_2 = \nu(\sigma_2 r)\,\tau_2\tau_1\tau_2$, puisque $\tau_2^2 = 1$. (6) Par (1), en remplaçant les deux drapeaux par leurs images sous g^{-1}, où g envoie $(0, 1, 2)$ sur le premier, on se ramène au cas où le premier est $(0, 1, 2)$: les trois conditions sur les drapeaux sont conservées par g, et les trois conditions sur les numérotations par la composition à gauche avec une permutation de T. Le cas du drapeau $(0, 1, 2)$ se vérifie sur les 120 drapeaux. (7) On vérifie que les numérotations qui tracent le pentagone $1\,2\,3\,4\,5$ sont les dix éléments du groupe diédral et que ces dix permutations sont paires ; si deux numérotations a, b tracent le même pentagone, $a^{-1}b$ trace le pentagone standard, donc a et b ont même parité. Les trois décomptes sont des calculs sur les 120 drapeaux. □

Remarque. L'orientation ϖ est celle des pages 21 et 22 : la parité de $\nu(s, t, u)$ ne dépend ni du drapeau ni du sens de parcours, grâce au cas $n \equiv 1 \pmod 4$ du pentagone, dont les dix symétries sont paires ; pour un hexagone, la symétrie qui échange les extrémités de deux côtés opposés est un produit de trois transpositions, donc impaire. Les pages 26 à 32 donnent les bijections et les ensembles de la page 31 sans les incidences ; les incidences du point 6 et les points 4 et 5 sont de l'édition. La vérification confirme les remarques de la lecture sur les pages 31 et 32. Le σ_1 de la page n'est pas celui que donne le dictionnaire de la page 30 ; il s'en déduit par conjugaison par σ_2, et correspond au dictionnaire qui lit le pentagone de s à partir de t en direction de u. Les deux triples définissent donc des ensembles à opérateurs isomorphes. L'étiquette « $\sigma = \sigma_0\sigma_1$ » de la page 32 accompagne la valeur de $\sigma_0\sigma_2$, d'ordre 2. L'étiquetage des trièdres a été choisi de sorte que ϖ soit la classe des numérotations paires ; un autre étiquetage changerait la classe, non l'énoncé.

Ne sont pas démontrés ici : les axiomes des polyèdres combinatoires de la page 2 et le théorème de pleine fidélité des pages 10 à 16, l'icosaèdre étant donné par sa liste de voisins ; l'identification des trièdres aux repères orthogonaux et aux cinq octaèdres inscrits de l'icosaèdre régulier ; la décomposition $G = \{1, \iota\} \times G^+$ et l'isomorphisme $G^+ \simeq \mathrm{Alt}_T$ du corollaire de la

page 26, faute d'une définition de l'orientation de Π ; la description des arêtes par les triplets (t, γ, α) de la page 27 et les incidences a) à d) des pages 28 et 29 sous cette forme, que l'on a remplacées par les partitions et les parties à trois éléments de la page 31 ; les lignes $\vec{A}$, $A^{\uparrow}$, $A^{\wedge}$, $\tilde{S}$, $\tilde{A}$, $\tilde{F}$ du tableau de la page 31 ; la génération de Alt_5 par τ_0, τ_1, τ_2 et leur action simplement transitive sur les 60 numérotations, qui suivraient de la connexité du graphe des drapeaux, non vérifiée.

64 Cote 72 : réalisations par pseudo-réflexions d'un polytope régulier [67]

La cote 72, *Polyèdres réguliers et hyperpolyèdres réguliers (calculs en dimension quelconque)*, que l'inventaire date « [à partir de 1978] », étudie les réalisations du polytope régulier universel de rang $n+1$ par des pseudo-réflexions $\tau_i = \mathrm{id} + a_i' \otimes a_i$ $(0 \le i \le n)$ d'un module E de rang $n+2$ sur une base quelconque, les τ_i non consécutifs commutant. Avec le point de départ s_0, $s_{i+1} = \tau_i s_i$ et $a_i = s_{i+1} - s_i$, les accouplements sont $\langle a_{i-1}, a_i' \rangle = 1$, $\langle a_i, a_i' \rangle = \mu_i = \lambda_i - 1$, $\langle a_{i+1}, a_i' \rangle = \beta_i$, les autres nuls. On travaille ici dans la base $(s_0, a_0, \dots, a_n)$ de $E = R^{n+2}$, R un anneau commutatif ; π est la première coordonnée et $\tilde{c}$ l'unique vecteur annulé par tous les a_i' dont la coordonnée sur a_n vaut 1, obtenu par substitution remontante.

Page 37, $\mathcal{U}_\rho = \mathrm{Spec}\, \mathcal{O}_S[T]_{(1+\rho T)}$, de loi $\lambda * \lambda' = \lambda + \lambda' + \rho\lambda\lambda'$, opère par $u_\lambda = \mathrm{id} + \lambda\, \pi \otimes \tilde{c}$, où $\rho = \pi(\tilde{c})$; le « Théorème » de la page 38 affirme sans démonstration que $\mathbb{G}_m \ltimes \mathcal{U}_\rho \to \mathrm{Aut}(E, (\tau_i))$ est un isomorphisme et que $D_0 \smallsetminus \{c, d\}$, $D_0 = H_1 \cap \dots \cap H_n$, est un torseur sous $\mathcal{U}_\rho$ trivialisé par s_0 (72, lot 2, p. 38). Les pages 87 et 88 le reprennent sous forme projective.

Théorème 64.1 (D'après les pages 37 et 38, en coordonnées, sur les points ♦). *Les $\lambda \in R$ avec $1+\rho\lambda$ inversible forment un groupe commutatif $\mathcal{U}_\rho(R)$; $\lambda \mapsto 1+\rho\lambda$ est surjectif sur les inversibles de toute R-algèbre si et seulement si ρ est inversible, et $\mathcal{U}_0 = \mathbb{G}_a$. On a $u_\lambda u_{\lambda'} = u_{\lambda * \lambda'}$, $\det u_\lambda = 1 + \rho\lambda$, et un endomorphisme de E commute à tous les τ_i si et seulement s'il s'écrit $c + t\,\pi \otimes \tilde{c}$, avec (c, t) unique ; il est inversible si et seulement si c et $c + t\rho$ le sont. D'où $R^\times \times \mathcal{U}_\rho(R) \simeq \mathrm{Aut}(E, (\tau_i))$, $(c, \lambda) \mapsto c\, u_\lambda$. Les points de D_0 sont les $as_0 + t\tilde{c}$, et ceux qui évitent c et d, normalisés par $\langle s, a_0' \rangle = 1$, sont exactement les $u_\lambda s_0 = s_0 + \lambda\tilde{c}$, chacun pour un seul λ, avec $u_\mu(u_\lambda s_0) = u_{\lambda * \mu} s_0$.*

L'énoncé tient sur les points, pour tout anneau : voir `forall_surjective_iff`, `u_mul`, `det_u`, `commute_iff`, `isUnit_iff`, `centraliserEquiv`, `mem_startPoints_iff` et `u_e0_injective` dans `Folder72.lean`. Le test de la réciproque est l'anneau des nombres duaux, où $1 + \varepsilon$ n'est atteint que si ρ est inversible. Pour $n = 1$, $\rho = \mu_0\mu_1 - \beta_0$, soit $4 - \beta_0$ pour des réflexions, comme à la page 41.

Les points de D_0 sont la direction c de $\tilde{c}$, le centre, et les $s_0 + \lambda\tilde{c}$; le point $d = D_0 \cap C$ est celui où $\pi(s_0 + \lambda\tilde{c}) = 1 + \rho\lambda$ s'annule. Comme $u_\mu(s_0 + \lambda\tilde{c}) = s_0 + (\lambda * \mu)\tilde{c}$ et $\lambda * \mu + 1/\rho = (1 + \rho\mu)(\lambda + 1/\rho)$ quand ρ est inversible, u_μ agit sur la coordonnée λ par l'homothétie de centre d et de rapport $1 + \rho\mu$; pour $\rho = 0$, d et c se confondent et u_μ est la translation de μ (figure 18).

Aux pages 79 à 82, sur un corps k, la cote décrit les sous-espaces invariants (72, lot 4, p. 79). Avec $Z_i' = H_0 \cap \dots \cap H_i$ et $Z_i^* = \mathrm{Lin}(h_{i+1}, \dots, h_n)$, $h_i = ka_i$ et $H_i = \mathrm{Ker}\, a_i'$:

Théorème 64.2 (Grothendieck, page 79 ♦). *Sur un corps, les μ_i quelconques (caractéristique 2 comprise), un sous-espace de E est stable par tous les τ_i si et seulement s'il est 0, E, la droite $k\tilde{c}$ du centre, l'hyperplan C d'équation $\pi = 0$, ou bien Z_i' ou Z_i^* pour un $i < n$ tel que $\beta_i = 0$.*

67. Preuve vérifiée : `lean/Grothendieck/Folder72.lean`.

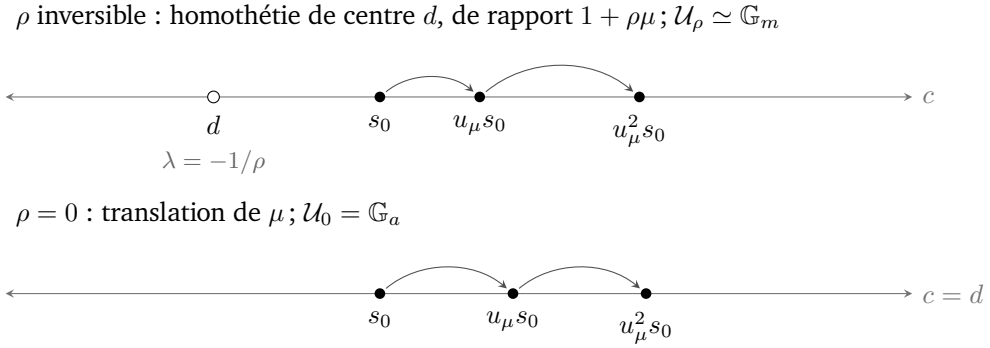


FIGURE 18 – La droite projective D_0 des points de départ, dans la carte $\langle s, a_0' \rangle = 1$, où $s_0 + \lambda\tilde{c}$ a pour coordonnée λ et où le centre c est à l'infini. En haut, ρ inversible : $D_0 \smallsetminus \{c, d\}$ est l'orbite de s_0, et u_μ en multiplie la distance à d par $1+\rho\mu$. En bas, $\rho = 0$: $c = d$, et $D_0 \smallsetminus \{c\}$ est une droite affine sur laquelle $\mathcal{U}_0$ agit par translations. Les points sont dessinés pour $\rho = 1$, $\mu = 0{,}6$, puis $\rho = 0$, $\mu = 0{,}8$.

La vérification porte sur l'énoncé tel quel (`invariant_iff` dans `Folder72.lean`) et sur le corollaire (c) de la page 80 (`invariant_iff_of_ne_zero`). Pour $i < n$, $Z_i^* \subset Z_i'$ si et seulement si $\beta_i = 0$ (`Zs_le_Zp_iff`) : c'est le « $\in$ » de la marge de la page 79 que la lecture retient, non le « $\notin$ » de la page 81.

Aux pages 80 à 82, la cote en tire l'irréductibilité de la représentation sur l'hyperplan C ; le d) barré de la page 80 demande $\rho \neq 0$ et tous les $\beta_i \neq 0$, le c) de la page 82 omet $\rho \neq 0$.

Théorème 64.3 (D'après les pages 80 à 82, forme complétée par l'édition ♦). *Sur un corps, les μ_i quelconques, les sous-espaces de C stables par tous les τ_i sont 0, C, la droite $k\tilde{c}$ si $\rho = 0$, et, pour $i < n$ tel que $\beta_i = 0$, Z_i^* et Z_i' lorsque $Z_i' \subset C$. Si tous les β_i sont non nuls, il ne reste que 0, C et, si $\rho = 0$, $k\tilde{c}$. La représentation sur C est donc irréductible si et seulement si tous les β_i sont non nuls et, pour $n \geq 1$, $\rho \neq 0$; pour $n = 0$, C est une droite.*

Voir `invariant_le_Vh_iff`, `invariant_le_Vh_iff_of_ne_zero` et `irreducible_on_C_iff` dans `Folder72.lean`. On intersecte la liste de `invariant_iff` avec C : $E \not\subset C$ puisque $\pi(s_0) = 1$, $k\tilde{c} \subset C$ si et seulement si $\pi(\tilde{c}) = \rho = 0$, et $Z_i^* \subset C$ toujours. Pour la nécessité, Z_i^* contient h_{i+1} et non h_0, qui est dans C ; si $\rho = 0$ et $n \geq 1$, $k\tilde{c}$ est une droite de C distincte de C, car $h_0 \in C$ n'est pas multiple de $\tilde{c}$, dont la dernière coordonnée vaut 1. Le seul « tous les $\beta_i \neq 0$ » du c) de la page 82 ne suffit donc pas : $\rho = 0$ laisse la droite invariante $k\tilde{c} \subset C$.

Aux pages 96 à 100, sur un anneau k, pour un k-module E, des pseudo-réflexions $\tau_i = \mathrm{id} + a_i' \otimes a_i$ et $s_0 \in E$, avec $\nu_i = \langle s_0, a_0' \rangle \langle a_0, a_1' \rangle \cdots \langle a_{i-1}, a_i' \rangle$, la cote démontre l'équivalence des conditions (A) (commutation des τ_i non consécutifs, $\tau_i s_0 = s_0$ pour $i \geq 1$, liberté des s_i) et (B) (accouplements nuls hors des indices consécutifs, $\langle s_0, a_i' \rangle = 0$ pour $i \geq 1$, liberté de $(s_0, a_0, \ldots, a_n)$, ν_n inversible) ; la remarque de la page 102 la reprend avec des bases de E (72, lot 5, p. 96).

Théorème 64.4 (D'après les pages 96 à 100 et 102 ♦). *Sur tout anneau commutatif, (Ā) « les τ_i non consécutifs commutent, $\tau_i s_0 = s_0$ pour $1 \leq i \leq n$, $(s_0, \ldots, s_{n+1})$ est une base de E » équivaut à (B̄) « $\langle a_i, a_j' \rangle = 0$ pour i, j non consécutifs, $\langle s_0, a_i' \rangle = 0$ pour $1 \leq i \leq n$, $(s_0, a_0, \ldots, a_n)$ est une base de E, ν_n est inversible ».*

L'énoncé tient, sans l'hypothèse que les a_i' soient partout non nulles : voir `condA_iff_condB` dans `Folder72.lean`. Sous (Ā), $s_{i+1} - s_i = \langle s_i, a_i' \rangle a_i$ et les s_i forment une base, donc chaque

$\langle s_i, a'_i\rangle$ est inversible, ce qui tient lieu de cette hypothèse dans le passage de la commutation à $\langle a_i, a'_j\rangle = 0$; sous (10) et (11), $\langle s_i, a'_i\rangle = \nu_i$, et dans les deux sens la matrice de passage est triangulaire à diagonale inversible.

Théorème 64.5 (Énoncé de l'édition, d'après la marge de la page 13 et les pages 91 à 100)**.** *Une réalisation qui vérifie ($\bar{B}$), normalisée par $\langle s_0, a'_0\rangle = 1$ et $\langle a_{i-1}, a'_i\rangle = 1$, est isomorphe, par un unique isomorphisme qui envoie s_0 sur e_0 et conjugue les τ_i, à la réalisation en coordonnées de paramètres $\mu_i = \langle a_i, a'_i\rangle$, $\beta_i = \langle a_{i+1}, a'_i\rangle$. Celle-ci vérifie ($\bar{B}$) pour tous μ, β, et τ_i y est inversible si et seulement si $\lambda_i = 1 + \mu_i$ l'est. Une application linéaire compatible à s_0 et aux τ_i entre deux réalisations normalisées force l'égalité des (μ_i, β_i). Les réalisations épinglées non dégénérées sur E libre de rang $n+2$ sont donc classées, rigidement, par les $2n+1$ paramètres $(\lambda_0, \beta_0, \lambda_1, \ldots, \beta_{n-1}, \lambda_n)$, les λ_i inversibles et les β_i quelconques.*

Les déclarations `pinned_classification`, `pinned_rigid`, `model_condB`, `model_isUnit_iff` et `invariants_eq` vérifient l'énoncé. Les invariants se lisent sur (τ_i, s_0) seuls : normalisée, $a_i = s_{i+1} - s_i$, $\tau_i a_i = \lambda_i a_i$ et $\tau_i a_{i+1} = a_{i+1} + \beta_i a_i$.

Aux pages 96 à 100, « libre » s'entend au sens fort de la page 103 : une famille est libre si elle est indépendante et engendre un facteur direct.

Théorème 64.6 (D'après les pages 96 à 100 et 103 ♦)**.** *Sur tout anneau commutatif k et pour tout k-module E, libre ou non, (A) « les τ_i non consécutifs commutent, $\tau_i s_0 = s_0$ pour $1 \le i \le n$, $(s_0, \ldots, s_{n+1})$ est libre » équivaut à (B) « $\langle a_i, a'_j\rangle = 0$ pour i, j non consécutifs, $\langle s_0, a'_i\rangle = 0$ pour $1 \le i \le n$, $(s_0, a_0, \ldots, a_n)$ est libre, ν_n est inversible », « libre » au sens fort. Au sens faible (indépendance seule), (A) n'entraîne pas (13) : sur $\mathbb{Z}$, $n = 0$, $s_0 = e_0$, $a_0 = e_1$, $a'_0 = 2e_0^*$, la famille $(s_0, s_1) = (e_0, e_0 + 2e_1)$ est indépendante et $\nu_0 = 2$. Enfin ($\bar{A}$) force E à être libre.*

Voir `condAs_iff_condBs`, `not_condAw_imp` et `free_of_condA` dans `Folder72.lean`. On se ramène au sous-module N engendré par la famille, où elle est une base, et au théorème précédent. Sous (A), la coordonnée sur s_{i+1} de la projection sur N parallèlement au supplémentaire vaut 1 en s_{i+1} et 0 en s_i, donc $\langle s_i, a'_i\rangle$ est inversible et $a_i \in N$; les τ_i se restreignent à N. Sur un E localement libre non libre, il n'y a donc pas de point de départ global : l'existence des pages 102 à 105 n'est que locale.

La proposition des pages 102 à 105 ne demande b) que pour $i < j$: c'est la moitié triangulaire de (10), qui intervient dans les conditions ($\bar{B}'$) du corollaire des pages 97 et 98 ; ($\bar{B}$) est ($\bar{B}'$) plus l'autre moitié de (10), qui ne fait pas intervenir s_0.

Théorème 64.7 (D'après les pages 102 à 105 ♦)**.** *Sur un anneau local k, il existe s_0 vérifiant ($\bar{B}'$) « $\langle a_i, a'_j\rangle = 0$ pour $i + 2 \le j$, $\langle s_0, a'_i\rangle = 0$ pour $1 \le i \le n$, $(s_0, a_0, \ldots, a_n)$ est une base, ν_n est inversible » si et seulement si a) $(a_0, \ldots, a_n)$ se complète en une base par un vecteur, a') $x \mapsto (\langle x, a'_i\rangle)_{0 \le i \le n}$ est surjective, b) $\langle a_i, a'_j\rangle = 0$ pour $i + 2 \le j$, c) les $\langle a_i, a'_{i+1}\rangle$ sont inversibles ; avec en plus $\langle a_j, a'_i\rangle = 0$ pour $i + 2 \le j$, il existe s_0 vérifiant ($\bar{A}$). Si E est libre de rang $n+2$, a) et a') au sens « strictement libre » de la page (dans E et dans $E^\vee$) donnent ces formes-ci. Sur un anneau quelconque, si $(v, a_0, \ldots, a_n)$ est une base et φ la coordonnée sur v, s_0 vérifie ($\bar{B}'$) si et seulement si s_0 est dans le noyau commun F des a'_i ($1 \le i \le n$) et si $\langle s_0, a'_0\rangle$ et $\varphi(s_0)$ sont inversibles.*

Voir `exists_condB'_iff`, `exists_condA_iff`, `exists_completion`, `surjective_of_strict`, `exists_condB'_of_strict` et `condB'_iff_of_basis` dans `Folder72.lean`. La dernière assertion est le « $s_0 \notin D$, $s_0 \notin \Delta$ » de la page 105 : $(s_0, a_0, \ldots, a_n)$ est triangulaire dans $(v, a_0, \ldots, a_n)$,

de diagonale $(\varphi(s_0), 1, \ldots, 1)$, et $\nu_n = \langle s_0, a'_0\rangle c_0 \cdots c_{n-1}$. Par b) et c), une substitution remontante sur $a_{n-1}, \ldots, a_0$ donne $s \in F$ avec $\varphi(s) = \varphi(v) = 1$, et a′) donne $t \in F$ avec $\langle t, a'_0\rangle = 1$; dans un anneau local, l'un de t, s, $s + t$ convient, ce qui vaut même si le corps résiduel est $\mathbb{F}_2$. Pour la nécessité de a′), la matrice des $\langle x, a'_j\rangle$ pour $x = s_0, a_0, \ldots, a_{n-1}$ est triangulaire de déterminant ν_n, comme à la page 103. Pour a), le supplémentaire de $k(a_0, \ldots, a_n)$ est projectif de type fini sur un anneau local, donc libre, de rang 1.

Ne sont pas démontrés ici : le schéma en groupes $\mathcal{U}_\rho$ et sa lissité, l'énoncé projectif sur une base (automorphismes de $X = \mathbf{P}(E)$ commutant aux τ_i projectifs), le torseur des drapeaux de la page 87, les comptes des pages 79 et 80, et l'existence du point de départ sous forme locale sur un anneau quelconque (après localisation en un premier, ou sur un recouvrement de Zariski), que l'énoncé sur un anneau local ne formule qu'aux anneaux locaux.

Partie 25

Théorie de l’homotopie et catégories tests

La lettre à Daniel Quillen du 19 février 1983, continuée jusqu’au 23, ouvre *À la poursuite des champs* (134-2, lot 1, p. 14) ; la cote 114 est datée de cette année. La dernière lettre datée du fonds sur ces questions est la réponse de Ronald Brown du 16 avril 1991, sur les groupoïdes multiples et le groupoïde de Teichmüller (119, lot 15, p. 282), contemporaine de la cote 158.

Ailleurs : le dépôt d’OpenAI cité dans l’introduction annonce l’hypothèse d’homotopie pour les ∞-groupoïdes globulaires faibles de tout cohérateur de Grothendieck, dans une convention qu’il fixe, et la conjecture sur les sommes amalgamées dont une prépublication la fait dépendre (Henry 2016, conjecture 5.3.3 [71]). Le post-scriptum d’une lettre de 1975, rangée avec celles à Lawrence Breen, expose le « yoga » de cette hypothèse (134-2, lot 3, p. 42). Seul est formalisé le théorème des expansions élémentaires : pour tout cohérateur dans cette convention et tout modèle à bord cellulaire, attacher un $(n+1)$-disque le long de sa n-face source induit une équivalence faible. La structure de semi-modèles et la comparaison avec la théorie de l’homotopie des espaces ne le sont pas, et le projet n’a pas exécuté ce code. Les énoncés des cotes 136, 106, 114, 158 et 104 démontrés ci-dessous sont un lemme sur les coefficients binomiaux et des lemmes sur les catégories à cofibrations, les localisateurs fondamentaux, les monoïdes finis et les catégories de « modèles » ; ils ne touchent pas à l’hypothèse elle-même.

L’hypothèse d’homotopie. Le post-scriptum de 1975 (134-2, lot 3, p. 42) et *À la poursuite des champs* (1983 ; volume I publié en 2022 [65]) posent que les n-groupoïdes non stricts, et à la limite les ∞-groupoïdes, sont des modèles algébriques des n-types et des types d’homotopie. Dans la forme qu’en donne le tapuscrit de 1983, un *cohérateur* est une théorie globulaire, catégorie engendrée par les sommes globulaires des disques D_n, construite en ajoutant de proche en proche des opérations et des homotopies entre opérations parallèles ; un ∞-groupoïde de Grothendieck est un préfaisceau sur un cohérateur qui envoie les sommes globulaires sur des limites projectives (mise en forme : Maltsiniotis, prépublication [95]). L’hypothèse d’homotopie demande que la catégorie homotopique de ces objets, localisée aux morphismes qui induisent des bijections sur les groupes d’homotopie, soit équivalente à celle des types d’homotopie, de façon compatible aux troncations. Henry et Lanari (2023) [72] montrent que, si la structure de semi-modèle à gauche canonique existe sur les n-groupoïdes de Grothendieck, elle est équivalente à la structure de modèles des n-types, et en déduisent l’hypothèse pour $n = 3$; pour $n = \infty$, une prépublication la ramène, pour un cohérateur fixé, à une conjecture sur les sommes amalgamées (Henry 2016, conjecture 5.3.3 et corollaire 5.3.13 [71]), et elle reste ouverte. Les ∞-groupoïdes stricts ne suffisent pas : parmi les types simplement connexes, ceux qu’ils modélisent sont exactement les produits d’espaces d’Eilenberg–Mac Lane (Ara 2013 [4]). La seconde voie du tapuscrit, celle des catégories test et des localisateurs fondamentaux, modélise les types d’homotopie par des préfaisceaux d’ensembles (Maltsiniotis 2005 [94] ; Cisinski 2006 [32]). Les sections qui suivent en vérifient des lemmes : le complexe de chaînes d’un ensemble globulaire, de carré nul (section 70) ; les catégories à cofibrations de Baues (section 66) ; l’encadrement des localisateurs fondamentaux et la proposition 4 (section 67) ; les produits stables sans asphéricité (section 68) ; les monoïdes finis de la cote 158 (section 69) ; un lemme binomial (section 65). Aucune ne définit les cohérateurs, les ∞-groupoïdes de Grothendieck ni les espaces topologiques, et aucune ne compare deux théories homotopiques.

65 Cote 136 : le lemme binomial des ombres [68]

La cote 136, *Complexe de De Rham à puissance divisée [conférence de 1976 à l'IHÉS] : notes manuscrites (s.d.)*, que l'inventaire date « [à partir de 1975-1976] », est une liasse de notes autour d'une conférence : le complexe de De Rham à puissances divisées d'un ensemble simplicial, sa cohomologie, ses « ombres », la version duale et les automorphismes. L'algèbre des ombres est $S = k\{T\}$, l'algèbre des polynômes à puissances divisées sur un anneau commutatif k, de base les $T^{(i)}$, avec $T^{(i)}T^{(j)} = c_{i,j}\,T^{(i+j)}$, où $c_{i,j} = \binom{i+j}{i}$. Pour un k-module M et $N \geq 0$, l'ombre $\omega_N(M) = M \otimes_k S^{+(N)}$, où $S^{+(N)} = \sum_{i \geq N} k\,T^{(i)}$, est un S-module gradué. Les pages 19 à 22 démontrent par le critère de Lucas un lemme sur les coefficients binomiaux, le théorème 1 (136, lot 2, p. 22). La page 22 en tire que ω_N est pleinement fidèle : un morphisme $\omega_N(M) \to \omega_N(M')$ est une famille $u_i : M \to M'$, $i \geq N$, telle que $c_{i,j}(u_{i+j} - u_i) = 0$, et le théorème 1 dans le groupe $\mathrm{Hom}(M, M')$ la rend constante. Les pages 26 à 31 étendent le théorème au degré i, sous la forme qu'en donne la lecture : l'homomorphisme $M \otimes_k S \to \varphi_N\tau_N(M \otimes_k S)$ est un isomorphisme, φ_N adjoint à droite de la troncature, et cela revient à un énoncé sur des familles d'éléments d'un groupe abélien (136, lot 2, p. 26). Dans la démonstration du théorème 1, la phrase qui vérifie les hypothèses du lemme 2 finit sur un mot illisible. Les noms de Lucas et de Kummer sont de la lecture.

Théorème 65.1 (Grothendieck, page 22, théorème 1 ♦)**.** *Soient E un groupe abélien, $N \in \mathbf{N}$ et $(x_i)_{i\in\mathbf{N}}$ une famille d'éléments de E telle que $\binom{j}{i}(x_j - x_i) = 0$ pour $j > i \geq N$. Alors $x_i = x_N$ pour tout $i \geq N$.*

Théorème 65.2 (D'après les pages 26 à 31, la forme en degré i, sous une forme plus générale ♦)**.** *Soient $i, N \in \mathbf{N}$, M un groupe abélien et $(\xi_k)_{k\geq N}$ une famille d'éléments de M telle que $c_{l,k}\,\xi_k = c_{l,k-i}\,\xi_{k+l}$ pour tous $k \geq N$ et $l \geq 0$. Il existe un unique $\xi \in M$ tel que $\xi_k = \binom{k}{i}\xi$ pour tout $k \geq N$.*

La lecture suppose $i \leq N$, pour que $c_{l,k-i}$ ait un sens ; on lit ici $k - i$ comme une soustraction tronquée à 0, et l'énoncé vaut pour tout i. Pour $i = 0$, la relation s'écrit $c_{l,k}(\xi_{k+l} - \xi_k) = 0$, et le théorème 65.2 donne le théorème 65.1, puisque $\binom{k}{0} = 1$. On démontre donc le second. La démonstration n'est pas celle de la page : elle ne localise pas et ne passe pas par le décalage des chiffres p-adiques du lemme 2.

Lemme 65.3. *Soient p premier, $r \geq 0$ et $0 \leq b \leq p^r - 1$. Alors $\binom{p^r-1}{b} \equiv (-1)^b \pmod p$; en particulier p ne divise pas $\binom{p^r-1}{b}$.*

Résultat général, démontré en Lean dans
`Upstream/ChoosePrimePowSubOne.lean` *; la démonstration n'est pas reprise ici.*

C'est le « lemme commun » de la page 31 : quand $\mu + \nu = p^r - 1$, aucune retenue n'est possible et $c_{\mu,\nu} \not\equiv 0 \pmod p$.

Lemme 65.4. *Pour tous $k, l, i \in \mathbf{N}$, $\binom{k+l}{l}\binom{k}{i} = \binom{k+l}{i}\binom{k+l-i}{l}$, la soustraction étant tronquée.*

Démonstration. Si $i \leq k$, les deux membres valent $(k+l)!/(l!\,i!\,(k-i)!)$. Si $i > k$, le premier membre est nul, et le second aussi : pour $l = 0$, $\binom{k}{i} = 0$; pour $l > 0$, $k + l - i < l$. □

Lemme 65.5. *Soit z un élément d'un groupe abélien tel que, pour tout nombre premier p, un entier c non divisible par p vérifie $cz = 0$. Alors $z = 0$.*

68. Preuve vérifiée : `lean/Grothendieck/Folder136.lean`.

Démonstration. Soit d l'ordre de z, éventuellement nul. Si $d \neq 1$, soit p le plus petit facteur premier de d ($p = 2$ si $d = 0$). L'entier c associé à p vérifie $cz = 0$, donc $d \mid c$, et $p \mid c$, contradiction. Donc $d = 1$ et $z = 0$. □

Lemme 65.6. *Sous les hypothèses du théorème 65.2,* $\binom{k}{i}\xi_{k'} = \binom{k'}{i}\xi_k$ *pour tous* $k, k' \geq N$.

Démonstration. Soit $z = \binom{k}{i}\xi_{k'} - \binom{k'}{i}\xi_k$, et soit p premier. Choisissons r tel que $K = p^r - 1 \geq k + k'$. La relation pour $(k, K-k)$ et pour $(k', K-k')$ s'écrit $u\,\xi_k = a\,\xi_K$ et $u'\,\xi_{k'} = a'\,\xi_K$, avec $u = \binom{K}{K-k}$, $a = \binom{K-i}{K-k}$, $u' = \binom{K}{K-k'}$, $a' = \binom{K-i}{K-k'}$. Le lemme 65.4 donne $u\binom{k}{i} = \binom{K}{i}\,a$ et $u'\binom{k'}{i} = \binom{K}{i}\,a'$. Alors

$$uu'z = \tbinom{k}{i}u \cdot u'\xi_{k'} - \tbinom{k'}{i}u' \cdot u\xi_k = \tbinom{K}{i}\,aa'\,\xi_K - \tbinom{K}{i}\,a'a\,\xi_K = 0,$$

et p ne divise pas uu' par le lemme 65.3. Le lemme 65.5 conclut. □

Démonstration du théorème 65.2. Les $\binom{k}{i}$, $k \geq N$, engendrent l'idéal unité de $\mathbf{Z}$. En effet, cet idéal est principal, de générateur $g \geq 0$; si $g \neq 1$, soit p un facteur premier de g ($p = 2$ si $g = 0$) et r tel que $p^r - 1 \geq N + i$. Alors g divise $\binom{p^r-1}{i}$, que p ne divise pas par le lemme 65.3, contradiction. Il existe donc des $k_1, \ldots, k_n \geq N$ et des entiers $m_1, \ldots, m_n$ tels que $\sum_\alpha m_\alpha \binom{k_\alpha}{i} = 1$. Posons $\xi = \sum_\alpha m_\alpha\,\xi_{k_\alpha}$. Pour $k \geq N$, le lemme 65.6 donne

$$\tbinom{k}{i}\xi = \sum_\alpha m_\alpha \tbinom{k}{i}\xi_{k_\alpha} = \sum_\alpha m_\alpha \tbinom{k_\alpha}{i}\xi_k = \xi_k.$$

Si η vérifie aussi $\xi_k = \binom{k}{i}\eta$ pour tout $k \geq N$, alors $\eta = \sum_\alpha m_\alpha \binom{k_\alpha}{i}\eta = \sum_\alpha m_\alpha \xi_{k_\alpha} = \xi$. □

Remarque. Les deux énoncés tiennent tels que la lecture les donne. La combinaison de Bézout qui définit ξ et en donne l'unicité est celle de la page 27 ; le reste diffère. La page se ramène à un $\mathbf{Z}_{(p)}$-module, retranche la solution évidente et procède en deux lemmes sur les unités parmi les $c_{i,j}$. Ici, un seul indice $K = p^r - 1$ au-dessus de k et k' relie directement ξ_k et $\xi_{k'}$, et le lemme 65.5 remplace la localisation. Le théorème 1 de la page 22 se ramène lui aussi au lemme 2, $\mathbf{Z}_{(p)}$-local et pour un ensemble fini d'indices ; il est obtenu ici comme le cas $i = 0$. La pleine fidélité de ω_N en est l'instance dans le groupe des homomorphismes $M \to M'$, que le fichier énonce sur les familles d'homomorphismes, sans les modules gradués. La piste demande si le lemme ou la pleine fidélité figurent dans la littérature sur les modules sur les algèbres à puissances divisées ; sa partie modulaire n'est démontrée ici que sur les coefficients.

Ne sont pas démontrés ici : le critère de Lucas et le lemme 2 sous leur forme p-adique (pages 19 à 22) ; la pleine fidélité de ω_N et l'isomorphisme $M \otimes_k S \to \varphi_N\tau_N(M \otimes_k S)$ comme énoncés sur les S-modules gradués ; le corollaire $\mathrm{Ext}^n(\tau_{N-i}(S)[-i], M \otimes_k S) = 0$ et la pleine fidélité dans la catégorie dérivée (pages 262 à 272) ; la cohomologie des formes à puissances divisées et le schéma en groupes des automorphismes, dont les pistes figurent à la fin de la partie.

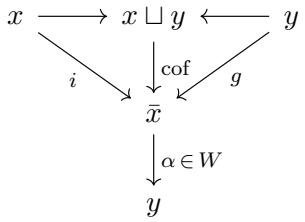
66 Cote 106 : catégories à cofibrations, factorisation de Brown et critère $(\star\star)$ [69]

La cote 106, *[Champs (stacks) 3] : notes manuscrites (s.d.)*, seize pages que l'inventaire date « [à partir de 1982] », est faite de huit feuillets de bloc entre lesquels sont intercalées des feuilles de listing ; certaines portent les dates d'impression des 24 et 25 août 1982. Elle s'ouvre sur « Soit $(\mathcal{C}, W, \mathrm{cof})$ une catégorie satisfaisant à C1 : C3 de Baues », construit le remplacement cofibrant et invoque le « weak lifting lemma » (106, lot 1, p. 1). La page 9 factorise une équivalence faible entre objets cofibrants et note en marge « On utilise $y \in \mathcal{C}_{\mathrm{cof}}$ ici » (106, lot 1, p. 9). La page 11 écrit : « Mais je doute qu'il ne suffise d'inverser les équiv. faibles *cofibrantes*, pour que les équiv. faibles deviennent inversibles ! » (106, lot 1, p. 11).

Définition. Une *catégorie à cofibrations* est une catégorie $\mathcal{C}$ à objet initial $\emptyset$, munie de deux classes de flèches, les équivalences faibles W et les cofibrations cof, qui vérifient les axiomes C1 à C3 des catégories à cofibrations de Baues [12], tels que la lecture les rappelle : C1, les isomorphismes sont dans W et dans cof, les composés de cofibrations sont des cofibrations, et W satisfait au deux-sur-trois ; C2, pour une cofibration $c : b \to a$ et une flèche $u : b \to y$, la somme amalgamée $a \vee_b y$ existe, la flèche $y \to a \vee_b y$ est une cofibration, et une équivalence faible si c en est une, et la flèche $a \to a \vee_b y$ est une équivalence faible si u en est une ; C3, toute flèche se factorise en une cofibration suivie d'une équivalence faible. Un objet x est *cofibrant* si $\emptyset \to x$ est une cofibration. On note $W_0 = W \cap \mathrm{cof}$.

Énoncé (Remplacement cofibrant et relèvement faible, page 1)**.** *Pour tout objet x, il existe $\alpha_x : \widetilde{x} \to x$ dans W avec $\widetilde{x}$ cofibrant. Soient $f : x \to y$, et $\alpha_x : \widetilde{x} \to x$, $\alpha_y : \widetilde{y} \to y$ dans W avec $\widetilde{x}$ et $\widetilde{y}$ cofibrants. Il existe $i : \widetilde{y} \to \widetilde{y}'$ dans $\mathrm{cof} \cap W$, $\alpha'_y : \widetilde{y}' \to y$ dans W avec $\alpha_y = \alpha'_y\, i$, et $\widetilde{f} : \widetilde{x} \to \widetilde{y}'$ avec $\alpha'_y \widetilde{f} = f \alpha_x$.*

Énoncé (Factorisation, page 9)**.** *Soient x, y cofibrants et $f : x \to y$ dans W. En factorisant $(f, 1_y) : x \sqcup y \to y$ en une cofibration $x \sqcup y \to \bar{x}$ suivie d'une équivalence faible $\alpha : \bar{x} \to y$, et en notant i et g les composés de $x \to x \sqcup y$ et $y \to x \sqcup y$ avec $x \sqcup y \to \bar{x}$, on a $\alpha i = f$, $\alpha g = 1_y$ et $i, g \in \mathrm{cof} \cap W$.*



$$\alpha i = f, \quad \alpha g = 1_y.$$

Énoncé (Le doute levé, page 11)**.** *Si tous les objets de $\mathcal{C}$ sont cofibrants, le foncteur $W_0^{-1}\mathcal{C} \to W^{-1}\mathcal{C}$ est un isomorphisme de catégories.*

Lemme 66.1. *Si x est cofibrant et $i : x \to z$ une cofibration, z est cofibrant.*

Démonstration. Par initialité, $\emptyset \to z$ est le composé de $\emptyset \to x$ et de i, qui est une cofibration par C1. □

69. Preuve vérifiée : `lean/Grothendieck/Folder106.lean`.

Lemme 66.2. *Soient $p : a \to y$ et $q : b \to y$, avec b cofibrant. La somme $a \sqcup b$ existe ; factorisons $(p, q) : a \sqcup b \to y$ par C3 en une cofibration $c : a \sqcup b \to z$ suivie de $w : z \to y$ dans W, et notons j_a, j_b les composés de c avec les injections de a et de b. Alors $wj_a = p$, $wj_b = q$, j_a est une cofibration, et j_b en est une si a est cofibrant.*

Démonstration. La somme $a \sqcup b$ est la somme amalgamée de $\emptyset \to b$ et de $\emptyset \to a$; comme $\emptyset \to b$ est une cofibration, elle existe par C2, et l'injection $a \to a \sqcup b$ est une cofibration. Donc j_a en est une par C1. Les égalités $wj_a = p$ et $wj_b = q$ résultent de $wc = (p, q)$. Si a est cofibrant, le même carré, lu dans l'autre sens, fait de $b \to a \sqcup b$ une cofibration, et j_b en est une. □

Démonstration du remplacement cofibrant et du relèvement faible. Par C3, $\emptyset \to x$ se factorise en une cofibration $\emptyset \to \widetilde{x}$ suivie de $\alpha_x : \widetilde{x} \to x$ dans W ; par initialité, la cofibration est la flèche $\emptyset \to \widetilde{x}$, et $\widetilde{x}$ est cofibrant.

Pour le relèvement, appliquons le lemme 66.2 à $a = \widetilde{y}$, $b = \widetilde{x}$, $p = \alpha_y$ et $q = f\alpha_x$; c'est la factorisation de $(\alpha_y, f\alpha_x) : \widetilde{y} \vee \widetilde{x} \to y$ que propose la lecture. Posons $\widetilde{y}' = z$, $i = j_a$, $\alpha'_y = w$ et $\widetilde{f} = j_b$. Alors i est une cofibration, parce que $\widetilde{x}$ est cofibrant ; $\alpha'_y \in W$; $\alpha'_y i = \alpha_y$ et $\alpha'_y \widetilde{f} = f\alpha_x$. Comme α'_y et $\alpha'_y i = \alpha_y$ sont dans W, i y est par deux-sur-trois. Enfin $\widetilde{y}'$ est cofibrant par le lemme 66.1, puisque $\widetilde{y}$ l'est. □

Démonstration de la factorisation. Appliquons le lemme 66.2 à $a = x$, $b = y$, $p = f$ et $q = 1_y$, et posons $\bar{x} = z$, $\alpha = w$, $i = j_a$, $g = j_b$. Alors $\alpha i = f$ et $\alpha g = 1_y$; i est une cofibration parce que y est cofibrant, et g en est une parce que x l'est. Comme α et $\alpha g = 1_y$, isomorphisme, sont dans W, $g \in W$ par deux-sur-trois ; comme α et $\alpha i = f$ sont dans W, $i \in W$. □

Démonstration de l'énoncé de la page 11. Montrons d'abord que tout foncteur $F : \mathcal{C} \to \mathcal{D}$ qui rend inversibles les flèches de W_0 rend inversibles celles de W. Soit $f : x \to y$ dans W ; x et y sont cofibrants, et la factorisation de la page 9 donne $f = \alpha i$ et $\alpha g = 1_y$ avec $i, g \in W_0$. Alors $F(g)$ est inversible et $F(\alpha)F(g) = 1$, donc $F(\alpha) = F(g)^{-1}$ est inversible, et $F(f) = F(\alpha)F(i)$ aussi.

Soient $Q_0 : \mathcal{C} \to W_0^{-1}\mathcal{C}$ et $Q : \mathcal{C} \to W^{-1}\mathcal{C}$ les foncteurs de localisation. Comme $W_0 \subseteq W$, Q rend inversibles les flèches de W_0, et la propriété universelle de Q_0 donne un unique $\bar{F} : W_0^{-1}\mathcal{C} \to W^{-1}\mathcal{C}$ tel que $\bar{F}Q_0 = Q$. Par ce qui précède, Q_0 rend inversibles les flèches de W, d'où un unique $\bar{G} : W^{-1}\mathcal{C} \to W_0^{-1}\mathcal{C}$ tel que $\bar{G}Q = Q_0$. Alors $\bar{G}\bar{F}Q_0 = Q_0$ et $\bar{F}\bar{G}Q = Q$, et l'unicité dans les deux propriétés universelles donne $\bar{G}\bar{F} = \mathrm{id}$ et $\bar{F}\bar{G} = \mathrm{id}$. □

Remarque. Dans le relèvement faible, l'hypothèse $\alpha_x \in W$ ne sert pas. L'hypothèse $\widetilde{y}$ cofibrant sert seulement à rendre $\widetilde{y}'$ cofibrant ; la lecture s'en sert sans le dire quand elle place $[i]^{-1}[\widetilde{f}]$ dans $W_{\mathrm{cof}}^{-1}\mathcal{C}_{\mathrm{cof}}$.

Remarque. Dans la factorisation, $f \in W$ sert seulement à mettre i dans W. Pour toute f entre objets cofibrants, on obtient encore $i \in \mathrm{cof}$, $g \in \mathrm{cof} \cap W$ et $\alpha \in W$. C'est le lemme de factorisation de K. S. Brown, publié en 1973 [25].

Remarque. Pour ces trois énoncés, seules servent, dans C2, l'existence des sommes amalgamées le long d'une cofibration et la stabilité des cofibrations par changement de base. Les deux clauses de C2 sur les équivalences faibles, et la clause de C1 qui fait des isomorphismes des cofibrations, ne servent pas.

Remarque. Lorsque tous les objets sont cofibrants, cadre où se place la page depuis la réduction de la page 5, le doute de la page 11 n'est pas fondé. L'argument est celui de la lecture, et tous ses éléments sont sur la page 9.

La page 11 rectifie la définition des diagrammes : la condition de cofibration passe de la flèche de retour à la flèche d'aller (106, lot 1, p. 11). Les pages 13 à 15 comparent deux factorisations d'une même flèche et posent la condition $(\star\star)$ sur deux sections d'une équivalence faible. Elles concluent : « Cette condition est (nec. et) suffis. pour que $\widetilde{\mathcal{C}} \to W^{-1}\mathcal{C}$ soit *fidèle* (donc un iso) » (106, lot 1, p. 15). La suffisance n'est pas écrite.

Définition. Soient x, y deux objets. On note $\mathrm{Ch}'_0(x,y)$ la catégorie des diagrammes $x \xrightarrow{f} \widetilde{y} \xleftarrow{i} y$ avec $f \in \mathrm{cof}$ et $i \in W$, une flèche $(f,i) \to (f',i')$ étant une $u : \widetilde{y} \to \widetilde{y}'$ telle que $uf = f'$ et $ui = i'$; deux diagrammes sont dans la même *composante connexe* s'ils sont reliés par la relation d'équivalence qu'engendre l'existence d'une telle flèche. Pour $(f,i) \in \mathrm{Ch}'_0(x,y)$ et $(g,j) \in \mathrm{Ch}'_0(y,z)$, soit P la somme amalgamée de $\widetilde{y} \xleftarrow{i} y \xrightarrow{g} \widetilde{z}$, qui existe par C2 puisque g est une cofibration, et soient $g' : \widetilde{y} \to P$, $k : \widetilde{z} \to P$ ses flèches ; on pose $(g,j) \circ (f,i) = (g'f, kj)$. La catégorie $\widetilde{\mathcal{C}}'$ a pour objets ceux de $\mathcal{C}$ et pour flèches $x \to y$ les composantes connexes de $\mathrm{Ch}'_0(x,y)$, l'unité de x étant la composante de $(1_x, 1_x)$. Le foncteur $q' : \widetilde{\mathcal{C}}' \to W^{-1}\mathcal{C}$ est l'identité sur les objets et envoie la composante de (f,i) sur $[i]^{-1}[f]$. La condition $(\star\star)$ est la suivante : pour toute $f : x \to y$ dans W et deux sections i, i' de f ($fi = fi' = 1_y$), les diagrammes $(1_x, i)$ et $(1_x, i')$ sont dans la même composante connexe de $\mathrm{Ch}'_0(x,y)$.

Théorème 66.3 (D'après les pages 11 à 15, le critère $(\star\star)$, forme complétée par l'édition ♦)**.** *Supposons tous les objets de $\mathcal{C}$ cofibrants. Alors $\widetilde{\mathcal{C}}'$ est une catégorie et q' un foncteur, et q' est fidèle si et seulement si $(\star\star)$ est vérifiée. Plus précisément : si q' est fidèle, $(\star\star)$ est vérifiée ; et q' est fidèle et plein, et c'est un isomorphisme de catégories, sans autre hypothèse. En particulier, $(\star\star)$ est toujours vérifiée.*

Lemme 66.4. *La composition de $\widetilde{\mathcal{C}}'$ est bien définie sur les composantes, associative, et admet les composantes des $(1_x, 1_x)$ pour unités ; q' est bien défini et c'est un foncteur.*

Démonstration. La flèche k est une équivalence faible par C2, comme somme amalgamée de l'équivalence faible i le long de la cofibration g, donc $kj \in W$; g' est une cofibration par C2, donc $g'f$ en est une. Si $u : (f,i) \to (f_1, i_1)$, la flèche $P \to P_1$ induite par u sur $\widetilde{y}$ et l'identité sur $\widetilde{z}$ est une flèche entre les deux composés ; de même si $v : (g,j) \to (g_1, j_1)$, avec v sur $\widetilde{z}$ et l'identité sur $\widetilde{y}$. La composition passe donc aux composantes. Pour trois diagrammes, la propriété universelle des sommes amalgamées donne une flèche du sommet de $((h,l) \circ (g,j)) \circ (f,i)$ vers celui de $(h,l) \circ ((g,j) \circ (f,i))$ compatible aux deux diagrammes, d'où l'associativité. Pour les unités, $(1_y, 1_y) \circ (f,i)$ a pour sommet la somme amalgamée de i et de 1_y, et la flèche $\widetilde{y} \to P$ relie (f,i) à ce composé ; de même à gauche. Si $u : (f,i) \to (f',i')$, alors $u \in W$ par deux-sur-trois et $[i']^{-1}[f'] = [ui]^{-1}[uf] = [i]^{-1}[f]$. Enfin, le carré $g'i = kg$ donne, dans la localisation, $[k]^{-1}[g'] = [g][i]^{-1}$, d'où $q'((g,j) \circ (f,i)) = [kj]^{-1}[g'f] = [j]^{-1}[k]^{-1}[g'][f] = [j]^{-1}[g][i]^{-1}[f]$. □

Lemme 66.5. *Soit $F : x \to z$, et soient $x \sqcup z \xrightarrow{c} \bar{z} \xrightarrow{\alpha} z$ une factorisation de $(F, 1_z)$ par C3, c cofibration, $\alpha \in W$, et (F_0, g) le diagramme $x \to \bar{z} \leftarrow z$ que forment les composés de c avec les injections. Si $(f,i) \in \mathrm{Ch}'_0(x,z)$ admet $\psi : \widetilde{z} \to z$ avec $\psi i = 1_z$ et $\psi f = F$, alors (f,i) et (F_0, g) sont dans la même composante.*

Démonstration. Le diagramme (F_0, g) est dans $\mathrm{Ch}'_0(x,z)$: F_0 est une cofibration (lemme 66.2, z étant cofibrant), et $g \in W$ par deux-sur-trois, puisque $\alpha g = 1_z$. Soit $h = (f,i) : x \sqcup z \to \widetilde{z}$, et soit Q la somme amalgamée de c et de h, qui existe puisque c est une cofibration ; la flèche $\widetilde{z} \to Q$ est une cofibration. Les flèches α et ψ coïncident sur $x \sqcup z$ après c et h (sur x, $\alpha F_0 = F = \psi f$; sur z,

$\alpha g = 1_z = \psi i$) et induisent $\theta : Q \to z$. Factorisons θ par C3 en une cofibration $\kappa : Q \to R$ suivie de $\beta : R \to z$ dans W. Le diagramme (f_R, i_R) obtenu en composant (f, i) avec $\widetilde{z} \to Q \xrightarrow{\kappa} R$ est dans $\mathrm{Ch}'_0(x, z)$: f_R est un composé de cofibrations, et $\beta i_R = \psi i = 1_z$ met i_R dans W par deux-sur-trois. La flèche $\widetilde{z} \to R$ va de (f, i) à (f_R, i_R) ; la flèche $\bar{z} \to Q \to R$ va de (F_0, g) à (f_R, i_R), puisque le carré de la somme amalgamée identifie les composés de c et de h. □

Lemme 66.6. *Choisissons pour toute F une factorisation comme au lemme 66.5, et notons $\varphi(F)$ la composante de (F_0, g), qui n'en dépend pas. Alors $\varphi : \mathcal{C} \to \widetilde{\mathcal{C}'}$ est un foncteur, $\varphi(f)$ est la composante de $(f, 1)$ pour toute cofibration f, φ rend inversibles les flèches de W, et pour $w : y \to \widetilde{y}$ dans W la composante de $(1_{\widetilde{y}}, w)$ est l'inverse de $\varphi(w)$.*

Démonstration. Tout repose sur le lemme 66.5. Avec $\psi = 1_x$, $\varphi(1_x)$ est l'unité, et avec $\psi = 1$, $\varphi(f)$ est la composante de $(f, 1)$ si f est une cofibration. Pour $f : x \to y$ et $h : y \to z$, de diagrammes (F_0, g), α et (H_0, g'), α', le composé de (F_0, g) et de (H_0, g') a pour sommet la somme amalgamée de g et de H_0, et $\psi = (\alpha', h\alpha)$ y est bien défini ($\alpha' H_0 = h = h\alpha g$) et vérifie les deux conditions pour hf : d'où $\varphi(hf) = \varphi(h)\varphi(f)$. Pour $w : y \to \widetilde{y}$ dans W, de diagramme (W_0, g) et α, le composé $\varphi(w) \circ (1_{\widetilde{y}}, w)$, c'est-à-dire $(W_0, g) \circ (1_{\widetilde{y}}, w)$, de sommet la somme amalgamée de w et de W_0, admet $\psi = (1_{\widetilde{y}}, \alpha)$ pour $F = 1_{\widetilde{y}}$: la composante de $(1_{\widetilde{y}}, w)$ est un inverse à droite de $\varphi(w)$. Si de plus $w \in \mathrm{cof}$, $\varphi(w)$ est la composante de $(w, 1)$, et le composé $(1_{\widetilde{y}}, w) \circ (w, 1)$ est $(kw, k'w)$, de sommet la somme amalgamée de $1_{\widetilde{y}}$ et de $1_{\widetilde{y}}$, où $k = k'$; la flèche kw le relie à $(1_y, 1_y)$. Donc φ rend inversibles les flèches de W_0, et par l'argument de la page 11 (démonstration de l'énoncé de la page 11) celles de W ; l'inverse à droite est alors l'inverse. □

Démonstration du critère. Nécessité. Soient $f : x \to y$ dans W et i, i' deux sections de f. De $fi = 1_y$ on tire $[i]^{-1} = [f]$, donc $q'(1_x, i) = [i]^{-1} = [f] = [i']^{-1} = q'(1_x, i')$; si q' est fidèle, $(1_x, i)$ et $(1_x, i')$ sont dans la même composante. C'est l'argument de la lecture.

q' est un isomorphisme. Pour toute F, le diagramme (F_0, g) admet α, avec $\alpha g = 1_z$, d'où $q'\varphi(F) = [g]^{-1}[F_0] = [\alpha][F_0] = [F]$: $q'\varphi = Q$. Par le lemme 66.6 et la propriété universelle de Q, il existe un unique $\bar{\varphi} : W^{-1}\mathcal{C} \to \widetilde{\mathcal{C}'}$ avec $\bar{\varphi}Q = \varphi$. Alors $q'\bar{\varphi}Q = q'\varphi = Q$, donc $q'\bar{\varphi} = \mathrm{id}$ par unicité. D'autre part, la composante de (f, i) est le composé $(1_{\widetilde{y}}, i) \circ (f, 1)$ (le sommet du composé est la somme amalgamée de $1_{\widetilde{y}}$ et de $1_{\widetilde{y}}$), c'est-à-dire $\varphi(i)^{-1}\varphi(f)$ par le lemme 66.6 ; donc $\bar{\varphi}q'(f, i) = \bar{\varphi}([i])^{-1}\bar{\varphi}([f]) = \varphi(i)^{-1}\varphi(f)$ est la composante de (f, i), et $\bar{\varphi}q' = \mathrm{id}$. Ainsi q' est un isomorphisme de catégories, d'inverse $\bar{\varphi}$: il est fidèle et plein, et $(\star\star)$ suit de la nécessité. □

Remarque. L'énoncé de la piste tient tel qu'il est écrit, et ses deux membres sont vrais : sous C1–C3, tous les objets étant cofibrants, q' est un isomorphisme et $(\star\star)$ est toujours vérifiée. La page énonce le critère ; l'isomorphisme sans autre hypothèse est de l'édition. Les pages 13 à 15 factorisent f seule, puis lui choisissent une section, et doivent alors comparer deux sections. La démonstration ci-dessus suit un autre chemin : elle factorise $(F, 1_z)$ hors de $x \sqcup z$, comme la page 9 ; la section fait alors partie de la cofibration, et toute comparaison passe par le lemme 66.5. La preuve ne dit rien de la littérature, où une description des flèches de $W^{-1}\mathcal{C}$ par composantes de diagrammes de ce type peut figurer, et la question de la piste reste ouverte.

Remarque. La composition de $\widetilde{\mathcal{C}'}$ utilise la clause de C2 que la lecture signale : la somme amalgamée d'une équivalence faible le long d'une cofibration est une équivalence faible. L'autre clause de C2 sur les équivalences faibles ne sert nulle part. La clause de C1 qui fait des isomorphismes des cofibrations sert ici, car l'unité $(1_x, 1_x)$ et les diagrammes $(1_x, i)$ de $(\star\star)$

demandent $1_x \in \mathrm{cof}$. L'hypothèse que tous les objets sont cofibrants sert deux fois : pour que les injections de $x \sqcup z$ soient des cofibrations, et pour que φ rende inversibles toutes les flèches de W.

Ne sont pas démontrés ici : l'équivalence $W_{\mathrm{cof}}^{-1}\mathcal{C}_{\mathrm{cof}} \simeq W^{-1}\mathcal{C}$ et la proposition de la page 5 ; Ch_0, $\widetilde{\mathcal{C}}$ et la plénitude de q (pages 5 à 9) ; la construction de la page 13 et la comparaison des factorisations (pages 13 à 15).

67 Cote 114 : les localisateurs fondamentaux et la proposition 4 [70]

La cote 114, *Asphéricité : notes manuscrites (s.d.)*, cinq pages que l'inventaire date « [1983] », contient quatre feuillets manuscrits et une page dactylographiée de *À la poursuite des champs*, numérotée 350. La page 2 pose la question « 0-connexité totale $\Rightarrow$ asphéricité totale ? » (114, lot 1, p. 2). La page 350 y répond par la proposition 4, précédée de l'aveu « After a minute's thought, I feel very silly ». La démonstration qui suit tient en trois lignes ; ses signes d'implication sont laissés en blanc, et elle s'interrompt sur « namely » (114, lot 1, p. 3). La page énonce la proposition pour « W a basic localizer satisfying Loc 4) » et appelle W_0 « the coarsest basic localizer satisfying Loc 4) ».

Définition. On fixe un univers ; une petite catégorie est une catégorie dont les objets et les flèches forment des ensembles de cet univers, et e désigne la catégorie ponctuelle. Pour des foncteurs $v : A \to B$ et $w : B \to C$ et un objet c de C, on note $A_{/c}$ la catégorie des couples $(a, \gamma : wv(a) \to c)$, $B_{/c}$ celle des couples $(b, \beta : w(b) \to c)$, et $v_{/c} : A_{/c} \to B_{/c}$ le foncteur $(a, \gamma) \mapsto (v(a), \gamma)$. Un *localisateur fondamental* est une classe W de foncteurs entre petites catégories qui vérifie :

- LA W est faiblement saturée : elle contient les identités, vérifie le deux-sur-trois, et si $i : A \to B$ et $r : B \to A$ vérifient $ri = 1_A$ et $ir \in W$, alors $r \in W$;
- LB si A a un objet final, $A \to e$ est dans W ;
- LC si, pour $v : A \to B$ et $w : B \to C$, tous les $v_{/c}$ sont dans W, alors $v \in W$.

Ce sont les axiomes usuels ; la lecture n'en donne qu'une description, « faiblement saturée », « les foncteurs $A \to e$ pour toute A ayant un objet final », « une condition du type « théorème A » de Quillen », qu'ils précisent. Une petite catégorie A est *W-asphérique* si $A \to e$ est dans W, et *totalement W-asphérique* si de plus, pour tous objets a, b de A, la catégorie $A_{/a\times b}$ des éléments du préfaisceau $a \times b$, formée des couples $(c, (p, q))$ avec $p : c \to a$, $q : c \to b$, est W-asphérique. Un préfaisceau X est *0-connexe* si $A_{/X}$ est non vide et connexe. On note $\pi_0(A)$ l'ensemble des composantes connexes de A, W_0 la classe des foncteurs u tels que $\pi_0(u)$ soit bijective, et W_∞ la classe des foncteurs qui appartiennent à tout localisateur fondamental.

Énoncé (Proposition 4, page 3)**.** *Soient A une petite catégorie, W un localisateur fondamental, W_∞ le localisateur fondamental le plus fin. Les conditions suivantes sont équivalentes :*

- *(i) A est totalement W_∞-asphérique ;*
- *(ii) A est totalement W-asphérique ;*
- *(iii) A est non vide et, pour tous objets a, b de A, le produit $a \times b$ est 0-connexe dans $\hat{A}$.*

70. Preuve vérifiée : `lean/Grothendieck/Folder114.lean`.

La démonstration repose sur l'encadrement $W_\infty \subseteq W \subseteq W_0$, où W_0 est le localisateur fondamental le plus grossier, celui pour lequel un foncteur est une équivalence dès qu'il induit une bijection sur les composantes connexes.

Lemme 67.1. *La classe W_0 est un localisateur fondamental.*

Démonstration. Comme π_0 est un foncteur, LA se ramène à des énoncés sur les bijections. Les identités sont bijectives, et si deux des applications $\pi_0(u)$, $\pi_0(u')$, $\pi_0(u'u)$ sont bijectives, la troisième l'est. Si $ri = 1_A$ et $\pi_0(i)\pi_0(r)$ est bijective, $\pi_0(r)$ est injective par la seconde relation et surjective par la première. Pour LB, une catégorie à objet final est non vide et connexe, et $\pi_0(A) \to \pi_0(e)$ est une bijection entre deux ensembles à un élément.

Pour LC, supposons tous les $\pi_0(v_{/c})$ bijectifs. Pour $b \in B$, choisissons, par surjectivité de $\pi_0(v_{/w(b)})$, un objet (a_b, γ_b) de $A_{/w(b)}$ dont l'image est dans la composante de $(b, 1_{w(b)})$, et posons $s(b) = [a_b] \in \pi_0(A)$. D'abord, $s(v(a)) = [a]$ pour tout $a \in A$: dans $A_{/wv(a)}$, les objets $(a_{v(a)}, \gamma_{v(a)})$ et $(a, 1)$ ont leurs images dans la composante de $(v(a), 1)$; par injectivité, ils sont dans la même composante, et l'oubli $(a', \gamma) \mapsto a'$ envoie un zigzag de $A_{/wv(a)}$ sur un zigzag de A. Ensuite, $s(b) = s(b')$ pour toute flèche $\beta : b \to b'$. La composition avec $w(\beta)$ définit des foncteurs $A_{/w(b)} \to A_{/w(b')}$ et $B_{/w(b)} \to B_{/w(b')}$ compatibles à $v_{/.}$; l'image de $(a_b, w(\beta)\gamma_b)$ par $v_{/w(b')}$ est donc dans la composante de $(b, w(\beta))$, que la flèche $\beta : (b, w(\beta)) \to (b', 1)$ relie à celle de $(b', 1)$, où se trouve aussi l'image de $(a_{b'}, \gamma_{b'})$. Par injectivité, $(a_b, w(\beta)\gamma_b)$ et $(a_{b'}, \gamma_{b'})$ sont dans la même composante de $A_{/w(b')}$, d'où $[a_b] = [a_{b'}]$. Par suite s est constante sur les zigzags de B et induit $\bar{s} : \pi_0(B) \to \pi_0(A)$ avec $\bar{s} \circ \pi_0(v) = \mathrm{id} : \pi_0(v)$ est injective. Elle est surjective, car l'oubli envoie le zigzag de $B_{/w(b)}$ qui relie $(v(a_b), \gamma_b)$ à $(b, 1)$ sur un zigzag de $v(a_b)$ à b dans B. □

Lemme 67.2. *Une petite catégorie est W_0-asphérique si et seulement si elle est non vide et connexe. Elle est totalement W_0-asphérique si et seulement si elle vérifie (iii).*

Démonstration. L'application $\pi_0(A) \to \pi_0(e)$ va dans un ensemble à un élément ; elle est bijective si et seulement si $\pi_0(A)$ a exactement un élément, c'est-à-dire si A est non vide et connexe. Pour la seconde assertion, être totalement W_0-asphérique, c'est donc être non vide et connexe, avec chaque $A_{/a\times b}$ non vide et connexe, et cela entraîne (iii). Réciproquement, sous (iii), A est non vide, et pour $a, b \in A$ un objet $(c, (p, q))$ de $A_{/a\times b}$ donne le zigzag $a \xleftarrow{p} c \xrightarrow{q} b$; A est donc connexe. C'est le « (iii) implies that A is 0-connected » de la page. □

Lemme 67.3. *La classe W_∞ est un localisateur fondamental, contenu dans tout localisateur fondamental.*

Démonstration. La seconde assertion est la définition. Chacun des axiomes LA à LC dit que certains foncteurs sont dans W dès que d'autres y sont ; si ces derniers sont dans W_∞, ils sont dans chaque localisateur fondamental W, les premiers aussi, et donc dans W_∞. □

Démonstration de (i) ⇒ (ii), et de (ii) ⇒ (iii) si $W \subseteq W_0$. L'asphéricité totale croît avec le localisateur : si $W \subseteq W'$, une catégorie totalement W-asphérique est totalement W'-asphérique, les foncteurs vers e en jeu étant dans W, donc dans W'. Comme W_∞ est contenu dans W (lemme 67.3), (i) entraîne (ii). Si $W \subseteq W_0$, (ii) entraîne que A est totalement W_0-asphérique, c'est-à-dire (iii) par le lemme 67.2. □

Deux localisateurs fondamentaux non contenus dans W_0. La classe de tous les foncteurs vérifie trivialement LA à LC. Soit W_{-1} la classe des foncteurs $u : A \to B$ tels que A soit vide si et seulement si B l'est. Elle contient les identités, et le deux-sur-trois vaut, l'équivalence « A vide $\iff$ B vide » étant transitive. Si $ri = 1_A$, A et B sont vides ensemble, par i et par r. Une catégorie à objet final n'est pas vide. Pour LC, si A n'est pas vide, B ne l'est pas ; si $b \in B$, $B_{/w(b)}$ contient $(b, 1)$, donc $A_{/w(b)}$ n'est pas vide, et A non plus. Le foncteur de la catégorie discrète à deux objets vers e est dans ces deux classes et n'est pas dans W_0.

Pour $W = W_{-1}$, soit $A = B(\mathbb{Z}/2)$ la catégorie à un objet $*$ dont le monoïde d'endomorphismes est le groupe $G = \mathbb{Z}/2$. Elle est non vide, et $A_{/*\times*}$ contient $(*, (1, 1)) : A$ est totalement W_{-1}-asphérique. Mais les objets de $A_{/*\times*}$ sont les couples $(p, q) \in G \times G$, et une flèche $g : (p', q') \to (p, q)$ vérifie $(p', q') = (pg, qg)$, de sorte que $p^{-1}q$ est constant sur chaque composante ; $(1, 1)$ et $(1, \sigma)$, où σ est l'élément non neutre, sont dans des composantes distinctes. Donc (iii) est en défaut, et (i) aussi : par les lemmes 67.1 et 67.3, $W_\infty \subseteq W_0$, et (i) entraînerait (iii) par ce qui précède. Pour la classe de tous les foncteurs, la catégorie vide est totalement asphérique et ne vérifie pas (iii). □

Remarque. L'inclusion $W \subseteq W_0$ est fausse pour les localisateurs fondamentaux définis par LA à LC seuls, et avec elle les implications (ii) $\Rightarrow$ (iii) et (ii) $\Rightarrow$ (i). Cisinski (2006, 9.3.1 et 9.3.2) [32] montre qu'un localisateur fondamental est contenu dans W_0 si et seulement s'il n'est pas grossier. La page impose la condition « satisfying Loc 4) », sans laquelle l'énoncé ne tient pas. Loc 4) est définie ailleurs dans *À la poursuite des champs*, hors de cette chemise, et l'on n'a pas vérifié si elle exclut les deux contre-exemples.

Remarque. La lecture identifie W_0 à la classe des foncteurs bijectifs sur π_0, que décrit Maltsiniotis (2005, 1.1.29 à 1.1.32) [94]. Cette classe est un localisateur fondamental (lemme 67.1) ; qu'elle soit le plus grossier de ceux qui vérifient Loc 4) n'est pas établi ici.

Remarque. L'implication (iii) $\Rightarrow$ (i), que la page affirme, a été réfutée plus tard dans la littérature par la catégorie des cubes (Maltsiniotis 2005 [94], Cisinski 2006 [32]).

Ne sont pas démontrés ici : la description de W_∞ comme classe des équivalences faibles usuelles (Cisinski) ; l'implication (iii) $\Rightarrow$ (i), réfutée dans la littérature ; le fait que W_0 soit le plus grossier sous Loc 4) ; le début de la page 3 ; les pages 1 et 2 ; le NB et la dominance (page 4) ; les contre-exemples et la question des pages 4 et 5.

68 Cote 118 : produits stables sans asphéricité[71]

La cote 118, *Cohomology properties of maps in (Cat)*, quarante pages que l'inventaire date « [à partir de 1983] », énonce page 32, avec un point d'interrogation, un lemme de conditions équivalentes pour une petite catégorie A. Les pages 33 et 34 établissent que (i) « A totalement asphérique » équivaut à (ii) « $\mathcal{W}_A$ stable par produits finis » jointe à l'asphéricité de A. La page 35 demande si une catégorie connexe qui satisfait (ii) est asphérique, et répond « Non » : pour A un groupoïde, $\mathcal{W}_A$ est formé des seuls isomorphismes, donc stable par produits finis (118, lot 2, p. 35). La connexité, l'hypothèse $G \neq 1$ et la raison donnée pour « formé des seuls iso » sont de la lecture.

Conventions. Pour $A = BG$, les préfaisceaux sur A sont les G-ensembles, et $A_{/X}$ est le groupoïde d'action $X//G$. Le modèle est tronqué en degré 1 : un foncteur entre groupoïdes est une

71. Preuve vérifiée : `lean/Grothendieck/Folder118.lean`.

équivalence faible s'il induit une bijection sur les composantes connexes et des isomorphismes sur les groupes d'automorphismes, et un groupoïde est asphérique s'il est connexe à groupes d'automorphismes triviaux. Ces caractérisations, classiques, servent de définitions et ne sont pas démontrées. Ainsi $f : X \to Y$ est dans $\mathcal{W}_A$ si f induit une bijection sur les orbites et si $\mathrm{Stab}(f(x)) = \mathrm{Stab}(x)$ pour tout x.

Contre-exemple 68.1 (Grothendieck, page 35, la réponse « Non » ⧫)**.** *Soit G un groupe non trivial et $A = BG$. Alors $\mathcal{W}_A$ est formé des bijections équivariantes, donc stable par produits de toute famille, finie ou non. Pourtant $A = A_{/e}$ n'est pas asphérique, ni le produit $a \times a$ du représentable a par lui-même.*

Démonstration. Si $f \in \mathcal{W}_A$ et $f(x) = f(x')$, la bijectivité sur les orbites donne h avec $hx = x'$; alors $h \in \mathrm{Stab}(f(x)) = \mathrm{Stab}(x)$ et $x' = x$. Tout y s'écrit $gf(x) = f(gx)$: f est bijective. La réciproque est immédiate, et un produit de bijections est une bijection. Le groupe d'automorphismes de l'unique objet de $A_{/e}$ est $G \neq 1$. Enfin a est le G-ensemble G, et dans $G \times G$ les points $(1,1)$ et $(1,g)$, $g \neq 1$, ne sont pas dans la même orbite : $A_{/a\times a}$ n'est pas connexe. □

Remarque. L'énoncé tient, y compris pour les produits infinis, que la page laisse en suspens dans le cas général. Il touche la proposition 4.3.2 de [32], qui range la condition (g) parmi des conditions équivalentes. Pour $A = BG$, la condition (g), stabilité des $\mathcal{W}$-équivalences de préfaisceaux par produits finis, est satisfaite, et la condition (a), asphéricité des $a \times b$, ne l'est pas : dans le modèle tronqué (`answer_page_35`), la première n'entraîne donc pas la seconde. Interrogé sur MathOverflow, l'auteur a précisé que l'implication (g) ⇒ (c) demande une hypothèse supplémentaire, par exemple que A soit déjà une catégorie test, et que le reste de l'ouvrage n'en dépend pas [33]. La page de 1983 porte déjà cette réserve : (ii) ne donne (i) que jointe à l'asphéricité de A.

L'écart entre (g) et (c), formalisé. La condition (c) de la proposition 4.3.2 demande que, pour tous préfaisceaux X et Y sur A, le foncteur canonique $A_{/X\times Y} \to A_{/X} \times A_{/Y}$ soit une équivalence faible. Pour $A = BG$, il s'écrit $(X \times Y)//G \to X//G \times Y//G$: sur les objets $(x,y) \mapsto (x,y)$, sur les flèches $g \mapsto (g,g)$. Le but est le groupoïde d'action de $G \times G$ sur $X \times Y$, où les deux coordonnées bougent indépendamment ; la source ne les laisse bouger qu'ensemble. Pour comparer deux groupoïdes d'action de groupes différents, le modèle tronqué s'étend sans changement : un foncteur donné par un morphisme $\varphi : G \to H$ et une application f avec $f(gx) = \varphi(g)f(x)$ est une équivalence faible s'il induit une bijection sur les orbites et, pour tout x, une bijection $\mathrm{Stab}(x) \to \mathrm{Stab}(f(x))$ par φ. Au-dessus de l'identité de G, on retrouve la définition précédente.

Contre-exemple 68.2 (l'écart entre (g) et (c), énoncé de l'édition)**.** *Soit G un groupe non trivial et $A = BG$. La condition (g) est satisfaite, et la condition (c) ne l'est pas : (g) n'entraîne pas (c). Dans le modèle, (c) vaut si et seulement si $G = 1$.*

Démonstration. La condition (g) est la stabilité par produits établie plus haut. Pour (c), prenons $X = Y = a$, le G-ensemble régulier G. Dans $a//G \times a//G$, on passe de $(1,1)$ à n'importe quel (g,h) par la flèche (g,h) : le but est connexe, et même équivalent au point, puisque l'action de $G \times G$ sur $G \times G$ est libre et transitive. Dans $(G \times G)//G$, en revanche, k envoie (g,h) sur (kg,kh) et conserve $g^{-1}h$: il y a une composante par élément de G, et chacune est un point puisque l'action reste libre. Pour $a \neq 1$, les objets $(1,1)$ et $(1,a)$ sont dans une même composante du but et dans deux composantes de la source ; le foncteur n'est pas bijectif sur les composantes. Avec $X = Y = e$, l'échec se lit sur les automorphismes : le foncteur $BG \to BG \times BG$ est la

diagonale $G \to G \times G$, qui n'atteint pas $(1, a)$. Enfin, si $G = 1$, les orbites sont des points et les stabilisateurs triviaux, et le foncteur canonique est l'identité. □

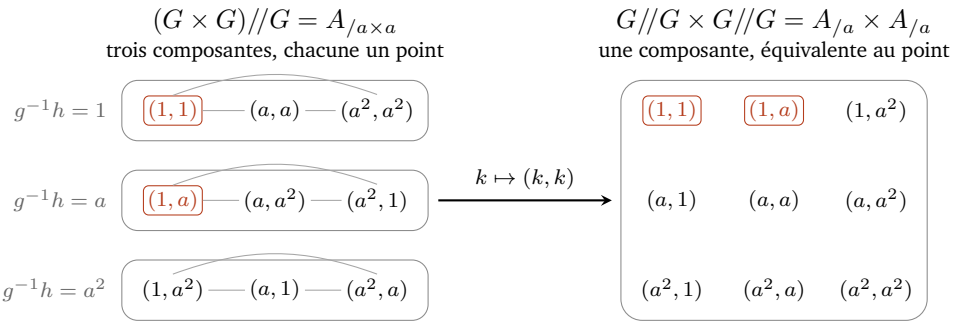


FIGURE 19 – Le foncteur canonique de la condition (c) pour $A = BG$, $G = \{1, a, a^2\}$ cyclique d'ordre 3, et $X = Y$ le G-ensemble régulier. À gauche, k envoie (g, h) sur (kg, kh) et conserve $g^{-1}h$: les neuf objets se répartissent en trois composantes, et deux objets d'une même composante sont reliés par une seule flèche. À droite, $G \times G$ agit librement et transitivement : la flèche $(1, a)$ relie $(1, 1)$ à $(1, a)$, encadrés, qui sont à gauche dans deux composantes distinctes. Le foncteur, bijectif sur les objets, n'est pas bijectif sur les composantes.

Le découpage de $A_{/a\times a}$ en $|G|$ morceaux, face au point $A_{/a} \times A_{/a}$ (figure 19), sépare les deux conditions : la stabilité de $\mathcal{W}$ par produits finis dans Cat donne (c) $\Rightarrow$ (g), et le sens réciproque demande l'hypothèse supplémentaire évoquée plus haut. Lean démontre, dans le modèle tronqué, que (g) est satisfaite et (c) non pour tout $G \neq 1$ (`g_not_imp_c`, avec les deux témoins `not_isWeqOver_regular` et `not_isWeqOver_point`), et que (c) équivaut à $G = 1$ (`condition_c_iff_subsingleton`). L'implication (c) $\Rightarrow$ (g), qui vaut en général, n'y est vraie que parce que (g) l'est toujours (`condition_g_of_c`) : elle n'est pas démontrée en général, pas plus que les autres conditions de la proposition 4.3.2 pour une catégorie A quelconque.
Les sommes, page 35. Pour montrer que (iv) est strictement plus faible que (i), la page avance que (iv) est « visiblement » stable par sommes de catégories, alors que (i) ne l'est pas, une somme n'étant pas connexe (118, lot 2, p. 35). La seconde lecture a trouvé l'argument faux, et Lean le vérifie cette fois sans modèle tronqué, dans les catégories de mathlib. Soit $A = A_1 \amalg A_2$, avec a dans A_1 et b dans A_2. Le préfaisceau $a \times b$ associe à un objet c l'ensemble des couples de flèches $c \to a$, $c \to b$; or aucun objet de la somme n'a de flèche vers les deux morceaux à la fois. Donc $a \times b$ est le préfaisceau vide, et $A_{/a\times b}$ est la catégorie vide. Une catégorie asphérique a un nerf contractile, elle est donc non vide et connexe, et la catégorie vide ne l'est pas. Lean n'emploie que cette conséquence, la connexité : l'échec vaut ainsi pour toute définition de l'asphéricité qui l'entraîne, celle du modèle tronqué comprise.

Contre-exemple 68.3 (correction de la seconde lecture, page 35)**.** *La condition « $A_{/a\times b}$ est non vide et connexe pour tous a, b », conséquence de (iv), est satisfaite par la catégorie ponctuelle et ne l'est pas par la somme de deux catégories ponctuelles ; elle échoue pour toute somme de deux catégories non vides. Elle force en outre une catégorie non vide à être connexe.*

Démonstration. Pour le point, $e \times e = e$ et $A_{/e}$ est le point. Pour une somme, on vient de voir que $A_{/a\times b}$ est vide. Enfin, si A satisfait la condition, $A_{/a\times b}$ a un objet, c'est-à-dire un objet c muni de flèches $c \to a$ et $c \to b$: le zigzag $a \leftarrow c \to b$ relie a à b, et A est connexe. □

La somme de deux points ne sépare donc pas (i) de (iv). Pour A non vide, (iv) donne déjà la connexité de A, et la dernière phrase de la proposition 4.3.2 de Cisinski [32] en tire l'asphéricité

de A, donc (i) ; les deux conditions ne diffèrent que pour A vide. Lean démontre les trois énoncés (`connectedProducts_not_stable_under_sums`, `not_connectedProducts_sum`, `isConnected_of_connectedProducts`) ; le passage de la connexité de A à son asphéricité n'est pas formalisé.

Ne sont pas démontrés ici : l'identification des équivalences faibles de groupoïdes à celles du modèle tronqué, les équivalences (i) $\Leftrightarrow$ (ii) $+$ « A asphérique » et (iv) $\Leftrightarrow$ asphéricité des $a \times b$ des pages 33 et 34, et le corollaire 2 de la page 31.

69 Cote 158 : monoïdes finis, monoïdes à élément minimal, catégories finies [72]

La cote 158, *[Autour des Dérivateurs] : notes manuscrites (s.d.)*, quatre-vingt-cinq pages que l'inventaire date « [vers 1990-1991] », étudie une seule question : une petite catégorie X est-elle cofiltrante dès que tout objet 0-connexe du topos des préfaisceaux sur X est 1-connexe ? Les pages 44 à 53, sous sa pagination 1 à 8, traitent le cas fini, en commençant par celui d'un monoïde, c'est-à-dire d'une catégorie à un objet. La proposition 1 est énoncée page 44 et démontrée jusqu'au haut de la page 46, qui conclut « cqfd » (158, lot 3, p. 44). Sous l'énoncé, un premier paragraphe, barré de deux longues diagonales, commence par « L'unicité de p est claire ». La démonstration reprend ensuite par la pseudo-cofiltrance et réalise M comme monoïde d'endomorphismes d'un ensemble E, le mot « fini » devant E étant biffé. Elle écrit : « comme E_0 est fini, on en conclut que $u(E_0) = E_0$ » (158, lot 3, p. 45).

Définition. Un monoïde M est *pseudo-cofiltrant* si, pour tous $u, v \in M$, il existe $u', v' \in M$ tels que $uu' = vv'$; il est *cofiltrant* s'il est pseudo-cofiltrant et si, pour tous $u, v \in M$, il existe $w \in M$ tel que $uw = vw$. Le *groupe enveloppant* de M est *trivial* si tout morphisme de monoïdes de M dans un groupe est trivial. La première définition est celle que la lecture tire de la page 55, où le manuscrit en donne l'équivalent ; la dernière est la propriété universelle du groupe enveloppant.

Théorème 69.1 (Grothendieck, Proposition 1, pages 44 à 46 ♦). *Soit M un monoïde fini dont le groupe enveloppant est trivial et qui est pseudo-cofiltrant. Alors il existe $p \in M$ tel que $up = p$ pour tout $u \in M$ (en particulier $p^2 = p$), et M est cofiltrant.*

Lemme 69.2. *Dans un monoïde fini pseudo-cofiltrant M, il existe p tel que, pour tout $u \in M$, on ait $p = uv$ pour un $v \in M$: p appartient à tous les idéaux à droite principaux uM.*

Résultat général, démontré en Lean dans `Upstream/MonoidRightZero.lean` *; la démonstration n'est pas reprise ici.*

Démonstration de la proposition 1. Soit p donné par le lemme 69.2, et $E_0 = pM$ l'ensemble des py, $y \in M$. C'est l'image de p dans la représentation régulière gauche de M, où u opère sur M par $x \mapsto ux$, et E_0 est fini puisque M l'est.

Chaque u envoie E_0 sur lui-même. Soit $u \in M$. D'abord $E_0 \subseteq uE_0$: le lemme appliqué à l'élément up donne v tel que $p = upv$, et pour $y \in M$, $py = upvy = u\big(p(vy)\big)$ est dans uE_0. D'autre part uE_0, image de E_0 par une application, a au plus autant d'éléments que E_0 ; comme E_0 est une partie de l'ensemble fini uE_0 et a au moins autant d'éléments que lui, $uE_0 = E_0$. L'application $x \mapsto ux$ est ainsi une surjection de l'ensemble fini E_0 sur lui-même, donc une bijection.

72. Preuve vérifiée : `lean/Grothendieck/Folder158.lean`.

Les deux premiers pas se lisent sur le carré suivant : $E_0 = pM$ est stable par la multiplication à gauche par u, qui y induit une bijection.

$$\begin{array}{ccc} E_0 = pM & \xrightarrow[\sim]{x\mapsto ux} & E_0 \\ \downarrow & & \downarrow \\ M & \xrightarrow[x\mapsto ux]{} & M \end{array}$$

Le morphisme vers un groupe. Notons $\varphi(u)$ la permutation $x \mapsto ux$ de E_0. On a $\varphi(1) = \mathrm{id}$ et, par associativité, $\varphi(uu') = \varphi(u) \circ \varphi(u')$: φ est un morphisme de monoïdes de M dans le groupe des permutations de E_0. Le groupe enveloppant de M étant trivial, $\varphi(u) = \mathrm{id}$ pour tout u. En l'appliquant à l'élément $p = p \cdot 1$ de E_0, on obtient $up = p$ pour tout $u \in M$.

Conclusion. Pour $u = p$, $p^2 = p$. Enfin M est pseudo-cofiltrant par hypothèse, et pour $u, v \in M$, $w = p$ vérifie $uw = p = vw$: M est cofiltrant. □

Remarque. La finitude sert deux fois : au lemme 69.2, pour passer de deux idéaux uM à tous, et pour changer l'inclusion $E_0 \subseteq uE_0$ en égalité. Le « comme E_0 est fini » de la page vaut parce que $E_0 = pM$ est contenu dans M. Il ne vaudrait pas pour un ensemble E quelconque, devant lequel la page a biffé « fini ».

Remarque. Sans la pseudo-cofiltrance, l'énoncé est faux : le monoïde $\{1, a, b\}$ où $ax = a$ et $bx = b$ pour tout x est fini, de groupe enveloppant trivial, et n'a pas d'élément p tel que $ap = p = bp$. Sans la finitude, il est faux pour le monoïde $\mathrm{Ep}(E)$ des surjections d'un ensemble infini E, que la lecture étudie à sa section 6. (Non démontré ici.)

Remarque. L'élément p n'est pas unique, et le noyau de Rees $MpM = pM$ n'est pas nécessairement réduit à un point. Soit $M = \{1, a, b\}$ avec $x \cdot 1 = x$, $x \cdot a = a$, $x \cdot b = b$ pour tout x ; cette loi est associative, d'unité 1, pseudo-cofiltrante ($ua = va$ pour tous u, v), de groupe enveloppant trivial ($g(a) = g(ba) = g(b)g(a)$ force $g(b) = 1$, et de même $g(a) = 1$) ; on a $ua = a$ et $ub = b$ pour tout u, aucun des deux n'est un zéro bilatère ($ab = b$), et l'intersection des idéaux MxM est $\{a, b\}$.

Remarque. La relation $up = p$ pour tout u fait de p un zéro à droite, et l'idéal à gauche $Mp = \{p\}$ est minimal. Une glose qui dirait p « zéro à gauche » et le noyau de Rees « ponctuel » serait fausse. Le paragraphe barré de la page 44 affirmait l'unicité de p, en identifiant pp' à $p'p$; l'exemple précédent la réfute.

Les monoïdes à élément minimal (pages 21 à 41). Un M-ensemble à droite X est un préfaisceau sur B_M ; sa catégorie d'éléments a pour objets les éléments de X et pour flèches $m : x \cdot m \to x$. Un foncteur de cette catégorie vers un groupe G est un cocycle, $c(x, mn) = c(x, m)\, c(x \cdot m, n)$, et il est isomorphe au foncteur trivial si $c(x, m) = g(x)\, g(x \cdot m)^{-1}$. On dit la catégorie d'éléments *simplement connexe* si tout cocycle, pour tout groupe G, est de cette forme ; pour une catégorie connexe, c'est $\pi_1 = 1$ (cette équivalence n'est pas formalisée). L'élément ψ est *minimal* si $\psi \in uM$ pour tout u.

Théorème 69.3 (Grothendieck, corollaire de la page 39 ♦). *Soit M un monoïde ayant un élément minimal ψ. Si tout M-ensemble à droite connexe a une catégorie d'éléments simplement connexe, M est cofiltrant. Réciproquement (énoncé de l'édition), pour tout monoïde cofiltrant, la catégorie d'éléments d'un M-ensemble connexe est simplement connexe.*

Démonstration. Cas où les puissances de ψ sont distinctes. C'est la proposition 2 de la page 31 avec $\varphi = \psi$, comme au corollaire de la page 33. Soit $F = M/R_\psi$, où $u \sim v$ si $\psi^p u = \psi^q v$. Pour

tout u, $\psi^p u = \psi^q u$ entraîne $p = q$: avec $ut = \psi$, on obtient $\psi^{p+1} = \psi^{q+1}$. Le degré relatif $d(u, v) = q - p$ est donc bien défini sur chaque classe, additif, et invariant par multiplication à droite. Avec un représentant $s(x)$ de chaque classe, $c(x, m) = d(s(x)m, s(x \cdot m))$ est un cocycle à valeurs dans $\mathbf{Z}$. Pour x la classe de $1 = \psi$, l'endomorphisme ψ a le degré 1, alors qu'un cobord y prend la valeur $g(x) - g(x) = 0$.

Cas où $\psi^r = \psi^s$ avec $r \neq s$. Une puissance $e = \psi^n$, $n \geq 1$, est idempotente et minimale. Les éléments minimaux forment eM, stable par multiplication à gauche : si $\lambda = u\lambda k$ et $\lambda = \lambda kj$, alors $u\lambda = \lambda j$. Avec $uek = e$ et $ekek_2 = e$, $x \mapsto ux$ est une bijection de eM, d'inverse $x \mapsto ek_2x$. On obtient ainsi un morphisme ρ de M dans le groupe des permutations de eM. Si ρ est trivial, $ue = e$ pour tout u, et M est cofiltrant ; sinon le point, dont la catégorie d'éléments est B_M, porte le cocycle non trivial ρ.

Réciproque. Si M est cofiltrant, deux éléments d'un M-ensemble connexe ont un descendant commun, et deux flèches parallèles ont même valeur, puisqu'elles sont égalisées plus loin. On fixe x_0 et, pour chaque x, des a, b avec $x \cdot a = x_0 \cdot b$, et l'on pose $g(x) = c(x, a)\, c(x_0, b)^{-1}$. Ce choix n'importe pas, et c est le cobord de g. □

Remarque. L'énoncé tient tel que la page 39 le donne, sous sa forme simplement connexe, et la dichotomie du corollaire fonctionne avec $\varphi = \psi$. Les hypothèses (B) à (D) des pages 22 à 30 s'y réduisent à « les puissances de ψ sont distinctes », et le degré se passe du plus petit objet comme de la présentation de π_1 (proposition 1, page 19). Dans l'autre cas, la stabilité de eM par multiplication à gauche est l'étape que la page 41 laisse sous ses mots illisibles. La variante « $H^1(X, \mathbf{Q}) = 0$ » de la page 39 n'est pas traitée ici.

Les catégories finies (pages 50 à 53). Le corollaire de la page 52 énonce : une catégorie finie X dont tout objet 0-connexe de $\widehat{X}$ est 1-connexe est cofiltrante (158, lot 3, p. 52). Un préfaisceau F sur X a pour catégorie d'éléments les couples (z, t), $t \in F(z)$; la simple connexité s'entend comme plus haut, par les cocycles. Notons (H) l'hypothèse.

Contre-exemple 69.4 (énoncé de l'édition ♦)**.** *La catégorie discrète à deux objets vérifie (H) et n'est pas cofiltrante.*

Démonstration. Une flèche y est une identité, donc tout cocycle est trivial, pour tout préfaisceau. La catégorie n'est pas connexe. □

Théorème 69.5 (d'après la page 52, cas X connexe)**.**
1. *(Pour toute petite catégorie.) Sous (H), deux éléments d'un préfaisceau connexe ont un ancêtre commun. En particulier, si X est non vide et connexe, deux objets sont buts de flèches issues d'un même objet, et deux flèches $u : x \to c$, $v : y \to c$ se complètent en un carré $uu' = vv'$.*
2. *Une catégorie finie, non vide et connexe, qui vérifie (H) est cofiltrante.*

Le carré du point 1 :

$$\begin{array}{ccc} z & \xrightarrow{v'} & y \\ {\scriptstyle u'}\downarrow & & \downarrow{\scriptstyle v} \\ x & \xrightarrow[u]{} & c \end{array} \qquad uu' = vv'.$$

Démonstration. (1) Si ξ et η n'ont pas d'ancêtre commun, les sous-préfaisceaux T_1 et T_2 qu'ils engendrent sont disjoints. On recolle deux copies de F le long de $T = T_1 \sqcup T_2$. Le préfaisceau obtenu est connexe, et compter 1 pour chaque flèche d'un élément de T_1 vers un élément de la seconde copie hors de T définit un cocycle à valeurs dans $\mathbf{Z}$. S'il était le cobord de g, la

différence $h(t) = g(t,2) - g(t,1)$ entre les deux copies serait constante le long des flèches hors de T, égale à 1 près de T_1 et à 0 près de T_2. Un zigzag de ξ à η mène à une contradiction. On applique ce lemme au préfaisceau final pour les cônes, et à $\mathrm{Hom}(-,c)$ pour les carrés.

(2) La finitude et (1) donnent un objet e qui envoie une flèche vers tout objet. Le monoïde $M = \mathrm{End}(e)$ est fini et pseudo-cofiltrant ; le lemme 69.2 et une puissance donnent un idempotent p minimal, $p \in uM$ pour tout u. Posons $L(z) = \{f : e \to z \mid fp = f\}$. Pour $k : z \to z'$, $f \mapsto kf$ envoie $L(z)$ sur $L(z')$: pour $f' \in L(z')$, le carré $ka = f'b$, une flèche $j : e \to w$ et $p = bj\theta$ donnent $f' = k(aj\theta p)$. Entre deux objets de l'ouvert X_0 des plus petits objets, qui ont des flèches dans les deux sens, ces surjections entre ensembles finis sont des bijections. L'ouvert X_0 est la catégorie d'éléments d'un sous-préfaisceau connexe du préfaisceau final. Par (H), ce système local est constant : il existe des bijections $\varphi_z : L(z) \to L(e)$ avec $\varphi_{z'}(kf) = \varphi_z(f)$. Pour $u : z \to y$, $z \in X_0$, l'application $s \mapsto u\,\varphi_z^{-1}(s)$ ne change pas le long d'une flèche, et deux tels couples (z,u) se relient par un carré. Pour $f, g : x \rightrightarrows y$ et $c : e \to x$, appliquée à (e, fc), (e, gc) et $s = \varphi_e(p)$, elle donne $fcp = gcp$. □

Remarque. Tel que la page le donne, le corollaire est faux pour une catégorie non connexe ; il faut que l'objet final de $\widehat{X}$ soit lui-même 0-connexe. Avec cette hypothèse, il tient, et le passage de (H) à la pseudo-cofiltrance, affirmé page 53 sans argument, vaut pour toute petite catégorie. La démonstration suit les pages 50 à 52, et l'ouvert X_0 y est le lieu où le système local H_x de la page 51 a des transitions bijectives.

Ne sont pas démontrés ici : la présentation de π_1 par les crochets de la proposition 1 (pages 19 et 20), dont la preuve ci-dessus se passe ; la proposition 2 « (??) » et le corollaire « Faux ! » ; $\mathrm{Ep}(E)$ et $\mathrm{Mon}(E)$; les pages 60 à 83.

70 Cote 104 : catégories de modèles, trois exemples, épinglages, un complexe globulaire [73]

La cote 104, *[Champs (stacks) 1] : copies de notes manuscrites (s.d.)*, seize pages sans date, appartient au groupe « Autour de *Pursuing stacks* », que l'inventaire date « 1968-1984 ». Les pages 6 à 16, sous sa pagination 1 à 6, sont une rédaction suivie. Une catégorie M de « modèles » y est remplacée par des ensembles ordonnés dont elle se reconstruit : l'ensemble $\mathbb{N}$ de ses classes d'isomorphisme, les ensembles I_n de sous-objets, les applications type τ_n. La page 6 pose les deux hypothèses (dans la seconde, « automorphisme » est biffé et remplacé par « end. ») et affirme que l'application $(*)$ ci-dessous « est injective par (i)(ii) » (104, lot 1, p. 6). La page 7 ajoute « On a donc (par (ii)) $\tau_n^{-1}(n) = \{d_n\}$ » (104, lot 1, p. 7). La page 10 affirme la réciproque et donne trois exemples, avec leurs dénombrements en marge (104, lot 1, p. 10). Parmi les feuillets d'essai qui précèdent, celui de la page 4 porte une suite $\mathbb{Z}[F_{n+1}] \to \mathbb{Z}[F_n] \xrightarrow{t_n - s_n} \mathbb{Z}[F_{n-1}]$ et, sous une accolade, le calcul $t_{n-1}(t_n y - s_n y) - s_{n-1}(t_n y - s_n y) = 0$ (104, lot 1, p. 4).

Définition. Soit M une catégorie telle que (i) toute flèche de M est un monomorphisme, et (ii) tout endomorphisme d'un objet de M est l'identité. Pour un objet D, un sous-objet de D est une classe de monomorphismes de but D, deux monomorphismes u, v étant équivalents s'ils se factorisent l'un par l'autre ; les sous-objets sont ordonnés par factorisation, et l'on note $u(D')$ le sous-objet défini par $u : D' \to D$. Pour un sous-objet x, on note encore x un objet qui le

73. Preuve vérifiée : `lean/Grothendieck/Folder104.lean`.

représente. Les classes d'isomorphisme d'objets de M sont préordonnées par l'existence d'une flèche.

Énoncé (Pages 6 et 7). *1. L'application $(*) : \mathrm{Hom}_M(D', D) \to \widetilde{D}$, $u \mapsto u(D')$, est injective.*

2. Si $f : D' \to D$ et $g : D \to D'$, alors f est un isomorphisme d'inverse g; le préordre sur les classes est donc un ordre.

3. Si $x \leq y$ sont deux sous-objets de D et s'il existe une flèche $y \to x$ (en particulier si x et y sont de même type), alors $x = y$. Par suite $\tau_n^{-1}(n) = \{d_n\}$, et τ_n est strictement croissante.

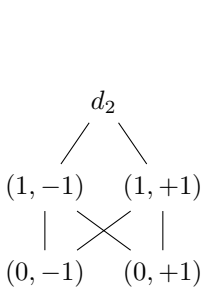
Énoncé (Page 10, la réciproque : un pas). *Soit f une application bijective d'un ensemble dans lui-même telle que $f \circ f = f$. Alors $f = \mathrm{id}$. En particulier la loi de composition $u_{d_n} \circ u_{d_n} = u_{d_n}$ force $u_{d_n} = \mathrm{id}$.*

Énoncé (Page 10, les trois exemples). *1. La catégorie des $\Delta_n = \{0, \ldots, n\}$ et des applications strictement croissantes vérifie (i) et (ii), et l'ensemble $\mathfrak{P}^*(\Delta_n)$ des parties non vides de Δ_n a $2^{n+1} - 1$ éléments.*

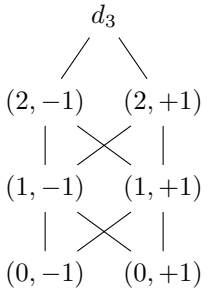
2. Les faces de $[0, 1]^n$, qui fixent certaines coordonnées à 0 ou à 1 et laissent les autres libres, sont au nombre de $\sum_k \binom{n}{k} 2^k = 3^n$.

3. Sur $I_n = (\Delta_{n-1} \times \{\pm 1\}) \sqcup \{d_n\}$, la relation « $(k, \varepsilon) \leq (k', \varepsilon')$ si et seulement si $(k, \varepsilon) = (k', \varepsilon')$ ou $k < k'$, et d_n plus grand élément » est un ordre ; I_n a $2n + 1$ éléments, dont exactement deux de type k pour chaque $k < n$. Avec $\{\pm 1\}$ muni de l'ordre chaotique, le produit n'est qu'un préordre : $(k, +1)$ et $(k, -1)$, distincts, sont chacun inférieurs à l'autre.

Les diagrammes de Hasse de I_2 et de I_3 (exemple 3) : deux éléments de chaque type $k < n$, chacun au-dessous des deux éléments du type suivant, et d_n au-dessus de tout.



I_2, 5 éléments



I_3, 7 éléments

Énoncé (Page 4, le complexe globulaire). *Soient des applications $s_n, t_n : F_n \to F_{n-1}$ et $s_{n-1}, t_{n-1} : F_{n-1} \to F_{n-2}$ telles que $s_{n-1}s_n = s_{n-1}t_n$ et $t_{n-1}s_n = t_{n-1}t_n$. Alors les morphismes $t_n - s_n : \mathbb{Z}[F_n] \to \mathbb{Z}[F_{n-1}]$ et $t_{n-1} - s_{n-1} : \mathbb{Z}[F_{n-1}] \to \mathbb{Z}[F_{n-2}]$ induits sur les groupes abéliens libres composent en zéro.*

$$F_n \underset{s_n}{\overset{t_n}{\rightrightarrows}} F_{n-1} \underset{s_{n-1}}{\overset{t_{n-1}}{\rightrightarrows}} F_{n-2} \qquad \begin{matrix} s_{n-1}s_n = s_{n-1}t_n, \\ t_{n-1}s_n = t_{n-1}t_n \end{matrix} \implies (t_{n-1} - s_{n-1})(t_n - s_n) = 0.$$

Démonstration de l'énoncé des pages 6 et 7. (1) Soient $u, v : D' \to D$ tels que $u(D') = v(D')$. Comme $u(D') \leq v(D')$, il existe $\theta : D' \to D'$ avec $v\theta = u$. Par (ii), $\theta = \mathrm{id}$, donc $u = v$.

L'hypothèse (i) ne sert qu'à faire de u et v des monomorphismes, c'est-à-dire à donner un sens à $u(D')$.

(2) Le composé gf est un endomorphisme de D', et fg un endomorphisme de D ; par (ii), ce sont des identités.

(3) Écrivons $x \leq y$ sous la forme $a_x = a_y \circ j$, où a_x, a_y sont les monomorphismes de but D qui représentent x et y et $j : x \to y$. Soit $g : y \to x$. Le composé $j \circ g$ est un endomorphisme de y, donc l'identité par (ii), et $a_y = a_y \circ j \circ g = a_x \circ g : a_y$ se factorise par a_x, c'est-à-dire $y \leq x$, et $x = y$. Si $\tau_n(x) = n$, x est isomorphe à D_n, qui représente le plus grand sous-objet d_n ; on a $x \leq d_n$ et une flèche $d_n \to x$, donc $x = d_n$. Si $x < y$, il y a une flèche $x \to y$, donc $\tau_n(x) \leq \tau_n(y)$; l'égalité donnerait une flèche $y \to x$, donc $x = y$; ainsi $\tau_n(x) < \tau_n(y)$ dans l'ensemble ordonné des classes. □

Démonstration du pas de la réciproque. Pour tout x, $f(f(x)) = f(x)$, et l'injectivité de f donne $f(x) = x$. □

Démonstration des trois exemples. (1) Une application strictement croissante est injective, donc simplifiable à gauche : si $fg = fh$, alors $g = h$ point par point. Une application strictement croissante de Δ_n dans lui-même est l'identité : c'est l'unique application strictement croissante de $\{0, \ldots, n\}$ sur une partie à $n+1$ éléments de Δ_n, à savoir Δ_n tout entier, et l'identité en est une. Les parties de Δ_n sont au nombre de 2^{n+1}, dont une vide.

(2) Une face est la donnée, pour chaque coordonnée, de la valeur 0, de la valeur 1, ou de rien : c'est une application de $\{1, \ldots, n\}$ dans un ensemble à trois éléments, et il y en a 3^n ; la marge appelle une telle donnée une section partielle de $\Delta_{n-1} \times \{\pm 1\} \to \Delta_{n-1}$. En comptant les faces selon le nombre k des coordonnées fixées, on obtient $\binom{n}{k}2^k$ faces pour chaque k, et $\sum_k \binom{n}{k}2^k = (2+1)^n$ par la formule du binôme ; c'est la formule de la page 5.

(3) La relation est réflexive. Elle est transitive : d_n est au-dessus de tout et au-dessous de lui seul, et sur $\Delta_{n-1} \times \{\pm 1\}$ la composée de deux relations « égal ou de premier indice strictement plus petit » en est une. Elle est antisymétrique : si $(k, \varepsilon) \leq (k', \varepsilon')$ et $(k', \varepsilon') \leq (k, \varepsilon)$ avec des éléments distincts, on aurait $k < k'$ et $k' < k$. Le cardinal est $2n+1$, et les éléments de type k sont $(k, +1)$ et $(k, -1)$. Pour l'ordre chaotique, $(k, \varepsilon) \leq (k', \varepsilon')$ équivaut à $k \leq k'$, et $(k, +1)$, $(k, -1)$ sont chacun inférieurs à l'autre. □

Démonstration de l'énoncé de la page 4. Le passage de F à $\mathbb{Z}[F]$ est fonctoriel : l'application induite par un composé est le composé des applications induites. Le composé $(t_{n-1} - s_{n-1})(t_n - s_n)$ vaut donc $\mathbb{Z}[t_{n-1}t_n] - \mathbb{Z}[t_{n-1}s_n] - \mathbb{Z}[s_{n-1}t_n] + \mathbb{Z}[s_{n-1}s_n]$, et les identités globulaires annulent les termes deux à deux. □

Remarque. L'exemple 3 est démontré sous la forme que la lecture substitue à la page. Elle prend Δ_{n-1} au lieu de Δ_n, qui donnerait $2n+3$ éléments au lieu des $2n+1$ de la marge. Elle prend l'ordre des cellules du disque au lieu du produit par un préordre chaotique, qui n'est pas antisymétrique.

Remarque. L'hypothèse (i) n'intervient ni dans l'ordre sur les classes ni dans $u_{d_n} = \mathrm{id}$, que (ii) donne seule. Dans $(*)$, que la page dit injective « par (i)(ii) », elle sert seulement à définir $u(D')$.

Remarque. L'exemple 1 montre que la catégorie des Δ_n et des injections croissantes n'a pas de dégénérescence. Pour les exemples, seul le calcul sur les ensembles I_n est démontré. L'identification des sous-objets des catégories de cubes et de disques à ces ensembles est celle de la lecture et n'est pas démontrée ici.

Énoncé (Page 6, note de la lecture : la bonne fondation)**.** *Soit M une catégorie vérifiant (ii). Pour deux objets X, Y, écrivons $X \prec Y$ s'il existe une flèche $X \to Y$ et aucune flèche $Y \to X$.*

1. *Toute flèche $X \to Y$ qui n'est pas un isomorphisme donne $X \prec Y$; si M est squelettique, toute flèche qui n'est pas une identité le donne.*
2. *Si M est squelettique et si $\prec$ est bien fondée, le rang ordinal $\deg$ pour $\prec$ est un degré que toute flèche autre qu'une identité augmente strictement, et M est une catégorie directe : une structure de Reedy dont la classe descendante est formée des identités et la classe ascendante de toutes les flèches.*
3. *Réciproquement, s'il existe une application $\deg$ des objets dans un ensemble ordonné bien fondé que toute flèche autre qu'une identité augmente strictement, $\prec$ est bien fondée.*
4. *Les hypothèses (i) et (ii) ne suffisent pas : la catégorie définie par l'ensemble ordonné $\mathbb{Z}$ les vérifie, et $\prec$ n'y est pas bien fondée.*

Démonstration. (1) Si $g : Y \to X$, alors gf et fg sont des endomorphismes, donc des identités par (ii), et f serait un isomorphisme. Si M est squelettique et f un isomorphisme, $X = Y$, et f, endomorphisme de X, est l'identité par (ii) ; une flèche qui n'est pas une identité n'est donc pas un isomorphisme.

(2) Dans une catégorie squelettique vérifiant (ii), $X \prec Y$ équivaut à l'existence d'une flèche $X \to Y$ autre qu'une identité : par (1) dans un sens, et dans l'autre parce que $X \prec Y$ interdit $X = Y$. On conclut par l'énoncé général rappelé à la suite de la démonstration : si cette relation est bien fondée, son rang ordinal est un degré que toute flèche autre qu'une identité augmente strictement, et il fait de la catégorie une catégorie directe.

(3) Si $X \prec Y$, une flèche $f : X \to Y$ n'est pas une identité, puisque $X = Y$ donnerait la flèche id_X de Y vers X ; donc $\deg X < \deg Y$, et $\prec$ est contenue dans l'image réciproque par $\deg$ d'un ordre bien fondé, qui est bien fondée.

(4) Entre deux objets de $\mathbb{Z}$ il y a au plus une flèche : (i) et (ii) sont immédiats. Pour tout m, $m - 1 \prec m$, et $\mathbb{Z}$ n'a donc pas d'élément minimal pour $\prec$. □

Résultat général, démontré en Lean dans
`Upstream/SemiSimplexCategoryReedy.lean` *; la démonstration n'est pas reprise ici.*

Remarque. La lecture énonce qu'une catégorie vérifiant (i) et (ii) est directe au sens de Reedy « dès que » l'ordre de $\mathbb{N}$ est bien fondé. L'exemple de $\mathbb{Z}$ montre que cette condition est une hypothèse supplémentaire, qui ne découle pas de (i) et (ii). La structure de Reedy est celle que définit la bibliothèque mathlib. L'hypothèse (i) n'y sert pas ; elle dit seulement que la classe ascendante est formée de monomorphismes. La catégorie squelettique est celle que la page 9 appelle « rigide ». Sans elle, un isomorphisme entre deux objets distincts n'augmenterait aucun degré ; la bonne fondation porte donc sur l'ordre des classes d'isomorphisme.

Énoncé (Page 10, exemple 1 : les identités simpliciales)**.** *Notons $\delta_i : \Delta_n \to \Delta_{n+1}$, pour $0 \le i \le n+1$, l'application strictement croissante qui évite i.*

1. *Pour $i \le j$, $\delta_{j+1} \circ \delta_i = \delta_i \circ \delta_j$.*
2. *Toute application strictement croissante $f : \Delta_m \to \Delta_{n+1}$ avec $m \le n$ s'écrit $\delta_i \circ g$, avec $g : \Delta_m \to \Delta_n$ strictement croissante.*
3. *La catégorie des Δ_n et des applications strictement croissantes est squelettique, toute flèche autre qu'une identité y augmente strictement n, et c'est une catégorie directe au sens de l'énoncé précédent.*

Démonstration. (1) Les deux membres envoient $k \in \Delta_n$ sur k si $k < i$, sur $k+1$ si $i \leq k < j$, et sur $k+2$ si $k \geq j$: c'est une vérification cas par cas sur les inégalités entre i, j et k. C'est la première identité simpliciale, que mathlib démontre dans la catégorie simpliciale ; elle est refaite ici dans la catégorie sans dégénérescences.

(2) Comme f est injective, une surjection de Δ_m, qui a $m+1 \leq n+1$ éléments, sur Δ_{n+1}, qui en a $n+2$, est impossible : f évite un i. Chaque $f(k)$, distinct de i, s'écrit $\delta_i(g(k))$ pour un unique $g(k)$, et g est strictement croissante parce que δ_i l'est et reflète donc l'ordre.

(3) Une flèche $\Delta_m \to \Delta_n$ est injective, donc $m \leq n$. Si $\Delta_m \simeq \Delta_n$, on a $m \leq n$ et $n \leq m$. Si $m = n$, la flèche est un endomorphisme, donc l'identité (exemple 1 ci-dessus). Le degré n, à valeurs dans les entiers, vérifie donc l'hypothèse de la partie (3) de l'énoncé précédent, et la partie (2) s'applique. □

Remarque. Ni les identités simpliciales ni la factorisation par les faces ne sont sur la page. Elles justifient l'identification, faite par la lecture, des préfaisceaux sur cette catégorie aux ensembles semi-simpliciaux. Par (2) et une récurrence sur $n - m$, toute flèche est un composé de faces, et (1) donne, en passant aux préfaisceaux, les relations $d_i d_j = d_{j-1} d_i$ pour $i < j$. Seul le pas de la récurrence est formalisé ici. Dans cet exemple $\mathbb{N} = \mathbf{N}$, comme la page 10 le dit des « cas que j'ai en tête », et la bonne fondation est celle des entiers.

Objets admissibles et ensembles ordonnés épinglés (pages 12 à 16). La page 12 définit les objets admissibles de $\widehat{M}$ par deux conditions : X est la borne supérieure de ses sous-objets isomorphes à des objets de M (ses sous-objets modèles), et l'intersection de deux sous-objets modèles est la borne supérieure des sous-objets modèles qu'elle contient. La page 13 affirme que leur catégorie « est équivalente à » celle des ensembles ordonnés M-épinglés, et la page 16 qu'elle est stable par sommes et sommes amalgamées, « de façon évidente » (104, lot 1, p. 13, 104, lot 1, p. 16). On suppose M squelettique, comme la lecture à partir de la page 9 ; I_D est alors l'ensemble des flèches de but D, ordonné par factorisation.

Théorème 70.1 (Grothendieck, pages 12 à 16, ensembles ordonnés épinglés ♦). *Soit M une petite catégorie squelettique dont toutes les flèches sont des monomorphismes et dont les seuls endomorphismes sont les identités.*

1. *Un préfaisceau X sur M est admissible si et seulement si tout élément $x \in X(D)$, vu comme morphisme $h_D \to X$, est un monomorphisme ; la première condition de la page 12 suffit.*
2. *Le foncteur $X \mapsto \widetilde{X}$, où $\widetilde{X}$ est l'ensemble des couples (D, x), $x \in X(D)$, ordonné par $(D', x') \leq (D, x)$ si $x' = X(a)(x)$ pour une flèche $a : D' \to D$, de type $(D, x) \mapsto D$ et épinglé par $u_{(D,x)}(a) = (D', X(a)(x))$, est une équivalence entre la catégorie des objets admissibles et celle des ensembles ordonnés M-épinglés ; un morphisme de $\widehat{M}$ est un monomorphisme si et seulement si l'application $\widetilde{X} \to \widetilde{Y}$ est injective.*
3. *Les sommes et les sommes amalgamées le long de monomorphismes, calculées dans $\widehat{M}$, d'objets admissibles sont admissibles, et $X \mapsto \widetilde{X}$ les envoie sur des sommes et des sommes amalgamées d'ensembles ordonnés épinglés.*

Démonstration. (1) Si X est réunion de sous-objets modèles, un élément x appartient à un sous-objet $S \simeq h_E$ et y correspond à une flèche $g : D \to E$; si $X(a)(x) = X(b)(x)$, alors $ag = bg$, et $a = b$ puisque g est un monomorphisme. Réciproquement, l'image de $h_D \to X$

est alors un sous-objet modèle qui contient x et reste dans tout sous-préfaisceau contenant x ; on obtient ainsi les deux conditions. (2) L'antisymétrie de l'ordre vient de (ii) et du caractère squelettique de M, et l'injectivité de $u_{(D,x)}$ de (1). En sens inverse, un ensemble ordonné épinglé K donne le préfaisceau $X_K(D) = \tau_K^{-1}(D)$, sur lequel une flèche a agit par $\xi \mapsto u_\xi(a)$; l'axiome (2) est la fonctorialité, et $\widetilde{X_K} \simeq K$ parce que u_ξ a pour image $K_{\leq\xi}$. Un morphisme épinglé $\widetilde{X} \to \widetilde{Y}$ préserve le type, donc s'écrit $(D,x) \mapsto (D, \alpha_D(x))$, et la commutation des triangles est la naturalité de α. (3) Un élément d'une somme, ou d'une somme amalgamée le long de monomorphismes, provient d'un des termes, par un morphisme qui est un monomorphisme (les préfaisceaux forment une catégorie extensive et adhésive) ; il reste donc un monomorphisme. Une équivalence préserve les limites inductives, et la sous-catégorie pleine des objets admissibles les reflète (Lean : `admissible_iff`, `versEpingle_isEquivalence`, `mono_iff_injective_versEpingle`, `admissible_coproduit`, `admissible_pushout`, `versEpingle_coproduit`, `versEpingle_pushout`). □

Remarque. L'ensemble ordonné $\widetilde{X}$ est la catégorie des éléments de X, que (ii), le caractère squelettique de M et la condition de (1) rendent ordonnée ; l'équivalence est la restriction de l'équivalence classique entre préfaisceaux et catégories fibrées en ensembles. Plus que la page 16 ne le dit, tout préfaisceau muni d'un morphisme vers un objet admissible est admissible. Les parties fermées et le recollement des pages 14 et 15 font l'objet de l'énoncé suivant ; le N.B. de la page 16 n'est pas démontré.

Parties fermées, et épinglages par les éléments maximaux (pages 14 et 15). La page 14 regarde un morphisme $f : K \to L$ d'ensembles ordonnés épinglés, surtout quand il est injectif : f est alors un isomorphisme de K sur son image $L' = f(K)$, partie fermée de L (stable par passage aux éléments plus petits), et une partie fermée porte un unique épinglage induit pour lequel l'inclusion est admissible. La page 15 suppose que K n'a qu'un nombre fini d'éléments maximaux et que tout élément est inférieur à l'un d'eux ; un épinglage est alors connu par les u_α, α maximal, et une telle famille définit un épinglage si et seulement si, pour $\xi \leq \alpha, \beta$, les deux isomorphismes $I_n \simeq K_{\leq\xi}$ induits sont « les mêmes » (104, lot 1, p. 14, 104, lot 1, p. 15).

Théorème 70.2 (Grothendieck, pages 14 et 15, parties fermées et recollement ♦)**.** *Soit M une petite catégorie squelettique dont toutes les flèches sont des monomorphismes et dont les seuls endomorphismes sont les identités, et soit $f : K \to L$ un morphisme d'ensembles ordonnés M-épinglés.*

1. *Pour tout $\xi \in K$, f induit une bijection croissante et à réciproque croissante de $K_{\leq\xi}$ sur $L_{\leq f(\xi)}$.*
2. *f est un monomorphisme d'ensembles ordonnés épinglés si et seulement s'il est injectif. Il est alors un isomorphisme d'ensembles ordonnés de K sur $f(K)$, et $f(K)$ est une partie fermée de L.*
3. *Une partie fermée S de L porte un épinglage, $u_\xi^S = u_\xi^L$, pour lequel l'inclusion est un morphisme ; il est unique : tout P muni d'un morphisme injectif $P \to L$ d'image S lui est isomorphe, au-dessus de L. En particulier un morphisme injectif f est un isomorphisme épinglé de K sur $f(K)$ suivi de l'inclusion.*
4. *Soient K un ensemble ordonné muni d'une application type strictement croissante, et $A \subset K$ une partie telle que tout élément soit inférieur à un élément de A (par exemple les éléments maximaux, s'il y en a un nombre fini et que tout élément est sous l'un*

d'eux, ou si K est fini). Un épinglage de K est déterminé par les u_α, $\alpha \in A$: pour $\xi = u_\alpha(y)$, $u_\xi = u_\alpha \circ (- \circ y)$. Une famille d'isomorphismes $v_\alpha : I_{\tau(\alpha)} \simeq K_{\leq\alpha}$, $\alpha \in A$, avec $v_\alpha(d) = \alpha$ et $\tau \circ v_\alpha = \tau_{\tau(\alpha)}$, provient d'un épinglage si et seulement si, chaque fois que $v_\alpha(y) = v_\beta(y') = \xi$, les antécédents y et y' ont même type et $v_\alpha \circ (- \circ y) = v_\beta \circ (- \circ y')$; l'épinglage est alors unique.

Démonstration. (1) Par l'axiome b) et la commutation des triangles, $f(K_{\leq\xi}) = f(u^K_\xi(I_n)) = u^L_{f(\xi)}(I_n) = L_{\leq f(\xi)}$, et f est injective sur $K_{\leq\xi}$ parce que $u^L_{f(\xi)}$ l'est ; si $f(a) \leq f(b)$ avec $a, b \leq \xi$, $f(a) = f(c)$ pour un $c \leq b$, et $a = c$. (2) Si f est injectif, le même argument donne $f(a) \leq f(b) \Rightarrow a \leq b$, et $\eta \leq f(\xi)$ entraîne $\eta \in f(K_{\leq\xi})$. Si f est un monomorphisme et $f(\xi) = f(\eta)$, ξ et η ont même type D ; les deux morphismes $\widetilde{h_D} \to K$, $a \mapsto u_\xi(a)$ et $a \mapsto u_\eta(a)$, ont même composé avec f, donc sont égaux, et l'image de id_D donne $\xi = \eta$. (3) Si $\eta \leq \xi \in S$, u^L_ξ prend ses valeurs dans $L_{\leq\xi} \subset S$, et les axiomes passent à S. Un morphisme épinglé bijectif dont la réciproque est croissante est un isomorphisme, la réciproque commutant aux épinglages par injectivité. (4) L'axiome (2) donne $u_\xi = u_\alpha \circ (- \circ y)$, d'où l'unicité et la nécessité de la condition (le type de y est $\tau(\xi)$ par (1)). Réciproquement, on pose $u_\xi = v_\alpha \circ (- \circ y)$ pour un $\alpha \in A$ et un y avec $v_\alpha(y) = \xi$ choisis ; la condition dit que le résultat ne dépend pas du choix, et les axiomes s'en déduisent, l'injectivité de u_ξ et l'axiome b) parce que y est un monomorphisme (Lean : `Epingle.Hom.image_Iic`, `Epingle.Hom.injOn_Iic`, `Epingle.Hom.le_iff_of_le`, `Epingle.mono_iff_injective`, `Epingle.Hom.le_iff_of_injective`, `Epingle.Hom.isLowerSet_range`, `Epingle.restreint`, `Epingle.inclusion`, `Epingle.Hom.isIso_versImage`, `Epingle.unique_restreint`, `Epingle.u_eq_of_le`, `Epingle.recollement`, `Recollement.recolle`, `Recollement.recolle_u_of_mem`, `Recollement.recolle_unique`, `exists_le_isMax`). □

Remarque. La finitude de l'ensemble des éléments maximaux ne sert pas : seul compte que tout élément soit sous l'un des $\alpha \in A$, et A peut être n'importe quelle famille ayant cette propriété. La condition que les deux antécédents aient même type, implicite sur la page, découle de l'axiome (1). Le monomorphisme du point (2) est pris dans la catégorie des ensembles ordonnés épinglés ; par l'équivalence de la page 13, ce sont aussi les monomorphismes de $\widehat{M}$.

Ne sont pas démontrés ici : la décomposition de toute flèche de l'exemple 1 en composé de faces, dont seul le pas est démontré ; l'isomorphisme $M \simeq M_0$ et la réciproque (pages 9 et 10) ; la sphéricité et la régularité de $|I^*_n|$; la page 11 ; le N.B. de la page 16 ; les conditions (C_i) de la page 4 ; les sous-objets des exemples. Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 42 à 45, excision pour deux cribles ouverts ♦). *Soient $\mathbb{D}$ un dérivateur et X une petite catégorie recouverte par deux cribles ouverts U et U'. Si $U \cap U' \to U'$ est une $\mathbb{D}$-équivalence cohomologique, alors $U \to X$ en est une. C'est la moitié de l'axiome W7 pour $W_\mathbb{D}$, tirée des seuls axiomes des dérivateurs.*

♢ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (page 45). L'identification de $\gamma(1,1)$ à $H^\bullet_\mathbb{D}(X, \xi)$ porte en marge « à vérifier (ou à mettre comme axiome sur les dérivateurs) », et l'édition donne le pas qui manque. Mathlib n'a pas les dérivateurs. On se reportera aux notes de Grothendieck (105, lot 3, p. 42).

Théorème (Grothendieck, pages 20 et 22, rectification d'un carré relatif ♦). *Dans une catégorie de modèles, soit un carré $pg = g'i$ où $i : X \to X'$ est une cofibration et $p : Y \to Y'$*

une fibration, et soient des cylindres $X \otimes J$, $X' \otimes J$ reliés par $i \otimes J$, tels que la flèche de coin $X \otimes J \sqcup_X X' \to X' \otimes J$ soit une cofibration triviale. Soit $\varphi : X' \to Y$ une diagonale. Il existe une diagonale $\overline{\varphi}$, homotope à φ, avec $\overline{\varphi} i = g$ et $p\overline{\varphi} = g'$, si et seulement s'il existe des homotopies $k : \varphi i \to g$ et $h : p\varphi \to g'$ compatibles, c'est-à-dire $p \circ k = h \circ (i \otimes J)$. Si Y' est l'objet final, la compatibilité est automatique.

Démonstration. Suffisance : les données φ sur $X' \otimes \{0\}$ et k sur $X \otimes J$ se recollent en une flèche $X \otimes J \sqcup_X X' \to Y$; la compatibilité dit exactement que, composée avec p, elle est la restriction de h. Le carré ainsi formé a une cofibration triviale à gauche et la fibration p à droite : il a un relèvement $L : X' \otimes J \to Y$, homotopie de φ à $\overline{\varphi} = L \circ i_1$. Alors $\overline{\varphi} i = L \circ (i \otimes J) \circ i_1 = k \circ i_1 = g$ et $p\overline{\varphi} = h \circ i_1 = g'$. Nécessité : une homotopie $K : \varphi \to \overline{\varphi}$ donne $k = K \circ (i \otimes J)$ et $h = p \circ K$, qui sont compatibles par associativité. Si Y' est final, deux flèches vers Y' sont égales. Lean (`Folder107.lean`) démontre la suffisance (`rectification`) sous la seule propriété de relèvement de $i \otimes J$ contre p, la nécessité (`compatible_of_rectification`), le critère (`rectification_iff`, et `rectification_modelCategory` dans une `ModelCategory` de Mathlib, où la propriété vient de l'axiome de relèvement) et le cas final (`rectification_of_isTerminal`).

La compatibilité est prise au sens strict de la page 22. Ne sont pas démontrés : la forme « à homotopie relative aux extrémités près » de la marge de la page 20, lecture de l'édition, qui demande des cylindres de cylindres ; l'existence, dans une catégorie de modèles quelconque, de cylindres relatifs dont la flèche de coin est une cofibration triviale (axiome SM7 dans le cas simplicial), qui est ici une hypothèse ; et le contre-exemple de l'édition (fibration des chemins sur S^1) montrant que la condition peut manquer. On se reportera aux notes de Grothendieck (107, lot 1, p. 20).

Théorème (Grothendieck, page 2, Δ° et les catégories test ♦). *La catégorie Δ° n'est pas une catégorie test.*

◊ non vérifié en Lean

La question 6 de la liste reçoit pour réponse un « non » souligné, sans argument ; la page ne définit ni modélisateur ni catégorie test, et l'édition ne reconstruit pas d'argument. Mathlib n'a pas les catégories test. On se reportera aux notes de Grothendieck (108, lot 1, p. 2).

Théorème (D'après les pages 18 à 20, forme complétée par l'édition, sommes amalgamées le long d'opfibrations ; voir aussi Cisinski [32] ♦). *Soient $\mathcal{W}$ un localisateur fondamental et, dans* **Cat**, *un carré cocartésien et cartésien formé de $i : Y \to X$, $g : Y \to Y'$, $f : X \to X'$ et $i' : Y' \to X'$, où i' et f sont des opfibrations de Grothendieck et où, au-dessus de chaque objet de X', l'une des fibres de f ou de i' est équivalente au point. Ce carré est homotopiquement cocartésien : si $i \in \mathcal{W}$, alors $i' \in \mathcal{W}$, et si $g \in \mathcal{W}$, alors $f \in \mathcal{W}$.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 18 à 20). L'argument de cocartésianité s'interrompt, et l'hypothèse cartésienne est de la lecture. Cisinski conditionne ses énoncés voisins à des immersions, non à des opfibrations. Mathlib n'a pas les localisateurs fondamentaux. On se reportera aux notes de Grothendieck (118, lot 1, p. 18).

Théorème (Grothendieck, pages 161 à 179 et 189 à 199, schéma en groupes des automorphismes ♦). *Les homomorphismes d'anneaux simpliciaux entre algèbres de de Rham à puissances divisées $\mathcal{A}(S, S^+, t)_*$, sans graduation, filtration ni puissances divisées imposées, sont classés par des données $(\varphi_0, A'_1, (B'_i))$ soumises à trois conditions, la troisième étant $(2B'_i)J' = 0$. Le foncteur des automorphismes de l'algèbre complétée sur $k\{T\}$ est donc un schéma en groupes affine sur* **Z**, *produit semi-direct de $\mathbf{G}_m$ par un groupe unipotent dont les facteurs sont tués par 2. Quand 2 est inversible, tout automorphisme respecte la graduation extérieure et opère sur la cohomologie par $\mathbf{G}_m$ seul.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 173 à 179) : la condition 3) est affirmée sans raison, et la raison qu'en donne la lecture est la sienne. Mathlib n'a pas les algèbres simpliciales à puissances divisées. On se reportera aux notes de Grothendieck (136, lot 9, p. 161).

Théorème (Page 8, forme démontrée par l'édition, la ligne de degré total n sur un simplexe ♦). *Soient k un anneau commutatif et $m \geq 0$. Sur le m-simplexe, $C^{\bullet\bullet}_{[m]} \simeq k\{T\}\{Y_1,\dots,Y_m\}[dY_1,\dots,dY_m]$, avec $dT = 0$. En degré total n, la ligne $0 \to k \xrightarrow{1\mapsto T^{(n)}} C^{n,0}_{[m]} \to C^{n-1,1}_{[m]} \to \cdots \to C^{0,n}_{[m]} \to 0$ est exacte : tout cocycle de degré extérieur $q \geq 1$ est un cobord, et les cocycles de degré extérieur 0 sont les $cT^{(n)}$, $c \in k$ unique. La multiplication par $T^{(j)}$ envoie la classe $T^{(n)}$ sur $c_{j,n}\,T^{(n+j)}$. Graduée par le degré total, la cohomologie de $\Delta[m]$ est donc $k\{T\} = \tau_{\geq 0}(H^0(\Delta[m],k) \otimes_k k\{T\})$.*

Démonstration. Une forme s'écrit $\sum f(a,\beta,I)\,T^{(a)}Y^{(\beta)}dY_I$, et $d(Y^{(\beta)}dY_I) = \sum_j Y^{(\beta-e_j)}dY_j \wedge dY_I$; le carré de d est nul, les deux ordres d'enlever dY_i et dY_j différant d'un signe. On construit une homotopie contractante sans division. Pour un monôme non constant, soit j la plus petite variable qu'il fait intervenir, par $Y_j^{(\beta_j)}$ avec $\beta_j \geq 1$ ou par dY_j. On pose $H(Y^{(\beta)}dY_I) = Y^{(\beta+e_j)}dY_{I\smallsetminus j}$ si $j \in I$, et 0 sinon. Quand $j \in I$, seul le terme où d remet dY_j survit dans dH ; quand $j \notin I$, Hd redonne le monôme, et les autres termes de Hd et de dH se compensent deux à deux. On obtient $Hd + dH = 1 - P$, où P projette sur les constantes $T^{(a)}$. C'est l'homotopie du produit tensoriel des complexes à une variable $Y^{(a)} \mapsto Y^{(a-1)}dY$. Les puissances divisées la rendent entière, là où l'homotopie d'Euler diviserait par le poids. H et d conservent le degré total. Un cocycle f de degré extérieur $q \geq 1$ vérifie $Pf = 0$, donc $f = d(Hf)$. En degré extérieur 0, $Hf = 0$, donc $f = Pf$ est un multiple de $T^{(n)}$. Enfin $T^{(j)}T^{(a)} = c_{j,a}T^{(a+j)}$ commute à d. Lean (`Folder136.lean`), sur un ensemble fini totalement ordonné de variables quelconque, démontre $d \circ d = 0$ (`pdD_pdD`), la formule d'homotopie (`pdH_pdD_add`), l'exactitude en degré extérieur $q \geq 1$ (`exact_of_pos`), le degré 0 (`cocycle_zero`, `smul_tPow_eq_zero`), la structure de $k\{T\}$-module (`pdD_tMul`, `tMul_tMul`, `tMul_tPow`), et les réunit dans `pd_row_cohomology`.

Le modèle en coordonnées $(T, Y_1, \dots, Y_m)$, avec $Y_i = X_i$ et $X_0 = T - \sum Y_i$, est l'isomorphisme que les pages 5 à 7 énoncent ; il est identifié à $\Gamma\Phi_{[m]} \otimes \Lambda^q\Psi_{[m]}$, comme module et avec sa structure simpliciale, au théorème suivant. C'est le premier pas de l'argument de la page 8, l'exactitude de chaque ligne. Le second pas, l'acyclicité des $C^{p,q}_*$ pour $p \geq 1$, n'est pas formalisé, et l'énoncé pour un ensemble simplicial quelconque reste non vérifié (ci-dessous).

Théorème (Pages 5 à 7, forme démontrée par l'édition, le modèle en coordonnées et sa structure simpliciale ♦). *Soit k un anneau commutatif. Si $(b_i)_{i\in\sigma}$ est une base finie d'un k-module M, les produits $\prod_i b_i^{(a_i)}$, $a \in \mathbf{N}^{(\sigma)}$, forment une base de l'algèbre à puissances divisées $\Gamma_k(M)$. Soient $\Phi_{[m]} = k^{m+1}$, $T = (1,\dots,1)$ et $\Psi_{[m]} = \Phi_{[m]}/kT$. Les $T, Y_1, \dots, Y_m$, où Y_i est le i-ième vecteur de base, forment une base de $\Phi_{[m]}$, les classes $dY_1,\dots,dY_m$ des Y_i une base de $\Psi_{[m]}$, et les $T^{(a)}Y^{(\beta)} \otimes dY_I$, $|I| = q$, une base de $\Gamma(\Phi_{[m]}) \otimes \Lambda^q\Psi_{[m]}$: ce sont les monômes du modèle en coordonnées. On a $T^{(j)} \cdot T^{(a)}Y^{(\beta)} = c_{j,a}\,T^{(a+j)}Y^{(\beta)}$. Enfin $[n] \mapsto \Gamma(\Phi_{[n]}) \otimes \Lambda^q\Psi_{[n]}$, $\theta \mapsto \Gamma(\Phi(\theta)) \otimes \Lambda^q(\Psi(\theta))$, où $\Phi(\theta)(f) = f \circ \theta$, est un k-module simplicial, dont les $T^{(p)}$ sont des sections.*

Démonstration. Mathlib définit $\Gamma_k(M)$ par générateurs et relations et montre que les produits $\prod_i b_i^{(a_i)}$ l'engendrent ; reste leur indépendance, sans division. L'algèbre symétrique $\operatorname{Sym} M^\vee$ est une bigèbre cocommutative où les $\varphi \in M^\vee$ sont primitifs, de sorte que son dual $(\operatorname{Sym} M^\vee)^*$, muni de la convolution, est un anneau commutatif. Pour $x \in M$, soit $F_n(x)$ la forme linéaire qui envoie u sur le coefficient de X^n dans l'image de u par $\varphi \mapsto \varphi(x)X$. On a $F_0(x) = 1$, $F_n(rx) = r^nF_n(x)$, $F_n(x)F_p(x) = \binom{n+p}{n}F_{n+p}(x)$, car $X \mapsto X \otimes 1 + 1 \otimes X$ envoie X^N sur $\sum \binom{N}{i}X^i \otimes X^{N-i}$, et $F_n(x+y) = \sum_{i+j=n} F_i(x)F_j(y)$. La propriété universelle donne un morphisme d'algèbres $\Gamma_k(M) \to (\operatorname{Sym} M^\vee)^*$, $x^{(n)} \mapsto F_n(x)$. Par récurrence sur le support de a, il envoie $\prod_i b_i^{(a_i)}$ sur la forme « coefficient de X^a après $\varphi \mapsto \sum_i \varphi(b_i)X_i$ », qui vaut

1 sur $\prod_i (b_i^\vee)^{a_i}$ et 0 sur les autres monômes en les $b_i^\vee$. Les images sont donc indépendantes, et les produits aussi. Le reste est de l'algèbre linéaire : $\Psi_{[m]} \simeq k^m$ par $f \mapsto (f(i) - f(0))_i$, de noyau kT ; les puissances extérieures d'un module libre ont la base des dY_I (Mathlib) ; la formule pour $T^{(j)}$ est $T^{(j)}T^{(a)} = c_{j,a}T^{(a+j)}$; $\Phi(\theta)$ fixe T, passe donc au quotient Ψ, et la fonctorialité de Γ et de Λ^q donne celle du produit tensoriel. Lean (`Folder136.lean`) démontre l'indépendance (`dp_prod_linearIndependent`), la base (`dpBasis`), les bases T, Y et dY (`tyBasis`, `psiBasis`), la base des monômes (`pdModelBasis_apply`), l'action de $T^{(j)}$ (`dp_one_mul_dpBasis`), le module simplicial (`pdSimplicial`) et la section $T^{(p)}$ (`pdModelMap_tPow`).

La démonstration n'est pas celle des pages, qui écrivent l'isomorphisme $k\{T, X_0, \dots, X_n\}/(\sum X_i - T)_{\mathrm{pd}} \simeq k\{X_0, \dots, X_n\}$ sans le justifier. L'identification porte sur les modules et sur l'action de $k\{T\}$. Ne sont pas formalisés : la différentielle $d(x^{(n)}) = x^{(n-1)}\,dx$ sur $\Gamma\Phi \otimes \Lambda^\bullet\Psi$ et son accord avec celle du modèle en coordonnées, la graduation par p (le Γ de Mathlib n'est pas encore gradué), le produit de $\Gamma \otimes \Lambda^\bullet$, la présentation $S\{X_0, \dots, X_n\}[dX]/(\sum X_i - t, \sum dX_i)_{\mathrm{pd}}$ de la page 5, et l'écriture des opérateurs de faces dans les coordonnées (T, Y).

Théorème (Grothendieck, pages 5 à 10 et 226 à 232, ombres de la cohomologie entière ; voir aussi Kageyama 2022 ♦). *Soit $C^{p,q} = \Gamma^p\Phi \otimes \Lambda^q\Psi$ la $k\{T\}$-algèbre simpliciale des formes à puissances divisées sur le simplexe $\sum X_i = T$. Pour tout ensemble simplicial X, la cohomologie de ses sections sur X est $H^q(X, k)$ en tout degré complémentaire $p \geq 0$; graduée par le degré total, $H^{\bullet,q}$ est la troncature $\tau_{\geq q}(H^q(X, k) \otimes_k k\{T\})$. La cohomologie entière n'est retrouvée que sous la forme de ces ombres.*

◊ non vérifié en Lean

La page 8 affirme sans démonstration l'exactitude de chaque ligne ; la lecture la démontre à partir du complexe de Koszul à puissances divisées, et les pages 226 à 232 refont le calcul. Kageyama construit la même algèbre sans en calculer la cohomologie. L'exactitude de chaque ligne est démontrée ci-dessus, simplexe par simplexe, ce qui donne l'énoncé pour $X = \Delta[m]$. Le passage à un ensemble simplicial quelconque n'est pas démontré : il demande l'acyclicité des $C_*^{p,q}$ pour $p \geq 1$ (proposition 1 de la page 226, $\Phi_* \simeq 0$) et la cohomologie d'un ensemble simplicial à coefficients dans un module simplicial, que Mathlib n'a pas. On se reportera aux notes de Grothendieck (136, lot 1, p. 5).

Théorème (Grothendieck, pages 10 à 14 et 17, hyperrecouvrements indexés par une catégorie quelconque ♦). *Un hyperrecouvrement d'un topos X indexé par une petite catégorie quelconque A, et non par un objet simplicial, est caractérisé par un seul axiome : la flèche de comparaison $\varphi_!(\varprojlim_I F_i) \to \varprojlim_I \varphi_!(F_i)$ est un épimorphisme pour tout diagramme fini de $\hat{A}$. La version où elle est un isomorphisme équivaut à l'exactitude à gauche de $\varphi_!$, c'est-à-dire à un morphisme de topos $X \to \hat{A}$.*

◊ non vérifié en Lean

Les quatre axiomes des pages 10 à 13 se ramènent à celui-ci par $F = \varinjlim_{A/F} \alpha$ (pages 13, 14 et 17). Mathlib a les préfaisceaux et les extensions de Kan, mais pas les hyperrecouvrements d'un topos. On se reportera aux notes de Grothendieck (151, lot 1, p. 10).

Définition (Pages 59, 60 et 74, forme corrigée par l'édition, tubes mixtes ♦). Pour $i \leq j \leq k$, le tube mixte $V_{i,k}^j$ s'obtient en retirant du tube de X_i dans X_k la réunion $R_{i,k} \cup S_{j,k}$ de deux parties complémentaires du bord de X_k. Ces tubes interpolent de façon monotone entre le tube épointé $V_{i,k}^*$, pour $j = i$, et le tube plein $V_{i,k}$, pour $j = k$.

La page écrit $R_{j,k} \cup S_{j,k}$, qui est le bord de X_k pour tout j : la famille serait constante, et l'indice i est de l'édition. La page 74 commence une généralisation indexée par des cribles et s'interrompt. Mathlib n'a pas les espaces stratifiés ni leurs tubes. On se reportera aux notes de Grothendieck (151, lot 3, p. 59).

Exemple (Grothendieck, pages 38 à 42, Π_1 trop grossier pour la sphère ♦). Sur $\mathbf{P}^1_{\mathbf{C}} \simeq S^2$, stratifié par un point, un plan et un cercle, la somme amalgamée du diagramme des tubes au niveau du groupoïde fondamental est homotopiquement triviale, alors que la sphère ne l'est pas. En montant d'un niveau, aux gerbes, on retrouve $H^2(S^2, A) \simeq A$.

◊ non vérifié en Lean

Mathlib n'a pas la théorie de l'homotopie des espaces stratifiés ni les gerbes. On se reportera aux notes de Grothendieck (151, lot 2, p. 38).

Théorème (Grothendieck, pages 62 à 68, recollement par les paires de couverture ♦). *Un espace stratifié est la limite inductive d'un diagramme indexé par les seules paires (i, j) de l'ensemble ordonné des strates où j couvre i, avec trois flèches par paire, $X_i^* \to V_{i,j} \leftarrow V_{i,j}^* \to X_j^*$; aucune comparaison entre strates non adjacentes n'est nécessaire.*

Les feuillets en esquissent une démonstration incomplète (pages 62 et 63) : ils établissent, sous trois hypothèses, que ces trois inclusions sont les seules entre les pièces élémentaires. Le théorème de recollement de la page 68 est sans démonstration, et le mot qui y nomme l'opération est illisible. Mathlib n'a pas les espaces stratifiés. On se reportera aux notes de Grothendieck (151, lot 4, p. 62).

Contre-exemple 70.3 (Pages 62 à 68, le recollement en profondeur deux). [a] *Soit $X = \mathbf{R}^2 \supset X_1 = \mathbf{R} \times \{0\} \supset X_0 = \{0\}$, et des tubes $\overline{V}_{0,1} \subset X_1$, $\overline{V}_{1,2} \subset \mathbf{R}^2$ quelconques contenant leurs âmes. Les hypothèses de recensement des pages 62 et 63 sont satisfaites ; la limite inductive, dans les espaces topologiques, du diagramme des paires de couverture $0 \lessdot 1 \lessdot 2$ est $\mathbf{R}^2$ muni de la topologie finale des sept pièces, strictement plus fine que celle de $\mathbf{R}^2$: le plan privé de l'axe vertical épointé y est ouvert, et ne l'est pas dans $\mathbf{R}^2$.*

a. Preuve vérifiée : `lean/Grothendieck/Folder151.lean`.

Démonstration. Les sept pièces et les six flèches du diagramme sont des inclusions, et une famille compatible d'applications continues sur les pièces se recolle en une unique application continue sur $\mathbf{R}^2$ muni de la topologie finale (`exists_unique_desc`) : c'est la limite inductive. Le point 0 ne voit que l'axe horizontal ; son voisinage dans $\mathbf{R}^2$ est le tube de la paire non adjacente $0 < 2$, qui n'entre pas dans le diagramme (`colimTop_ne`). Lue comme limite inductive homotopique, l'affirmation échoue aussi : la caractéristique d'Euler du diagramme est $14 - 17 + 2 = -1$, et non 1 ; ce calcul est fait à la main, non en Lean. Reste la lecture « au topos », que le mot barré juste avant suggère, et que le fac-similé doit trancher. Un énoncé juste doit faire intervenir les comparaisons entre strates non adjacentes, comme la catégorie des chemins de sortie, ou se borner à la profondeur un.

Théorème (Pages 62 à 68, le recollement en profondeur un). [a] *Soit X un espace topologique, $X_0 \subset X$ une strate fermée et $\overline{V} \subset X$ un tube de X_0 qui en est un voisinage. Alors X, muni des inclusions des quatre pièces $X_0^* = X_0$, $V_{0,1} = \overline{V}$, $V_{0,1}^* = \overline{V} \smallsetminus X_0$ et $X_1^* = X \smallsetminus X_0$, est la limite inductive dans les espaces topologiques du diagramme $X_0^* \to V_{0,1} \leftarrow V_{0,1}^* \to X_1^*$; la topologie finale des quatre pièces est celle de X.*

a. Preuve vérifiée : `lean/Grothendieck/Folder151.lean`.

Démonstration. Une famille compatible d'applications continues sur les pièces se recolle en une application g égale à f_0 sur X_0 et à f_3 hors de X_0 ; la compatibilité le long des trois flèches montre que g coïncide avec f_i sur chaque pièce. Comme $\overline{V}$ est voisinage de chaque point de X_0 et $X \smallsetminus X_0$ est ouvert, ces deux pièces recouvrent X par des voisinages, et la continuité de g sur chacune entraîne sa continuité (`exists_unique_desc`). De même, un ouvert U de la topologie finale s'écrit $(W' \smallsetminus X_0) \cup (W \cap \operatorname{int} \overline{V})$, avec W, W' ouverts de X (`colimTop_eq`). Le cas de plusieurs strates sans chaîne de longueur deux n'est pas formalisé.

Partie 26

Topologie modérée et espaces stratifiés

71 Cote 121 : la décomposition cellulaire admissible la plus grossière [74]

La cote 121, *Topologie modérée*, cherche dans sa première mouture une notion de partie « modérée » d'un espace topologique X. Les pages 3 à 5 posent une algèbre de Boole $\mathcal{F}$ de parties de X et les conditions c bis) ($A \in \mathcal{F} \Rightarrow \overline{A} \in \mathcal{F}$), d) (tout $A \in \mathcal{F}$ contient un ouvert dense de son adhérence) et e) (toute suite décroissante de fermés de $\mathcal{F}$, chacun rare dans le précédent, est stationnaire à $\varnothing$) (121, lot 1, p. 4, 121, lot 1, p. 5). La page 8 montre que la frontière d'un membre est rare (121, lot 1, p. 8). La page 10 appelle décomposition cellulaire une partition finie de X telle que (1) l'adhérence de chaque cellule soit une réunion de cellules et (2) deux cellules distinctes aient des adhérences distinctes ; elle est $\mathcal{F}$-admissible si ses cellules sont dans $\mathcal{F}$ (121, lot 1, p. 10). La page 14 énonce la proposition suivante et en démontre l'existence par récurrence, en retirant la réunion des frontières et en s'arrêtant par e) (121, lot 1, p. 14). Comme dans la lecture, on prend dans d) l'intérieur relatif à l'adhérence.

Théorème 71.1 (Grothendieck, page 14 ♦). *Soit $\mathcal{F}$ une algèbre de Boole de parties d'un espace topologique, stable par adhérence, dont chaque membre contient un ouvert dense de son adhérence, et dans laquelle toute suite décroissante de membres fermés, chacun rare dans le précédent, aboutit à $\varnothing$. Toute sous-famille finie $\mathcal{L} \subset \mathcal{F}$ admet une décomposition cellulaire $\mathcal{F}$-admissible dont chaque élément de $\mathcal{L}$ est réunion de cellules, et parmi ces décompositions une plus grossière que toutes les autres.*

L'énoncé tient : voir `page14`, avec le lemme de la page 8 (`Tame.rare_bd`), dans `Folder121.lean`. La récurrence porte sur un fermé $Z \in \mathcal{F}$ quelconque à la place de X (`exists_coarsest`), la frontière d'un membre étant prise relativement à Z. La page affirme sans argument que la décomposition obtenue est la plus grossière ; l'argument de l'édition (`subset_bd`) est qu'une cellule d'une décomposition dont Y est réunion de cellules, si elle rencontre la frontière de Y, y est contenue, de sorte que toute décomposition admissible convenable se restreint à la partie retirée et raffine les cellules ouvertes.

La page 9 ajoute la condition f) : pour B, C fermés de $\mathcal{F}$, les composantes connexes du localement fermé $B \setminus C$ sont en nombre fini et appartiennent à $\mathcal{F}$ (121, lot 1, p. 9). La remarque de la page 16 en tire la version à cellules connexes (121, lot 1, p. 16).

Théorème 71.2 (Grothendieck, page 16 ♦). *Si $\mathcal{F}$ satisfait de plus f), toute sous-famille finie $\mathcal{L} \subset \mathcal{F}$ admet une décomposition cellulaire $\mathcal{F}$-admissible à cellules connexes dont chaque élément de $\mathcal{L}$ est réunion de cellules, et parmi ces décompositions à cellules connexes une plus grossière que toutes les autres.*

L'énoncé tient : voir `page16` et `exists_coarsest_conn`. La récurrence est celle de la page 14, les cellules ouvertes U_i étant remplacées par leurs composantes connexes, comme le dit la

74. Preuve vérifiée : `lean/Grothendieck/Folder121.lean`.

page. Une cellule U_i s'écrit $\overline{U_i} \setminus X'$, de sorte que f) s'applique à elle. Une composante V de U_i vérifie $\overline{V} \cap U_i \subset V$, car $\overline{V} \cap U_i$ est connexe ; avec le fait que l'adhérence d'une U_i ne rencontre aucune autre U_j, cela donne la condition de frontière et la distinction des adhérences. Pour « la plus grossière », une cellule connexe d'une décomposition concurrente contenue dans U_i est contenue dans une composante de U_i ; chaque composante est donc réunion de cellules de la décomposition concurrente, qui se restreint alors à X' en une décomposition convenable pour la famille $\{Y \cap X'\} \cup \{\overline{V} \cap X'\}$.

Ne sont pas démontrés ici : les corollaires de la page 15 et les décompositions régulières de la page 17.

72 Cote 120 : sommes amalgamées, écraser une partie modérée sur un corps [75]

La cote 120, *Topologie modérée*, vingt-quatre pages que l'inventaire date « à partir de 1973 — à partir de 1978 », cherche des axiomes pour les parties « modérées » des puissances d'un ensemble R. La page 2 pose les axiomes (M1) à (M4) sur des familles $\mathcal{M}_n$ de parties de R^n, que la page 4 transcrit pour des ensembles d'indices finis quelconques ; la page 5 appelle modérée une application dont le graphe est une partie modérée. L'axiome (M6) de la page 12 demande que toute partie modérée Y d'un espace modéré X soit une fibre $\bigcap_\alpha f_\alpha^{-1}(e_\alpha)$ d'un nombre fini de fonctions modérées, les e_α étant des points modérés, « de plus, on peut supposer » que les f_α séparent les points de $X \setminus Y$: c'est dire que le quotient X/Y, où Y est écrasé en un point, existe au sens strict. La section (VI) suppose R un corps et ajoute l'axiome (M11) : 0 et 1 sont des points modérés, $x - y$ et xy sont des fonctions modérées sur toute partie modérée de R^2, et les inverses d'une partie modérée de R^* sont contenus dans une partie modérée (120, lot 1, p. 20). Les pages 22 et 23 en tirent que la seconde moitié de (M6) découle de la première : la page 22 se ramène à $e_\alpha = 0$ par translation et introduit les produits $f_\alpha g_\beta$, la page 23 vérifie la séparation et énonce la proposition « Si on a M1 : M7 et M11 … », dont la « Dém : » reste vide (120, lot 2, p. 22). Le manuscrit écrit « $e_\alpha \in R$ » et « sépare les pts de X » ; la lecture corrige en $e_\alpha \in R_0$ et en $X \setminus Y$.

Conventions. Pour un ensemble fini I, $\mathcal{M}_I$ est un ensemble de parties de R^I ; pour $u : I \to J$, $u^* : R^J \to R^I$ est $x \mapsto x \circ u$. Les axiomes, sous la forme (M′1) à (M′4) de la page 4, sont : (M′1) $u^*(A) \in \mathcal{M}_I$ pour $A \in \mathcal{M}_J$; (M′2) $(u^*)^{-1}(B) \in \mathcal{M}_J$ pour u surjective et $B \in \mathcal{M}_I$; (M′3) $(u^*)^{-1}(B) \cap A \in \mathcal{M}_J$; (M′4) $A \times B \in \mathcal{M}_{I \sqcup J}$ pour $A \in \mathcal{M}_I$, $B \in \mathcal{M}_J$. Le graphe d'une famille $F : R^I \to R^K$ au-dessus de $X \subset R^I$ est $\Gamma_F = \{(x, F(x)) \mid x \in X\} \subset R^{I \sqcup K}$. Une fonction $f : X \to R$ est modérée si son graphe est dans $\mathcal{M}_{I \sqcup \{*\}}$, et R_0 est l'ensemble des $c \in R$ tels que $\{c\} \in \mathcal{M}_{\{*\}}$. Un espace modéré est ici une partie modérée $X \in \mathcal{M}_I$, et des fonctions modérées g_β le plongent si $x \mapsto (g_\beta(x))_\beta$ est injective sur X.

Lemme 72.1 (pages 5 et 20)**.** *Soient $X \in \mathcal{M}_I$ et f, g des fonctions modérées sur X.*

1. *Le graphe de $(f, g) : X \to R^2$ est modéré, ainsi que son image.*
2. *Si $F : R^I \to R^K$ a un graphe modéré au-dessus de X et si h est une fonction modérée sur $F(X)$, alors $h \circ F$ est modérée sur X.*
3. *Si R est un anneau commutatif vérifiant (M11) b), $f - g$ et fg sont modérées. Les constantes $c \in R_0$ et les coordonnées $x \mapsto x_i$ sont modérées sur X.*

75. Preuve vérifiée : `lean/Grothendieck/Folder120.lean`.

Seuls servent (M′1), (M′2), (M′4) et (M11) b).

Démonstration. 1. Soit $w : (I \sqcup \{*\}) \sqcup (I \sqcup \{*\}) \to I \sqcup \{0,1\}$ l'application qui envoie les deux copies de I sur I, la première étoile sur 0 et la seconde sur 1 ; elle est surjective. Un $y \in R^{I \sqcup \{0,1\}}$ a son image $w^*(y)$ dans $\Gamma_f \times \Gamma_g$ si et seulement si $y|_I \in X$, $y_0 = f(y|_I)$ et $y_1 = g(y|_I)$: la préimage de $\Gamma_f \times \Gamma_g$, modérée par (M′4) puis (M′2), est le graphe de (f, g). Plus généralement, l'image $F(X)$ d'une famille de graphe modéré est la projection de ce graphe sur R^K, modérée par (M′1).

2. On forme $\Gamma_F \times \Gamma_h \subset R^{(I \sqcup K) \sqcup (K \sqcup \{*\})}$, modéré par (M′4), et on le tire en arrière par la surjection $(I \sqcup K) \sqcup (K \sqcup \{*\}) \to (I \sqcup K) \sqcup \{*\}$ qui identifie les deux copies de K : on obtient, par (M′2), l'ensemble des $(x, F(x), h(F(x)))$, $x \in X$. Sa projection sur $R^{I \sqcup \{*\}}$, modérée par (M′1), est le graphe de $h \circ F$.

3. On applique le point 2 à $F = (f, g)$, dont l'image est modérée par le point 1, et à h égale à $(z_0, z_1) \mapsto z_0 - z_1$ ou $z_0 z_1$, modérée sur cette image par (M11) b). Le graphe de la constante c est $X \times \{c\}$, modéré par (M′4) ; celui de la coordonnée x_i est l'image de X par u^*, où $u : I \sqcup \{*\} \to I$ est l'identité sur I et envoie $*$ sur i, modérée par (M′1). □

Lemme 72.2 (pages 22 et 23, l'argument)**.** *Soient R un anneau sans diviseur de zéro, X un ensemble, $(f_\alpha)_{\alpha \in A}$ et $(g_\beta)_{\beta \in B}$ des familles quelconques de fonctions $X \to R$. La famille formée des f_α et des $f_\alpha g_\beta$ a pour lieu des zéros communs celui des f_α. Si x n'est pas un zéro commun des f_α et si un g_β sépare x et y, cette famille sépare x et y.*

Démonstration. Un zéro commun des f_α annule les $f_\alpha g_\beta$. Pour la séparation, si un f_α sépare x et y, c'est fini. Sinon $f_\alpha(x) = f_\alpha(y)$ pour tout α ; on choisit α avec $\lambda = f_\alpha(x) \neq 0$ et β avec $g_\beta(x) \neq g_\beta(y)$. Alors $f_\alpha g_\beta(x) - f_\alpha g_\beta(y) = \lambda\,(g_\beta(x) - g_\beta(y))$ n'est pas nul, puisque R n'a pas de diviseur de zéro. □

Théorème 72.3 (Pages 22 et 23, écrasement sur un corps, forme corrigée par l'édition ♦)**.** *Supposons (M′1) à (M′4) et (M11), R étant un corps. Soient $X \in \mathcal{M}_I$, des fonctions modérées f_α sur X en nombre fini, des $e_\alpha \in R_0$, $Y = \bigcap_\alpha f_\alpha^{-1}(e_\alpha)$, et des fonctions modérées g_β qui plongent X. Les fonctions $f_\alpha - e_\alpha$ et $(f_\alpha - e_\alpha)\, g_\beta$ sont modérées, ont Y pour lieu des zéros communs, et séparent les points de $X \smallsetminus Y$. En particulier Y est le lieu des zéros communs d'une famille finie de fonctions modérées qui sépare les points de $X \smallsetminus Y$: la seconde moitié de (M6) découle de la première, et X/Y est un espace modéré au sens strict.*

Démonstration. Par le lemme 72.1, la constante e_α est modérée parce que $e_\alpha \in R_0$, donc $f_\alpha - e_\alpha$ aussi, et les produits $(f_\alpha - e_\alpha)\, g_\beta$ le sont. Les zéros communs des $f_\alpha - e_\alpha$ forment Y. Pour $x \neq y$ dans $X \smallsetminus Y$, un $f_\alpha - e_\alpha$ ne s'annule pas en x, et comme les g_β plongent X, l'un d'eux sépare x et y : le lemme 72.2 conclut. Pour l'énoncé d'existence, les coordonnées, modérées par le lemme 72.1, plongent X, et la famille est indexée par $A \sqcup (A \times I)$, qui est fini. □

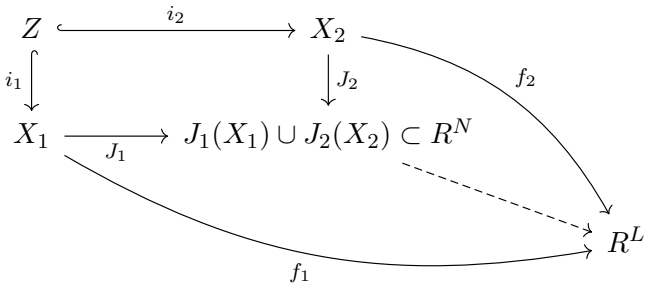
Remarque. L'énoncé tient tel que la lecture le donne, et plus généralement. Ni (M′3), ni (M5) à (M7), ni les parties a) et c) de (M11), ni la finitude des familles ne servent ; de (M11), seule sert la partie b), sur un anneau commutatif sans diviseur de zéro. L'hypothèse d'intégrité ne peut être omise : sur $\mathbf{Z}/4\mathbf{Z}$, avec $f = 2$ et $g = \mathrm{id}$, la famille $2,\ 2x$ ne sépare pas 0 et 2, bien que $f(0) \neq 0$ et $g(0) \neq g(2)$. Les deux corrections de la lecture sont nécessaires. Sans $e_\alpha \in R_0$, la constante e_α n'est pas modérée et la translation n'est pas permise. Et une famille qui s'annule sur Y ne sépare aucun couple de points de Y : « sépare les points de X » ne peut s'entendre que de $X \smallsetminus Y$.

Sommes amalgamées (pages 8 à 13). On ajoute (M5′), $\emptyset \in \mathcal{M}_I$ et la stabilité par réunion de deux parties (page 9) ; (M6), toute partie modérée Z d'un $X \in \mathcal{M}_I$ est la fibre $F^{-1}(e)$, $e \in R_0^A$, d'une famille modérée finie F injective hors de Z ; (M7), une fonction modérée sur Z se prolonge en une fonction modérée sur X (page 12). Un espace est un $X \in \mathcal{M}_I$, une application modérée une famille à graphe modéré.

Théorème 72.4 (D'après les pages 10 à 13, conclusion restituée par la lecture ♦)**.** *Supposons R non vide et (M5′). Soient $i_1 : Z \hookrightarrow X_1$ et $i_2 : Z \hookrightarrow X_2$ deux plongements modérés.*

1. *(Critère de la page 10, suffisance.) Si des familles modérées $J_1 : X_1 \to R^N$, $J_2 : X_2 \to R^N$ sont injectives, vérifient $J_1 i_1 = J_2 i_2$ sur Z et $J_1(x_1) \neq J_2(x_2)$ hors de $i_1(Z)$ et de $i_2(Z)$, alors $J_1(X_1) \cup J_2(X_2)$ est modérée, c'est la somme amalgamée ensembliste ($J_1 x_1 = J_2 x_2$ si et seulement si $x_1 = i_1 z$ et $x_2 = i_2 z$), et toute paire d'applications modérées f_1, f_2 compatibles sur Z se factorise par une application modérée.*
2. *(Proposition de la page 12.) Sous (M6) et (M7), de telles familles existent : la somme amalgamée existe et l'oubli la respecte.*
3. *(Critère de la page 10, nécessité.) Inversement, si une partie modérée $P \subset R^N$ et des familles modérées $q_1 : X_1 \to P$, $q_2 : X_2 \to P$ forment une somme amalgamée dans les ensembles ($q_1 i_1 = q_2 i_2$ sur Z, $P = q_1(X_1) \cup q_2(X_2)$, et toute paire d'applications vers un ensemble non vide compatibles sur Z se factorise par P), les coordonnées de q_1 et q_2 sont des fonctions modérées vérifiant a), b), c). Les conditions a), b), c) équivalent donc à l'existence d'une somme amalgamée modérée que l'oubli respecte.*

L'énoncé tient (`pushout_of_criterion`, `pushout_exists`), y compris la conclusion restituée à la page 13 : les deux images se rencontrent exactement le long de Z. La nécessité tient aussi (`criterion_of_pushout`, `criterion_iff`) : le plongement F de la lecture est l'inclusion $P \subset R^N$, et $f = q_1$, $g = q_2$. Pour b), on factorise par P le couple à valeurs dans les propositions $u_1(y) = (y = x)$, $u_2(y) = (\exists z \in Z,\ y = i_2 z \text{ et } i_1 z = x)$, compatible sur Z parce que i_2 est injectif : $q_1 x = q_1 x'$ force $x' = x$. Pour c), le couple $u_1 = \text{vrai}$, $u_2(y) = (y \in i_2(Z))$ montre que $q_1 x_1 = q_2 x_2$ force $x_2 \in i_2(Z)$, ce qui est plus fort que c). Ni (M5′), ni (M6), ni (M7), ni le caractère modéré de P ne servent à cette direction ; l'injectivité de i_1 et i_2 y sert.



C'est le point 1 : si $f_1 i_1 = f_2 i_2$, il existe une application modérée, en tirets, dont les composés avec J_1 et J_2 sont f_1 et f_2 ; elle est unique, les deux images recouvrant la réunion.

Remarque. La propriété universelle demande R non vide, puisqu'il faut une application vers R^L ; ce sont les cas triviaux que la page 4 exclut. (M5′) ne sert qu'à la réunion $J_1(X_1) \cup J_2(X_2)$ et au graphe de l'application induite. (M6) sert avec sa seconde moitié, l'injectivité hors de Z, que la lecture ne déduit de la première que sur un corps.

Ne sont pas démontrés ici : la catégorie Σ des espaces modérés et ses limites finies (pages 5

à 7), le NB de la page 10 pour les diagrammes finis, les ind-espaces et la topologie des pages 14 à 19, et le programme de trivialité de la page 24.

73 Cote 150 : voisinages coniques, un contre-exemple sur $[0,1]$ [76]

La cote 150, *Espaces stratifiés et voisinages côniques (ou : déploiement des espaces stratifiés)*, quatre-vingt-dix-huit pages de décembre 1981 et janvier 1982, cherche à déplier un espace stratifié : remplacer chaque strate par une version rognée, sans jointure, et garder la trace de la façon dont les morceaux se recollaient. Les pages 11 à 19 en posent le vocabulaire. Un *voisinage conique* d'un fermé Y dans un espace X est un voisinage T de Y muni d'une action $(\lambda, t) \mapsto \lambda t$ du monoïde multiplicatif $\mathbf{I} = [0,1]$, qui fixe Y et écrase T sur Y pour $\lambda = 0$. Son bord $\dot{T}$ est la base du cône, et $f : \dot{T} \to Y$, $t \mapsto 0 \cdot t$, envoie chaque point du bord sur la pointe de son segment. Ôter l'intérieur de T laisse un espace à bord $X^\sharp = X \smallsetminus \mathring{T}$, que la page note X^*, dont le bord est $\dot{T}$.

La page 19 énonce une proposition de reconstruction (150, lot 1, p. 19). Les systèmes $(X, Y, (X_i)_{i\in I}, T)$, où les X_i sont des fermés et T un voisinage conique de Y compatible avec eux, seraient équivalents, en ne gardant pour morphismes que les isomorphismes, aux systèmes $(X^\sharp, \dot{X}, (X_i^\sharp), Y, f : \dot{X} \to Y)$, où $\dot{X} = \dot{T}$ et $X_i^\sharp = X_i \cap X^\sharp$. Dans l'autre sens, on recolle à $X^\sharp$, le long de $\dot{X}$, le cylindre de l'application f. Intuitivement, couper le voisinage conique ne perd rien, puisque le cône se reconstruit à partir de sa base et de la projection sur la pointe.

Les définitions. Une partie $T' \subset T$ est *conique* quand elle est formée des segments issus de sa trace sur le bord et de sa trace sur Y : $T' = \mathbf{I} \cdot (T' \cap \dot{T}) \cup (T' \cap Y)$. C'est la remarque de la page 15 (150, lot 1, p. 15) ; elle contient la stabilité par l'action. Le voisinage T est *compatible* avec un fermé X' si $X' \cap T$ est conique. Un *collier* de $\dot{T}$ dans $X^\sharp$ est un voisinage E de $\dot{T}$ identifié à $\dot{T} \times [0,1]$, et X' lui est compatible si $X' \cap E$ s'écrit $X'_0 \times [0,1]$. La partie conique T' est *stricte* si sa trace sur Y se réduit aux pointes de ses segments, $T' \cap Y = 0 \cdot (T' \cap \dot{T})$: c'est la condition que la page 16 ajoute au bas du feuillet et entoure (150, lot 1, p. 16).

Pourquoi la proposition demande une condition. Les données de droite ne voient de X_i que sa partie hors de l'intérieur de T. Dans T, la compatibilité reconstruit les segments à partir de leur base $X_i \cap \dot{T}$, mais elle laisse libre un morceau de Y que X_i peut contenir sans qu'aucun segment n'y aboutisse. Ce morceau est invisible à droite. L'exemple le plus petit est sur un segment.

L'exemple. On prend $X = [0,1]$, $Y = \{0\}$ et $T = [0, \frac{1}{2}]$, avec l'action $(\lambda, t) \mapsto \lambda t$. Le bord est $\dot{T} = \{\frac{1}{2}\}$, l'application f envoie $\frac{1}{2}$ sur 0, et $X^\sharp = [\frac{1}{2}, 1]$. Le collier est $E = [\frac{1}{2}, \frac{3}{4}]$, identifié à $\dot{T} \times [0,1]$ par $(\frac{1}{2}, s) \mapsto \frac{1}{2} + \frac{s}{4}$. Le voisinage T est strict, au sens de la page 14 : c'est $\frac{1}{2} \cdot X$, et X est lui-même un voisinage conique de Y pour la même action (figure 20).

Contre-exemple 73.1 (contre-exemple de l'édition, page 19)**.** *Dans l'exemple ci-dessus, les fermés $X_1 = \{0\}$ et $X_1 = \emptyset$ de $[0,1]$ sont tous deux compatibles avec T et avec le collier E, et ils ont la même trace, vide, sur $X^\sharp$. Les deux systèmes ont donc les mêmes données de droite, mais ils ne sont pas isomorphes, puisque l'un des fermés est vide et l'autre non. Le fermé $\{0\}$ ne vérifie pas la condition $X_1 \cap Y = f(\dot{X}_1)$, où $\dot{X}_1 = X_1 \cap \dot{T}$.*

Démonstration. Pour $X_1 = \{0\}$: $X_1 \cap T = \{0\}$, sa trace sur le bord est vide et sa trace sur Y est $\{0\}$, de sorte que $\mathbf{I} \cdot \emptyset \cup \{0\} = \{0\}$: la partie est conique. Elle ne rencontre pas E, et

76. Preuve vérifiée : `lean/Grothendieck/Folder150.lean`.

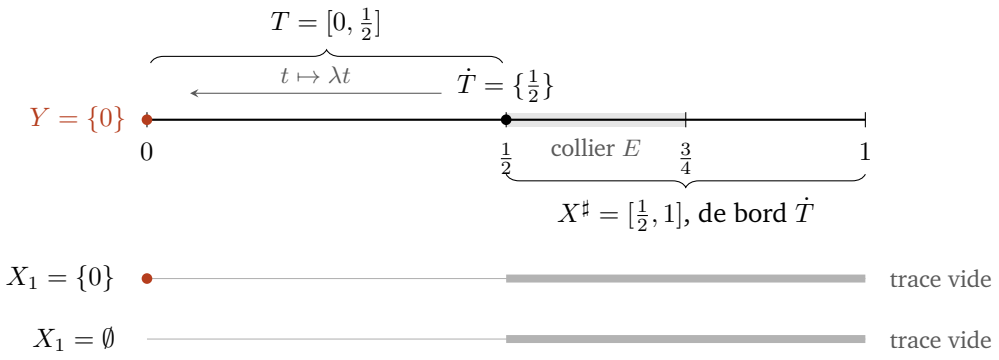


FIGURE 20 – L'exemple de la page 19 sur $X = [0, 1]$. Le voisinage conique T de Y est écrasé sur 0 par l'action $t \mapsto \lambda t$, son bord est le point $\frac{1}{2}$, et $X^\sharp$ est ce qui reste quand on ôte l'intérieur de T. Les deux fermés du bas sont compatibles avec T et avec le collier, et leur trace sur $X^\sharp$, en gris épais, est vide dans les deux cas : les données de droite ne les distinguent pas. Le point 0 du premier n'est la pointe d'aucun segment issu du bord, puisque $\dot{X}_1$ est vide ; c'est la condition $X_1 \cap Y = f(\dot{X}_1)$ qui l'exclut.

$X_1 \cap E = \emptyset = \emptyset \times [0, 1]$. Pour $X_1 = \emptyset$, tout est vide. Les deux traces sur $X^\sharp = [\frac{1}{2}, 1]$ sont vides. Enfin $\{0\} \cap Y = \{0\}$, alors que $\dot{X}_1 = \emptyset$ et $f(\emptyset) = \emptyset$. □

Le contre-exemple tient encore si l'on demande que T soit strict, comme le faisait la première définition de « strictement compatible » de la lecture, et si l'on ajoute le collier : ni l'une ni l'autre condition ne regarde la trace de X_1 sur Y. La lecture a donc mis dans la définition la condition $X_i \cap Y = f(\dot{X}_i)$, que la page impose elle-même au bas de la page 16. Sous cette condition, l'exemple ne présente plus d'ambiguïté.

Énoncé (énoncé de l'édition, page 19, dans l'exemple)**.** *Dans l'exemple ci-dessus, soient X_1 et X_2 deux fermés de $[0, 1]$ compatibles avec T et avec le collier, qui vérifient $X_k \cap Y = f(\dot{X}_k)$. Si $X_1 \cap X^\sharp = X_2 \cap X^\sharp$, alors $X_1 = X_2$.*

Démonstration. Une partie conique C de T est T tout entier si elle contient $\frac{1}{2}$, puisqu'elle contient alors le segment $\mathbf{I} \cdot \frac{1}{2} = [0, \frac{1}{2}]$; sinon sa trace sur le bord est vide et $C = C \cap Y \subset \{0\}$. Sous la condition stricte, le second cas donne $C \cap Y = f(\emptyset) = \emptyset$, donc $C = \emptyset$. Ainsi $X_k \cap T$ vaut T ou $\emptyset$ selon que $\frac{1}{2}$ est dans X_k ou non. Or $\frac{1}{2}$ appartient à $X^\sharp$, et l'on lit sur la trace $X_k \cap X^\sharp$ s'il est dans X_k. Comme $[0, 1] = T \cup X^\sharp$, on a $X_k = (X_k \cap T) \cup (X_k \cap X^\sharp)$, et les deux morceaux sont déterminés par la trace sur $X^\sharp$. □

Remarque. Le collier ne sert pas à la démonstration de l'énoncé : dans l'exemple, la condition stricte suffit. La page laisse deux réparations possibles : demander la condition stricte, ou ajouter les traces $X_i \cap Y$ aux données de droite. La lecture a retenu la première, et l'exemple montre qu'elle répare le défaut qu'il met en évidence ; il ne démontre pas la proposition corrigée en général.

Portée de la vérification. Lean traite l'exemple seul, dans $\mathbb{R}$: les parties X, Y, T, $\dot{T}$, $X^\sharp$ et le collier y sont des intervalles explicites, et les notions de partie conique, de compatibilité, de compatibilité au collier et de compatibilité stricte y sont écrites pour cette action. Il démontre que T est conique et strict (`isConic_T`, `T_eq_half_smul`), le contre-exemple (`compatible_not_determined`, `not_strictlyCompatible_singleton_zero`) et l'énoncé (`eq_`

`of_strictlyCompatible`). Ne sont pas formalisés : les deux catégories de la proposition et le foncteur de recollement $X = X^\sharp \amalg_{\dot{X}} \mathcal{C}(f)$ pour des espaces quelconques, la transversalité et l'équisingularité de la même page. Mathlib n'a pas les espaces stratifiés ni les voisinages coniques.

Ne sont pas démontrés ici, de la même cote :

Théorème (Grothendieck, pages 1 et 45 à 47, lissité des fibrations de drapeaux ♦). *Dans le déploiement d'une stratification équisingulière non singulière, présenté comme foncteur sur les drapeaux de I, soit $d = (i_1, \dots, i_p)$ un segment initial de $d' = (i_1, \dots, i_n)$. Le bord des fibres de $\Sigma_{d'} \to \Sigma_d$ est stratifié cylindriquement par les drapeaux non vides de la somme ordinale $I_{]i_p, i_{p+1}[} \sqcup \cdots \sqcup I_{]i_{n-1}, i_n[}$. La fibration est donc à fibres sans bord exactement quand i_{k+1} couvre i_k dans I pour $p \leq k < n$, condition où $i_1, \dots, i_{p-1}$ n'interviennent pas.*

◊ non vérifié en Lean

Le mot qui qualifie « successeur » à la page 47 est une addition incertaine ; le critère est fixé par la page 46, lisible. Mathlib n'a pas les stratifications équisingulières ni leurs déploiements. On se reportera aux notes de Grothendieck (150, lot 1, p. 1).

Le critère combinatoire, vérifié. Le théorème reste non démontré, mais sa partie purement ordinale est vérifiée par Lean (`Folder150.Flags`). Soit I un ensemble ordonné quelconque, $d' = (i_1 < \cdots < i_n)$ un drapeau, $m = i_p$ l'un de ses termes et $d = (i_1, \dots, i_p)$ le segment initial qu'il détermine. On note J la réunion des intervalles ouverts $]i_k, i_{k+1}[$, $p \leq k < n$, et l'on appelle *drapeaux au-dessus de d'* les drapeaux $e \supset d'$ qui ont les mêmes termes que d' jusqu'à i_p et le même dernier terme i_n : ce sont les indices des strates Σ_e du bord des fibres.

Énoncé (énoncé de l'édition, pages 45 à 47, partie combinatoire). *(i) J est la somme ordinale des $I_{]i_k, i_{k+1}[}$: un point d'un intervalle est en dessous de tout point d'un intervalle plus haut. C'est l'ensemble des points hors de d', strictement compris entre i_p et i_n et comparables à tous les termes de d'.*

(ii) $e \mapsto e \smallsetminus d'$ est un isomorphisme d'ensembles ordonnés (par inclusion) des drapeaux au-dessus de d' sur les drapeaux de J, qui envoie d' sur le drapeau vide.

(iii) Les conditions suivantes sont équivalentes : J est vide ; J n'a aucun drapeau non vide ; d' est le seul drapeau au-dessus de lui-même ; i_{k+1} couvre i_k dans I pour $p \leq k < n$. Les termes $i_1, \dots, i_{p-1}$ n'interviennent pas.

Démonstration. (i) Si $x \in]i_k, i_{k+1}[$ et $y \in]i_l, i_{l+1}[$ avec $k < l$, on a $i_{k+1} \leq i_l$, sans quoi i_l serait un terme de d' strictement entre i_k et i_{k+1} ; donc $x < i_{k+1} \leq i_l < y$. Un point de $]i_k, i_{k+1}[$ n'est pas un terme, puisque les termes sont consécutifs, et il est comparable à tous les termes, qui sont soit $\leq i_k$, soit $\geq i_{k+1}$. Réciproquement, si $x \notin d'$ est comparable à tous les termes et $i_p < x < i_n$, soit a le plus grand terme $< x$ et b le plus petit terme $> x$; ils sont consécutifs, et $a \geq i_p$.

(ii) Soit e au-dessus de d' et $x \in e \smallsetminus d'$. Comme e est une chaîne qui contient d', x est comparable à tous les termes ; il n'est pas $\leq i_p$, puisque e et d' ont les mêmes termes jusqu'à i_p, ni égal à i_n, et il est $\leq i_n$: par (i), $x \in J$. Inversement, si c est un drapeau de J, $c \cup d'$ est une chaîne, puisque les points de J sont comparables aux termes, et elle est au-dessus de d' par (i). Les deux applications sont inverses l'une de l'autre parce que J ne rencontre pas d', et elles respectent l'inclusion.

(iii) J est vide si et seulement si chaque $]i_k, i_{k+1}[$, $k \geq p$, l'est, c'est-à-dire si i_{k+1} couvre i_k ; un point de J est un drapeau non vide ; et par (ii) les drapeaux au-dessus de d' autres que d'

correspondent aux drapeaux non vides de J. □

Portée de la vérification. Lean vérifie (i) à (iii) pour un ensemble ordonné quelconque, les drapeaux étant des chaînes finies (`lt_of_mem_Ioo`, `mem_gaps_iff`, `aboveEquiv`, `aboveEquiv_eq_empty`, `aboveEquiv_subset`, `gaps_eq_empty_iff`, `flags_gaps_iff`, `above_eq_iff`). Ne sont pas formalisés : le déploiement, les variétés à bord Σ_d, les fibrations $\Sigma_{d'} \to \Sigma_d$, la stratification cylindrique de leur bord et l'identification de ses strates aux Σ_e, c'est-à-dire tout ce qui fait passer du critère ordinal à la lissité. C'est pourquoi l'encadré ci-dessus reste non vérifié.

Théorème (Grothendieck, pages 47 à 66 et 70, le déploiement comme espace ordonné ♦). *Les données déployées d'une stratification équisingulière indexée par un ensemble ordonné fini I (strates déployées Σ_i, tubes de raccord Σ_{ij} fibrés sur Σ_i et plongés de façon fermée, avec collier, dans Σ_j) équivalent à un seul espace topologique ordonné Σ, dont le graphe de l'ordre est la réunion des tubes. Cet espace est soumis à des conditions de propreté, de transversalité et de finitude, chaque $\Sigma_{<x}$ étant fini et totalement ordonné, et muni d'une application strictement croissante $\pi_0(\Sigma) \to I$, non nécessairement surjective.*

◊ non vérifié en Lean

Les feuillets en esquissent une démonstration incomplète (pages 57 à 70). Seules la reconstitution de l'ordre et la condition b) y sont démontrées, et l'argument de dimension des pages 67 à 69 demande des hypothèses que l'édition ajoute. Mathlib n'a pas les stratifications équisingulières. On se reportera aux notes de Grothendieck (150, lot 3, p. 47).

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

Théorème (Grothendieck, pages 144 et 145, quotients des feuilletages ; voir aussi Kock—Moerdijk [84] ♦). *La catégorie des couples (X, R), où X est un espace topologique et R une relation d'équivalence locale sur X, localement ouverte et à fibres localement connexes, est équivalente à celle des triplets $(X, \mathcal{Y}, f)$, où $\mathcal{Y}$ est une « multiplicité topologique » et $f : \mathrm{Top}(X) \to \mathcal{Y}$ un morphisme localement ouvert à fibres localement connexes.*

◊ non vérifié en Lean

La page l'énonce sans démonstration. L'édition rapproche les multiplicités topologiques des étendues, topos localement équivalents à des topos de faisceaux sur un espace, et les relations d'équivalence locales de celle des feuilles d'un feuilletage. Kock et Moerdijk (1992) [84] montrent que toute étendue est équivalente au topos $\mathrm{sh}(L, r)$ des r-faisceaux sur un locale L muni d'une relation d'équivalence locale r localement simplement connexe, et que $\mathrm{sh}(L, r)$ est une étendue pour un tel r ; leur introduction renvoie à SGA 4, exposé IV, pour les relations d'équivalence locales. Kock et Moerdijk (1996) [85] identifient $\mathrm{sh}(M, r)$ aux faisceaux sur un groupoïde étale sous des hypothèses de connexité. L'équivalence de catégories de la page, entre couples (X, R) et morphismes $\mathrm{Top}(X) \to \mathcal{Y}$, n'a pas été vue dans les pages lues de ces deux articles. Voir aussi les morphismes de topos des sections 26 et 28. Mathlib n'a pas les relations d'équivalence locales ni les multiplicités topologiques. On se reportera aux notes de Grothendieck (119, lot 8, p. 144).

Partie 27

Géométrie anabélienne et dessins

74 Cote 146 : les exposants trivialisants de L_i et de L sur $M_{0,n}$ [77]

La cote 146, *Groupoïdes de Teichmüller*, cent trente-trois pages que l'inventaire date « [à partir de 1978] », porte page 70 un tableau : pour $n = \operatorname{card} I = 4, 5, 6$, le plus petit exposant qui rend trivial, de façon compatible au groupe symétrique, le fibré $L = \bigotimes L_i$ sur $M_{0,I}$, et les fibrés L_i attachés aux points marqués (146, lot 4, p. 70). Pour $n = 4$ il donne 3 pour L et 6 pour L_i ; les colonnes $n = 5$ et 6 portent des points d'interrogation. La lecture ne vérifie pas le tableau, et la piste tombe si les valeurs pour $n = 4$ ne se vérifient pas.
Conventions. $M_{0,4} = U = \mathbf{P}^1 \setminus \{0, 1, \infty\}$, de coordonnée λ, le quatrième point étant mobile. Le groupe $\mathfrak{S}_{I\setminus\{4\}} \simeq \mathfrak{S}_3$ permute 0, 1, ∞ et agit sur U par les six substitutions anharmoniques g, et sur la droite tangente L_4 au point mobile par la dérivée $g'(\lambda)$. Par la règle de dérivation des fonctions composées, $g \mapsto g'(\lambda)$ est un 1-cocycle de $\mathfrak{S}_3$ à valeurs dans les unités de $\mathcal{O}(U)$. Comme $\operatorname{Pic}(U) = 0$, l'exposant cherché est l'ordre de sa classe : le plus petit $m \geq 1$ tel que $g'(\lambda)^m = h(g\lambda)/h(\lambda)$ pour une unité h.

Théorème 74.1 (Grothendieck, page 70, colonne $n = 4$, pour L_4 ♦). *Soit K un corps où 2 et 3 sont inversibles et qui contient une racine ζ de $\zeta^2 - \zeta + 1$. La classe de L_4 est d'ordre exactement 6 : on a $g'(\lambda)^6 = h(g\lambda)/h(\lambda)$ avec $h = \lambda^4(1-\lambda)^4$, et si $g'(\lambda)^m = h(g\lambda)/h(\lambda)$ pour tous g et $\lambda \in U(K)$, pour une fonction h quelconque sans zéro sur $U(K)$, alors $6 \mid m$.*

Démonstration. L'égalité pour $m = 6$ se vérifie sur les six substitutions ; par exemple, pour $g(\lambda) = 1/\lambda$, $g'(\lambda)^6 = \lambda^{-12}$ et $h(1/\lambda) = \lambda^{-8}(\lambda-1)^4$. Réciproquement, en un point λ_0 fixé par g, le second membre vaut 1. Le point -1 est fixé par $g(\lambda) = 1/\lambda$, et $g'(-1) = -1$, d'où $(-1)^m = 1$ et $2 \mid m$. Le point ζ est fixé par $g(\lambda) = 1/(1-\lambda)$, car $\zeta(1-\zeta) = 1$, et $g'(\zeta) = 1/(1-\zeta)^2 = \zeta^2$, racine primitive cubique de l'unité puisque $3 \neq 0$; d'où $3 \mid m$. □

La figure 21 montre où se trouvent ces points fixes. Sur la droite réelle, chacune des trois transpositions fixe un point de U : $1/\lambda$ fixe -1, $1-\lambda$ fixe $1/2$ et $\lambda/(\lambda-1)$ fixe 2, et la dérivée y vaut -1 dans les trois cas. Les deux 3-cycles permutent circulairement ces trois points et ne fixent que ζ et $\bar{\zeta}$, les sommets des deux triangles équilatéraux de base $[0, 1]$, où la dérivée est une racine primitive cubique de l'unité. Ce sont les seuls points de U de stabilisateur non trivial.

Remarque. La valeur 6 du tableau tient, et la piste ne tombe pas. L'argument par les points fixes est celui que la lecture de la cote 140-1 donne pour $\mathcal{O}(1)$ sur $\mathbf{P}(V_J)$ (§ 75) ; il ne demande pas de calculer les unités de U, et la minoration vaut même parmi toutes les fonctions sans zéro sur $U(K)$.

La preuve vérifiée contient la loi de groupe des six substitutions et la règle de cocycle, $g \mapsto g'(\lambda)$ vérifiant $(gh)'(\lambda) = g'(h\lambda)\, h'(\lambda)$ (`anh_mul`, `der_mul`), l'égalité pour $m = 6$ (`der_pow_six`) et la divisibilité $6 \mid m$ (`six_dvd`), pour tout $m \in \mathbf{Z}$. Elle ne contient ni le fibré L_4 ni le groupe de Picard équivariant : l'énoncé est celui du cocycle, et sa traduction en fibrés est la convention ci-dessus.

77. Preuve vérifiée : `lean/Grothendieck/Folder146.lean`.

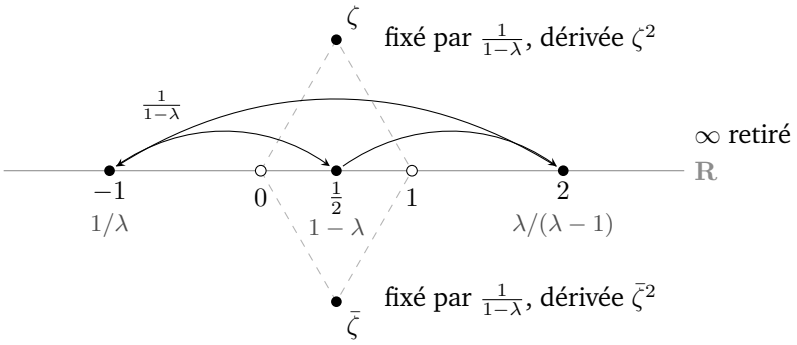


FIGURE 21 – $M_{0,4} = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ et ses points de stabilisateur non trivial. Les points -1, $1/2$, 2 sont fixés par les transpositions $1/\lambda$, $1-\lambda$, $\lambda/(\lambda-1)$; les flèches figurent le 3-cycle $\lambda \mapsto 1/(1-\lambda)$, qui les permute et fixe ζ et $\bar\zeta$. Le facteur -1 force $2 \mid m$, le facteur ζ^2 force $3 \mid m$.

Remarque. La fibre de L_4 en λ est la droite des vecteurs tangents en λ, c'est-à-dire l'ensemble des points base tangentiels de Deligne [41] au point mobile, privé de zéro ; l'exposant 6 dit que $L_4^{\otimes 6}$, et aucune puissance plus petite, admet une section partout non nulle compatible à $\mathfrak{S}_3$. Le groupe et l'action sont ceux de la section 50, où le quotient de U par $\mathfrak{S}_3$ est la fonction j, et de l'épinglage de Legendre de la section 42, où $\mathfrak{S}_3$ opère sur $U_{0,3} = U$ et sur un μ_4-torseur ; le groupe profini $\hat\pi$ de U est l'objet de la section 61. Les points fixes -1 et ζ de la démonstration sont les points de U au-dessus de $j = 0$ et $j = 1$ dans la normalisation de la section 50, la seule où le stabilisateur n'est pas trivial.

Passons à la seconde entrée de la colonne $n = 4$, celle du fibré $L = L_1 \otimes L_2 \otimes L_3 \otimes L_4$ sous le groupe $\mathfrak{S}_4$ tout entier. Une permutation des quatre points marqués induit un automorphisme de la fibre $\mathbf{P}^1$, et elle agit sur L par le produit des dérivées de cet automorphisme aux quatre points. Deux remarques ramènent ce calcul à celui de L_4. D'abord, le groupe de Klein $V_4 \subset \mathfrak{S}_4$, formé des trois produits de deux transpositions disjointes, agit trivialement sur U : la permutation $(12)(34)$ ne change pas le birapport. Il agit aussi trivialement sur L, car l'automorphisme échange les deux points de chaque paire et les dérivées en ces deux points ont pour produit 1. Le quotient $\mathfrak{S}_4/V_4$ s'identifie au stabilisateur $\mathfrak{S}_3$ du quatrième point. Ensuite, pour g dans ce stabilisateur, les dérivées en 0, 1 et ∞ (dans la carte $1/\lambda$ en ∞) ont un produit constant, égal à la signature $\varepsilon(g)$, et la dérivée au point mobile est $g'(\lambda)$. Le cocycle de L est donc $g \mapsto \varepsilon(g)\, g'(\lambda)$.

Théorème 74.2 (Grothendieck, page 70, colonne $n = 4$, pour L ♦). *Soit K un corps où 3 est inversible et qui contient une racine ζ de $\zeta^2 - \zeta + 1$. Le cocycle $g \mapsto \varepsilon(g)\, g'(\lambda)$ est d'ordre exactement 3 : sa puissance m-ième est le cobord $h(g\lambda)/h(\lambda)$ d'une fonction h sans zéro sur $U(K)$ si et seulement si $3 \mid m$, et pour $m = 3$ on peut prendre $h = \lambda^2(1-\lambda)^2$.*

Démonstration. Pour $m = 3$, on vérifie l'égalité sur les six substitutions ; pour $g(\lambda) = 1/\lambda$, le cocycle vaut $(-1)\cdot(-\lambda^{-2}) = \lambda^{-2}$, son cube λ^{-6}, et $h(1/\lambda)/h(\lambda) = \lambda^{-4}(\lambda-1)^2/(\lambda^2(1-\lambda)^2) = \lambda^{-6}$. Les multiples de 3 suivent en prenant $h^{m/3}$. Réciproquement, au point ζ fixé par $g(\lambda) = 1/(1-\lambda)$, une permutation paire, le cocycle vaut ζ^2 et le second membre vaut 1, d'où $3 \mid m$ comme pour L_4. □

La signature tue exactement le facteur d'ordre 2 : au point -1, fixé par $1/\lambda$, le cocycle de L vaut $(-1)\cdot(-1) = 1$, et il ne reste que l'ordre 3 venu de ζ. La valeur 3 du tableau tient donc. La page 72 n'affirme, elle, que $L^{\otimes 6} \simeq 1$, ce qui est vrai et plus faible.

Vérifié au niveau des cocycles (`sgn_mul`, `derL_mul`, `derL_pow_three`, `coboundary_derL_iff`). Lean ne démontre ni que V_4 agit trivialement, ni que le produit des dérivées en 0, 1, ∞ est la signature, ni que l'ordre sous $\mathfrak{S}_4$ est celui sous $\mathfrak{S}_3$ (injectivité de l'inflation $H^1(\mathfrak{S}_3,\cdot) \to H^1(\mathfrak{S}_4,\cdot)$) : ces trois points forment la traduction du fibré L en cocycle, faite dans le texte ci-dessus.

Passons à la colonne $n=5$. Le tableau y porte « 12 ? » pour L comme pour L_i, et, plus bas sur la même page, un calcul aboutit à $(L^4)^3 \simeq \mathcal{O}$, c'est-à-dire $L^{\otimes 12} \simeq \mathcal{O}$. La question est donc de savoir si 12 est le meilleur exposant dans les deux cas.

Le modèle. Un point de $M_{0,5}$ est une droite projective munie de cinq points distincts ; on envoie les trois premiers en 0, 1, ∞, et il reste deux coordonnées (λ,μ), avec $\lambda,\mu \notin \{0,1\}$ et $\lambda \neq \mu$. Le groupe $\mathfrak{S}_5$ est engendré par les quatre transpositions $s_1=(12)$, $s_2=(23)$, $s_3=(34)$, $s_4=(45)$. Chacune permute les étiquettes ; on renvoie alors les trois premiers points en 0, 1, ∞ par une homographie φ, ce qui donne une substitution rationnelle :

$$s_1 : (1-\lambda,\ 1-\mu), \quad s_2 : \Big(\frac{\lambda}{\lambda-1},\ \frac{\mu}{\mu-1}\Big), \quad s_3 : \Big(1-\lambda,\ \frac{\mu(\lambda-1)}{\lambda-\mu}\Big), \quad s_4 : (\mu,\lambda).$$

L'homographie φ agit aussi sur les droites tangentes aux points marqués, par sa dérivée. Sur L_5, la tangente au cinquième point, le facteur est $\varphi'(\mu)$; il n'a de sens que pour les permutations qui fixent le cinquième point, d'où le groupe $\mathfrak{S}_4$ engendré par s_1, s_2, s_3. Sur L, le facteur est le produit des dérivées aux cinq points (dans la carte $1/z$ en ∞). On trouve, pour s_1, s_2, s_3, s_4 :

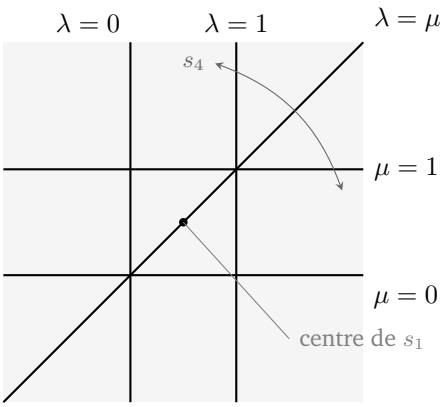
$$c_L = -1,\ \frac{-1}{(\lambda-1)^2(\mu-1)^2},\ \frac{\lambda(\lambda-1)}{(\lambda-\mu)^2},\ 1; \qquad c_5 = -1,\ \frac{-1}{(\mu-1)^2},\ \frac{\lambda(\lambda-1)}{(\lambda-\mu)^2}.$$

Sur un produit de générateurs, le facteur se calcule par la règle de cocycle $c(gh)(x) = c(g)(hx)\,c(h)(x)$, qui n'est autre que la dérivation des fonctions composées. Comme pour $n=4$, $M_{0,5}$ est le complémentaire d'un arrangement de droites, son groupe de Picard est nul, et l'exposant cherché est l'ordre de la classe du cocycle : le plus petit $m \geq 1$ tel que c^m soit le cobord $h(gx)/h(x)$ d'une fonction h sans zéro.

Le calcul. Les fonctions inversibles sur $M_{0,5}$ sont, à une constante près, les monômes en λ, μ, $1-\lambda$, $1-\mu$ et $\lambda-\mu$. Chercher h revient à résoudre un système linéaire sur les exposants de ces cinq facteurs, plus une condition de signe sur la constante. Un calcul formel (sympy), qui retrouve d'abord les valeurs 3 et 6 pour $n=4$, donne l'ordre 4 pour L et l'ordre 12 pour L_5, avec les fonctions h ci-dessous. Pour minorer, on raisonne comme pour $n=4$ par les points fixes. Prenons i avec $i^2=-1$. Le 4-cycle $s_1s_2s_3$ fixe le point $(\lambda,\mu)=(-1,i)$: l'homographie correspondante est $z \mapsto (z+1)/(1-z)$, qui envoie $0 \mapsto 1 \mapsto \infty \mapsto -1 \mapsto 0$ et fixe i. Sa dérivée en i vaut $2/(1-i)^2 = i$, une racine primitive quatrième de l'unité. Le 3-cycle s_1s_2, lui, fixe $(1-\zeta,\zeta)$, où $\zeta^2-\zeta+1=0$; l'homographie est $z \mapsto 1/(1-z)$, et sa dérivée en ζ vaut ζ^2.

La figure 22 dessine la partie réelle de ce modèle. Les cinq droites retirées sont les lieux d'annulation des cinq unités λ, μ, $1-\lambda$, $1-\mu$, $\lambda-\mu$, d'où le système linéaire sur leurs exposants. Deux des générateurs s'y voient : s_4 est la symétrie par rapport à la diagonale, s_1 la symétrie de centre $(1/2,1/2)$. Les deux points fixes qui servent de certificats sont complexes et ne figurent que par leurs coordonnées.

Théorème 74.3 (conjecture de la page 70, colonne $n=5$, pour L_i (« 12 ? »), démontrée par l'édition ♦). *Soit K un corps où 2 et 3 sont inversibles, qui contient i avec $i^2=-1$ et une racine ζ de $\zeta^2-\zeta+1$. La puissance m-ième du cocycle c_5 de L_5 sous $\mathfrak{S}_4$ est le cobord d'une fonction sans*



Points complexes fixes :
$(-1, i)$, fixé par le 4-cycle $s_1 s_2 s_3$,
facteur i sur L_5 et sur L ;
$(1-\zeta, \zeta)$, fixé par le 3-cycle $s_1 s_2$,
facteur ζ^2 sur L_5, 1 sur L.

FIGURE 22 – La partie réelle de $M_{0,5}$ dans les coordonnées (λ, μ) : le complémentaire des cinq droites $\lambda = 0$, $\lambda = 1$, $\mu = 0$, $\mu = 1$, $\lambda = \mu$. Les points fixes qui donnent les minorations $4 \mid m$ et $3 \mid m$ ne sont pas réels.

zéro sur $M_{0,5}(K)$ si et seulement si $12 \mid m$. Pour $m = 12$ on peut prendre

$$h = \frac{\mu^6(1-\mu)^6(\lambda-\mu)^6}{\lambda^2(1-\lambda)^2}.$$

Démonstration. Pour $m = 12$, l'égalité $c_5(s)^{12} = h(sx)/h(x)$ se vérifie sur les trois générateurs, par exemple pour s_1 : $c_5 = -1$, et h est invariante par $(\lambda, \mu) \mapsto (1-\lambda, 1-\mu)$. Elle passe aux produits de générateurs, puisque les deux membres suivent la même règle de cocycle. Réciproquement, au point $(-1, i)$, fixé par $s_1 s_2 s_3$, le second membre vaut 1 et le cocycle vaut i, d'où $i^m = 1$ et $4 \mid m$; au point $(1-\zeta, \zeta)$, fixé par $s_1 s_2$, il vaut ζ^2, d'où $3 \mid m$. □

Contre-exemple 74.4 (page 70, colonne $n = 5$, pour L : le « 12 ? » n'est pas le meilleur exposant ♦). *Sous les mêmes hypothèses (il suffit que 2 soit inversible et que i existe), la puissance m-ième du cocycle c_L de L sous $\mathfrak{S}_5$ est un cobord si et seulement si $4 \mid m$. Pour $m = 4$ on peut prendre $h = \big(\lambda\mu(1-\lambda)(1-\mu)(\lambda-\mu)\big)^2$. Le meilleur exposant pour L est donc 4, et non 12.*

Démonstration. Sur les générateurs, $c_L(s)^4 = h(sx)/h(x)$ se vérifie directement ; par exemple pour s_4, $c_L = 1$ et h est symétrique en λ, μ. Au point $(-1, i)$, le facteur de L est encore i : les quatre autres points forment un seul cycle, et le produit des dérivées le long d'un cycle de longueur 4 est la dérivée de $\varphi^4 = \mathrm{id}$, soit 1. D'où $4 \mid m$. L'ordre 3 disparaît : au point $(1-\zeta, \zeta)$, les dérivées aux deux points fixes ζ et $1-\zeta$ sont inverses l'une de l'autre, comme la signature compensait la dérivée en -1 pour $n = 4$. □

Le 12 de la page pour L est donc un exposant qui trivialise, celui que donne le calcul $(L^4)^3 \simeq \mathcal{O}$, mais pas le meilleur ; c'est la même situation que pour $n = 4$, où la page 72 trouvait $L^{\otimes 6} \simeq 1$ quand l'ordre est 3.
Vérifié au niveau des cocycles (`cL_pow_four`, `coboundary_cL_iff`, `c5_pow_twelve`, `coboundary_c5_iff`). Lean manipule les mots en $s_1, \ldots, s_4$: la substitution d'un mot est la composée, son facteur est donné par la règle de cocycle (`wAct`, `wCoc`), et l'énoncé « pour tout élément du groupe » devient « pour tout mot ». Que les mots passent au groupe, c'est-à-dire que substitutions et facteurs vérifient les relations de Coxeter de $\mathfrak{S}_5$, est démontré plus bas (énoncé « relations de Coxeter », après la colonne $n = 6$). N'est pas démontrée en Lean la dérivation des facteurs c_L, c_5 à partir des homographies, faite ci-dessus.

Passons à la colonne $n = 6$, où la page porte « 20 ? » pour L et « 60 ? » pour L_i.
Le modèle. On envoie encore les trois premiers points en 0, 1, ∞ ; il reste trois coordonnées (λ, μ, ν), hors de $\{0, 1\}$ et deux à deux distinctes. Les cinq transpositions $s_1, \dots, s_5$ agissent comme pour $n = 5$, la troisième coordonnée suivant la deuxième :

$$s_1 : (1-\lambda,\ 1-\mu,\ 1-\nu), \qquad s_2 : \Big(\frac{\lambda}{\lambda-1},\ \frac{\mu}{\mu-1},\ \frac{\nu}{\nu-1}\Big),$$

$$s_3 : \Big(1-\lambda,\ \frac{\mu(\lambda-1)}{\lambda-\mu},\ \frac{\nu(\lambda-1)}{\lambda-\nu}\Big), \qquad s_4 : (\mu, \lambda, \nu), \qquad s_5 : (\lambda, \nu, \mu).$$

Le facteur sur L_6 est la dérivée de l'homographie au sixième point, pour le groupe $\mathfrak{S}_5$ engendré par $s_1, \dots, s_4$; le facteur sur L est le produit des six dérivées. On trouve, pour $s_1, \dots, s_5$ et $s_1, \dots, s_4$:

$$c_L = 1,\ \ \frac{1}{(\lambda-1)^2(\mu-1)^2(\nu-1)^2},\ \ \frac{\lambda^2(\lambda-1)^2}{(\lambda-\mu)^2(\lambda-\nu)^2},\ \ 1,\ \ 1;$$

$$c_6 = -1,\ \ \frac{-1}{(\nu-1)^2},\ \ \frac{\lambda(\lambda-1)}{(\lambda-\nu)^2},\ \ 1.$$

Le calcul. Les unités de $M_{0,6}$ sont, à une constante près, les monômes en neuf facteurs : λ, μ, ν, $1-\lambda$, $1-\mu$, $1-\nu$, $\lambda-\mu$, $\lambda-\nu$, $\mu-\nu$. Chaque générateur envoie chacun d'eux sur un monôme, au signe près ; par exemple s_2 envoie $\lambda - \mu$ sur $(\mu-\lambda)/((\lambda-1)(\mu-1))$. Chercher h revient donc encore à un système linéaire en neuf inconnues entières, plus une condition de signe. Un programme d'algèbre linéaire exacte sur $\mathbf{Z}$ le résout. Pour L, la solution est simple : c_L^5 est le cobord du carré du produit des neuf unités. Pour L_6, le système a une solution dès $m = 10$, avec

$$g = \frac{\nu^4(1-\nu)^4(\lambda-\nu)^4(\mu-\nu)^4}{\lambda\mu(1-\lambda)(1-\mu)(\lambda-\mu)},$$

mais le signe ne suit pas : $c_6(s)^{10} = -g(sx)/g(x)$ pour chacun des quatre générateurs. Une constante ne corrige pas ce signe, puisqu'elle disparaît du quotient $h(sx)/h(x)$. Il faut donc passer à $m = 20$, où c_6^{20} est le cobord de g^2.
Les points fixes. Pour minorer, on cherche comme pour $n = 5$ des points fixés par un élément d'ordre 5 et par un élément d'ordre 4. Le 5-cycle $s_1 s_2 s_3 s_4$ correspond à une homographie ψ d'ordre 5 qui envoie $0 \mapsto 1 \mapsto \infty \mapsto \lambda \mapsto \mu \mapsto 0$ et fixe ν. Une telle homographie est conjuguée à la rotation $z \mapsto \omega z$, où ω est une racine primitive cinquième de l'unité ; la configuration est celle de 0 et des cinq racines cinquièmes de l'unité, à une homographie près. Dans nos coordonnées, avec $\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$, c'est le point

$$(\lambda, \mu, \nu) = (\omega^2 + \omega^3,\ 1 + \omega^2 + \omega^3,\ -\omega^4).$$

Le facteur de L_6 y est la dérivée $\psi'(\nu)$, qui vaut ω. Celui de L aussi : les cinq autres points forment un seul cycle, et le produit des dérivées le long de ce cycle est la dérivée de $\psi^5 = \mathrm{id}$, soit 1. Les coordonnées de ce point et les dénominateurs rencontrés en chemin sont des unités de $\mathbf{Z}[\omega]$: il n'y faut aucune hypothèse sur le corps. Seule la conclusion $\omega^m = 1 \Rightarrow 5 \mid m$ demande que 5 soit inversible. Le 4-cycle $s_1 s_2 s_3$ correspond, comme pour $n = 5$, à $z \mapsto (z+1)/(1-z)$, qui fixe i et $-i$; il fixe donc le point $(-1, -i, i)$. Le facteur de L_6 y vaut i. Celui de L vaut $i \cdot (-i) = 1$, car les dérivées aux deux points fixes se compensent.

Contre-exemple 74.5 (page 70, colonne $n = 6$, pour L : le « 20 ? » n'est pas le meilleur

exposant ♦). *Soit K un corps où 5 est inversible et qui contient une racine ω de $\omega^4+\omega^3+\omega^2+\omega+1$. La puissance m-ième du cocycle c_L de L sous $\mathfrak{S}_6$ est le cobord d'une fonction sans zéro sur $M_{0,6}(K)$ si et seulement si $5 \mid m$. Pour $m=5$ on peut prendre*

$$h = \big(\lambda\mu\nu(1-\lambda)(1-\mu)(1-\nu)(\lambda-\mu)(\lambda-\nu)(\mu-\nu)\big)^2.$$

Le meilleur exposant pour L est donc 5, et non 20.

Démonstration. Sur les générateurs, $c_L(s)^5 = h(sx)/h(x)$ se vérifie directement. Par exemple pour s_2, le produit H des neuf unités vérifie $H(s_2x)/H(x) = \pm 1/((\lambda-1)(\mu-1)(\nu-1))^5$: pour $x=\lambda$, le facteur $\lambda-1$ vient de l'image de λ, de celle de $1-\lambda$, des images des deux différences où λ figure, et du facteur $1-\lambda$ de $H(x)$. Au carré, on trouve $c_L(s_2)^5$. Les mots en suivent par la règle de cocycle. Au point fixé par $s_1s_2s_3s_4$, le second membre vaut 1 et le cocycle vaut ω, d'où $\omega^m = 1$ et $5 \mid m$. □

Contre-exemple 74.6 (page 70, colonne $n=6$, pour L_i : le « 60 ? » n'est pas le meilleur exposant ♦). *Soit K un corps où 2 et 5 sont inversibles, qui contient i avec $i^2=-1$ et une racine ω de $\omega^4+\omega^3+\omega^2+\omega+1$. La puissance m-ième du cocycle c_6 de L_6 sous $\mathfrak{S}_5$ est le cobord d'une fonction sans zéro sur $M_{0,6}(K)$ si et seulement si $20 \mid m$. Pour $m=20$ on peut prendre $h=g^2$, avec g ci-dessus. Le meilleur exposant pour L_i est donc 20, et non 60.*

Démonstration. Sur les générateurs, $c_6(s)^{10} = -g(sx)/g(x)$, d'où $c_6(s)^{20} = g(sx)^2/g(x)^2$, et les mots en suivent. Au point fixé par $s_1s_2s_3s_4$, le cocycle vaut ω, d'où $5 \mid m$; au point $(-1,-i,i)$, fixé par $s_1s_2s_3$, il vaut i, d'où $4 \mid m$. □

Les deux valeurs de la page sont des exposants qui trivialisent, puisque $5 \mid 20$ et $20 \mid 60$, mais aucune n'est la plus petite. L'ordre 3, que suggère le $60 = 3 \cdot 20$ de la page, n'apparaît pas : comme c_6^{20} est un cobord, le facteur f en un point fixé par un 3-cycle vérifie $f^{20}=1$ et $f^3=1$, donc $f=1$. Sur les trois colonnes, L est d'ordre $n-1$ et L_i d'ordre $(n-1)(n-2)$, le nombre de la première ligne du tableau.[78]

Vérifié au niveau des cocycles (`act6_U6`, `cL6_pow_five`, `c6_pow_ten`, `fix_five`, `fix_four6`, `coboundary_cL6_iff`, `coboundary_c6_iff`), avec les mots en $s_1,\dots,s_5$ comme pour $n=5$ (`wAct`, `wCoc`). Les relations de Coxeter de $\mathfrak{S}_6$ pour ces substitutions et ces facteurs sont démontrées ci-dessous (énoncé « relations de Coxeter »). Ne sont pas démontrées en Lean la dérivation des facteurs à partir des homographies, et la résolution du système linéaire, dont Lean ne vérifie que la solution.

Les relations de Coxeter. Les substitutions et les facteurs n'ont été donnés que sur les transpositions adjacentes, et les énoncés ci-dessus portent sur les mots. Pour qu'ils portent sur le groupe, il faut que deux mots qui représentent la même permutation aient même substitution et même facteur, c'est-à-dire que les générateurs vérifient les relations de Coxeter.

Énoncé (De l'édition : relations de Coxeter ♦). *Sur tout corps K, les quatre familles de générateurs ci-dessus — $s_1,\dots,s_4$ avec c_L et s_1,s_2,s_3 avec c_5 sur $M_{0,5}(K)$, $s_1,\dots,s_5$ avec c_L*

78. Le groupe lui-même est connu : $H^1(\mathfrak{S}_n, \mathcal{O}(M_{0,n})^*) = \mathrm{Pic}\,[M_{0,n}/\mathfrak{S}_n]$ est cyclique d'ordre $2(n-1)$ pour n pair en caractéristique ne divisant pas n (Gorchinskiy–Viviani [60, th. 3.6] ; Arsie–Vistoli [5, th. 5.1] calculent le groupe de Picard du champ des courbes hyperelliptiques, dont celui-ci est un sous-groupe d'indice 1 ou 2) ; les ordres de L et des L_i en découlent, mais ne sont énoncés pour ces fibrés dans aucun texte trouvé.

et $s_1, \dots, s_4$ avec c_6 sur $M_{0,6}(K)$ — vérifient les relations de Coxeter de type A :

$$s_i^2 = 1, \qquad s_i s_j s_i = s_j s_i s_j \ (|i-j| = 1), \qquad s_i s_j = s_j s_i \ (|i-j| \geq 2),$$

pour la substitution et pour le facteur composé par la règle de cocycle. Les applications $(x, t) \mapsto (s_i x, c(s_i)(x)\, t)$ du fibré trivial $M_{0,n}(K) \times K$ définissent donc une action du groupe de Coxeter de type A_{n-1}, et la substitution et le facteur d'un mot ne dépendent que de son image dans ce groupe.

Démonstration. Chaque relation est une identité entre fractions rationnelles, à vérifier sur $M_{0,n}(K)$. Le calcul direct bute sur les dénominateurs emboîtés : dans $s_3 s_3$, par exemple, apparaît $1/\big((1-\lambda) - \mu(\lambda-1)/(\lambda-\mu)\big)$, dont il faut savoir qu'il ne s'annule pas. On nomme donc les points intermédiaires : pour $s_i s_j s_i = s_j s_i s_j$, on pose $q = s_i x$, $r = s_j q$, $q' = s_j x$, $r' = s_i q'$, qui sont dans $M_{0,n}(K)$ puisque les substitutions le préservent. L'identité, écrite en r et r', n'a pour dénominateurs que leurs coordonnées et leurs différences, non nulles ; on les chasse, on remplace r et r' par leurs expressions en q et q', on chasse de nouveau, puis on descend à x, où il reste une identité polynomiale. Les relations entraînent $(s_i s_j)^3 = 1$ et $(s_i s_j)^2 = 1$ dans le monoïde des applications du fibré, ce qui est la présentation du groupe de Coxeter de type A_{n-1}. Que ce groupe soit $\mathfrak{S}_n$ est classique. □

Vérifié dans `Folder146.lean` : `CoxRel` pour les relations sur les générateurs, `coxRel_cL`, `coxRel_c5`, `coxRel_cL6`, `coxRel_c6` pour les quatre familles, `CoxRel.isLiftable` et `CoxRel.lift` pour l'action du groupe de Coxeter (par `CoxeterSystem.lift` de Mathlib), `CoxRel.lift_word` et `CoxRel.wAct_eq` pour le passage des mots au groupe. Mathlib n'identifie pas le groupe de Coxeter de type A_{n-1} à $\mathfrak{S}_n$; ce dernier pas n'est pas formalisé.

Le tableau 2 met en regard les valeurs de la page et les ordres calculés.

	$n=4$	$n=5$	$n=6$
L, page 70	3	12 ?	20 ?
L, ordre calculé, $n-1$	3	**4**	**5**
L_i, page 70	6	12 ?	60 ?
L_i, ordre calculé, $(n-1)(n-2)$	6	12	**20**
statut	Lean th. 74.1, 74.2	Lean th. 74.3, c.-ex. 74.4	Lean c.-ex. 74.5, 74.6

TABLE 2 – Le tableau de la page 70 et les ordres calculés. En gras, les valeurs qui diffèrent de celles de la page ; les points d'interrogation sont ceux du manuscrit.

Tous les n

Les trois colonnes suggèrent une règle : $n-1$ pour L et $(n-1)(n-2)$ pour L_i. Elle se démontre pour tout n, à condition de changer de modèle. Les coordonnées normalisées des colonnes précédentes, où trois points sont envoyés en 0, 1 et ∞, obligent à écrire une homographie de renormalisation par permutation, et leur forme dépend de n. Le modèle homogène évite cette étape.

Un point de $\mathbb{P}^1(K)$ est un vecteur non nul $v = (v_1, v_2)$ de K^2, à un scalaire près. Deux vecteurs donnent le même point si et seulement si leur crochet $[v\, w] = v_1 w_2 - v_2 w_1$ est nul.

Une configuration de n points distincts est donc une famille $v_1, \dots, v_n$ de vecteurs dont tous les crochets $[v_i\, v_j]$, $i \neq j$, sont non nuls. Une fonction sur $M_{0,n}(K)$ est une fonction de la configuration invariante par $\mathrm{GL}_2(K)$ et par le changement de chaque v_i en un multiple. La droite tangente à $\mathbb{P}^1$ au point $\langle v\rangle$ est $\mathrm{Hom}(\langle v\rangle, K^2/\langle v\rangle)$, isomorphe à $\langle v\rangle^{\otimes -2} \otimes \det K^2$. Une section partout non nulle de $L_i^{\otimes m}$ devient ainsi, quitte à l'inverser, une fonction sans zéro qui est multipliée par t^{2m} quand v_i est multiplié par t, qui ne change pas quand on multiplie les autres vecteurs, et qui est multipliée par $\det(g)^m$ sous $g \in \mathrm{GL}_2(K)$. Pour $L = L_1 \otimes \cdots \otimes L_n$, les poids sont t_i^{2m} pour chaque vecteur et $\det(g)^{mn}$. Trivialiser $L^{\otimes m}$ de façon compatible au groupe symétrique, c'est trouver une telle fonction invariante par toute renumérotation des points ; pour L_n, invariante par les renumérotations qui fixent le n-ième point. Comme dans les colonnes précédentes, la fonction n'est pas supposée régulière.

Théorème 74.7 (énoncé de l'édition, d'après le tableau de la page 70 ♦). *Soit $n \geq 3$ et soit K un corps qui contient une racine primitive $(n-1)$-ième de l'unité ω et une racine primitive $(n-2)$-ième de l'unité ζ. Dans le modèle homogène :*

1. *$L^{\otimes m}$ se trivialise de façon compatible à $\mathfrak{S}_n$ si et seulement si $n-1$ divise m (pour cette partie, $n \geq 2$ et seule ω sert) ;*
2. *$L_n^{\otimes m}$ se trivialise de façon compatible au stabilisateur $\mathfrak{S}_{n-1}$ du n-ième point si et seulement si $(n-1)(n-2)$ divise m.*

Les fonctions qui trivialisent existent sur tout corps.

Pour $n = 4$, 5 et 6 on retrouve 3, 4, 5 et 6, 12, 20, les ordres trouvés plus haut dans les coordonnées normalisées.

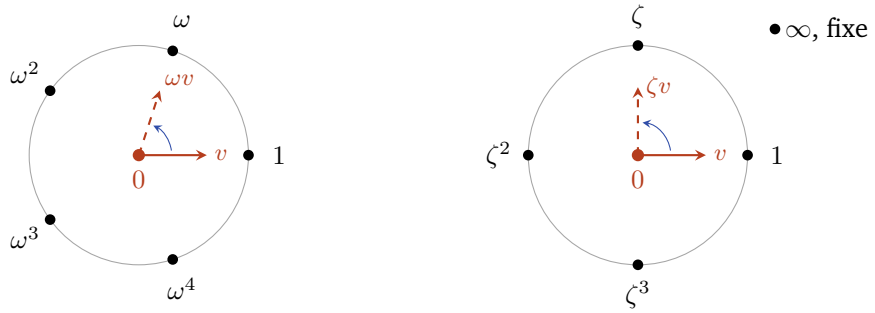
Démonstration. Les fonctions qui trivialisent sont des produits de crochets. Soit D le produit des crochets $[v_i\, v_j]$ sur les couples ordonnés $i \neq j$; c'est, au signe près, le carré du produit de Vandermonde $\prod_{i<j}[v_i\, v_j]$, et le carré efface le signe que fait apparaître une permutation. Chaque indice figure dans $2(n-1)$ facteurs : multiplier v_i par t_i multiplie D par $t_i^{2(n-1)}$, et g le multiplie par $\det(g)^{n(n-1)}$, car $[gv\, gw] = \det(g)\,[v\, w]$. Ce sont les poids de $L^{\otimes(n-1)}$: D trivialise $L^{\otimes(n-1)}$. Pour L_n, notons p le n-ième point et $v_1, \dots, v_k$ les $k = n-1$ autres, et posons

$$F = \frac{\left(\prod_i [v_i\, p]\right)^{2(k-1)}}{D(v_1, \dots, v_k)}.$$

Chaque v_i figure $2(k-1)$ fois au numérateur et $2(k-1)$ fois au dénominateur, donc son poids est nul ; p a le poids $2k(k-1)$, et $\det(g)$ l'exposant $2k(k-1) - k(k-1) = k(k-1)$. Ce sont les poids de $L_n^{\otimes k(k-1)}$, avec $k(k-1) = (n-1)(n-2)$. Pour $n = 5$, avec $p = \mu$ et les autres points en 0, 1, ∞, λ, on reconnaît en coordonnées affines, au signe près, la fonction $\mu^6(1-\mu)^6(\lambda-\mu)^6/(\lambda^2(1-\lambda)^2)$ du théorème 74.3.

Pour la minoration, on cherche des configurations qu'une renumérotation σ envoie sur leur image par une matrice g (figure 23). Si F trivialise, $F(v) = F(v \circ \sigma) = F(gv)$, qui vaut $F(v)$ multiplié par le poids de g, et ce poids vaut donc 1. Pour L, on prend le point 0 et les $n-1$ racines $(n-1)$-ièmes de l'unité, que la matrice $g = \mathrm{diag}(\omega, 1)$, de déterminant ω, fait tourner ; on obtient $\omega^{mn} = 1$, donc $n-1$ divise mn, et comme $n \equiv 1$ modulo $n-1$, il divise m. Pour L_n, le n-ième point est en 0. La même configuration donne $\omega^m = 1$, d'où $n-1 \mid m$. La configuration formée de 0, de ∞ et des racines $(n-2)$-ièmes de l'unité, que $\mathrm{diag}(\zeta, 1)$ fait tourner en fixant 0 et ∞, donne $\zeta^m = 1$, d'où $n-2 \mid m$. Le vecteur $(1, 0)$ de ∞ y est multiplié par ζ, ce qui

ne compte pas, car F ne voit pas les multiples des autres points. Comme $n-1$ et $n-2$ sont premiers entre eux, leur produit divise m. □



$\{0\} \cup \mu_5$, tournée par $z \mapsto \omega z$
(L, et L_n avec le n-ième point en 0)

$\{0, \infty\} \cup \mu_4$, tournée par $z \mapsto \zeta z$
(L_n, le n-ième point en 0)

FIGURE 23 – Les deux configurations de la minoration, pour $n = 6$. À gauche, 0 et les $n-1 = 5$ racines cinquièmes de l'unité ; la matrice $\mathrm{diag}(\omega, 1)$ les fait tourner, ce qui revient à les renuméroter, et fixe 0. À droite, 0, ∞ et les $n-2 = 4$ racines quatrièmes de l'unité, que $\mathrm{diag}(\zeta, 1)$ fait tourner en fixant 0 et ∞. Le point 0, qui porte L_n, est fixe, mais son vecteur tangent v tourne avec la figure et devient ωv, ou ζv ; une trivialisation compatible à la renumérotation doit donner la même valeur aux deux, et le poids $\det(g)^m$ de la matrice doit valoir 1 : $\omega^m = 1$ à gauche, $\zeta^m = 1$ à droite, d'où $5 \mid m$ et $4 \mid m$, donc $20 \mid m$ pour L_6.

Vérifié (`br`, `Conf`, `disc`, `TrivL`, `TrivLi`, `disc_smul`, `disc_lin`, `disc_perm`, `trivL_of_dvd`, `trivLi_of_dvd`, `dvd_of_trivL`, `dvd_of_trivLi`, `trivL_iff`, `trivLi_iff`). Ne sont pas démontrés en Lean : le dictionnaire entre fibrés en droites équivariants sur $M_{0,n}$ et fonctions de poids sur les configurations, et le fait que le groupe de Picard équivariant soit le H^1 des unités. Mathlib n'a pas les espaces de modules $M_{0,n}$.

Pour n pair, ces ordres sont dans la littérature. Edidin et Hu, partant de la description de Pernice [104], qu'ils présentent par un sous-groupe de Borel, décrivent $[M_{0,2g+2}/\mathfrak{S}_{2g+1}]$ comme le champ des formes binaires de degré $2g+2$ munies d'une racine marquée, et calculent son anneau de Chow entier sur un corps algébriquement clos de caractéristique ne divisant pas $2g+2$: $\mathbf{Z}[l]/(2g(2g+1)\,l)$ pour $g \geqslant 2$ [47, théorème 1.3]. Le groupe de Picard est donc cyclique d'ordre $(n-1)(n-2)$ pour $n = 2g+2 \geqslant 6$. Leur générateur l est la classe d'un caractère d'un tore ; comme L_n y est d'ordre $(n-1)(n-2)$, il engendre aussi ce groupe, ce qu'ils n'énoncent pas. Pour $n = 4$, $M_{1,1}$ est une gerbe en μ_2 au-dessus de $[M_{0,4}/\mathfrak{S}_3]$, et $\mathrm{Pic}(M_{1,1}) = \mathbf{Z}/12$ [103, 52] donne l'ordre 6. Pour n impair, en particulier pour la colonne $n = 5$ de la page, aucun énoncé imprimé n'a été trouvé, et D. Edidin confirme que leur article ne traite que le cas pair et qu'il ne connaît pas de référence pour le cas impair [46]. Un argument par tranches donne pourtant le même ordre pour tout n, en caractéristique 0 : on place le n-ième point à l'infini, ce qui laisse le groupe affine agir sur les polynômes unitaires sans racine multiple de degré $m = n-1$; on impose ensuite aux racines d'être de somme nulle, et il reste $\mathbb{G}_m$, de poids $2, \ldots, m$ sur les coefficients. Le discriminant, irréductible et de poids $m(m-1)$, donne $\mathrm{Pic}[M_{0,n}/\mathfrak{S}_{n-1}] \cong \mathbf{Z}/(n-1)(n-2)$, engendré par la droite tangente au point à l'infini [97]. Le théorème 70.7 en est la contrepartie dans le modèle homogène, le seul que Lean vérifie.

Les deux modèles s'accordent

Les colonnes $n = 4$, 5, 6 ont été traitées par des cocycles en coordonnées normalisées, la règle générale par des fonctions de poids sur des configurations. Les deux calculs donnent les mêmes ordres, mais rien ne disait encore qu'ils parlent du même objet. On le vérifie ici en restreignant le modèle homogène aux configurations normalisées.

Restreindre. Pour $n = 5$, la configuration normalisée de (λ, μ) est la famille de vecteurs

$$(0,1),\ (1,1),\ (1,0),\ (\lambda,1),\ (\mu,1),$$

qui représente les points 0, 1, ∞, λ, μ. Une fonction F de poids, qui trivialise $L^{\otimes m}$ dans le modèle homogène, donne par restriction une fonction sans zéro sur $M_{0,5}(K)$,

$$h(\lambda,\mu) = F\big((0,1),(1,1),(1,0),(\lambda,1),(\mu,1)\big).$$

La question est de savoir comment h change sous les générateurs $s_1, \dots, s_4$.

Un générateur. Prenons s_3, qui échange les étiquettes de ∞ et de λ. Après échange, les trois premiers points sont 0, 1, λ, et la substitution de renormalisation est l'homographie $g(z) = (1-\lambda)z/(z-\lambda)$, qui les envoie sur 0, 1, ∞ ; elle envoie le nouveau quatrième point, ∞, sur $1-\lambda$, et μ sur $\mu(\lambda-1)/(\lambda-\mu)$. C'est la substitution s_3 de la colonne $n = 5$. En vecteurs, g est la matrice $\begin{pmatrix} 1-\lambda & 0 \\ 1 & -\lambda \end{pmatrix}$, de déterminant $\lambda(\lambda-1)$, et elle envoie chaque vecteur de la configuration renumérotée sur un multiple du vecteur normalisé correspondant : $(0,1) \mapsto (0,-\lambda)$, $(1,1) \mapsto (1-\lambda)(1,1)$, $(\lambda,1) \mapsto \lambda(1-\lambda)(1,0)$, $(1,0) \mapsto (1-\lambda,1)$ et $(\mu,1) \mapsto (\mu-\lambda)\big(\mu(1-\lambda)/(\mu-\lambda),1\big)$. Les poids de F donnent

$$h(s_3(\lambda,\mu)) = \Big(\big(\textstyle\prod_i t_i\big)^2 \det(g)^5\Big)^m h(\lambda,\mu), \qquad \textstyle\prod_i t_i = \frac{-1}{\lambda^2(1-\lambda)^2(\mu-\lambda)},$$

où les t_i sont les inverses des multiples ci-dessus, et l'invariance de F par renumérotation absorbe l'échange. Le facteur vaut $\lambda(\lambda-1)/(\lambda-\mu)^2$: c'est exactement le facteur de s_3 sur L dans la colonne $n = 5$. Les autres générateurs se traitent de même, avec des matrices plus simples. Pour L_5, seul le cinquième vecteur porte un poids, et le facteur devient $t_5^2 \det(g)$, qui redonne le cocycle de L_5.

Énoncé (De l'édition : accord des deux modèles ♦)**.** *Pour $n = 4$, 5, 6, sur tout corps K, une trivialisation de $L^{\otimes m}$ (resp. de $L_n^{\otimes m}$ sous le stabiliseur du n-ième point) dans le modèle homogène se restreint aux configurations normalisées en une fonction sans zéro h dont le cobord est la puissance m-ième du cocycle des coordonnées normalisées :* $\operatorname{sgn} g \cdot g'(\lambda)$ *et* $g'(\lambda)$ *pour $n = 4$, les cocycles de L et de L_5 pour $n = 5$, ceux de L et de L_6 pour $n = 6$. Sous les hypothèses sur K des colonnes, les deux conditions sont équivalentes.*

Démonstration. Pour chaque générateur, on écrit la matrice de renormalisation et les multiples, comme pour s_3 ci-dessus, et l'on vérifie que $(\prod_i t_i)^2 \det(g)^n$, resp. $t_n^2 \det(g)$, est le facteur du cocycle ; pour $n = 4$, on le fait pour les six éléments de $\mathfrak{S}_3$. La relation de cobord passe des générateurs aux mots par la règle de cocycle. Pour la réciproque, une puissance m-ième du cocycle qui est un cobord force m à être multiple de l'ordre calculé dans la colonne, et la fonction de poids de l'énoncé général trivialise alors $L^{\otimes m}$ ou $L_n^{\otimes m}$. □

La réciproque passe donc par les nombres, non par la construction : on ne prolonge pas h

en une fonction de poids sur toutes les configurations. Le sens direct suffit à relier les deux calculs : toute trivialisation du modèle homogène en donne une des cocycles normalisés, par simple restriction.
Vérifié dans `Folder146.lean` : `trivL_step` et `trivLi_step` pour le changement d'une fonction de poids sous une renormalisation, `cob_of_trivL` et `cob_of_trivLi` pour la restriction, `step4`, `step5`, `step5i`, `step6` et `step6i` pour les matrices et les multiples, `coboundary_derL_of_trivL`, `coboundary_der_of_trivLi`, `coboundary_cL_of_trivL`, `coboundary_c5_of_trivLi`, `coboundary_cL6_of_trivL` et `coboundary_c6_of_trivLi` pour le sens direct, et `trivL_four_iff`, `trivLi_four_iff`, `trivL_five_iff`, `trivLi_five_iff`, `trivL_six_iff`, `trivLi_six_iff` pour l'équivalence. Le dictionnaire avec les fibrés équivariants reste hors de portée.

75 Cote 140-1 : le groupe $H^1(U_{0,3}, \mathfrak{S}_3; \mathbf{G}_m)$ [79]

La cote 140-1, brouillon de la *Longue Marche*, trente-six pages que l'inventaire date « [à partir de 1978-à partir de 1982] », encadre page 22 un lemme : pour S régulier intègre, $\mathrm{Pic}(S) = 0$, de caractéristique générique $\neq 2$, le groupe $H^1(U_{0,3}, \mathfrak{S}_3; \mathbf{G}_m)$ des $\mathbf{G}_m$-torseurs $\mathfrak{S}_3$-équivariants sur $U_{0,3} = \mathbf{P}^1 - \{0, 1, \infty\}$ est $\mathbf{Z}/6$, engendré par $\mathcal{O}(1)$, et $\mathbf{Z}/3$ en caractéristique générique 2 (140-1, lot 2, p. 22). Une note marginale le majore par deux suites exactes : H^1 équivariant $= H^1(\mathfrak{S}_3, \mathcal{O}(U_{0,3})^*)$, et $0 \to \mathcal{O}(S)^* \to \mathcal{O}(U_{0,3})^* \to V(J) \to 0$, où $V(J) = \mathrm{Ker}(\mathbf{Z}^J \to \mathbf{Z})$ est le groupe des diviseurs des unités, J l'ensemble des trois points retirés. Les calculs de $H^1(\mathfrak{S}_3, \cdot)$ qui concluent ne sont pas sur la page ; la lecture les ajoute.
Conventions. H^1 est la cohomologie des groupes de mathlib, $H^1(G, M)$ pour la représentation de G sur un groupe abélien M ; Lean l'identifie aux cocycles modulo les cobords. Le groupe $\mathcal{O}(S)^*$ est remplacé par les unités k^* d'un anneau intègre, avec l'action triviale.

Théorème 75.1 (énoncé de l'édition, d'après la note marginale de la page 22)**.** *On a $H^1(\mathfrak{S}_3, V(J)) \simeq \mathbf{Z}/3$ et $H^1(\mathfrak{S}_3, k^*) \simeq \mu_2(k)$. Pour toute extension de $\mathfrak{S}_3$-modules $0 \to k^* \to M \to V(J) \to 0$, l'ordre de $H^1(\mathfrak{S}_3, M)$ divise 6, et divise 3 si $2 = 0$ dans k.*

Vérifié tel quel (`H1_VJ`, `card_H1_VJ`, `card_H1_triv`, `card_mu2_dvd`, `card_H1_dvd`). La classe d'un cocycle f à valeurs dans $V(J)$ est $\sum_j m_j \bmod 3$, où $m_j = -f(\tau_j)_j$, τ_j la transposition de 0 et j : c'est la forme explicite de $H^1(\mathfrak{S}_3, \mathbf{Z}^J) = 0$ et du bord $\mathbf{Z} \to H^1(\mathfrak{S}_3, V(J))$.

La majoration ne dit pas encore que le groupe vaut $\mathbf{Z}/6$: il faut une classe d'ordre exactement 6. La page 24 la cherche du côté de $\mathcal{O}(1)$. On en prend ici une autre, plus facile à manier, la classe du fibré tangent, et l'on travaille dans un modèle explicite des unités.
Le modèle. Sur un corps k, les unités de $U_{0,3} = \mathrm{Spec}\, k[\lambda, 1/\lambda, 1/(1-\lambda)]$ sont les $c\,\lambda^a(1-\lambda)^b$, $c \in k^*$, $a, b \in \mathbf{Z}$. On les code par le couple (c, v), où $v = (a, b, -a-b) \in V(J)$ est le diviseur sur les points 0, 1, ∞. Une permutation σ de ces trois points est induite par une unique substitution anharmonique, et σ envoie f sur $f \circ h$, où h est la substitution qui induit σ^{-1}. Sur le diviseur, l'action permute les coordonnées. Sur la constante, elle fait apparaître des signes : par exemple $\lambda/(\lambda-1) = -\lambda(1-\lambda)^{-1}$, de sorte que composer λ^a avec cette substitution multiplie la constante par $(-1)^a$. C'est ce signe qui rend l'extension $0 \to k^* \to \mathcal{O}(U_{0,3})^* \to V(J) \to 0$ de la note marginale non scindée en général. Lean définit ce module, sur un anneau intègre k, par cette formule, et vérifie sur un corps que son action est celle des substitutions : évaluées en un point x de $U(k)$, les images de λ et de $1-\lambda$ par σ valent $h(x)$ et $1-h(x)$, et les constantes sont fixes.

79. Preuve vérifiée : `lean/Grothendieck/Folder140_1.lean`.

La figure 24 montre le réseau $V(J)$ des diviseurs d'unités, dessiné dans le plan $a+b+c=0$ de $\mathbf{Z}^J$. Les six diviseurs les plus courts sont ceux de λ, $1-\lambda$, $\lambda/(\lambda-1)$ et de leurs inverses ; $\mathfrak{S}_3$ agit par les symétries d'axes les trois droites en tirets, une par transposition. Le $\mathfrak{S}_3$-module $V(J)$ ne voit pas les constantes : le signe de $\lambda/(\lambda-1) = -\lambda(1-\lambda)^{-1}$, que le modèle garde, est invisible sur le dessin, et c'est lui qui porte la partie d'ordre 2.

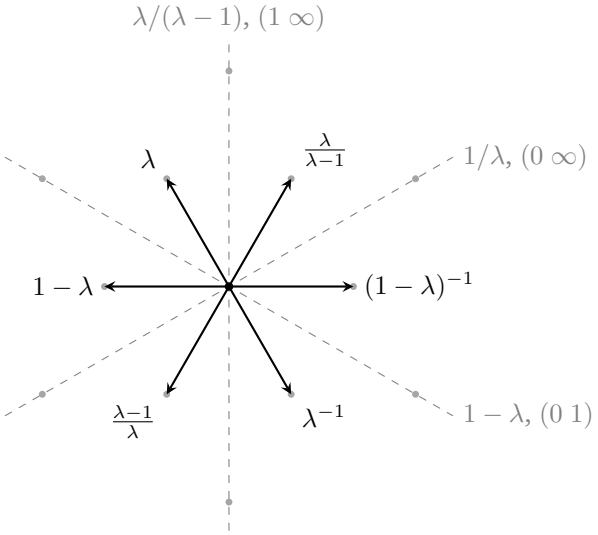


FIGURE 24 – Le réseau $V(J) = \mathrm{Ker}(\mathbf{Z}^J \to \mathbf{Z})$, $J = \{0, 1, \infty\}$, et les six unités de diviseur minimal : $\mathrm{div}\,\lambda = [0]-[\infty]$, $\mathrm{div}(1-\lambda) = [1]-[\infty]$, $\mathrm{div}\,\frac{\lambda}{\lambda-1} = [0]-[1]$. Chaque transposition, induite par la substitution indiquée, agit par la symétrie d'axe la droite en tirets correspondante.

La classe tangente. Le cocycle $\sigma \mapsto (h^{-1})'(\lambda)$, h comme ci-dessus, décrit l'action de $\mathfrak{S}_3$ sur la droite tangente au point mobile ; c'est le cocycle de la cote 146 (§ 74). Dans le modèle, sa constante est la signature de σ et son diviseur est $2[\infty] - 2[\sigma(\infty)]$. Par exemple, pour $h = 1/\lambda$, qui échange 0 et ∞, on trouve $-\lambda^{-2}$.

Théorème 75.2 (énoncé de l'édition, pour la page 24)**.** *Soit k un anneau intègre. Si $2 \neq 0$ dans k, le groupe $H^1(\mathfrak{S}_3, \mathcal{O}(U_{0,3})^*)$ du modèle est cyclique d'ordre 6, engendré par la classe tangente. Si $2 = 0$, il est cyclique d'ordre 3, engendré par la même classe.*

Démonstration. L'ordre du groupe divise 6, et 3 si $2 = 0$, par le théorème 75.1. Il suffit de voir que si m fois la classe tangente est nulle, alors $3 \mid m$, et $2 \mid m$ quand $2 \neq 0$. Supposons $m\,c = \delta(x)$, où c est le cocycle tangent et x une unité. Le diviseur de c vaut -2 fois le cobord de $[\infty]$ dans $\mathbf{Z}^J$; avec la description de $H^1(\mathfrak{S}_3, V(J)) = \mathbf{Z}/3$ par la somme des potentiels, sa classe est $-2 \equiv 1 \pmod 3$, un générateur. Comme $m\,c$ est un cobord, son image m est nulle dans $\mathbf{Z}/3$. Prenons ensuite pour σ la transposition de 0 et 1, induite par $h = 1-\lambda$. Elle fixe ∞, et l'action de σ sur la constante d'une unité ne fait apparaître aucun signe. La constante de $\sigma(x) - x$ vaut donc 1, alors que celle de $m\,c(\sigma)$ vaut $(-1)^m$. Si $2 \neq 0$, on a $-1 \neq 1$, et m est pair. □

La minoration n'utilise ni racine de $\zeta^2 - \zeta + 1$ ni l'hypothèse $3 \neq 0$: la caractéristique 3 est couverte, comme la lecture l'annonce. Dans la cote 146, l'ordre 6 du même cocycle se lit aux points fixes -1 et ζ ; ici la partie d'ordre 3 se lit sur le diviseur et la partie d'ordre 2 sur la constante.

Vérifié dans le modèle (`card_H1_units_dvd`, `dvd_of_zsmul_tan`, `H1_units`, `H1_units_char_two`) ; le modèle est comparé aux substitutions et aux dérivées de la cote 146 par `ev_smul_lam`, `ev_smul_lam'`, `smul_incl` et `ev_tan`. Que les unités de $U_{0,3}$ soient celles du modèle est le calcul classique des unités de $k[\lambda, 1/\lambda, 1/(1-\lambda)]$; il est démontré ci-dessous.

Théorème 75.3 (calcul classique, ajouté par l'édition)**.** *Soit k un anneau intègre et $A = k[\lambda, 1/\lambda, 1/(1-\lambda)]$, le localisé de $k[\lambda]$ en $\lambda(1-\lambda)$. L'application $(c, a, b) \mapsto c\,\lambda^a(1-\lambda)^b$ est un isomorphisme de $k^* \times \mathbf{Z} \times \mathbf{Z}$ sur A^* ; autrement dit $\mathcal{O}(U_{0,3})^*$ est le modèle $k^* \times V(J)$, les constantes s'envoyant sur les constantes. Si k est un corps, $\mathrm{Pic}(A) = 0$.*

Démonstration. Les éléments λ et $1-\lambda$ sont premiers dans $k[\lambda]$ et ne se divisent pas l'un l'autre (évaluer en 0 et en 1). Injectivité : si $c\,\lambda^a(1-\lambda)^b = 1$, on chasse les dénominateurs, $c\,\lambda^{a+}(1-\lambda)^{b+} = \lambda^{a-}(1-\lambda)^{b-}$ dans $k[\lambda]$, qui s'injecte dans A ; un premier qui ne divise ni une unité ni l'autre premier se simplifie, d'où $a_+ = a_-$, $b_+ = b_-$ et $c = 1$. Surjectivité : une unité u s'écrit $p/(\lambda(1-\lambda))^n$ et son inverse $q/(\lambda(1-\lambda))^m$, donc $pq = \lambda^N(1-\lambda)^N$ dans $k[\lambda]$. Par récurrence sur N, un diviseur d'un produit de premiers est associé à un sous-produit : $p = w\,\lambda^i(1-\lambda)^j$ avec $w \in k[\lambda]^* = k^*$ (k intègre), et $u = w\,\lambda^{i-n}(1-\lambda)^{j-n}$. Sur un corps, A est un localisé de l'anneau principal $k[\lambda]$, donc factoriel, et le groupe de Picard d'un anneau factoriel est nul. □

Vérifié tel quel (`dvd_pow_mul_pow`, `C_mul_pow_inj`, `unitOf_eq_one`, `exists_unitOf`, `toUnits_bijective`, `unitsEquiv`, `toUnits_incl`, `pic_O3_subsingleton`). Lean ne définit pas l'action de $\mathfrak{S}_3$ sur A par les substitutions anharmoniques et ne vérifie pas que `unitsEquiv` est équivariant ; l'action du modèle n'est comparée aux substitutions que point par point, par `ev_smul_lam` et `ev_smul_lam'`.

Ne sont pas démontrés ici : l'équivariance de l'identification des unités, $\mathrm{Pic}(U_{0,3}) = 0$ sur une base S générale (il l'est sur un corps, théorème 75.3) et la suite de Hochschild–Serre, qui identifient le groupe de Picard du champ quotient à ce H^1, et le choix de la page, qui prend pour générateur $\mathcal{O}(1)$ sur $\mathbf{P}(V_J)$ au lieu de la classe tangente. L'énoncé de la page reste donc ouvert sous sa forme géométrique :

Théorème (Grothendieck, pages 22, 24 et 29, Picard du champ $[U_{0,3}/\mathfrak{S}_3]$ ♦)**.** *Soit S régulier intègre avec $\mathrm{Pic}(S) = 0$. Le groupe de Picard du champ quotient $[(\mathbf{P}^1 - \{0,1,\infty\})_S/\mathfrak{S}_3]$, $\mathfrak{S}_3$ agissant par les substitutions anharmoniques, est $\mathbf{Z}/6$, engendré par $\mathcal{O}(1)$ sur $\mathbf{P}(V_J)$, en caractéristique générique $\neq 2$, et $\mathbf{Z}/3$ en caractéristique générique 2.*

◊ non vérifié en Lean

Le groupe $H^1(\mathfrak{S}_3, \mathcal{O}(U_{0,3})^*)$ est calculé au théorème 75.2 pour S le spectre d'un corps. Restent le passage de H^1 au groupe de Picard, la base S générale et l'identification du générateur à $\mathcal{O}(1)$. Mathlib n'a pas les champs quotients ni leur groupe de Picard.

Autres pistes de l'onglet Findings pour ce thème, dans des cotes qui n'ont pas de section ici :

— Cote 138 : critère pour qu'une partie A de la sphère définisse par image réciproque une nouvelle structure de carte : A connexe, et A contient au plus un des points 0, 1, ∞ ; telle qu'elle est lue, la seconde condition est contredite par l'exemple $A = [0,1]$, et la lecture de la page doit être vérifiée sur le fac-similé avant toute formalisation. Mathlib n'a pas les cartes sur les surfaces. On se reportera aux notes de Grothendieck (138, lot 7, p. 122). ♦

Théorème (Grothendieck, pages 122 à 124 et 127, opérations sur les cartes ♦)**.** *Une opération sur les cartes orientées donnée par une partie A de la sphère de référence, tirée en*

◊ non vérifié en Lean

arrière le long du revêtement $f : X \to S$ de chaque carte, est, sauf un cas exceptionnel, la composition avec un revêtement $\varphi : S \to S$ ramifié seulement au-dessus de 0, 1, ∞, avec $\varphi^{-1}\{0,1,\infty\} \supset \{0,1,\infty\}$ et une ramification 2 au-dessus de 1, de sorte que $A = \varphi^{-1}([0,1])$. La page demande ce qu'il advient dans le cas exceptionnel.

Une carte orientée est un revêtement fini de la sphère non ramifié hors de 0, 1, ∞, la carte étant l'image réciproque de $[0,1]$; c'est le dictionnaire des cartes et des revêtements de Jones et Singerman (1978) [77]. Par le théorème de Belyi (1979) [14], les courbes qui portent de tels revêtements sont exactement les courbes définies sur $\overline{\mathbf{Q}}$, et $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ opère sur les cartes par son action sur le groupe profini $\hat{F}_2$ de la section 61, qui se factorise par $\widehat{GT}$ (Drinfeld 1990 [44] ; Ihara 1991 [73]). L'opération de l'encadré est la composition avec un revêtement φ du même type, ramifié seulement au-dessus de 0, 1, ∞. Mathlib n'a pas les revêtements de Belyi de la sphère. On se reportera aux notes de Grothendieck (138, lot 7, p. 122).

Partie 28

Ordres et géométrie des formes

Les quatre sections de cette partie viennent d'un même texte, *Vers une géométrie des formes*, écrit du 5 juin au 15 juillet 1986 : neuf chapitres (cotes 156-1 à 156-9, 691 pages selon l'inventaire) qui cherchent à fonder la topologie sur des figures et leurs incidences plutôt que sur des points. Le texte n'a jamais été édité. Grothendieck comptait pourtant le publier : le 4 juillet 1986, il écrit à Tsuji que ce sera « le premier texte mathématique que je publierai, après mon départ de 1970 » [121]. Les sections suivantes démontrent des énoncés des chapitres I à IV ; les chapitres V à IX n'en ont pas.

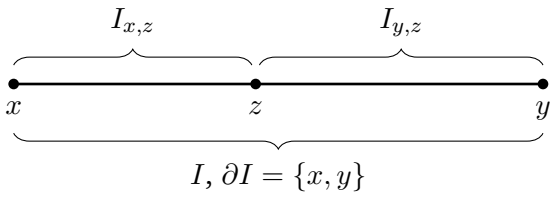
76 Cote 156-1 : le modèle-segment est un biordre [80]

La cote 156-1, *[Chapitre] I. Vers une géométrie des formes (topologiques) : notes manuscrites (05/06/1986)*, vingt-six pages datées du 5 au 7 juin 1986, propose une axiomatique combinatoire des formes de dimension 1. Elle se donne un ensemble $\mathcal{L}$ de *lieux*, un ensemble S de *segments*, et pour chaque segment I l'ensemble $\widetilde{I} \subset \mathcal{L}$ de ses lieux et la paire $\partial I \subset \widetilde{I}$ de ses extrémités. La troisième mouture, à partir de la page 5, pose les axiomes F1 à F5 (156-1, lot 1, p. 5, 156-1, lot 1, p. 7). La page 10 appelle *modèle-segment* un modèle où $\mathcal{L}$ est lui-même un segment, et la page 11 y définit, à partir d'une extrémité x_0, la relation $x \preccurlyeq y$ par $x \in [x_0, y]$, et affirme que c'est un ordre (156-1, lot 1, p. 11). On lit à la page 12 : « Cette relation d'ordre a un plus petit élément, x_0, et un plus grand élément, x_1. Elle permet de reconstituer la structure de modèle de 1-forme ». Les segments y sont les $[x, y]$, $x < y$, et l'ordre est « infiniment divisible » et « localement filtrante décroissante » ; la clause « filtrante croissante » est ajoutée entre les lignes et lue en partie. Une ligne qui porte plusieurs mots illisibles esquisse la réciproque (156-1, lot 1, p. 12). La page 13 conclut qu'« une structure de modèle de segment équivaut à une structure de *biordre* » (156-1, lot 1, p. 13). Aucune des deux directions n'est démontrée sur la page.

Conventions. On écrit les axiomes comme la lecture les énonce, en notant $I_{x,z}$ le sous-segment de I d'extrémités x, z donné par F1 : un segment J avec $\widetilde{J} \subset \widetilde{I}$ et $\partial J = \{x, z\}$. On pose $I^\circ = \widetilde{I} \setminus \partial I$, et un lieu est *régulier* s'il est intérieur à un segment.

- F1 Si $x \in \partial I$ et $z \in \widetilde{I} \setminus \{x\}$, il existe un unique $I_{x,z}$.
- F2 $I^\circ \neq \emptyset$; si $\partial I = \{x, y\}$ et $z \in I^\circ$, alors $\widetilde{I}_{x,z} \cap \widetilde{I}_{y,z} = \{z\}$, et tout segment J avec $\widetilde{J} \subset \widetilde{I}$ et $z \in \partial J$ vérifie $\widetilde{J} \subset \widetilde{I}_{x,z}$ ou $\widetilde{J} \subset \widetilde{I}_{y,z}$.
- F3 Si $x \in \partial I \cap \partial J$, il existe $u \in \widetilde{I} \setminus \{x\}$ et $v \in \widetilde{J} \setminus \{x\}$ avec $I_{x,u} = J_{x,v}$ ou $\widetilde{I}_{x,u} \cap \widetilde{J}_{x,v} = \{x\}$ (la forme de la marge).
- F′3 Si $x \in \partial I$ et $u, v \in I^\circ$, il existe $w \in I^\circ$ avec $\widetilde{I}_{x,w} \subset \widetilde{I}_{x,u} \cap \widetilde{I}_{x,v}$ (la reconstruction de la lecture, d'après la note du bas de la page 6).
- F4 Si z est régulier, $\widetilde{I'} \cap \widetilde{I''} = \{z\}$, $\partial I' = \{x, z\}$ et $\partial I'' = \{y, z\}$, il existe un unique I avec $\widetilde{I} \supset \widetilde{I'} \cup \widetilde{I''}$ et $\partial I = \{x, y\}$.
- F5 Un lieu régulier est d'ordre 2 : il existe deux segments issus de lui qui ne définissent pas la même branche, et tout segment issu de lui définit la même branche que l'un d'eux.

80. Preuve vérifiée : `lean/Grothendieck/Folder156_1.lean`.



F2 : pour z intérieur à I, les sous-segments $I_{x,z}$ et $I_{y,z}$ ne se rencontrent qu'en z. F4 est le sens inverse : deux segments qui ne se rencontrent qu'en un lieu régulier z se recollent en un unique segment d'extrémités x, y.

Dans un modèle-segment, $\mathcal{L} = \widetilde{I_0}$ avec $\partial I_0 = \{x_0, x_1\}$, on pose $a \leq b$ si $a = b$ ou s'il existe un segment J avec $\partial J = \{x_0, b\}$ et $a \in \widetilde{J}$; par l'unicité dans F1, un tel J est $I_{0\,x_0,b}$, et l'on note $[x_0, b] = \widetilde{J}$. Un ensemble ordonné est *localement filtrant décroissant* si $x < y_1$ et $x < y_2$ entraînent l'existence de y avec $x < y \leq y_1, y_2$, *localement filtrant croissant* dans l'énoncé dual.

Théorème 76.1 (Grothendieck, pages 10 à 13, *le modèle-segment est un biordre* ♦). *Soit un modèle satisfaisant F1, F2, F′3 et F4, dont l'ensemble des lieux est un segment I_0, $\partial I_0 = \{x_0, x_1\}$. La relation $\leq$ est un ordre sur $\mathcal{L}$, de plus petit élément x_0 et de plus grand élément x_1, distincts ; il est dense, localement filtrant décroissant et localement filtrant croissant ; les segments sont exactement les intervalles $[a, b] = \{z \mid a \leq z \leq b\}$, $a < b$, avec $\partial = \{a, b\}$, chacun porté par un seul segment. L'ordre défini à partir de x_1 est l'ordre opposé.*
Réciproquement, soit $\mathcal{L}$ un ensemble ordonné ayant un plus petit et un plus grand élément distincts, dense et localement filtrant dans les deux sens. Les intervalles $[a, b]$, $a < b$, avec $\partial[a, b] = \{a, b\}$, satisfont F1 à F5 et F′3, $\mathcal{L}$ est un segment, et l'ordre relu à partir du plus petit élément est l'ordre donné.

Démonstration du sens direct. Deux unicités. Un segment J avec $\partial J = \{x_0, b\}$ est unique : c'est F1 dans I_0, puisque $\widetilde{J} \subset \mathcal{L} = \widetilde{I_0}$. Pour la même raison, deux segments qui ont une extrémité dans $\{x_0, x_1\}$ et les mêmes extrémités sont égaux. Si $u, v \notin \{x_0, x_1\}$ et $\partial J = \partial K = \{u, v\}$, alors $u \in I_0^\circ$; F2 dans I_0 en u place $\widetilde{J}$, et de même $\widetilde{K}$, dans $[x_0, u]$ ou dans $\widetilde{I}_{0\,x_1,u}$. S'ils tombent dans des sous-segments différents, v est dans leur intersection, qui est $\{u\}$, ce qui est exclu ; s'ils tombent dans le même, F1 dans ce sous-segment, en son extrémité u, donne $J = K$. Ainsi *un segment est déterminé par ses extrémités* (le corollaire 3 a de la page 5).

C'est un ordre. Si $b \in [x_0, c]$, $b \neq x_0$, F1 dans le segment $[x_0, c]$ fournit un sous-segment d'extrémités x_0, b, qui est $[x_0, b]$; donc $[x_0, b] \subset [x_0, c]$, d'où la transitivité. Pour l'antisymétrie, soient $a \neq b$ avec $a \in [x_0, b]$ et $b \in [x_0, a]$; alors $a \neq x_0$ (aucun segment n'a $\{x_0\}$ pour bord), $[x_0, a] = [x_0, b]$ par ce qui précède, et a est intérieur à $[x_0, b]$. F2 dans $[x_0, b]$ en a dit que $[x_0, a]$ et le sous-segment d'extrémités b, a ne se rencontrent qu'en a ; or b est dans les deux. On a $x_0 \leq a$ puisque $x_0 \in [x_0, a]$, et $a \leq x_1$ puisque $[x_0, x_1] = \mathcal{L}$; $x_0 \neq x_1$ parce que ∂I_0 a deux éléments.

Recollement. Soient a un lieu régulier, $[x_0, a]$, et Q un segment d'extrémités a, z tel que $[x_0, a] \cap \widetilde{Q} = \{a\}$. F4 fournit un segment G d'extrémités x_0, z contenant $[x_0, a]$; donc $a \in [x_0, z]$, c'est-à-dire $a \leq z$.

Les extrémités d'un segment sont comparables. Soit $\partial J = \{u, v\}$. Si l'une est x_0 ou x_1, c'est clair. Sinon $u \in I_0^\circ$ et F2 place $\widetilde{J}$ dans $[x_0, u]$, d'où $v \leq u$, ou dans $P = \widetilde{I}_{0\,x_1,u}$. Dans le second cas, le sous-segment Q de P d'extrémités u, v ne rencontre $[x_0, u]$ qu'en u, puisque $[x_0, u] \cap P = \{u\}$, et le recollement donne $u \leq v$.

Un segment d'extrémités $a < b$ est l'intervalle $[a, b]$. Si $a = x_0$, c'est la définition. Sinon, soit K ce segment ; il est le sous-segment de $[x_0, b]$ d'extrémités b, a, par l'unicité. Le lieu a est intérieur à $[x_0, b]$, et régulier (il est intérieur à I_0, car $a \neq x_1$). F2 dans $[x_0, b]$ en a donne $[x_0, a] \cap \widetilde{K} = \{a\}$, et place tout sous-segment de $[x_0, b]$ issu de a dans $[x_0, a]$ ou dans $\widetilde{K}$. Si $z \in \widetilde{K}$, $z \neq a$, le sous-segment de K d'extrémités a, z ne rencontre $[x_0, a]$ qu'en a, et le recollement donne $a \leq z$; et $z \leq b$ puisque $\widetilde{K} \subset [x_0, b]$. Inversement, soit $a < z < b$; alors $[x_0, z] \subset [x_0, b]$ contient a, et le sous-segment de $[x_0, z]$ d'extrémités z, a est un sous-segment de $[x_0, b]$ issu de a. S'il était dans $[x_0, a]$, on aurait $z \leq a$, donc $z = a$; il est donc dans $\widetilde{K}$, et $z \in \widetilde{K}$. Un tel segment existe toujours : F1 dans $[x_0, b]$ en b fournit le sous-segment d'extrémités b, a. Avec l'unicité, chaque intervalle $[a, b]$, $a < b$, est porté par un seul segment, et tout segment est un tel intervalle.

Densité, filtrations. Si $a < b$, F2 donne un lieu intérieur au segment $[a, b]$, strictement entre a et b. Si $a < y_1$ et $a < y_2$, et si aucun des deux n'est x_1 (sinon l'autre convient), y_1 et y_2 sont intérieurs au segment $[a, x_1]$; F′3 en son extrémité a fournit w intérieur avec $[a, w] \subset [a, y_1] \cap [a, y_2]$, donc $a < w \leq y_1, y_2$. Dualement, F′3 appliqué au segment $[x_0, a]$ en son extrémité a donne la filtration croissante.

Biordre. Pour l'ordre défini à partir de x_1, $a \leq_1 b$ signifie $a = b$, ou a dans le segment d'extrémités x_1, b, qui est l'intervalle $[b, x_1]$ de l'ordre défini à partir de x_0 : c'est $b \leq a$. □

Démonstration de la réciproque. Un segment est un couple $a < b$, de lieux $[a, b]$ et de bord $\{a, b\}$; il est déterminé par son bord, la condition $a < b$ fixant l'ordre de la paire. F1 : le sous-segment de $[a, b]$ issu de a d'autre extrémité z est $[a, z]$, celui issu de b est $[z, b]$. F2 : $]a, b[$ est non vide par densité ; si $a < z < b$, $[a, z] \cap [z, b] = \{z\}$, et un intervalle contenu dans $[a, b]$ qui a z pour extrémité est $[z, c] \subset [z, b]$ ou $[c, z] \subset [a, z]$. F3 : si deux segments partent de x vers le haut, $[x, b]$ et $[x, d]$, la filtration décroissante donne y avec $x < y \leq b, d$, et $[x, y]$ est un début commun ; vers le bas, de même par la filtration croissante ; si l'un monte et l'autre descend, $[x, b] \cap [c, x] = \{x\}$. F′3 : si x est l'extrémité inférieure de $[x, b]$ et $u, v \in]x, b[$, la filtration décroissante donne w avec $x < w \leq u, v$, d'où $[x, w] \subset [x, u] \cap [x, v]$; dualement en l'extrémité supérieure. F4 : si $[x, z]$ et $[y, z]$ sont tous deux sous z, la filtration croissante donne w avec $x, y \leq w < z$, qui est dans l'intersection, exclu ; de même s'ils sont tous deux au-dessus ; sinon $x < z < y$ (ou l'inverse) et $[x, y]$ est l'unique segment d'extrémités x, y, qui contient $[x, z] \cup [z, y]$. F5 : si $a < x < b$, les segments $[a, x]$ et $[x, b]$ n'ont aucun point intérieur commun, donc ne définissent pas la même branche ; un segment $[x, d]$ définit la même branche que $[x, b]$: la filtration donne y avec $x < y \leq d, b$, la densité z avec $x < z < y$, et $[x, z]$ est le sous-segment commun ; dualement pour $[c, x]$ et $[a, x]$. Enfin $[\bot, \top] = \mathcal{L}$, et $a \in [\bot, b]$ équivaut à $a \leq b$. □

Remarque. Le sens direct n'utilise ni F3 ni F5 : il suffit de F1, F2, F′3 et F4. F′3 donne les deux filtrations b) et b′), comme le dit l'esquisse de la lecture. F4, en un lieu régulier, fait de chaque intervalle un segment ; il intervient dès la comparabilité des extrémités d'un segment. Dans la réciproque, F4 vaut sans son hypothèse de régularité, et la densité et les deux filtrations suffisent à F1–F5 et F′3. Les bornes servent seulement à faire de $\mathcal{L}$ lui-même un segment.

Remarque. L'ordre n'est pas total en général, comme la lecture le signale. Soit, sur $\mathbb{Q}^2$, l'ordre du cône ouvert, $p \prec q$ si $|q_2 - p_2| < q_1 - p_1$, et soit T l'ensemble des points compris, pour cet ordre, entre $(0, 0)$ et $(2, 0)$. C'est un ensemble ordonné borné et dense (le milieu de $p \prec q$ est strictement entre eux). Il est localement filtrant dans les deux sens : si $x \prec y_1, y_2$, le point $x + (\varepsilon, 0)$ convient pour $\varepsilon > 0$ assez petit, et dualement $x - (\varepsilon, 0)$. Les points $(1, \frac{1}{2})$ et $(1, -\frac{1}{2})$

y sont incomparables. Ses intervalles forment donc un modèle-segment dont l'ordre n'est pas total.

Ne sont pas démontrés ici : les corollaires de F1 et F2 hors du modèle-segment et la transitivité de « même branche » ; les corollaires 1 et 2 de F4 et l'équivalence F5 $\Leftrightarrow$ F′5 ; la restriction (pages 8 et 9) ; l'orientation (pages 14 à 17) ; le contre-exemple de la page 21 et F6 ; les réseaux (pages 23 et 24) ; les pages 24 à 26.

77 Cote 156-2 : les rives d'une partie fermée [81]

La cote 156-2, chapitre II de *Vers une géométrie des formes*, dix-huit pages des 6 et 7 juin 1986 intitulées « Réalisations topologiques des réseaux », cherche à couper un espace quelconque le long d'une partie fermée sans le supposer variété ni triangulé. Pour A fermé dans X, $j : X \smallsetminus A \hookrightarrow X$, et $\mathrm{Comp}(Z)$ l'anneau booléen des parties ouvertes et fermées de Z, la page 14 pose $\mathrm{Riv}(A,X) = \varinjlim_{V \supset A} \mathrm{Comp}(V \smallsetminus A)$, limite sur les voisinages de A, et $\widetilde{A} = \mathrm{Spec}(j_*\mathbf{F}_2)$; la page 15 en tire une application canonique $(*)\ \mathrm{Riv}(A,X) \to \mathrm{Comp}(\widetilde{A})$, « injective, et » ajouté au-dessus de « bijective si X paracompact » (156-2, lot 1, p. 14, 156-2, lot 1, p. 15). La lecture prend $\widetilde{A} \to A$ pour le spectre de Stone relatif de $(j_*\mathbf{F}_2)|_A$ et note que l'injectivité « n'utilise rien ».

On code une partie ouverte et fermée de $V \smallsetminus A$ par son indicatrice, fonction $X \to \mathbf{F}_2$ localement constante sur $V \smallsetminus A$; $\mathrm{Riv}(A,X)$ est l'anneau de leurs germes le long de A, la fibre B_x de $j_*\mathbf{F}_2$ en x celui de leurs germes en x dans $X \smallsetminus A$. On prend pour $\widetilde{A}$ l'ensemble des couples (x,χ), $x \in A$, $\chi : B_x \to \mathbf{F}_2$ un morphisme d'anneaux (un point du spectre de B_x), muni de la topologie engendrée par les parties $\{(y,\chi) : y \in W,\ \chi(f_y) = 1\}$, W ouvert et f localement constante sur $W \smallsetminus A$; $(*)$ envoie ρ sur $\{(x,\chi) : \chi(\rho_x) = 1\}$.

Théorème 77.1 (D'après les pages 14 et 15, injectivité ♦). *Pour toute partie A de tout espace X, l'image de chaque rive par $(*)$ est ouverte et fermée dans $\widetilde{A}$, $(*)$ est un morphisme d'algèbres de Boole, et $(*)$ est injective. L'anneau $\mathrm{Riv}(A,X)$ est nul si et seulement si A est ouvert.*

L'énoncé tient, sans hypothèse : voir les théorèmes `toComp_injective`, `toComp_mul`, `toComp_one`, `toSpecSet_compl` et `riv_one_eq_zero_iff` dans `Folder156_2.lean`. La fermeture de A ne sert pas. Deux germes distincts en x sont séparés par un point du spectre de B_x, obtenu ici comme évaluation le long d'un ultrafiltre plus fin que le filtre des voisinages de x dans $X \smallsetminus A$. La dernière assertion est la correction « A non ouvert » que la lecture apporte au « $A \neq \emptyset$ » de la remarque sur les bi-rives. Ne sont pas démontrés : la bijectivité pour X paracompact, l'identification $\mathrm{Comp}(\widetilde{A}) \simeq \Gamma(A, (j_*\mathbf{F}_2)|_A)$, le cas régulièrement immergé et l'espace découpé $\overline{X}$ des pages 16 et 17.

78 Cote 156-3 : l'intermédiarité se lit sur les découpages [82]

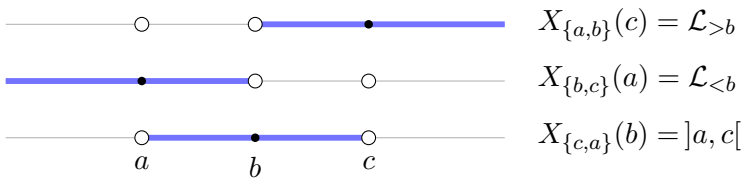
La cote 156-3, chapitre III de *Vers une géométrie des formes*, quarante pages datées des 8 et 9 juin 1986, intitulée de sa main « Réseaux via découpages », propose une troisième axiomatique des réseaux. Elle se donne des lieux, les paires de lieux en position relative modérée, et pour chaque partie finie modérée T le découpage de son complémentaire modéré $C(T)$ en

81. Preuve vérifiée : `lean/Grothendieck/Folder156_2.lean`.
82. Preuve vérifiée : `lean/Grothendieck/Folder156_3.lean`.

composantes. La page 8 définit le *tronçon ordonné* : un ensemble ordonné où, pour tout a, $\mathcal{L}_{>a}$ est filtrant décroissant et $\mathcal{L}_{<a}$ filtrant croissant (a, a′), qui est filtrant croissant et décroissant (b), divisible (c) et de cardinal > 1 (d). Les 0-sphères y sont les paires comparables $\varepsilon = \{a, b\}$, $a < b$, et les composantes de $C(\varepsilon)$ sont $\mathcal{L}_{<a}$, $]a, b[$ et $\mathcal{L}_{>b}$ (156-3, lot 1, p. 8). Les pages 11 à 13 montrent que l'intermédiarité stricte $\mathcal{R}$ et la comparabilité déterminent l'ordre à l'opposé près (156-3, lot 1, p. 11, 156-3, lot 1, p. 13). Le problème est posé page 14 : « la connaissance de $\mathrm{Drap}_2(\mathcal{L})$, et [...] de la décomp. de $C(\varepsilon)$ [...] en composantes connexes, implique la connaissance de la relation $\mathcal{R}(a, b, c)$ » (156-3, lot 1, p. 14). La page 15 calcule les trois composantes attachées à $a < b < c$, $X_{\{a,b\}} = \mathcal{L}_{>b}$, $X_{\{b,c\}} = \mathcal{L}_{<b}$, $X_{\{c,a\}} =]a, c[$. Elle trouve la première intersection vide et les deux autres non vides, « divisibilité ! », et conclut « On gagne ! » (156-3, lot 1, p. 15).
Conventions. Pour a, b, c on note $\mathcal{R}(a, b, c)$ si $a < b < c$ ou $c < b < a$, et $\overline{\mathcal{R}}(a, b, c)$ si $a \leq b \leq c$ ou $c \leq b \leq a$. Pour $a \neq b$ comparables, $C(\{a, b\})$ est l'ensemble des éléments distincts de a et b et comparables aux deux ; deux de ses éléments sont dans le même *morceau* s'ils sont tous deux au-dessous de a et b, tous deux strictement entre eux, ou tous deux au-dessus : la relation ne dépend que de la paire. On note $X_{\{a,b\}}(t)$ le morceau de $C(\{a, b\})$ qui contient t. La donnée de la page 14 est celle de la comparabilité et, pour chaque paire comparable, de la partition de $C(\varepsilon)$ en morceaux, sans étiquette ; une bijection e entre deux ensembles ordonnés *respecte les découpages* si elle respecte la comparabilité et si, pour toute paire comparable $\{a, b\}$ et tous $s, t \in C(\{a, b\})$, s et t sont dans le même morceau de $C(\{a, b\})$ si et seulement si $e(s)$ et $e(t)$ sont dans le même morceau de $C(\{e(a), e(b)\})$.

Énoncé (Page 15). *Soient $a < b < c$ dans un ensemble ordonné. Alors $X_{\{a,b\}}(c) = \mathcal{L}_{>b}$, $X_{\{b,c\}}(a) = \mathcal{L}_{<b}$ et $X_{\{c,a\}}(b) =]a, c[$. Si l'ordre est dense et si p, q, r sont deux à deux distincts et comparables, $\mathcal{R}(p, q, r)$ a lieu si et seulement si $X_{\{p,q\}}(r) \cap X_{\{q,r\}}(p) = \emptyset$.*

Sur une chaîne $a < b < c$, chaque paire découpe le reste de la chaîne en trois morceaux : au-dessous, entre, au-dessus. Le trait épais est le morceau qui contient le troisième point.



Les cercles blancs sont les deux points de la paire, exclus de $C(\varepsilon)$.

Démonstration. Si $b < t$ et $a < b$, un élément s est dans le même morceau que t exactement quand il est au-dessus de a et de b : t n'est ni sous a ni strictement entre a et b. Un tel s est dans $C(\{a, b\})$, d'où $X_{\{a,b\}}(c) = \mathcal{L}_{>b}$; de même $X_{\{b,c\}}(a) = \mathcal{L}_{<b}$, et, la relation étant symétrique en la paire, $X_{\{c,a\}}(b) =]a, c[$. Trois éléments deux à deux distincts et comparables forment une chaîne, et l'un des six ordres possibles a lieu. Si q est au milieu, les deux morceaux sont $\mathcal{L}_{>q}$ et $\mathcal{L}_{<q}$, disjoints. Si le milieu est p, disons $q < p < r$, les morceaux sont $\mathcal{L}_{>p}$ et $]q, r[$, qui contiennent tous deux un point de $]p, r[$, non vide par densité ; les quatre autres cas sont semblables. □

Énoncé (Pages 11 à 13). *Soient deux ensembles ordonnés filtrants croissants et décroissants, et e une bijection de l'un sur l'autre qui respecte la comparabilité et l'intermédiarité stricte. Alors e est un isomorphisme d'ordres ou un anti-isomorphisme. Plus précisément, si $a < b$, on a $u \leq v$ si et seulement s'il existe x et y, avec $x = a$ ou $\mathcal{R}(b, a, x)$, $y = b$ ou $\mathcal{R}(a, b, y)$, tels que $\overline{\mathcal{R}}(x, u, y)$, $\overline{\mathcal{R}}(x, v, y)$ et $\overline{\mathcal{R}}(x, u, v)$. Enfin, $\overline{\mathcal{R}}(a, b, c)$ équivaut à : $\mathcal{R}(a, b, c)$, ou $b \in \{a, c\}$ avec a et c comparables.*

Démonstration. La condition sur x dit $x \leq a$, celle sur y dit $y \geq b$. Si $u \leq v$, la filtration b) donne $x \leq u, a$ et $y \geq v, b$, et $x \leq u \leq v \leq y$ donne les trois conditions. Inversement, $x \leq a < b \leq y$ donne $x < y$; $\overline{\mathcal{R}}(x,u,y)$ ne peut alors avoir lieu que sous la forme $x \leq u \leq y$, et de même pour v ; si $\overline{\mathcal{R}}(x,u,v)$ a lieu sous la forme $v \leq u \leq x$, alors $u = x$ et $v \leq x \leq v$, donc $u = v$; dans tous les cas $u \leq v$. La forme exacte de $\overline{\mathcal{R}}$ se vérifie cas par cas. Ainsi $\leq$ s'écrit à partir de a, b, de $\mathcal{R}$ et de la comparabilité seuls. Si l'ordre de départ n'a aucun couple $a < b$, c'est l'égalité, et la comparabilité respectée force l'égalité à l'arrivée. Sinon, soit $a < b$; $e(a)$ et $e(b)$ sont comparables et distincts. Si $e(a) < e(b)$, la description précédente, transportée par e, donne $u \leq v \Leftrightarrow e(u) \leq e(v)$. Si $e(b) < e(a)$, on remplace l'ordre d'arrivée par l'ordre opposé, qui a la même intermédiarité, la même comparabilité, et reste filtrant dans les deux sens. □

Théorème 78.1 (D'après les pages 11 à 15, *l'ordre se lit sur les découpages*, forme complétée par l'édition ♦)**.** *Une bijection entre deux tronçons ordonnés qui respecte la comparabilité et, pour chaque paire comparable ε, la partition de $C(\varepsilon)$ en morceaux, est un isomorphisme d'ordres ou un anti-isomorphisme. La comparabilité seule n'y suffit pas : sur le tronçon $\mathbb{Q}$, la transposition de 0 et 1 respecte la comparabilité sans être ni croissante ni décroissante.*

Démonstration. D'après l'énoncé de la page 15, appliqué dans les deux tronçons, et parce que e envoie le morceau $X_{\{p,q\}}(r)$ sur le morceau $X_{\{e(p),e(q)\}}(e(r))$, la bijection e respecte l'intermédiarité stricte ; on conclut par l'énoncé des pages 11 à 13. Pour $\mathbb{Q}$, les conditions a) à d) sont immédiates (minimum, maximum, milieu) ; tout couple y est comparable, et la transposition σ de 0 et 1 vérifie $\sigma(1) = 0 < 1 = \sigma(0)$, alors que $\sigma(1) = 0 < 2 = \sigma(2)$. □

Remarque. La seconde phrase de l'énoncé, sur la comparabilité seule, est de l'édition. Des conditions de la page 8, seules la divisibilité c) et la filtration b) servent ; a), a′) et d) n'interviennent pas. La divisibilité rend non vides les deux autres intersections de la page 15. La filtration b) sert seulement dans le lemme des pages 11 à 13. Il n'est pas nécessaire de déduire Drap_2 de $\mathcal{R}$, puisque la comparabilité fait partie des données de la page 14. L'énoncé vaut donc pour tout ensemble ordonné dense et filtrant dans les deux sens.

Remarque. La version large de l'intermédiarité est $\mathcal{R}(a,b,c)$, ou $b \in \{a,c\}$ *avec a et c comparables*. La forme « $\mathcal{R}(a,b,c)$ ou $b \in \{a,c\}$ » que la lecture substitue à la marge de la page 11 est fausse pour a et c incomparables. Dans $\mathbb{N}^2$ ordonné produit, $\overline{\mathcal{R}}((0,1),(0,1),(1,0))$ n'a pas lieu. Le lemme de la page 13 ne rencontre pas ce cas, puisqu'il est appliqué avec $x < y$.

Remarque. La reconstruction d'un ordre partiel, à l'opposé près, à partir de son intermédiarité stricte, objet des pages 11 à 13, est étudiée par Courcelle (2020, § 1 et théorème 7) [37], qui cite pour l'axiomatisation J. Lihová (2000).

Ne sont pas démontrés ici : les axiomes des réseaux par découpages (pages 1 à 5) ; les remarques de la page 16 ; les parties modérées fermées (pages 17 à 21) ; la topologie (pages 21 à 24) ; le bord et les pseudo-tronçons (pages 24 à 28) ; l'algèbre des parties modérées (pages 29 à 39).

79 Cote 156-4 : les parties saturées ne forment pas une algèbre de Boole[83]

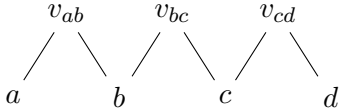
La cote 156-4, chapitre IV de *Vers une géométrie des formes*, « Analysis situs (première mouture) », est datée de sa main du 10 au 12 juin 1986. Elle part d'un espace stratifié et en dégage peu à peu une structure abstraite : un ensemble ordonné $(\mathcal{M}, \leq)$ de *multistrates* et une relation symétrique R, la *compatibilité*, réflexive et héritée vers le bas. Aux pages 65 à 68, deux multistrates sont *disjointes* si elles sont compatibles et n'ont aucun minorant commun ; le *cosupport* d'une partie $\Phi \subset \mathcal{M}$ est l'ensemble des multistrates disjointes de tous les éléments de Φ, le *support* est le cosupport du cosupport, et une partie est *saturée* si elle est égale à son support (156-4, lot 4, p. 65). La page 68 conclut : « Je présume qu'on a en fait une algèbre de Boole (*ultra-stonienne*, à cause des Sup quelc.) » (156-4, lot 4, p. 68).

Une relation symétrique $\perp$ sur un ensemble définit une *polarité*, notion classique : à une partie Φ on associe $\Phi^{\perp}$, les éléments orthogonaux à tous ceux de Φ, et les parties fermées sont celles qui vérifient $\Phi^{\perp\perp} = \Phi$. Pour l'orthogonalité dans un espace euclidien, les fermés sont les sous-espaces, et ils ne forment pas une algèbre de Boole. Les axiomes du dossier n'excluent pas ce phénomène.

Énoncé (Lecture, pages 66 et 67, forme générale)**.** *Soient $(\mathcal{M}, \leq)$ un ensemble ordonné et R une relation symétrique sur $\mathcal{M}$. Toute intersection de parties saturées est saturée, le cosupport d'une partie quelconque est saturé, et sur les parties saturées le cosupport est une involution qui renverse l'inclusion, avec $S \cap \operatorname{cosupp}(S) = \emptyset$ et $\operatorname{supp}(S \cup \operatorname{cosupp}(S)) = \mathcal{M}$. Les parties saturées forment donc un treillis complet orthocomplémenté, de borne inférieure l'intersection et de borne supérieure le support de la réunion.*

Démonstration. Écrivons Φ' pour le cosupport. La disjonction est symétrique, puisque R l'est et que la condition sur les minorants l'est aussi. Si $\Phi \subset \Psi$, alors $\Psi' \subset \Phi'$, et tout élément de Φ est disjoint de tout élément de Φ', d'où $\Phi \subset \Phi''$. En appliquant cette inclusion à Φ', puis la décroissance à $\Phi \subset \Phi''$, on obtient $\Phi''' = \Phi'$: un cosupport est saturé. Si les S_i sont saturées et $S = \bigcap S_i$, alors $S \subset S_i$ donne $S'' \subset S_i'' = S_i$ pour tout i, donc $S'' \subset S$, et l'inclusion inverse est toujours vraie. Aucune multistrate n'est disjointe d'elle-même, puisqu'elle est son propre minorant : $S \cap S' = \emptyset$. Enfin, pour S saturée, un élément disjoint de tout $S \cup S'$ serait dans S' et dans $S'' = S$, ce qui est exclu ; le cosupport de $S \cup S'$ est vide, et le cosupport du vide est $\mathcal{M}$. □

Le contre-exemple est un modèle à sept éléments : quatre multistrates minimales a, b, c, d et trois multistrates v_{ab}, v_{bc}, v_{cd}, chacune au-dessus de la paire qu'elle indexe. La compatibilité est la relation engendrée par les paires d'éléments d'un même $\mathcal{M}_{\leq v}$.



Contre-exemple 79.1 (Énoncé de l'édition, page 68)**.** *Dans ce modèle, $\leq$ est un ordre, R est réflexive, symétrique et héritée vers le bas, chaque $\mathcal{M}_{\leq v}$ est formé d'éléments deux à deux compatibles et $\mathcal{M}$ est connexe, de sorte que la condition C 4 est vide. Les parties saturées sont*

83. Preuve vérifiée : `lean/Grothendieck/Folder156_4.lean`.

exactement

$$\emptyset, \quad \{b\}, \quad \{c\}, \quad \{a,c\}, \quad \{b,d\}, \quad \mathcal{M},$$

et le treillis qu'elles forment n'est pas distributif : $\{b,d\} \wedge (\{b\} \vee \{c\}) = \{b,d\}$*, tandis que* $(\{b,d\} \wedge \{b\}) \vee (\{b,d\} \wedge \{c\}) = \{b\}$.

Démonstration. Deux éléments sont compatibles quand un même $\mathcal{M}_{\leq v}$ les contient ; ils sont disjoints quand de plus aucun élément n'est sous les deux. Les paires disjointes sont donc $\{a,b\}$, $\{b,c\}$ et $\{c,d\}$: les trois v ont un minorant commun avec chacun de leurs voisins, et a, c par exemple ne sont pas compatibles. Le cosupport d'une partie est alors l'ensemble des voisins communs à tous ses éléments dans le chemin $a - b - c - d$, et le calcul des cent vingt-huit parties donne la liste annoncée : par exemple $\{b\}' = \{a,c\}$ et $\{a,c\}' = \{b\}$, $\{c\}' = \{b,d\}$ et $\{b,d\}' = \{c\}$, tandis que $\{b,c\}' = \emptyset$. Le support de $\{b\} \cup \{c\}$ est donc $\mathcal{M}$, et $\{b,d\} \cap \mathcal{M} = \{b,d\}$. De l'autre côté, $\{b,d\} \cap \{b\} = \{b\}$ et $\{b,d\} \cap \{c\} = \emptyset$, et le support de $\{b\}$ est $\{b\}$. En Lean, la liste des parties saturées et les deux calculs sont vérifiés par énumération exhaustive dans le noyau. □

Remarque. Le treillis obtenu est un hexagone : deux chaînes $\emptyset \subset \{b\} \subset \{b,d\} \subset \mathcal{M}$ et $\emptyset \subset \{c\} \subset \{a,c\} \subset \mathcal{M}$. La lecture notait que la distributivité tombe en général pour une relation symétrique quelconque ; le modèle montre qu'elle tombe déjà sous les hypothèses que le dossier pose sur $(\mathcal{M}, \leq, R)$ jusqu'à la page 64. Le modèle ne code que cette structure ; les figures et les axiomes C 1 à C 3, qui portent sur elles, ne sont pas représentés.

Ne sont pas démontrés ici : que les axiomes de disjonction ultérieurs (C 5 de la page 69, le « paquet d'axiomes de disjonction » de la page 85) rétablissent la distributivité ; le cas d'une relation R toujours vraie, où les parties saturées sont les ouverts réguliers de $(\mathcal{M}, \leq)$ et forment une algèbre de Boole complète.

Bilan

80 Erreurs, pistes et énoncés restants

Les énoncés de chaque cote qui ne sont pas démontrés ici sont donnés à la fin de sa section. Les quatre parties sans énoncé vérifié donnent la liste des pistes de leurs cotes, huit en tout. Sept sont ouvertes et portent le losange rouge ♦ ; la huitième, la majoration de la dimension cohomologique de la cote 31, est publiée par M. Artin (SGA 4, exposé X, théorème 4.1) et porte le losange gris. Seize autres parties finissent par quatre-vingt-douze pistes que leurs sections ne traitent pas, toutes de cotes sans section ici sauf deux de la cote 10, une de la cote 37, une de la cote 77, une de la cote 118 et deux de la cote 136. Trois de ces pistes sont démontrées : le cube des générisations de la cote 154 entièrement, sous la forme précisée par l'édition, et celles des cotes 137 et 148 en partie.

Les erreurs trouvées portent surtout sur les gloses modernes des lectures. La glose de la proposition 1 de la cote 158 était fausse, et la lecture de la cote 114 omettait une hypothèse de la page. Dans la cote 156-3, une note de la lecture sur la page 11 identifie l'intermédiarité large à la stricte augmentée des extrémités ; cela ne vaut que pour des extrémités comparables, et l'ordre produit sur $\mathbb{N}^2$ le dément. L'anneau universel $\Phi_0 = \mathbb{Z}[L_0, \Lambda_0]$ de la lecture de la cote 16 n'existe pas sur $\mathbb{Z}$ pour $n \geqslant 2$, car ξ_0^n est divisible par $n!$; l'obstruction disparaît sur $\mathbb{Q}$. Pour la cote 63, la lecture conclut que les quatre composantes du lieu $j = 0$ ont la même tangente en $p = 2$; elles en ont quatre, deux à deux distinctes. Dans la cote 50, la formule des traces demande une forme d'intersection symétrique, que l'axiome (e) ne pose pas, et la positivité de Rosati que la lecture tire du corollaire de la page 6 ne suit pas des axiomes. La lecture de la cote 44 tient l'intégralité des nombres de Cartan pour une conséquence des trois axiomes de la page 4. Un contre-exemple dans $\mathbb{Z}^2$, de groupe de Weyl B_2, le dément, alors que l'indivisibilité des racines la donne ; le système simple que la fiche invoquait ne l'est qu'à coefficients rationnels.

Sur la page elle-même, un contre-exemple réfute une affirmation dans dix cotes, et une présomption dans une onzième cote. Dans la cote 16, la réciproque (3) $\Rightarrow$ (1) que la page 9 annonce ne vaut que pour les projecteurs de la graduation : dans $M_2(R)$, le sous-anneau des matrices triangulaires inférieures contient tous les projecteurs et aucun inverse de L. Dans la cote 19, ce sont la nécessité dans le théorème 1.12 b) et la réserve « ou I fini » de la page 7 (un adjoint à gauche ne commute pas en général aux produits finis). Dans la cote 63, le scindage de l'espace tangent qu'affirme la page 99, sur lequel repose l'argument, n'est pas stable sous l'involution de Hesse. Dans la cote 72, l'irréductibilité sur l'hyperplan C, que le c) de la page 82 tire de la seule condition $\beta_i \neq 0$, demande aussi $\rho \neq 0$, comme le disait le d) barré de la page 80 : pour $\rho = 0$, la droite de $\tilde{c}$ est invariante. Le théorème des arrangements cruciaux de la page 24 de la cote 80 est faux déjà pour six droites : les côtés d'un triangle et une droite par chaque sommet. La parenthèse de la page 9 de la cote 90, qui lie les conditions du lemme 1 aux fibres des composantes, est fausse sans l'hypothèse de type fini : l'algèbre des polynômes de $K[T]$ à terme constant entier la met en défaut. Dans la cote 118, la stabilité par sommes que la page 35 dit « visible » est fausse : la somme de deux points la met en défaut. Un exemple sur $[0, 1]$ confirme la correction que la lecture apporte à la proposition de la page 19 de la

cote 150 : sans la condition $X_i \cap Y = f(\dot{X}_i)$, deux systèmes non isomorphes ont les mêmes données coupées. Dans la cote 158, le corollaire de la page 52 est faux pour une catégorie non connexe, et le paragraphe barré de la page 44, qui affirmait l'unicité de l'élément p de la proposition 1, l'est aussi. Le corollaire de la page 13 de la cote 160 demande les racines $(p-1)$-ièmes de $(-1)^n a_0$, et non de a_0. La présomption de la page 68 de la cote 156-4, que les parties saturées forment une algèbre de Boole, est démentie par un modèle à sept multistrates dont les parties saturées forment un hexagone. D'autres erreurs de la page sont de moindre portée. Dans la cote 16, le calcul confirme une erreur de la page 13 que la lecture relevait déjà, et dans la cote 78 les deux corrections que la lecture apporte au critère de fermeture : la conclusion $F_n(\alpha) = 0$ là où la page 112 écrit $= 1$, et le coefficient de Bézout de la page 113, faux pour $n = 4$. La page 3 de la cote 161-1 répète mot pour mot une de ses conditions. Dans la cote 104, la bonne fondation est une hypothèse supplémentaire, et $\mathbb{Z}$ vu comme catégorie montre qu'elle est nécessaire. Deux affirmations encore, dans les cotes 94 et 151, sont fausses sous une lecture et peut-être vraies sous une autre : la réciproque de la remarque 5 bis de la cote 94 tombe sous la seule finitude locale et tient sous la finitude globale, et le recollement en profondeur deux de la cote 151 échoue dans les espaces topologiques comme en homotopie, la lecture en termes de topos restant ouverte. Le fac-similé doit trancher.

Les quarante pistes entièrement démontrées tiennent telles qu'elles sont écrites, souvent sous des hypothèses plus faibles, et les démonstrations partielles apportent aussi des précisions. La cote 67 vaut pour un anneau non commutatif, et la cote 133 n'utilise pour la page 46 que $N' \subset \mathrm{Cent}(G)$. Dans la cote 106, quand tout objet est cofibrant, le foncteur q' est un isomorphisme sans condition ; le critère $(\star\star)$ est alors toujours vérifié, et les deux membres de l'équivalence sont vrais. Dans la cote 84, la réciproque du corollaire de la page 86 demande le changement de base que la page écrit : sur $\mathbb{Z}[X]$, avec $b_1 = X$ et $b_2 = 0$, l'application est un isomorphisme alors que l'idéal $(2, X)$ est propre. L'hypothèse « 2 régulier » de la page 48 est nécessaire : sur $\mathbf{F}_2$, $\mathbf{F}_2 \times \mathbf{F}_2$ et $\mathbf{F}_4$ ont le même discriminant et le même T_0. L'unicité de la symétrie canonique de la cote 77 (p. 123) demande une base connexe : sur un produit $R_1 \times R_2$, une isométrie peut être σ sur un facteur et l'identité sur l'autre. La phrase de la page 97 de la cote 74 est fausse sans la condition marginale (Ka) : un carré latin d'ordre 2 à revêtements triviaux satisfait les autres conditions et viole l'axiome 1. Dans la cote 79, l'énoncé sur l'étoile d'un sommet vaut sur tout anneau commutatif, sans l'hypothèse semi-locale, et la commutativité du groupe d'homothéties découle des autres conditions. Dans la cote 93, la translation par t^2 en caractéristique 2, par t^3 en caractéristique 3, change G_0 : le niveau p^2 est nécessaire, et la valeur test de la page 72 est $1/(4t^2)$, non $1/(2t)$. Sa rigidité, pour $\alpha = 0$, ne demande ni $\mathrm{Pic}(A) = 0$ ni A local, et l'homographie a pour déterminant une unité : la normalisation $ad - bc = 1$ ajoutée à la page 121 est fausse ($s = 2t$ sur $\mathbf{F}_5$). La bijectivité des applications de Stokes de la cote 68 doit être posée en axiome, et l'axiome du demi-espace opposé ne sert qu'à l'existence. Dans la cote 70, les incidences de l'icosaèdre valent aussi en caractéristiques 2 et 5, et la translation de la page 91 en caractéristique 2 est $(\alpha', \alpha, \alpha)$, non $(\alpha', 1, 1)$. La page 23 de la cote 86 écrit $\{u, v\}$ là où le trièdre demande $\{u, v_1\}$, et l'étiquette « $\sigma_0\sigma_1$ » de la page 32 porte la valeur de $\sigma_0\sigma_2$. Dans la cote 78, le critère $u_\alpha^n = 1 \iff F_n(\alpha) = 0$ vaut sur tout anneau commutatif et pour tout $n \in \mathbb{Z}$, et l'existence des deux $2p$-gones en bande, seule démontrée de la seconde piste, vaut en toute caractéristique, $p = 2$ et $p = 0$ compris. Les deux torseurs réguliers de la cote 40 sont des anneaux de valuation discrète sur tout anneau de valuation discrète, sans complétude ni caractéristique, et l'anneau $A[T]/(T^n - X^2)$ n'en est un pour aucun $n \geq 2$. Dans la cote 46, l'injectivité de la forme de Sylow vaut pour une algèbre non commutative quand

l'hypothèse de relèvement de la marge vaut pour l'action tordue par le second cocycle ; la page, qui ramène l'injectivité au noyau par torsion, ne le vérifie pas, et l'hypothèse non tordue suffit quand l'algèbre est commutative. La forme en degré i du lemme binomial de la cote 136 vaut sans l'hypothèse $i \leq N$, et sa démonstration se passe de localisation. La Proposition de la page 80 de la cote 19 se prolonge en une chaîne d'adjoints infinie dans les deux sens entre topos de préfaisceaux, dont aucun n'est fidèle : c'est la réponse à la Question de la page, contre une note de la lecture. Dans la cote 73, la dichotomie de la page 28 ne demande qu'un corps de plus de n éléments, non un corps infini, et le cas hyperspécial demande l'hypothèse de non-alignement que la lecture ajoute. Dans la cote 76, le lemme de surjectivité des drapeaux de type H vaut sous les deux hypothèses de la note marginale de la page 28, pour tout G-ensemble et sans que les σ_i soient des involutions.

Les énoncés restants demandent pour la plupart des théories classiques absentes de la bibliothèque : surfaces, dualité de Serre, complétion formelle, groupe fondamental d'une catégorie, lissité formelle, catégories Ind_π, équivalences faibles des petites catégories, géométrie des sections hyperplanes. Les pistes des parties vides demandent surtout les schémas abéliens et les variétés abéliennes, la cohomologie étale et cristalline, la descente, les champs et les topos ; cinq d'entre elles sont accessibles en tout ou en partie avec la bibliothèque actuelle.

Énoncés non vérifiés en Lean

Les 127 énoncés marqués ◊ dans la marge, dans l'ordre du texte : la cote, l'énoncé tel que le titre le donne, la vérification autre que Lean, la page. La vérification est *publié* quand la recherche bibliographique a trouvé l'énoncé imprimé, *réfuté* quand un contre-exemple le contredit, *problème ouvert* quand il est posé dans l'article des problèmes ouverts, *calcul* quand un programme du dossier `computations/` le teste sur de petits cas, avec son verdict (accord, désaccord, ou non testable par calcul) ; un tiret signale qu'aucune vérification n'est prévue.

Cote	Énoncé	Vérification	Page
16	page 49, variantes en dimension critique	problème ouvert	30
36	D'après les pages 9 à 16, forme corrigée par l'édition, théorème de Griffiths par voie ℓ-adique	—	33
36	pages 60 à 70, défaut des cycles invariants en H^1	—	34
36	pages 73 à 76, orthogonalité sur une base adique régulière	—	34
12	pages 115 à 119, poids et niveau d'une immersion	problème ouvert	36
13	pages 33 et 34, invariants d'un double réseau	—	39
60	pages 38 à 58, moyenne sur l'inertie et dualité	—	41
31	pages 64 à 70, majoration de la dimension cohomologique ; voir M. Artin, SGA 4, exposé X, théorème 4.1 (1973)	publié	41
31	page 22, minoration de la dimension cohomologique	problème ouvert	42
129	page 95, annulation de Ext^2	problème ouvert	43
161-2	pages 39, 41 et 42, deux topos classifiants non cohérents	problème ouvert	46
161-2	D'après les pages 47 à 49, anneaux de caractéristique définie	—	46
161-2	D'après les pages 92 à 95, le corps universel, forme complétée par l'édition	—	46

Cote	Énoncé	Vérification	Page
1	Pages 71 et 72, opérateurs compacts	calcul, non testable	55
43	pages 165 à 169, $\mathrm{Ext}^1(\mathbf{G}_a, \mathbf{Z}/p\mathbf{Z})$ et perfection	—	60
43	D'après les pages 70 à 74, forme corrigée par l'édition, concentration de la cohomologie locale	—	60
101	pages 10, 14 et 15, dualité locale en dimension deux	—	62
125	pages 2, 4 et 7, dimension cohomologique du complémentaire	publié	64
32	pages 10 et 11, noyau de l'image réciproque et indice	—	66
58	pages 40 à 43, permanence de la condition de Lefschetz	—	66
58	pages 45 à 51, comparaison des Hom hors de Y	—	66
128	pages 8 et 9, corollaires 2 et 3	—	73
128	pages 19 à 29, descente infinitésimale	—	73
126	pages 17 à 23, factorisation radicielle-étale	—	77
126	D'après les pages 4 à 7, forme complétée par l'édition, quotient d'une déformation nilpotente	—	77
126	pages 26 à 29, descente générique	—	77
161-3	pages 3 à 8, 2-produit de topos	publié	81
161-3	pages 11 et 12, topos d'un produit infini	—	81
23	pages 86 à 88, finitude de la normalisation	—	84
37	page 22, quand $\mathrm{Ind}(C)$ est un topos	réfuté	84
116	pages 6 et 7, recollement de topos de préfaisceaux	publié	85
100	pages 2, 3 et 20, pleine fidélité et composantes connexes	—	93
100	pages 22 à 24, descente des morphismes le long d'un épimorphisme propre	—	94
100	pages 30 à 38, algébrisation par les courbes	—	94
100	pages 47 à 52, prolongement vers un modèle de Néron	—	94
14	pages 93 et 94, amplitude par la caractéristique d'Euler	publié	94
59	D'après les pages 1 à 22, forme corrigée par l'édition, section canonique par le déterminant	—	94
130	pages 39 à 48, faisceau des quasi-fonctions	—	95
9	pages 22 à 28, déterminants des parties étales	—	95
9	pages 24 et 26, déterminant et racine du degré	—	95
14	pages 23 à 29 et 33, équivalence d'Albanese	—	95
47	pages 9 et 10, Riemann–Roch et transformation de Fourier sur une base	—	95
51	pages 16, 17 et 20, bonne réduction de l'Albanese	—	96
57	pages 98 et 99, section hyperplane générique	—	96
57	pages 226 à 228 et 247 à 271, Picard analytique et complété	—	96
59	pages 11 à 13, torseur de Picard en dimension 2	problème ouvert	97
49	D'après la page 3, forme reconstituée par l'édition, critère de platitude	—	97
57	pages 42 à 49, rigidité des sous-groupes	—	97
130	pages 3 à 5, symbole local de Néron	—	97
133	pages 42 et 43, quotient affine non constructible	—	125
162-5	Quillen, d'après les pages 43 à 45, universalité des correspondances de bordisme	—	131

Cote	Énoncé	Vérification	Page
162-5	pages 27 à 30, de Rham et Hochschild pour une catégorie formelle	—	132
162-5	Quillen, d'après les pages 21 à 26, catégories formelles à conormal plat	—	132
41	D'après les pages 3 et 8 à 10, composantes irréductibles des fibres, forme reconstituée par l'édition	—	137
102	page 12, critère d'immersion ouverte	—	143
127	pages 2 à 4, 15 et 19, critère valuatif de platitude d'une adhérence	—	143
127	pages 7, 9, 10 et 12, ouverture de Hironaka sur une base réduite	—	144
127	pages 2 et 3, descente non plate sur une base artinienne	—	144
131	pages 1 à 5, 13 et 15, représentabilité par un schéma localement quasi-fini	—	144
94	pages 8, 9 et 19, Tor génériques et suites régulières : l'ouvert dense	—	145
94	pages 15 et 16, critère de représentabilité sur $\mathrm{Mod}(A)$	—	146
2	page 13, une classe non nulle de classe de Chern totale 1	calcul, désaccord	149
153	Pages 3 et 9, co-opérations de Int relatif, forme corrigée par l'édition	calcul, accord	160
5	page 7, les quotients $W^{(\nu,r)}$	calcul, accord	163
5	pages 49 et 50, dualité étale pour les sites annelés	publié	164
4	pages 1 et 4 à 7, valeurs propres unités de la cohomologie évanescente	—	164
6	pages 52 à 56, modules des variétés abéliennes ordinaires	—	164
6	pages 49 et 50, un groupe formel hors des variétés abéliennes	—	164
6	pages 47 et 48, même groupe formel, non isogènes	—	165
137	pages 39 à 44 et 48 à 56, propriété universelle des complexes libres	—	165
137	pages 74 à 83, catégories polynomiales	—	167
90	D'après les pages 13 à 23, sous-modules équivariants sur une base quelconque, forme précisée par la lecture	—	174
46	pages 84 à 89, Hilbert 90 semi-local et inertie	—	186
53	Page 9, forme corrigée par l'édition, critère d'irréductibilité géométrique	—	188
64	pages 44 à 52, configurations octaédrales sur une base	—	195
64	pages 74 à 79 et 84 à 91, épinglages de Legendre	—	195
80	D'après les pages 24 et 26, cas latticiel, condition b) lue par l'édition	réfuté	197
80	pages 39 à 54, squelette d'un arrangement sans bigones	problème ouvert	198
82	page 78, (61)	calcul, accord	201
84	Pages 45 et 48, *la forme globale*	publié	210
84	Pages 65 à 79, *le produit intrinsèque*	—	213
10	pages 11 à 16, polarisations hodgiennes	—	218

Cote	Énoncé	Vérification	Page
10	pages 62 à 65, caractère numérique et tore de rang un	—	218
123	pages 10 à 12, groupe de Picard de l'espace de Grothendieck–Springer	—	218
123	pages 21, 28, 30 et 34, rigidifications de Kostant	problème ouvert	218
123	pages 10 à 13, pas de résolution de Steinberg sans changement de base	—	219
15	pages 71 à 77, catégorie de Picard de Brandt	—	219
15	pages 116 à 118, foncteurs fibres réels	—	220
27	pages 27 à 36, semi-continuité des rangs	—	220
45	pages 10 à 14, liens sur un corps de Tsen	—	220
45	D'après les pages 3 à 10, forme corrigée par l'édition, surjectivité en H^1 en dimension un	—	220
55	page 13, principe d'identité et lemme B	—	220
93	pages 193 et 194, la remarque	—	228
148	pages 30 à 32 et 35, carte des structures spéciales de $M_{0,5}$	—	236
62	D'après les pages 41 à 53, trois descriptions des triplets	calcul, accord	239
103	pages 14 et 15, Gr-champs épinglés et cohomologie relative	—	240
134-1	pages 3 à 5, suite exacte des champs de Picard épinglés	—	240
134-1	page 5, réalisation de l'invariant de symétrie	problème ouvert	240
85	D'après les pages 4 à 7, modules des représentations de G_2, reformulation de l'édition	calcul, accord	284
85	pages 10 et 40, sous-groupes icosaédraux	calcul, accord	285
132	pages 1 à 3, groupoïde fondamental d'un produit fibré	publié	285
132	pages 16 à 20, extensions d'un groupe non connexe	—	285
132	D'après les pages 5 à 8, forme complétée par l'édition, Gr-catégorie périphérique d'une surface	—	285
147	pages 148 à 151, voisinage épointé et codimension deux	problème ouvert	286
147	D'après les pages 62 à 64, forme complétée par l'édition, classe stratifiée de $M_{1,1}$ sur $\mathbf{Z}$	calcul, accord	286
154	pages 55 à 63, 85 et 86, monodromie diédrale	calcul, accord	287
77	pages 132 à 143 et 155 à 157, revêtement d'Arf par factorisation de Stein	—	288
29	page 120, inertie modérée et matrice des multiplicités	—	292
29	pages 190 à 193, axiome R2 des domaines de ramification	—	295
29	page 197, proposition 6, homomorphismes de domaines de ramification, énoncée sans démonstration	problème ouvert	295
29	pages 87 à 97, π_1 modéré et auto-intersection	publié	295
29	pages 170 et 171, torseurs sous un groupe discret infini	—	295
34	pages 167 et 175 à 180, monodromie modérée à plusieurs paramètres	—	297
149	pages 36 à 39, le lemme du Complément	publié	298
34	pages 153 à 155, 1-asphéricité locale	—	298

Cote	Énoncé	Vérification	Page
105	pages 42 à 45, excision pour deux cribles ouverts	—	336
108	page 2, Δ° et les catégories test	—	337
118	D'après les pages 18 à 20, forme complétée par l'édition, sommes amalgamées le long d'opfibrations	—	337
136	pages 161 à 179 et 189 à 199, schéma en groupes des automorphismes	—	337
136	pages 5 à 10 et 226 à 232, ombres de la cohomologie entière	—	339
151	pages 10 à 14 et 17, hyperrecouvrements indexés par une catégorie quelconque	publié	339
151	pages 38 à 42, Π_1 trop grossier pour la sphère	calcul, accord	340
150	pages 1 et 45 à 47, lissité des fibrations de drapeaux	—	347
150	pages 47 à 66 et 70, le déploiement comme espace ordonné	—	348
119	pages 144 et 145, quotients des feuilletages	problème ouvert	348
140-1	pages 22, 24 et 29, Picard du champ $[U_{0,3}/\mathfrak{S}_3]$	calcul, accord	361
138	pages 122 à 124 et 127, opérations sur les cartes	calcul, non testable	361

Déclaration sur l'usage de l'intelligence artificielle

Les énoncés démontrés ici sont tirés des lectures modernisées du fonds. Celles-ci dérivent de transcriptions produites par des modèles de langage (Claude Opus 5, Opus 5.5, Fable 5 et Fable 5.1, d'Anthropic) sous des règles éditoriales écrites par l'auteur ; ces transcriptions n'ont pas été relues en entier par une personne. Les preuves formelles ont été écrites en Lean 4 par Claude Opus 5.5, sous la direction de l'auteur, et Lean en vérifie mécaniquement la correction contre la bibliothèque mathlib. Le même modèle en a tiré les démonstrations rédigées de cette annexe. L'auteur a relu le choix des énoncés, les corrections apportées aux lectures et le texte, et en assume l'entière responsabilité. Lean garantit qu'un énoncé tient sous les hypothèses écrites. Il ne garantit ni que l'énoncé rend fidèlement le feuillet, ni qu'il est nouveau.

Références

[1] J. Adámek et J. Rosický, *Locally Presentable and Accessible Categories*, London Mathematical Society Lecture Note Series 189, Cambridge University Press, 1994 ; doi :10.1017/CBO9780511600579.

[2] Y. André, « Sur la conjecture des p-courbures de Grothendieck–Katz et un problème de Dwork », dans *Geometric aspects of Dwork theory*, vol. I, Walter de Gruyter, Berlin, 2004, 55–112 ; doi :10.1515/9783110198133.1.55.

[3] B. Antieau et L. Meier, « The Brauer group of the moduli stack of elliptic curves », *Algebra & Number Theory* 14 (2020), 2295–2333 ; doi :10.2140/ant.2020.14.2295 ; arXiv :1608.00851.

[4] D. Ara, « On homotopy types modelized by strict ∞-groupoids », *Theory and Applications of Categories* 28 (2013), 552–576 ; doi :10.70930/tac/50iqmupv.

[5] A. Arsie et A. Vistoli, « Stacks of cyclic covers of projective spaces », *Compositio Mathematica* 140 (2004), 647–666 ; doi :10.1112/S0010437X03000253.

[6] M. Demazure et A. Grothendieck (dir.), *Schémas en groupes (SGA 3), tome I*, Lecture Notes in Mathematics 151, Springer, Berlin, 1970 ; doi :10.1007/BFb0058993.

[7] M. Artin, A. Grothendieck et J.-L. Verdier, *Théorie des topos et cohomologie étale des schémas (SGA 4)*, tome 1, Lecture Notes in Mathematics 269, Springer, Berlin, 1972 ; doi :10.1007/BFb0081551.

[8] M. Artin, A. Grothendieck et J.-L. Verdier, avec la collaboration de P. Deligne et B. Saint-Donat, *Théorie des topos et cohomologie étale des schémas (SGA 4)*, tome 3, exposés IX à XIX, Lecture Notes in Mathematics 305, Springer, Berlin, 1973 ; doi :10.1007/BFb0070714.

[9] J. Ax, « The elementary theory of finite fields », *Annals of Mathematics* 88 (1968), 239–271 ; doi :10.2307/1970573.

[10] R. Baer, « Abelian groups that are direct summands of every containing abelian group », *Bulletin of the American Mathematical Society* 46 (1940), 800–806 ; doi :10.1090/S0002-9904-1940-07306-9.

[11] H. Bass, « K-theory and stable algebra », *Publications mathématiques de l'IHÉS* 22 (1964), 5–60 ; doi :10.1007/BF02684689.

[12] H. J. Baues, *Algebraic Homotopy*, Cambridge Studies in Advanced Mathematics 15, Cambridge University Press, 1989 ; doi :10.1017/CBO9780511662522.

[13] A. Beauville, « Finite subgroups of $\mathrm{PGL}_2(K)$ », dans *Vector Bundles and Complex Geometry*, Contemporary Mathematics 522, American Mathematical Society, Providence, 2010, 23–29 ; doi :10.1090/conm/522/10289.

[14] G. V. Belyi, « On Galois extensions of a maximal cyclotomic field », *Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya* 43 (1979), 267–276.

[15] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics 169, Springer, New York, 1997 ; doi :10.1007/978-1-4612-0653-8.

[16] F. Bien et A. Borel, « Sous-groupes épimorphiques de groupes linéaires algébriques I », *Comptes rendus de l'Académie des sciences, Paris, série I* 315 (1992), 649–653.

[17] J. Bokowski et P. Pokora, « On the Sylvester–Gallai and the orchard problem for pseudoline arrangements », *Periodica Mathematica Hungarica* 77 (2018), 164–174 ; doi :10.1007/s10998-017-0224-x ; arXiv :1607.05864.

[18] F. Borceux, *Handbook of Categorical Algebra 1. Basic Category Theory*, Encyclopedia of Mathematics and its Applications 50, Cambridge University Press, 1994 ; doi :10.1017/CBO9780511525858.

[19] A. Borel, « Injective endomorphisms of algebraic varieties », *Archiv der Mathematik* 20 (1969), 531–537 ; doi :10.1007/BF01899460.

[20] J. Borger et B. Wieland, « Plethystic algebra », *Advances in Mathematics* 194 (2005), 246–283 ; doi :10.1016/j.aim.2004.06.006.

[21] J.-B. Bost, « Algebraic leaves of algebraic foliations over number fields », *Publications mathématiques de l'IHÉS* 93 (2001), 161–221 ; doi :10.1007/s10240-001-8191-3.

[22] J.-B. Bost et F. Charles, « Some remarks concerning the Grothendieck period conjecture », *Journal für die reine und angewandte Mathematik* 714 (2016), 175–208 ; doi :10.1515/crelle-2014-0025 ; arXiv :1307.1045.

[23] L. Breen, « Un théorème d'annulation pour certains Ext^i de faisceaux abéliens », *Annales scientifiques de l'École normale supérieure* (4) 8 (1975), 339–352 ; doi :10.24033/asens.1291.

[24] M. Brion, « On algebraic semigroups and monoids », dans M. Can, Z. Li, B. Steinberg et Q. Wang (éd.), *Algebraic Monoids, Group Embeddings, and Algebraic Combinatorics*, Fields Institute Communications 71, Springer, New York, 2014, 1–54 ; doi :10.1007/978-1-4939-0938-4_1 ; arXiv :1208.0675.

[25] K. S. Brown, « Abstract homotopy theory and generalized sheaf cohomology », *Transactions of the American Mathematical Society* 186 (1973), 419–458 ; doi :10.1090/S0002-9947-1973-0341469-9.

[26] C. Cadman, « Using stacks to impose tangency conditions on curves », *American Journal of Mathematics* 129 (2007), 405–427 ; doi :10.1353/ajm.2007.0007 ; arXiv :math/0312349.

[27] P.-J. Cahen et J.-L. Chabert, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs 48, American Mathematical Society, Providence, 1997.

[28] H. Cartan et S. Eilenberg, *Homological Algebra*, Princeton Mathematical Series 19, Princeton University Press, Princeton, 1956.

[29] S. U. Chase, « Direct products of modules », *Transactions of the American Mathematical Society* 97 (1960), 457–473 ; doi :10.1090/S0002-9947-1960-0120260-3.

[30] D. V. Chudnovsky et G. V. Chudnovsky, « Applications of Padé approximations to the Grothendieck conjecture on linear differential equations », dans *Number Theory (New York, 1983–84)*, Lecture Notes in Mathematics 1135, Springer, 1985, 52–100 ; doi :10.1007/BFb0074601.

[31] G. V. Chudnovsky, « Algebraic independence of values of exponential and elliptic functions », dans *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, vol. 1, Academia Scientiarum Fennica, Helsinki, 1980, 339–350.

[32] D.-C. Cisinski, *Les préfaisceaux comme modèles des types d'homotopie*, Astérisque 308, Société mathématique de France, 2006 ; doi :10.24033/ast.715.

[33] D.-C. Cisinski, réponse à la question 516223, *MathOverflow*, 21 octobre 2026, `https://mathoverflow.net/questions/516223`.

[34] D. Clausen et A. Mathew, « Hyperdescent and étale K-theory », *Inventiones mathematicae* 225 (2021), 981–1076 ; doi :10.1007/s00222-021-01043-3 ; arXiv :1905.06611.

[35] B. Conrad, « Reductive group schemes », dans *Autour des schémas en groupes I*, Panoramas et Synthèses 42–43, Société mathématique de France, 2014, 93–444.

[36] R. Cori, *Un code pour les graphes planaires et ses applications*, Astérisque 27, Société mathématique de France, 1975.

[37] B. Courcelle, « Betweenness of partial orders », *RAIRO – Theoretical Informatics and Applications* 54 (2020), article 7 ; doi :10.1051/ita/2020007 ; arXiv :2004.09777.

[38] H. S. M. Coxeter et W. O. J. Moser, *Generators and Relations for Discrete Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 14, Springer, Berlin, 1957.

[39] L. de Moura et S. Ullrich, « The Lean 4 theorem prover and programming language », dans *Automated Deduction – CADE 28*, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635 ; doi :10.1007/978-3-030-79876-5_37.

[40] P. Deligne, « Théorie de Hodge III », *Publications mathématiques de l'IHÉS* 44 (1974), 5–77 ; doi :10.1007/BF02685881.

[41] P. Deligne, « Le groupe fondamental de la droite projective moins trois points », dans *Galois Groups over* $\mathbf{Q}$, Mathematical Sciences Research Institute Publications 16, Springer, New York, 1989, 79–297 ; doi :10.1007/978-1-4613-9649-9_3.

[42] C. Deninger et J. Murre, « Motivic decomposition of abelian schemes and the Fourier transform », *Journal für die reine und angewandte Mathematik* 422 (1991), 201–219 ; doi :10.1515/crll.1991.422.201.

[43] A. Dold et D. Puppe, « Duality, trace, and transfer », dans *Proceedings of the International Conference on Geometric Topology (Varsovie, 1978)*, PWN, Varsovie, 1980, 81–102.

[44] V. G. Drinfeld, « On quasitriangular quasi-Hopf algebras and on a group that is closely connected with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ », *Algebra i Analiz* 2 (1990), n° 4, 149–181 ; traduction anglaise, *Leningrad Mathematical Journal* 2 (1991), 829–860.

[45] A. H. Durfee, « Mixed Hodge structures on punctured neighborhoods », *Duke Mathematical Journal* 50 (1983), 1017–1040 ; doi :10.1215/S0012-7094-83-05043-3.

[46] D. Edidin, communication personnelle, courriel du 28 octobre 2026.

[47] D. Edidin et Z. Hu, « The integral Chow rings of the stacks of hyperelliptic Weierstrass points », *Michigan Mathematical Journal* (2025) ; doi :10.1307/mmj/20236479, arXiv :2208.00556.

[48] J. Elliott, « Birings and plethories of integer-valued polynomials », *Actes des rencontres du CIRM* 2 (2010), n° 2, 53–58 ; version développée, arXiv :1109.3848 ; doi :10.5802/acirm.34.

[49] K. Fan, « Maximum properties and inequalities for the eigenvalues of completely continuous operators », *Proceedings of the National Academy of Sciences of the USA* 37 (1951), 760–766 ; doi :10.1073/pnas.37.11.760.

[50] D. Ferrand, « Sur les modules qui sont limite projective de leurs localisés », *Comptes rendus de l'Académie des sciences, Paris, série A* 262 (1966), 609–611.

[51] R. Friedman et R. Laza, « The higher Du Bois and higher rational properties for isolated singularities », *Journal of Algebraic Geometry* 33 (2024), n° 3, 493–520 ; doi :10.1090/jag/824 ; arXiv :2207.07566.

[52] W. Fulton et M. Olsson, « The Picard group of $\mathcal{M}_{1,1}$ », *Algebra & Number Theory* 4 (2010), 87–104 ; doi :10.2140/ant.2010.4.87 ; arXiv :0704.2214.

[53] H. Furusho, « Pentagon and hexagon equations », *Annals of Mathematics* (2) 171 (2010), 545–556 ; doi :10.4007/annals.2010.171.545.

[54] O. Gabber et F. Orgogozo, « Sur la p-dimension des corps », *Inventiones mathematicae* 174 (2008), 47–80 ; doi :10.1007/s00222-008-0133-y ; arXiv :0706.0671.

[55] O. Gabber et B. Zavyalov, « Algebraization techniques and rigid-analytic Artin–Grothendieck vanishing », *Annales scientifiques de l'École normale supérieure* (2026) ; arXiv :2402.08741.

[56] P. Gabriel et F. Ulmer, *Lokal präsentierbare Kategorien*, Lecture Notes in Mathematics 221, Springer, Berlin, 1971.

[57] P. Gabriel et M. Zisman, *Calculus of Fractions and Homotopy Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete 35, Springer, Berlin, 1967 ; doi :10.1007/978-3-642-85844-4.

[58] Google DeepMind, *Formal Conjectures*, dépôt GitHub, fichier `FormalConjectures/Wikipedia/ResolutionOfSingularities.lean`, consulté le 17 octobre 2026, `https://github.com/google-deepmind/formal-conjectures`.

[59] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove et D. S. Scott, *Continuous Lattices and Domains*, Encyclopedia of Mathematics and its Applications 93, Cambridge University Press, 2003 ; doi :10.1017/CBO9780511542725.

[60] S. Gorchinskiy et F. Viviani, « Picard group of moduli of hyperelliptic curves », *Mathematische Zeitschrift* 258 (2008), 319–331 ; doi :10.1007/s00209-007-0173-9.

[61] A. Grothendieck, avec la collaboration de J. Dieudonné, « Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas (première partie) », *Publications mathématiques de l'IHÉS* 20 (1964), 5–259 ; doi :10.1007/BF02684747.

[62] A. Grothendieck, avec la collaboration de J. Dieudonné, « Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas (troisième partie) », *Publications mathématiques de l'IHÉS* 28 (1966), 5–255 ; doi :10.1007/BF02684343.

[63] A. Grothendieck (dir.), *Revêtements étales et groupe fondamental (SGA 1)*, édition recomposée et annotée, augmentée de deux exposés de M. Raynaud, Documents mathématiques 3, Société mathématique de France, Paris, 2003 ; arXiv :math/0206203.

[64] A. Grothendieck et J. P. Murre, *The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme*, Lecture Notes in Mathematics 208, Springer, Berlin, 1971.

[65] A. Grothendieck, *À la poursuite des champs*, volume I, édité par G. Maltsiniotis, Documents mathématiques 20, Société mathématique de France, Paris, 2022 ; le tapuscrit de 1983 est aussi sur arXiv, `https://arxiv.org/abs/2111.01000`.

[66] P. H. Hai et J. P. dos Santos, « On the structure of affine flat group schemes over discrete valuation rings, II », arXiv :1802.06377.

[67] K. H. Hofmann et J. D. Lawson, « The spectral theory of distributive continuous lattices », *Transactions of the American Mathematical Society* 246 (1978), 285–310 ; doi :10.1090/S0002-9947-1978-0515540-7.

[68] R. Hartshorne, *Ample Subvarieties of Algebraic Varieties*, Lecture Notes in Mathematics 156, Springer, Berlin, 1970 ; doi :10.1007/BFb0067839.

[69] H. Hasse et F. K. Schmidt, « Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten », *Journal für die reine und angewandte Mathematik* 177 (1937), 215–237 ; doi :10.1515/crll.1937.177.215.

[70] A. Hatcher, P. Lochak et L. Schneps, « On the Teichmüller tower of mapping class groups », *Journal für die reine und angewandte Mathematik* 521 (2000), 1–24 ; doi :10.1515/crll.2000.028.

[71] S. Henry, « Algebraic models of homotopy types and the homotopy hypothesis », prépublication, arXiv :1609.04622, 2016.

[72] S. Henry et E. Lanari, « On the homotopy hypothesis for 3-groupoids », *Theory and Applications of Categories* 39 (2023), 735–768 ; doi :10.70930/tac/897kfv5y.

[73] Y. Ihara, « Braids, Galois groups, and some arithmetic functions », dans *Proceedings of the International Congress of Mathematicians (Kyoto, 1990)*, vol. I, Mathematical Society of Japan, Tokyo, 1991, 99–120.

[74] J. R. Isbell, « Product spaces in locales », *Proceedings of the American Mathematical Society* 81 (1981), 116–118 ; doi :10.1090/S0002-9939-1981-0589150-5.

[75] N. Jacobson, « Restricted Lie algebras of characteristic p », *Transactions of the American Mathematical Society* 50 (1941), 15–25 ; doi :10.1090/S0002-9947-1941-0005118-0.

[76] A. Jacques, « Sur le genre d'une paire de substitutions », *Comptes rendus de l'Académie des sciences, Paris, série A* 267 (1968), 625–627.

[77] G. A. Jones et D. Singerman, « Theory of maps on orientable surfaces », *Proceedings of the London Mathematical Society* (3) 37 (1978), 273–307 ; doi :10.1112/plms/s3-37.2.273.

[78] M. Karoubi, « Algèbres de Clifford et K-théorie », *Annales scientifiques de l'École normale supérieure* (4) 1 (1968), 161–270 ; doi :10.24033/asens.1163.

[79] N. M. Katz, « Nilpotent connections and the monodromy theorem : applications of a result of Turrittin », *Publications mathématiques de l'IHÉS* 39 (1970), 175–232 ; doi :10.1007/BF02684688.

[80] N. M. Katz, « Algebraic solutions of differential equations (p-curvature and the Hodge filtration) », *Inventiones mathematicae* 18 (1972), 1–118 ; doi :10.1007/BF01389714.

[81] N. M. Katz et T. Oda, « On the differentiation of De Rham cohomology classes with respect to parameters », *Journal of Mathematics of Kyoto University* 8 (1968), 199–213 ; doi :10.1215/kjm/1250524135.

[82] L. M. Kelly et R. Rottenberg, « Simple points in pseudoline arrangements », *Pacific Journal of Mathematics* 40 (1972), 617–622 ; doi :10.2140/pjm.1972.40.617.

[83] M. Kisin, « Prime to p fundamental groups, and tame Galois actions », *Annales de l'Institut Fourier* 50 (2000), 1099–1126 ; doi :10.5802/aif.1786.

[84] A. Kock et I. Moerdijk, « Every étendue comes from a local equivalence relation », *Journal of Pure and Applied Algebra* 82 (1992), 155–174 ; doi :10.1016/0022-4049(92)90118-Y.

[85] A. Kock et I. Moerdijk, « Spaces with local equivalence relations, and their monodromy », *Topology and its Applications* 72 (1996), 47–78 ; doi :10.1016/0166-8641(95)00101-8.

[86] B. Kostant, « The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group », *American Journal of Mathematics* 81 (1959), 973–1032 ; doi :10.2307/2372999.

[87] T. Kreutz, M. Shen et C. Vial, « De Rham–Betti classes with coefficients », prépublication, arXiv :2206.08618v3, 2026.

[88] H. Lenzing, « Endlich präsentierbare Moduln », *Archiv der Mathematik* 20 (1969), 262–266 ; doi :10.1007/BF01899297.

[89] L. G. Lewis, Jr., J. P. May et M. Steinberger, avec des contributions de J. E. McClure, *Equivariant stable homotopy theory*, Lecture Notes in Mathematics 1213, Springer, Berlin, 1986 ; doi :10.1007/BFb0075778.

[90] M. Lorenz, « K_0 of invariant rings and nonabelian H^1 », *Journal of Algebra* 214 (1999), 458–478 ; doi :10.1006/jabr.1998.7725 ; arXiv :math/9808032.

[91] É. Lucas, « Théorie des fonctions numériques simplement périodiques », *American Journal of Mathematics* 1 (1878), 184–240 et 289–321 ; doi :10.2307/2369308 et 10.2307/2369373.

[92] E. Mackall, « Universal additive Chern classes and a GRR-type theorem », *Journal of Algebra* 560 (2020), 1173–1189 ; doi :10.1016/j.jalgebra.2020.06.018 ; arXiv :2006.14664.

[93] S. Mac Lane, *Categories for the Working Mathematician*, 2e édition, Graduate Texts in Mathematics 5, Springer, New York, 1998 ; doi :10.1007/978-1-4757-4721-8.

[94] G. Maltsiniotis, *La théorie de l'homotopie de Grothendieck*, Astérisque 301, Société mathématique de France, 2005 ; doi :10.24033/ast.689.

[95] G. Maltsiniotis, « Grothendieck ∞-groupoids, and still another definition of ∞-categories », prépublication, arXiv :1009.2331, 2010.

[96] A. Mathew, « On K(1)-local TR », *Compositio Mathematica* 157 (2021), no 5, 1079–1119 ; doi :10.1112/S0010437X21007144 ; arXiv :2005.08744.

[97] M. Hua, réponse à sa question 516243, *MathOverflow*, octobre 2026, `https://mathoverflow.net/a/516350`.

[98] Réponse à la question 516361, *MathOverflow*, 25 octobre 2026, `https://mathoverflow.net/questions/516361`.

[99] The mathlib Community, « The Lean mathematical library », dans *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, ACM, 2020, 367–381 ; doi :10.1145/3372885.3373824.

[100] J. S. Milne, *Arithmetic Duality Theorems*, 2e éd., BookSurge, 2006.

[101] K. Morita, « Duality for modules and its applications to the theory of rings with minimum condition », *Science Reports of the Tokyo Kyoiku Daigaku, Section A* 6 (1958), 83–142.

[102] S. Mukai, « Fourier functor and its application to the moduli of bundles on an abelian variety », dans *Algebraic Geometry, Sendai, 1985*, Advanced Studies in Pure Mathematics 10, North-Holland, Amsterdam, 1987, 515–550 ; doi :10.2969/aspm/01010515.

[103] D. Mumford, « Picard groups of moduli problems », dans O. F. G. Schilling (éd.), *Arithmetical Algebraic Geometry* (Purdue, 1963), Harper & Row, New York, 1965, 33–81.

[104] M. Pernice, « The integral Chow ring of the stack of 1-pointed hyperelliptic curves », *International Mathematics Research Notices* 2022, no 15, 11539–11574 ; doi :10.1093/imrn/rnab072 ; arXiv :2005.01513.

[105] T. Plewe, « Localic products of spaces », *Proceedings of the London Mathematical Society* (3) 73 (1996), 642–678 ; doi :10.1112/plms/s3-73.3.642.

[106] G. Pólya, « Über ganzwertige Polynome in algebraischen Zahlkörpern », *Journal für die reine und angewandte Mathematik* 149 (1919), 97–116 ; doi :10.1515/crll.1919.149.97.

[107] F. Pop, « Finite tripod variants of I/OM : on Ihara's question/Oda–Matsumoto conjecture », *Inventiones mathematicae* 216 (2019), 745–797 ; doi :10.1007/s00222-019-00855-8.

[108] N. Popescu et P. Gabriel, « Caractérisation des catégories abéliennes avec générateurs et limites inductives exactes », *Comptes rendus de l'Académie des sciences, Paris* 258 (1964), 4188–4190.

[109] M. S. Putcha, *Linear Algebraic Monoids*, London Mathematical Society Lecture Note Series 133, Cambridge University Press, 1988 ; doi :10.1017/CBO9780511600661.

[110] D. Rees, « Two classical theorems of ideal theory », *Proceedings of the Cambridge Philosophical Society* 52 (1956), 155–157 ; doi :10.1017/S0305004100031091.

[111] M. Saito, « Mixed Hodge modules », *Publications of the Research Institute for Mathematical Sciences* 26 (1990), 221–333 ; doi :10.2977/prims/1195171082.

[112] C. Scheiderer, *Real and Étale Cohomology*, Lecture Notes in Mathematics 1588, Springer, 1994.

[113] J.-P. Serre, « Exemples de variétés projectives conjuguées non homéomorphes », *Comptes rendus de l'Académie des sciences, Paris* 258 (1964), 4194–4196.

[114] D. Singerman et J. Strudwick, « The Farey maps modulo N », *Acta Mathematica Universitatis Comenianae* 89 (2020), 39–52 ; arXiv :1803.08851.

[115] T. A. Springer, « Regular elements of finite reflection groups », *Inventiones mathematicae* 25 (1974), 159–198 ; doi :10.1007/BF01390173.

[116] The Stacks Project Authors, *The Stacks Project*, `https://stacks.math.columbia.edu`.

[117] D. O. Tall et G. C. Wraith, « Representable functors and operations on rings », *Proceedings of the London Mathematical Society* (3) 20 (1970), 619–643 ; doi :10.1112/plms/s3-20.4.619.

[118] R. W. Thomason, « The classification of triangulated subcategories », *Compositio Mathematica* 105 (1997), 1–27.

[119] A. Topaz, « The Galois action on geometric lattices and the mod-ℓ I/OM », *Inventiones mathematicae* 213 (2018), 371–459 ; doi :10.1007/s00222-018-0792-2.

[120] J. Voight, « Discriminants and the monoid of quadratic rings », *Pacific Journal of Mathematics* 283 (2016), 483–510 ; doi :10.2140/pjm.2016.283.483.

[121] J. A. Cruz Morales, *The notion of space in Grothendieck : from schemes to a geometry of forms*, arXiv :2105.08799, 2021.

[122] A. Grothendieck, « Techniques de construction et théorèmes d'existence en géométrie algébrique III : préschémas quotients », Séminaire Bourbaki 6 (1960/61), exposé 212, 99–118 ; `http://www.numdam.org/item/SB_1960-1961__6__99_0`.

[123] J. Venken, « Non effectivité de la descente de modules plats par un morphisme fini d'anneaux locaux artiniens », *C. R. Acad. Sci. Paris Sér. A* 272 (1971), A1553–A1554.

Open questions from Grothendieck's Montpellier notes

Abstract

The University of Montpellier has put online 178 folders of Alexandre Grothendieck's mathematical working notes. Since August 2026 an edition has transcribed 165 of them with a language model, restated each in current notation, searched the literature for the statements they contain, and formalised what it could in Lean 4 against Mathlib. Most of the statements that look new sit in theories Mathlib does not have yet: étale cohomology, topoi, stacks, abelian schemes, motives. This note collects thirteen of them for mathematicians, and adds one problem he stated aloud in a lecture at Buffalo in 1973. Each comes with its folder and page, the context, what the literature search found, the argument the page gives or sketches, the steps the edition added, and what would settle it. A last section takes seven conjectures that are in print under his name, from the standard conjectures to the p-curvature conjecture, and drafts from the pages the route he meant to take to each and where it stops. None of the statements has been checked by a specialist, and several may already be in print; a reference is as welcome as a proof or a counterexample.

Q1 Why this note

Grothendieck gave his mathematical papers to Jean Malgoire in 1990 and 1995. They were deposited at the University of Montpellier in 2010 and given to it in 2012, and the university placed 178 folders, 16,074 pages by its inventory's count, in open access as facsimiles. They are working notes: drafts in ink and pencil, restarted, struck, annotated, almost never dated. Twenty folders have been edited by hand. The rest had not been transcribed.

Since August 2026 an edition has read the remaining folders with a language model as first transcriber, and written for each folder a *modernised reading*, a restatement in current notation made from the transcription and never from the hand. A register of *findings* lists the statements of the folders that may not stand in the literature, each written as a claim about the literature with what was searched and what would settle it; at the time of writing it holds 456 rows, of which 83 turned out to be in print. Statements were then formalised in Lean 4 against a pinned revision of Mathlib, about two thousand theorems in all. A companion paper describes the formalisation [24].

Lean settles a statement only when the objects it speaks of exist in the library. In October 2026, 203 open findings with no proof were sorted by what Mathlib can reach: 16 were reachable as it stands, 39 in part and 147 not at all, and one was set aside as ill-posed; the 147 are out of reach because they live in étale or crystalline cohomology, topoi, stacks, derivators, motives or Hodge theory [24]. Most of Grothendieck's own work was in those theories. This note hands the most promising of them to people who can prove them with pen and paper, or say where they are already proved.

How to read the entries

Each problem gives its *source*: the folder (a link to Montpellier's facsimile), the pages in the archive's pagination, and the inventory's dating, whose brackets mark an inferred date. « The page » means what Grothendieck wrote, as transcribed; short quotations are his. « The reading » means the edition's modernised reading, made by a language model. « We » marks a step of the edition: an argument, a correction or a search made for this note or for the register, with a language model, and not checked by a specialist unless the entry says so. The entries make no claim of priority. A statement on an undated leaf says when he wrote it down and nothing about whether others had.

The transcriptions themselves are not public: the rights belong to Grothendieck's heirs, and the reading views stay off the site until they authorise them. The facsimiles are public, at Montpellier, and each entry cites the page to look at. Montpellier's servers were down at the end of October 2026; the links follow the archive's own scheme and should work again.

Q2 Étale cohomology and Hodge theory

Problem 1 (A global bound with a shift of 3)**.** For a field k of characteristic p put $p^{\nu(k)} = [k : k^p]$, and for a scheme Z of characteristic p let $\nu(Z)$ be the supremum of $\nu(k(z))$ over its maximal points. Let X be an affine scheme on which p is not invertible, so that $V(p) \subset X$ has characteristic p. Is it true that

$$\operatorname{cd}_p(X) \;\le\; \sup\Big(\sup_{x\in X} \operatorname{cd}_p k(x),\; \nu(V(p)) + 3\Big)\,?$$

Source. folder 31, p. 84, *SGA A [SGA 4] (résidus de rédaction)*, inventory dating [1963–1973]. The page is headed « Conjectures sur la cohomologie des schémas affines »; this is its conjecture 2°). The page writes ℓ for the prime; we write p, since it is the characteristic of $V(p)$ and not a prime invertible on X.

Context. M. Artin wrote in SGA 4 X 3.0 that in unequal characteristic one must « certainement tenir compte » of the rank of Ω^1_k, without a bound [45]. The same page states a local form, 4°): for U open in the spectrum of a henselian local domain A of residue characteristic p with fraction field of characteristic 0, $\operatorname{cd}_p(U) \le \dim A + \nu(k) + \operatorname{cd}_p(k)$. The words around « ouvert » in 4°) are hard to read, so whether U is meant to be affine, and whether it may meet $V(p)$, is not known.

What is known. The local form holds, in a sharper form, for U a non-empty affine open of $\operatorname{Spec} A[1/p]$ with A an excellent henselian local domain and $\operatorname{char} K = 0$: Gabber and Orgogozo prove $\operatorname{cd}_p(U) = \dim A + \dim_p(k)$ [17, Th. 6.1], and Kato's p-dimension satisfies $\dim_p(k) \le \nu(k) + \operatorname{cd}_p(k)$, which is immediate from their Définition 1.1. Mathew proves that the residue fields of $\operatorname{Spec} R[1/p]$ have $\operatorname{cd}_p \le d+1$ when R is an excellent normal domain, henselian along an ideal $I \ni p$, with $\dim R_{\mathfrak{p}} + \log_p[\kappa(\mathfrak{p}) : \kappa(\mathfrak{p})^p] \le d$ for $\mathfrak{p} \supseteq I$; the same bound for the affine opens $\operatorname{Spec} R[1/f]$ of $\operatorname{Spec} R[1/p]$ is established in the course of the proof [33, Prop. 4.5]. Globally, SGA 4 gives $\operatorname{cd}_p X \le 2\dim X + 1$ for X of finite type over $\mathbb{Z}$ [45, X 6.2], and Clausen and Mathew give $\operatorname{cd}_p(X) \le \dim X + \sup_x \operatorname{cd}_p k(x)$ for X qcqs of finite Krull dimension [12,

Cor. 3.29]; for $\operatorname{Spec}\mathbb{Z}_p[x_1,\dots,x_n]$, which is not of finite type over $\mathbb{Z}$, the latter gives $2n+3$ where the page's bound gives $n+3$. Gabber and Zavyalov settle the analogous expectation for affinoids [18, Th. 1.7]; the Travaux de Gabber treat ℓ invertible only.

Ideas. The constant cannot be lowered to 2 (our observation): for $X = \operatorname{Spec}\mathbb{Z}$ and p odd, $\nu(V(p)) = 0$ and $\sup_x \operatorname{cd}_p k(x) = \operatorname{cd}_p \mathbb{Q} = 2$, while $\operatorname{cd}_p(\operatorname{Spec}\mathbb{Z}) = 3$ [45, X 6.1]; by Artin–Verdier duality $H^3(\operatorname{Spec}\mathbb{Z}, j_!\mu_p) \cong \mathbb{Z}/p$ [34, II.3.2, 3.3]. A natural route, which is the one of Mathew's proof, is the excision sequence for $V(p) \subset X$ and its complement $X[1/p]$: for X noetherian, $V(p)$ is affine of characteristic p, so of p-cohomological dimension at most 1 [45, X 5.1] (for X not noetherian a limit argument is needed); local cohomology along $V(p)$ can be moved to the henselisation along $V(p)$ by Gabber's affine analogue of proper base change, where Gabber–Orgogozo and Mathew apply. The difficulty is to absorb the dimension terms of those local bounds into $\sup_x \operatorname{cd}_p k(x)$, which the page's bound allows, and to see where the shift 3 comes from: the page does not explain it.

Lean. Not attempted: Mathlib has no étale cohomology.

What would settle it. A printed bound of this shape for an arbitrary affine scheme of mixed characteristic, or a counterexample to the 3.

Problem 2 (Lower bound for a local domain: the exceptions)**.** Let A be a noetherian local domain with fraction field K and residue field k, and r a prime. The page states that

$$\operatorname{cd}_r(K) \;\geq\; \operatorname{cd}_r(k) + \dim A$$

with exactly two possible exceptions: (a) r is the characteristic of K; (b) $r = 2$ and some point x of $\operatorname{Spec} A$ has an orderable residue field $k(x)$ with $\operatorname{cd}_2 k(x)(\sqrt{-1})$ finite. It adds that exception (b) disappears when A is regular, and reduces to « k itself real » when A is catenary and universally japanese. Are these refinements true?

Source. folder 31, p. 22, inventory dating [1963–1973]. The margin gives the example that keeps exception (b) alive: the local ring at the origin of $\mathbb{R}[X,Y]/(X^2+Y^2)$, a real domain whose only real point is the origin (Artin's example after SGA 4 X 2.3). The margin also asks: « cette restriction est-elle essentielle ??? »

What is known. The inequality is SGA 4 X 2.4 when r is invertible in A, with the cruder exception « some residue field orderable » [45]. When r is the residue characteristic and $\operatorname{char} K = 0$, it follows for A excellent henselian from Gabber–Orgogozo §3 [17]. We found nothing on the finer exception (b), on the regular case, on the catenary refinement, or on r the residue characteristic for A neither excellent nor henselian. Serre's *Cohomologie galoisienne* II §4 and Scheiderer's *Real and Étale Cohomology* [43], where cohomological dimension in the presence of orderings is treated, remain to be read.

Ideas. Artin's proof of X 2.4 goes by induction on $\dim A$, down to a henselian local ring of dimension one through a height-one prime, where X 2.3 and 2.2 apply [45]. The finer exception (b) says that what matters is the virtual cohomological dimension of the real residue fields, which suggests running the same induction with cd_2 replaced by cd_2 of $k(x)(\sqrt{-1})$ at the real points. The page's exception list covers r equal to the residue characteristic in mixed characteristic, which SGA 4 X 2.4 does not.

Lean. Not attempted (Galois cohomology of fields is in Mathlib only in low degree).

What would settle it. A reference for (b) and the two refinements, or an example of a regular local domain where the inequality fails at $r = 2$.

Problem 3 (Hodge types of the deleted neighbourhood of a point)**.** Let Y be a complex algebraic variety of dimension n, $j : X \hookrightarrow Y$ an open immersion with X smooth and dense, $y \in Y \smallsetminus X$, and $H^i = H^i(X \cap B_y) = (R^i j_* \mathbb{Q})_y$ with its mixed Hodge structure (Durfee [14] when $(Y \smallsetminus X) \cap B_y = \{y\}$; in general through Saito's mixed Hodge modules [42]). Then

$$h^{p,q}(H^i) \neq 0 \implies p, q \in [\max(0, i-n+1),\ \min(i, n)],$$

so the weights lie in $[0, 2i]$ for $i \leq n-1$ and in $[2(i-n+1), 2n]$ for $n \leq i \leq 2n-1$ (and $H^i = 0$ for $i \geq 2n$), and the level $\max|p-q|$ is at most $\min(i, 2n-1-i) \leq \min(i, n-1)$. Is this in the literature, and what is the right relative statement for a proper morphism?

Source. folder 12, pp. 115–119, *Généralités (sous-groupes de Galois motiviques)*, inventory dating 1964–[c. 1971]. Page 119 boxes « poids $\leq 2\inf(i, n)$, niveau $\leq \inf(i, n-1)$ » for X regular, $F = \mathbb{Q}_\ell$ and f an immersion with $n = \dim \overline{f(X)}$, in his yoga of weights and levels of ℓ-adic sheaves. The same page asks, with a question mark, for a relative version with $n = d_y(f)$ and level $\leq \min(i, n)$. The typescript says of its own conclusions (p. 96): « la portée des « résultats » de notre travail est nécessairement sujette à caution, puisqu'ils dépendent de conjectures non prouvées à l'heure actuelle » (the Weil conjectures and resolution of singularities).

Context. The page's argument is a Leray spectral sequence for a factorisation of f as an open immersion with normal crossings complement followed by a proper map, conditional on resolution, purity and the Weil conjectures, with tables of weights and levels. The Hodge-theoretic statement above is our translation.

What is known. Deligne bounds the Hodge types of the cohomology of a variety [22, 8.2.4]; Durfee constructs the mixed Hodge structure on $H^i(X \cap B_y)$ and its weight spectral sequence; Durfee–Saito, Steenbrink, Navarro Aznar and El Zein bound weights; for isolated singularities the box is implicit in the literature on links: it follows from semipurity and duality as in [16, Th. 2.6, Def. 2.7]. We did not find the box, or the level bound, for arbitrary y.

Ideas. Our argument: take a resolution $\pi : \tilde{Y} \to Y$, an isomorphism over X, with $D = \pi^{-1}(Y \smallsetminus X)$ simple normal crossings; put $F = \pi^{-1}(y)$ and $F_q = F \cap D^{(q)}$. Then $\dim F_0 \leq n-1$ and $\dim F_q \leq n-q$. The weight spectral sequence $E_1 = H^{k-q}(F_q)(-q) \Rightarrow H^k(X \cap B_y)$ (Durfee's, in the case he treats; we have not checked its form in the general case) and Hodge III 8.2.4 (i), (ii) for the compact F_q put every E_1 term in the box. Locally the lower end moves up by one because $\pi^{-1}(y)$ has dimension at most $n-1$. The cone over a smooth projective V of dimension $n-1$ with $h^{i,0}(V) \neq 0$ attains level i for $i \leq n-1$ and $n-1$ at $i = n$. For a proper f with fibre dimension d the gain fails, since a smooth family of curves already has H^1 of level $1 = d$; so the relative question of page 119 cannot keep $n-1$ if $d_y(f)$ is the fibre dimension.

Lean. Not attempted: no Hodge structures on cohomology in Mathlib.

What would settle it. A reference for the box; a relative statement interpolating between the immersion case and the smooth proper case; its ℓ-adic form with level read as divisibility of

Frobenius eigenvalues.

Problem 4 (An Ext^2 that vanishes when 2 is invertible: beyond smooth coefficients)**.** On the fppf site of a base on which 2 is invertible, is $\mathcal{E}xt^2_{\mathbb{Z}}(G, M) = 0$ for every finite locally free commutative group scheme G and every quasi-coherent M, not only for the smooth coefficients covered by Breen's theorem below?

Source. folder 129, p. 95, *Notes séminaire Montréal*, inventory dating [1970]. A parenthetical NB after a theorem on Ext over truncated rings: « $\mathrm{Ext}^2_{\mathbb{Z}}(G, M) = 0$ si 2 inv., pour tt G fini loc. libre », with the remark that this simplifies the deformation theory of Barsotti–Tate groups for $p \neq 2$. The word « inv. » is uncertain in the transcription, and the page gives no proof. A year earlier, in a letter to Giraud of 13 June 1969 (IHÉS, fonds Grothendieck–Illusie, FG_IL_2_GIRAUD69, p. 6), he expects the obstruction to lifting a smooth commutative group scheme commutatively over a first-order thickening to lie in $\mathrm{Ext}^2(X_0, \mathrm{Lie}(X_0) \otimes J)$, and asks how to define it; the letter treats smooth groups only and says nothing of a vanishing.

What is known. Breen proved, five years later, that $\mathcal{E}xt^i(G, H) = 0$ for $1 < i < 2p - 2$, for G finite flat and H smooth commutative quasi-projective, when every residue characteristic is at least p and multiplication by every prime $q < p$ is an automorphism of G; and that $\mathcal{E}xt^{2p-2}(\alpha_p, H) \neq 0$ in characteristic p for $H = \mathbb{G}_a, \mathbb{G}_m$ [7]. With $p = 3$ this gives the NB for smooth coefficients, in particular for vector bundles, when 2 is invertible; with $p = 2$ it shows $\mathcal{E}xt^2(\alpha_2, \mathbb{G}_a) \neq 0$, which supports the reading « si 2 inv. ». Illusie places the obstruction to deforming a truncated Barsotti–Tate group over a perfect field in $\mathrm{Ext}^2_{\mathbb{Z}}(G_0, t_{G_0} \otimes J)$ and says that proving directly that it vanishes is out of reach [25, p. 2]; Breen's theorem, which he does not cite, bears on that group.

Ideas. Breen's theorem is stated for the étale sheafification of the Ext sheaves. The remaining cases are a quasi-coherent M that is not locally free, and the passage from Breen's sheaves to the global groups on the fppf site, through the local-to-global spectral sequence.

Lean. Not attempted: no fppf cohomology in Mathlib.

What would settle it. Breen's vanishing for an arbitrary quasi-coherent M, or a counterexample; and whether it gives Illusie's obstruction directly.

Q3 Algebraic cycles

Problem 5 (Splitting the critical Lefschetz condition)**.** Let X be smooth projective of dimension n over an algebraically closed field, with a Weil cohomology H, a smooth hyperplane section $\varphi : Y \hookrightarrow X$, and L the Lefschetz operator. Write H^{2i} for the cohomology in which codimension-i cycles live, and consider:
— $A'(X)$: for $2i \leq n-1$, a class $x \in H^{2i}(X)$ whose restriction $\varphi^* x$ is algebraic is algebraic;
— $A''(X)$: for $2i \geq n-1$, every algebraic class of $H^{2i+2}(X)$ is $\varphi_* y$ for an algebraic $y \in H^{2i}(Y)$;
and their critical versions A'^0, A''^0, with $2i = n-2$ for n even and $2i = n-1$ for n odd. Let $A^0(X)$ be the critical Lefschetz condition: $L^2 : H^{n-2}(X) \to H^{n+2}(X)$ for n even,

$L : H^{n-1}(X) \to H^{n+1}(X)$ for n odd, is a bijection on algebraic classes. In even dimension $A'^0(X)$ and $A''^0(X)$ imply $A^0(X)$ once the critical condition $A^0(Y)$ holds on the section, and in odd dimension the splitting is circular (below, proved in Lean). Is the resulting reduction of the Lefschetz standard conjecture,

$$C(X) \iff C(Y) + A'^0(X \times X) + A''^0(X \times X),$$

correct as stated, that is, can the condition $A^0(Y_T)$ on a hyperplane section Y_T of $T = X \times X$ be dropped?

Source. folder 16, p. 49, *Formalisme algébrique des correspondances et algèbres de Poincaré-Hodge*, inventory dating 1966–1967, in a letter of January 1967. The letters use A, C, D in senses that do not match the later published labels; the conditions above are the reading's restatement. The letter to Coates places the question in the motivic picture (p. 48): « The complete yoga then being that we have the category of motives which is semi-simple ! ».

What is known. The equivalence $C(X) \iff C(Y) + A^0(X \times X)$ and its descent along a chain of hyperplane sections are Kleiman's [27, Th. 2.13]. The splitting of A^0 into the two one-sided conditions was not found in Kleiman 1968 and 1994, Grothendieck 1969, Charles 2013, Ramón Marí, or Milne; André's book [1, ch. 5, §5.2] remains to be read.

Ideas. The page factors the critical operator through the section. For $n = 2m$: $L^2 = \varphi_* \circ L_Y \circ \varphi^* : H^{2m-2}(X) \to H^{2m-2}(Y) \to H^{2m}(Y) \to H^{2m+2}(X)$; for $n = 2m+1$: $L = \varphi_* \varphi^* : H^{2m}(X) \to H^{2m+2}(X)$. What follows is our reconstruction, unchecked by a specialist.

$n = 2m$ *even.* Let $z \in H^{2m+2}(X)$ be algebraic. By A''^0, $z = \varphi_* y$ with $y \in H^{2m}(Y)$ algebraic. Since $\dim Y = 2m - 1$, hard Lefschetz makes $L_Y : H^{2m-2}(Y) \to H^{2m}(Y)$ bijective and weak Lefschetz makes $\varphi^* : H^{2m-2}(X) \to H^{2m-2}(Y)$ bijective, so $y = L_Y \varphi^* x$ for a unique $x \in H^{2m-2}(X)$, and $z = L^2 x$. If $L_Y^{-1} : H^{2m}(Y) \to H^{2m-2}(Y)$ preserves algebraic classes, then $\varphi^* x = L_Y^{-1} y$ is algebraic, and x is algebraic by A'^0. This hypothesis is the critical Lefschetz condition $A^0(Y)$ of the odd-dimensional section. So, for n even,

$$A'^0(X) + A''^0(X) + A^0(Y) \implies A^0(X).$$

$n = 2m + 1$ *odd.* Here $z = \varphi_* y$ with $y \in H^{2m}(Y)$ algebraic, and $x = L^{-1} z$ satisfies $\varphi_*(\varphi^* x - y) = 0$. By the projection formula the kernel of φ_* on $H^{2m}(Y)$ is the orthogonal V of $\varphi^* H^{2m}(X)$, the vanishing cohomology, and $H^{2m}(Y) = \varphi^* H^{2m}(X) \oplus V$. So $\varphi^* x = p(y)$, where $p = \varphi^* L^{-1} \varphi_*$ is the projection along V, and A'^0 gives $A^0(X)$ as soon as p preserves algebraic classes. But that condition follows from $A^0(X)$ itself. In odd dimension the splitting is therefore a reformulation, unless the decomposition of the algebraic classes of $H^{2m}(Y)$ along $\varphi^* H^{2m}(X) \oplus V$ is supplied otherwise; we do not see that $C(Y)$ supplies it, since $\varphi^* H^{2m}(X)$ is not a Lefschetz piece of Y.

Application to $X \times X$. The displayed equivalence applies the even case to $T = X \times X$, of dimension $2n$. Its hyperplane section Y_T has dimension $2n - 1$ and is not $Y \times Y$, and the hypothesis needed is $A^0(Y_T)$, the critical Lefschetz condition in degrees $2n - 2$ and $2n$ of a variety of dimension $2n - 1$. The direction $\Rightarrow$ holds: $C(X)$ gives $C(X \times X)$ [27], and with Λ_T algebraic a class x with $\varphi^* x$ algebraic is $L_T^{-1} \varphi_* \varphi^* x$, hence algebraic, so $C(X)$ gives $A'^0(T)$, and $A''^0(T)$ likewise. For $\Leftarrow$, an induction on dimension supplies C only below $\dim X = n$, not for

Y_T. So what our reconstruction proves is

$$C(Y) + A'^0(X \times X) + A''^0(X \times X) + A^0(Y_T) \implies C(X),$$

and the question is whether the last term can be dropped, or replaced by a condition on varieties of dimension below n. If it cannot, the splitting gains nothing on Kleiman's $C(X) \iff C(Y) + A^0(X \times X)$, where A^0 already bears on $X \times X$ directly.

Lean. The two cases are proved as abstract linear algebra, the cohomology groups being modules and the algebraic classes submodules (`lean/Grothendieck/Folder16.lean`): `split_even` for the display above, `split_odd` and `split_odd_circular` for the odd case. Weak and hard Lefschetz, and the geometry of Y_T, are hypotheses, not theorems.

What would settle it. A reference for the splitting; or a proof that $A^0(Y_T)$ can be dropped from the last display, or replaced by conditions on varieties of dimension below n; or an argument that it cannot, in which case the reduction is circular.

Q4 Abelian varieties and reductive groups

Problem 6 (Polarised abelian surfaces with even Euler characteristic)**.** Let A/S be an abelian scheme of relative dimension 2 with dual B, and δ a section of $\mathrm{NS}_{A/S}$ with $\chi(\delta)$ even. Is the torsor $\mathrm{Pic}^{\delta}_{A/S}$ under B trivial? Over a field k, this says that the Poonen–Stoll class $c_\delta \in H^1(k, B)$ vanishes [39].

Source. folder 59, pp. 11–13, *Construction des faisceaux inversibles sur schémas de Picard*, inventory dating [années 1960–1970]. Page 11 gives a canonical isomorphism $\mathrm{Pic}^{\delta'}_{B/S} \simeq \tilde{\delta}'_* \mathrm{Pic}^{\delta}_{A/S}$; page 13 composes it with its analogue and concludes, for $n = 2$ and $\chi(\delta)$ even, that Pic^{δ} is trivial. That last line rests on an uncertain « si » and an illegible word.

What is known. Poonen and Stoll define c_λ and prove $2c_\lambda = 0$, with no criterion in terms of $\chi(\lambda)$ or the dimension [39, §4]. We found no such criterion elsewhere.

Ideas. The reading thought the conclusion depends on compatibilities of trivialisations that the folder asks for and never proves. Our argument, unchecked, needs none for mere triviality. Write $c = [\mathrm{Pic}^{\delta}_{A/S}] \in H^1(S, B)$, $\chi = \chi(\delta)$, and $\varphi_L : A \to B$ for the isogeny of a line bundle L of class δ, of degree χ^2.

Step 1, the map. For L of class δ, relatively ample of index 0, the Fourier–Mukai transform $\hat{L}$ is a vector bundle of rank χ on B, and $\varphi_L^* \hat{L} \cong \pi^*(\pi_* L) \otimes L^{-1}$ [36, §3]. Put $N = \det \hat{L}$. Then $\varphi_L^* N \cong L^{-\chi}$ up to a line bundle from S, so $\varphi_L \circ \varphi_N \circ \varphi_L = -\chi\, \varphi_L$, and since φ_L is an isogeny, $\varphi_L \circ \varphi_N = [-\chi]$ on B. The construction commutes with base change, since $\hat{L}$ is computed in degree 0; it defines a morphism of fppf sheaves $\Psi : \mathrm{Pic}^{\delta}_{A/S} \to \mathrm{Pic}^{[N]}_{B/S}$, which needs L only fppf-locally.

Step 2, equivariance. Translating L by $b \in B = \mathrm{Pic}^0_{A/S}$ translates $\hat{L}$: $\widehat{L \otimes P_b} \cong T_b^* \hat{L}$ [36, §3]. Taking determinants, $\Psi(L \otimes P_b) = T_b^* N = N \otimes P_{\varphi_N(b)}$ by the theorem of the square. So Ψ is equivariant along $\varphi_N : B \to A = \mathrm{Pic}^0_{B/S}$.

Step 3, the way back. The same construction on B sends N to $N' = \det \hat{N}$ on A, equivariantly along $\varphi_{N'} : A \to B$. From $\varphi_L \varphi_N = [-\chi]$ and $\deg \varphi_N = \chi^{2g}/\chi^2$ in relative dimension g, one gets $\chi(N) = \pm\chi^{g-1}$ and $\varphi_{N'} = \pm\chi^{g-2}\varphi_L$. This is where the dimension enters: for $g = 2$, N' has class $\pm\delta$, and composing with $L \mapsto L^{-1}$ if the sign is negative, $\Psi' \circ \Psi$ maps $\mathrm{Pic}^{\delta}_{A/S}$ to itself. For $g \neq 2$ the way back lands in the class $\pm\chi^{g-2}\delta$, and the argument does not close.

Step 4, the torsor class. The composite is equivariant along $\varphi_{N'} \circ \varphi_N = \pm\varphi_L\varphi_N = [\mp\chi]$. A morphism from a B-torsor to itself that is equivariant along an endomorphism ψ of B shows $\psi_* c = c$, so $(\chi \pm 1)\, c = 0$. Independently $2c = 0$ [39, §4], through $L \mapsto L \otimes [-1]^* L$. When χ is even, $\chi \pm 1$ is odd and prime to 2, so $c = 0$ whatever the sign.

The points a specialist should check are the sign conventions in Steps 1 and 2, which decide whether the composite is $[\chi]$ or $[-\chi]$ but not the conclusion; the passage from $\varphi_L\varphi_N\varphi_L = -\chi\varphi_L$ to $\varphi_L\varphi_N = [-\chi]$ over a base; and the compatibility of the Fourier–Mukai transform with base change for a polarisation that exists only fppf-locally. Whether the trivialisation obtained is canonical, which is what the folder asks, is a separate question.

Lean. Not attempted: no abelian schemes in Mathlib.

What would settle it. A specialist's check of the argument. One abelian surface over a number field with a polarisation of type $(1, 2)$ and $c_\lambda \neq 0$ refutes the statement. A sharp consequence to test (our heuristic, unchecked): for a genus-2 curve C/k whose Jacobian has real multiplication by $\mathcal{O}_D$, $D \equiv 1 \bmod 8$, defined over k, the theta class is a sum of two classes of even χ, so the statement would force Pic^1_C to have a k-point.

Problem 7 (Kostant's tori in apposition: are the Borels opposite?)**.** Let G be a complex simple adjoint group with Coxeter number h and Weyl group W, and let T, T' be maximal tori in apposition in Kostant's sense [32], with Borel subgroups $B \supset T$ and $B' \supset T'$. Are B and B' always in general position, that is, is $B \cap B'$ a maximal torus? If not for all such quadruples (T, B, T', B'), is there a distinguished conjugacy class of quadruples, stable under the outer automorphisms?

Source. folder 123, pp. 21–22, *[Autour de Kostant]*, letter to Kostant of 22 October 1969: « is it true that for some, or for all, such quadruples, B and B' are « in general position » [...] ? Is there in any sense a *distinguished* conjugacy class of such quadruples [...] ? » The letter states without proof that the quadruples form $|W|^2/(h\, z\, \varphi(h))$ conjugacy classes, z the order of the centre of the simply connected cover, and (in a footnote in his hand) that $N(T) \cap N(T')$ is an extension of $(\mathbb{Z}/h)^*$ by $\mathbb{Z}/h \times Z(\tilde{G})$.

What is known. The count, which this note listed as open until 26 October 2026, follows from standard theory (our argument, unchecked by a specialist). Let $x = \rho^\vee(e^{2\pi i/h})$, the principal element of T, and T' the centraliser of a cyclic element $E' = \sum_i c_i e_{\alpha_i} + c_0 e_{-\theta}$. An element $t \in T$ normalising T' sends E' into $\mathfrak{h}' \cap \mathfrak{g}^{\mathrm{Ad}(x)=\zeta}$, which is the line $\mathbb{C}E'$, so $\alpha_i(t) = \theta(t)^{-1} = \lambda$ with $\lambda^h = 1$: $T \cap N(T') = \langle x \rangle$, of order h. The image of $N(T) \cap N(T')$ in W is the set of w with $w(x) \in \langle x \rangle$: the stabiliser of x is the group $\Omega \cong P^\vee/Q^\vee$ of order z (in the adjoint group x has a disconnected centraliser), x is conjugate to x^k exactly for k prime to h [32, 47], and each such w lifts into $N(T')$, because regular semisimple elements of the eigenspaces $\mathfrak{g}^{\zeta^j}$, j prime to h, have the same centralisers as those of $\mathfrak{g}^\zeta$ and their Cartan subspaces are conjugate under $Z_G(x)^\circ = T$. Hence $|N(T) \cap N(T')| = h\, z\, \varphi(h)$; the stabiliser of a quadruple is $T \cap T' = 1$, and

the count follows. A computer count over $\mathbf{F}_q$ (`computations/kostant`) agrees: 2, 4 and 12 orbits for A_2, B_2 and G_2. For general position we found nothing.

Ideas. For A_2 all 36 pairs (B, B') are opposite: the eigenvectors of E' are the Fourier vectors $(1, \omega^k, \omega^{2k})$, and the standard flag is transverse to every flag they span. In general the question is the Bruhat cell of (B, B') for B' running over the $|W|$ Borels through T': whether it is always the open cell.

Lean. Only the arithmetic: the announced number $\mathrm{card}(W)^2/(h\, z\, \varphi(h))$ is an integer for every simple type of rank at most 8 and for E_6, E_7, E_8, F_4, G_2, and equals 1, 2, 4, 12 for A_1, A_2, B_2, G_2 (`lean/Grothendieck/Folder123Kostant.lean`). The geometry, and the relative position of B and B', are not attempted; the computer count above can be extended to that position in B_2 and G_2, which we have not done.

What would settle it. The relative position of B and B' for all quadruples, by an argument or by computation in each type.

Q5 Topoi and stacks

> **Problem 8** (Two classifying topoi that are not coherent)**.** The theories of commutative rings with irreducible spectrum (nilradical prime) and of rings with zero-dimensional spectrum are geometric. The page says their classifying topoi, subtopoi of the coherent classifying topos of rings, are not coherent, their presenting topologies on affine schemes of finite type over $\mathbb{Z}$ not being quasi-compact. Is that right, and do these topoi have enough points?

Source. folder 161-2, pp. 39, 41–42, *Algèbre universelle*, inventory dating [c. 1963–1973]. Page 39: « Cette topologie n'est pas quasi-compacte »; page 42, margin: « topologie non cohérente ! A-t-elle assez de pts ?? »; page 41, margin: « encore un topos non cohérent (bien que sous-topos d'un topos cohérent) ».

What is known. Locally coherent toposes have enough points (Deligne, [45, VI, 9.0]); these theories are geometric but, as presented, use the infinite disjunction hidden in « nilpotent ». We found neither non-coherence nor the existence of points stated for them, in Johnstone [15] or in Caramello's criteria for De Morgan classifying toposes, which take quotients of the theory of rings as examples [10, §5].

Ideas. Non-coherence needs more than the presentation: one must show that no coherent axiomatisation exists, for instance by exhibiting a cover in the classifying topos with no finite subcover. For points, Barr's theorem gives a Boolean cover, not points; a model-theoretic argument, or an explicit set of local rings detecting the theory, is needed.

Lean. Not attempted: classifying topoi are not in Mathlib.

What would settle it. A proof or reference for non-coherence, and an answer to the question about points.

Problem 9 (Foliations and their quotient topoi)**.** Is there an equivalence between the category of pairs (X, R), with X a topological space and R a local equivalence relation on X, locally open with locally connected fibres, and the category of triples $(X, \mathcal{Y}, f)$, with $f : \mathrm{Top}(X) \to \mathcal{Y}$ a locally open geometric morphism with locally connected fibres to a « multiplicité topologique », a 2-category whose Hom-categories are discrete?

Source. folder 119, pp. 144–145, dated « Mars 1986 » on p. 144. Under « Th »: « On a $C \rightleftarrows C'$ », both arrows marked $\approx$. No proof. A third condition on f is partly illegible; the reading suggests it may be a simple connectedness of the fibres.

What is known. SGA 4 IV, Exercise 9.8.3 j)–k), gives the functor $(X, R) \mapsto (\mathrm{Top}(X) \to \mathrm{Top}(X/R))$ [45]; Rosenthal states that the topos $\mathrm{sh}(X; r)$ exists for strictly open r (Th. 3.9, proof in his thesis) and proves it is an étendue for strictly regular r [41]; Kock and Moerdijk show that every étendue is of the form $\mathrm{sh}(M, r)$, construct the inverse $a \mapsto \mathrm{Lker}(a)$ and show the round trips are identities under simple connectedness or kernel-pair conditions [28], and study monodromy versus holonomy [29]. We found no statement of an equivalence of categories.

Ideas. The two functors are there; the problem is the right conditions on both sides so that they are mutually inverse, and which quotient topos the page means: the topos of R-invariant sheaves (sheaves on a monodromy groupoid) or the holonomy quotient, which Kock and Moerdijk distinguish.

Lean. Not attempted: no geometric morphisms of topoi in Mathlib.

What would settle it. A correct statement with proof, or Moerdijk's Zaragoza lectures [35], which we could not read and where it might be.

Problem 10 (Realising the symmetry invariant of a Picard stack)**.** Let M, N be abelian sheaves on a topos, and ${}_2N$ the 2-torsion of N. Is every homomorphism $M \to {}_2N$ the symmetry invariant of a Picard stack pinned by M and N?

Source. folder 134-1, p. 5, letter to Deligne, Lodève, 27 August 1974 (Breen's copy, forwarded by Deligne): « Je sais prouver (sauf erreur) que tout hom. $M \to {}_2N$ provient d'un champ de Picard convenable (épinglé par M, N) (a priori l'obstruction est dans $\mathrm{Ext}^3(X; M, N)$, mais un argument « universel » prouve qu'elle est nulle) ». No argument is written. On p. 6 the letter asks his own version of this problem: « Question : Le triangle exact (T) et la suite exacte (*) sont-ils connus par les compétences (Quillen, Breen, Illusie…) ? Connaissent-ils des variantes « supérieures » ? » (are they known to the experts, and do they know higher variants?). Grothendieck withdrew the vanishing in a letter to Breen of 5 February 1975 (IHÉS, fonds Grothendieck–Illusie, 1ILL21, p. 1; the copy of this letter in the appendix to *Pursuing Stacks*, folder 134-2, p. 37, skips its beginning). He grants that Breen's scepticism about the exact sequence of the Deligne letter was founded, and accepts Breen's reading of the invariant as an Ext^2 of a functor of M (written $X(M)$) into N. He keeps an obstruction homomorphism $\mathrm{Hom}(M, {}_2N) \to \mathrm{Ext}^3(M, N)$, found by a geometric route, and the reduction to the universal case, $M = N$ the universal sheaf of $\mathbb{F}_2$-vector spaces, which he calls correct; but the vanishing of $\mathrm{Ext}^i(M, N)$ for $i \geq 1$ in that case came, he writes, from a « calcul complètement canulé ».

What is known. Strict Picard stacks are classified by Ext^2 (Deligne, [45, XVIII, 1.4]); Breen classifies Gr-stacks by H^3 and gives the universal coefficient spectral sequence $\mathrm{Ext}^p(H_q(B), A) \Rightarrow H^{p+q}(B, A)$ [8, §6]. No printed source we found states the realisation, or refutes it on a topos.

Ideas. Two sketches disagree. The reading realises the invariant by hand for M free, on the split stack $M \times BN$ with an antisymmetric form b such that $b(e_i, e_i) = q(e_i)$, and passes to general M through a resolution. We doubt that step, which we have not checked: the construction depends on a basis. On the classifying topos of abelian groups, a Picard stack pinned by the generic group U and $U/2U$, with the projection as invariant, would make Moore spectra truncated above π_1 functorial in finitely presented abelian groups; but the stable Moore-space category on finitely generated groups is a non-split linear extension, split on cyclic groups [3, Rem. 1.5.5]. If that translation is right, the obstruction does not vanish universally. The letter of 1975 agrees with the second sketch on one point: the « universal » argument of 1974 rested on a miscalculation. It does not say whether the obstruction is non-zero. The statement does hold over a point and for M constant and free.

Lean. Not attempted: no stacks on a topos in Mathlib.

What would settle it. The obstruction $\mathrm{Hom}(M, {}_2N) \to \mathrm{Ext}^3(M, N)$ computed in a universal case: the identity of the universal sheaf of $\mathbb{F}_2$-vector spaces, to which the letter of 1975 reduces, or the differential $\mathrm{Hom}(M/2, N) \to \mathrm{Ext}^3(M, N)$ of the universal coefficient spectral sequence on the classifying topos of abelian groups. Since the 1974 argument is withdrawn, a non-zero value there would answer the problem in the negative.

Problem 11 (Morphisms of ramification domains are fully faithful)**.** Over a scheme S, a « domaine de ramification » is a stack of multigaloisian categories over the étale site of S with a continuous geometric realisation into relative schemes, subject to axioms R1 and R2 (pp. 190–193). For a domain (R, r) defined by a scheme Z with a finite group G of operators, is $\mathrm{Hom}((R, r), (R', r'))$ equivalent to the category of pairs (P', α), P' a galoisian object of R'_S of group G and α a G-isomorphism $r'(P') \simeq Z$, so that every homomorphism of domains is fully faithful?

Source. folder 29, p. 197, *Groupe fondamental [autour de SGA 4 et SGA 7]*, inventory dating 1959–1969: Proposition 6, stated without proof, with the corollary « nécessairement pleinement fidèle ». The axiom R2 of pp. 190–193 is itself not verified by the edition. Earlier in the folder (p. 24) he notes where removing the auxiliary choices leads: « il semble qu'on soit infailliblement conduit à prendre comme catégorie [...] la catégorie [...] elle-même qu'on se propose de construire et d'étudier ! », comparing it with sites and their topoi.

What is known. Nothing found. Tonini's work on stacks of ramified Galois covers [48, 49] is where an equivalent statement would sit; neither surfaced in our search, which is not the same as their not containing it.

Ideas. The corollary says that a ramification domain maps into another only as a subdomain. The proof should reduce to the case (R, r) given by (Z, G), where a morphism is determined by the image of the universal G-torsor.

Lean. Not attempted: no étale site or stacks of categories in Mathlib.

What would settle it. A proof of Proposition 6 from R1–R2, or a reference.

Q6 Moduli of curves and Galois actions

Problem 12 (The Galois image, seen on one curve)**.** Let X be an anabelian curve over a field K of finite type over $\mathbb{Q}$, and $\hat{\Pi}_1(X, I)$ its profinite fundamental groupoid on a finite set I of base points. The page lists necessary conditions for a vertex-fixing automorphism Θ of $\hat{\Pi}_1(X, I)$ to come from $\mathrm{Gal}(\bar{K}/K)$: it lifts to $\hat{\Pi}_1(X', I')$ for every finite étale cover X' of X defined over K; it preserves the kernels of $\hat{\pi}_1(X', x') \to \hat{\pi}_1(Y, f(x'))$ for every K-morphism $f : X' \to Y$; it is compatible with morphisms between covers; and it satisfies the loop condition at the cusps with a single multiplier. Are these conditions sufficient?

Source. folder 142, pp. 94–95, 98–101, *Action de Galois sur Teichmüller*, inventory dating [from 1978]. Page 95 conjectures the conditions sufficient « lorsque X est (disons) une courbe algébrique anabélienne, avec K extension de type fini de $\mathbb{Q}$ »; page 99 calls the loop condition « sûrement la plus importante de toutes, de très loin ! ». Pages 98–99 are largely illegible.

What is known. Ihara's question and the Oda–Matsumoto conjecture characterise the Galois group as the automorphisms of the geometric fundamental group functor on all varieties compatible with all morphisms; Pop proved it in that form, and finite tripod variants, built from varieties of dimension greater than one with finitely many dominant rational maps to $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ [40, Def. 2.2, Th. 2.9]. Hoshi–Mochizuki and others give injectivity for a single hyperbolic curve; Collas proposes a combinatorial model GT^{NF} as a candidate for $G_{\mathbb{Q}}$, left to forthcoming work [13, §4.3.3]. We found no characterisation attached to one curve and its covers, with base points and the inertia condition.

Ideas. Pop's variants need a base of dimension greater than one, so they do not cover the covers of one curve; that is what the page's loop condition at the cusps would have to supply. Here « anabelian curve » is the page's word for a hyperbolic curve.

Lean. Not attempted: no étale fundamental group in Mathlib.

What would settle it. A proof of sufficiency, a counterexample, or a published variant that implies it.

Problem 13 (The deleted neighbourhood of a normal crossings divisor)**.** Let X be a smooth complex analytic space (or orbifold) with a normal crossings divisor Θ, and $V^*_{\Theta,X}$ the deleted tubular neighbourhood of Θ. Is $V^*_{\Theta,X}$ the homotopy colimit of the semi-simplicial system of deleted tubular neighbourhoods of the strata of the unfolding of Θ, so that its fundamental groupoid is the amalgamated sum $\tilde{\Pi}_1 \leftarrow \tilde{\Pi}_{2,1} \to \tilde{\Pi}_2$ of the groupoids of the torus bundles over the open strata of codimension 1 and 2? And hence the same for $\Pi_1(X \smallsetminus \Theta)$ whenever $X \smallsetminus \Theta$ and its end have equivalent fundamental groupoids?

Source. folder 147, pp. 148–151, *Structure à l'infini des* $M_{g,\nu}$. The folder is undated; the inventory dates its group (141–149) [from 1978]–1983. We date it to the winter of 1982–1983, because its formalism is the one Grothendieck describes to Illusie in a letter of 22–25 January

1983 (IHÉS, fonds Grothendieck–Illusie, 1ILL35, p. 27) and in a *rapport d'activité* of which he sent Illusie a copy on 29 March 1983 (1ILL41, p. 4; copy in folder 119, pp. 141–142). Page 149 states a « Th. de recollement » as an equivalence of topoi and corrects it at once: « en fait, c'est une équivalence d'homotopie ». Pages 150–151 give the corollaries, with a purity argument for neglecting the strata of codimension 3. No proof is written.

Context. The folder describes the boundary of $\overline{M}_{g,\nu}$ by stable graphs, lists the strata of modular dimension at most 2, and writes on its p. 29 (archive p. 59) that a more or less complete understanding of the discrete π_1 in these small cases « donnera la clef pour une compréhension complète dans le cas général »: the two-level principle of the Teichmüller tower, about a year before the *Esquisse d'un programme*. Applied to $X \smallsetminus \Theta = M_{g,\nu}$, the corollaries would express the mapping class group through the strata of codimension 1 and 2; that application is the reading's, not the page's.

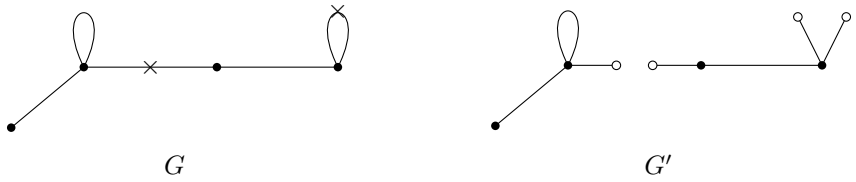


Figure 25 – Cutting a stable graph, after a sketch of folder 147, p. 97. Vertices are components of the curve, edges are its nodes, a loop is a node of one component with itself. Cutting at the crossed edges separates each of those nodes into two points (white), which become marked points, legs, of the components that carried them; G' is the graph of the partial normalisation. The page draws the new legs as small closed loops.

What is known. The two-level principle for the discrete tower was proved by Hatcher, Lochak and Schneps [21]. For the general gluing statement, the places to look are the real oriented blow-up and the Kato–Nakayama space of the log structure, whose boundary is a torus-bundle model of the deleted neighbourhood, and Looijenga's and Boggi's work on the boundary of $\overline{M}_{g,n}$. We did not find the statement in this form.

Ideas. The purity step reads: removing a subset of real codimension at least 3 does not change π_1. For $M_{g,\nu}$, the hypothesis of the last corollary (end and interior with the same Π_1) should follow from the simple connectivity of the curve complex (Harer).

Lean. Not attempted: no homotopy colimits of spaces or stratified spaces in Mathlib.

What would settle it. A reference for the gluing theorem, or a proof, and the check of the hypothesis for $M_{g,\nu}$.

Q7 Pseudoline arrangements

A pseudoline arrangement in the real projective plane is *bigonal along* one of its pseudolines D when D carries exactly two vertices of the arrangement, so that every other pseudoline meets D at one of them. In the page's notation, II_4 is four pseudolines in general position, II_5 five in general position, $\mathrm{II}'_{3,2}$ a pencil of three and a pencil of two without the line joining their

centres, and III_6 the complete quadrangle (the six lines joining four points, no three collinear); Figure 26 draws all four.

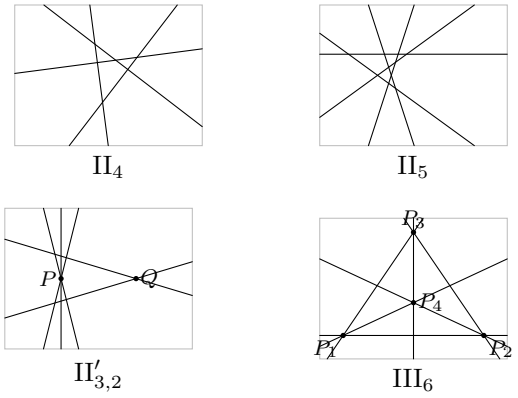


Figure 26 – The four arrangements of the dichotomy, drawn with straight lines in an affine chart chosen so that every crossing is visible. In $\mathrm{II}'_{3,2}$ the line PQ is absent; in the complete quadrangle III_6 the six lines join $P_1, \dots, P_4$, and the triangle $P_1P_2P_3$ has every other line through one of its vertices.

An arrangement is *bigon-free* when none of its pseudolines is bigonal, and four pseudolines are in *general position* when no three of them pass through one point. The page's boxed dichotomy, which this note listed as an open problem until 26 October 2026, has a short proof, and so does the numbering lemma of page 28; we record them here.

Proposition (Grothendieck, folder 80, pp. 20, 24, 28; the proof is ours)**.** *A bigon-free arrangement $\mathcal{A}$ either is II_4 or contains II_5, $\mathrm{II}'_{3,2}$ or III_6; and its pseudolines can be numbered, starting from a II_4 or a III_6, so that every partial arrangement is bigon-free.*

Proof. Four pseudolines in general position. $\mathcal{A}$ is not a near-pencil, since each pencil line of a near-pencil carries only the centre and its point on the transversal; so it has a simple crossing $p = a \cap b$ [26, Th. 3.6], see also [5, Th. 1.3]. Since a is not bigonal it carries vertices $q_1, \dots, q_k$ besides p, with $k \geq 2$. Take $c \neq a$ through q_i and $d \neq a$ through q_j, $i \neq j$. Then $\{a, b, c, d\}$ is in general position as soon as $c \cap b \neq d \cap b$: indeed c, d miss p, meet a at different points, and $c \cap d$ lies neither on a nor on b. If this fails for every choice, all these pseudolines meet b at one point r; two pseudolines meet only once, so each q_i lies on a and on a single other pseudoline c_i, all through r, and every pseudoline meets a at p or at some q_i. Then $\mathcal{A} = \{a, b, c_1, \dots, c_k\}$ and b carries only p and r, so it is bigonal, which is excluded.

The dichotomy. Let $Q \subset \mathcal{A}$ be four pseudolines in general position, and $\ell \in \mathcal{A} \smallsetminus Q$. If ℓ passes through none of the six vertices of Q, then $Q \cup \{\ell\}$ is a II_5; if through exactly one, a $\mathrm{II}'_{3,2}$. Otherwise ℓ passes through exactly two, which must be an opposite pair $\{x \cap y, z \cap w\}$ of the quadrilateral $Q = \{x, y, z, w\}$ (two vertices on a common side would force ℓ to be that side). Call such an ℓ a diagonal of Q; there are at most three. If $\mathcal{A}$ contains neither II_5 nor $\mathrm{II}'_{3,2}$, then $\mathcal{A}$ is Q plus some diagonals. One diagonal alone would be bigonal; two diagonals together with Q form a III_6 (the four triple points are the vertices of the quadrangle and the six pseudolines its sides); with three, $\mathcal{A}$ contains a III_6 again.

The numbering. Adding pseudolines never removes a vertex from a pseudoline already there, so it suffices that each pseudoline, when added, meets the earlier ones in at least three points.

A pseudoline meets the six sides of a III_6 in at least three points: its vertices have multiplicity at most three, and two triple points share a side, so two vertices cover at most five sides. So if $\mathcal{A} \supseteq \mathrm{III}_6$, start there and add the rest in any order. Otherwise $\mathcal{A}$ contains at most one diagonal δ of Q: start from Q, add every pseudoline other than δ (each meets Q in at least three points), and add δ last, when it has all its vertices in $\mathcal{A}$, at least three. □

This agrees with a computer enumeration of all arrangements of at most nine pseudolines (`computations/bigon`). The dichotomy is also checked in Lean for combinatorial maps (generalised maps of Euler characteristic 1 whose flags are labelled by the pseudolines; `lean/Grothendieck/Folder80Maps2.lean`, `map_dichotomy`); the numbering and the passage from a topological arrangement to its map are not formalised. We have not found the statement in print; it is elementary, and probably folklore among people who work on arrangements.

Q8 A problem stated in a lecture

One problem comes from the recordings of his 1973 courses at Buffalo rather than from the notes. On 11 July 1973, at the end of a lecture of the algebraic geometry course recorded on the second video of the course on algebraic groups, a listener having complained that he gave no open problems, he states one. It is not new: he had posed it in print twelve years earlier [23, §2, p. 212-05], and the lecture shows that he still held it open in 1973.

Problem 14 (Effectivity of finite equivalence relations on finite schemes over a field)**.** Let k be a field, X a finite k-scheme and $R \subset X \times_k X$ a closed equivalence relation (a subscheme whose points with values in any k-algebra form an equivalence relation), the projections $R \rightrightarrows X$ being finite but not necessarily flat. The quotient $Y = \mathrm{Spec}\big(\Gamma(X, \mathcal{O}_X)^R\big)$, the ring of R-invariant functions, exists in the category of schemes. Is R effective, that is, is $R \to X \times_Y X$ an isomorphism? More generally, the same question for X finite over a noetherian scheme.

Source. A. Grothendieck, course on algebraic groups (with algebraic geometry), State University of New York at Buffalo, video 2/2 of the « Erwin Schulhoff » YouTube channel, `https://www.youtube.com/watch?v=3ULFIl_2Wis`, 6:59:50–7:00:54 (lecture of 11 July 1973). He says it is not known, that he suspects the answer is no, that the question is « very elementary » and that nobody seems to have tried it seriously. Heard on the recording; the words are from its automatic captions, checked against a second transcription.

What is known. The question is in print: in 1961 he writes that, for finite schemes over S and without flatness, he does not know whether equivalence relations are always effective, that one reduces to S the spectrum of a local Artin ring with algebraically closed residue field, and that the answer is unknown even over a field [23, §2, p. 212-05]. For flat finite relations the quotient exists and is effective (SGA 3, exp. V [44]). Without flatness, the answer has been in print since 1971: Venken's note on the descent of flat modules [50] states, as its Corollary 3.1, that the ideal of $B \otimes_A B$ generated by $mxy \otimes w$, for a finite injection $A \to B$ of local Artin algebras over an arbitrary field K, $\dim_K B = 33$, is an equivalence ideal whose equivalence relation is not effective. This is a negative answer over every field, two years before the Buffalo lecture. Philippe studied descent along unramified morphisms [38]; Raicu gave finite equivalence

relations on $\mathbb{A}^2$ whose geometric quotient exists but which are not effective [30]. See the answer below. Kollár's question whether finite equivalence relations have geometric quotients in characteristic zero [30, Question 8] is a different question: for X finite over k the quotient exists.

Ideas. The question is about the finite-dimensional algebra $A = \Gamma(X, \mathcal{O}_X)$, the ideal I of R in $A \otimes_k A$ and the invariant subalgebra $B = A^R$: effectivity says that I is the ideal generated by the $b \otimes 1 - 1 \otimes b$, $b \in B$. Raicu's criterion (a 1-cocycle in the Amitsur complex of $B \to A$ that is not a coboundary) applies verbatim, so a search by computer over small local algebras, $A = k[x, y]/(x, y)^n$ for instance, is a natural first step; a counterexample would answer the question in the direction he expected.

Lean. Not attempted.

Answer. No, over every field: Venken's Corollary 3.1 [50], above. We checked it by linear algebra over every field (all pivots of the elimination over $\mathbb{Q}$ are ± 1): his relation satisfies the three axioms, its ring of invariants has dimension 10, and its ideal exceeds the ideal generated by the $b \otimes 1 - 1 \otimes b$ by one dimension in degree 4 (`computations/effective/venken`). A second example, of length 15 (16 in characteristic 2) in two variables, comes from Raicu's relation on $\mathbb{A}^2$, the ideal

$$I = \left(x_1^2 - y_1^2,\ x_1x_2 - x_2^2 - y_1y_2 + y_2^2,\ x_2^3 - y_2^3,\ (x_1y_2 - x_2y_1)\, y_2^3\right) \subset k[x_1, x_2, y_1, y_2]$$

[30, appendix, ¶50]: the functions $f_1 = x_1^2$, $f_2 = x_1x_2 - x_2^2$, $f_3 = x_2^3$ are invariant, and the restriction of R to $Z = V(f_1^2, f_2^2, f_3^2)$, of length 15 (16 in characteristic 2), is a closed equivalence relation whose ideal exceeds the one generated by the invariants in degree 5 ($52 > 51$), with $(x_1y_2 - x_2y_1)\, y_2^3$ as witness. The elimination over $\mathbb{Q}$ divides only by pivots whose prime factors are $2, 3, 5, 7, 13, 41$ and 61, and each of these characteristics was checked directly, so this example too holds over every field (`computations/effective/raicu`; both are written up in `https://github.com/Commutator-IO/grothendieck-project/blob/main/docs/effective/article.pdf`). A random search on 48 small monomial algebras over $\mathbb{F}_2$ and $\mathbb{F}_3$ had found nothing, which Raicu's exactness theorem for maps of monoid rings [31] may explain.

What would settle it. Settled by Venken in 1971. A specialist's check of the second example remains. The more general question, for X finite over a noetherian scheme, is answered by the same examples, a field being a noetherian base.

Q9 The large conjectures, and how the notes approach them

The thirteen problems above may not be in the literature. Seven conjectures of the notes are, under Grothendieck's name, and the companion paper lists where each first appears in the fonds [24]. This section reads the same pages for how he meant to prove them. For each conjecture it gives the statement in today's form, the pages, a draft of the route the pages take, where the route stops, and what is known now. The drafts are the edition's, made from the transcriptions with a language model. They report what the pages do, and say so when a step comes from the modernised reading instead. None of the seven is solved here, and no route is complete on the page.

Conjecture 1 (The standard conjectures)**.** Let X be smooth projective of dimension n over an algebraically closed field, with a Weil cohomology H and the Lefschetz operator L of an ample class. *Lefschetz type*: the inverse of $L^{n-i} : H^i(X) \to H^{2n-i}(X)$ is induced by an algebraic correspondence. *Hodge type*: on the primitive algebraic classes of $H^{2i}(X)$, $2i \leq n$, the form $(-1)^i\langle L^{n-2i}x, x\rangle$ is positive definite.

Source. folder 14, pp. 43–46, letter to Serre of 27 August 1965, printed in their correspondence; folder 14, pp. 105–113; folder 16, pp. 32–54, with letters to Coates (pp. 43–49), inventory dating 1966–1967; folder 12, pp. 158–166; folder 15, p. 169.

The route. The 1965 letter fixes the order of the argument. A Lefschetz condition on cycles gives a Künneth formula for cycles, hence characteristic polynomials of algebraic endomorphisms with integer coefficients, hence the Weil conjectures except the absolute values of the eigenvalues; the positivity gives the absolute values, and the two together make the motives semisimple. He says he can derive the full Lefschetz condition from a weak, restriction-type one, provided it holds over base fields that are not algebraically closed. Folder 16 then sets up an induction along hyperplane sections $\varphi : Y \hookrightarrow X$. The identity $\Lambda_Y = \varphi^*\Lambda_X^2\varphi_*$ (p. 39) gives $C(X) \Rightarrow C(Y)$, with C the Lefschetz-type conjecture; conversely, « Moyennant $C(Y)$, $C(X)$ équivaut à la condition » that $\Lambda_X\varphi_*$ be algebraic (p. 41), which is the Lefschetz condition on $X \times Y$ in the critical degree only. Iterating down a chain of sections reduces C for all varieties to that critical condition for all varieties (pp. 44–45); Problem 5 is the next step, which splits the critical condition into two one-sided ones (p. 49). A letter to Coates gives a second reduction (pp. 47–48): $C(X)$ follows from integral characteristic polynomials and the existence of *some* algebraic isomorphism $H^{2n-i} \to H^i$, by Cayley–Hamilton. For positivity the route goes through algebras: the rings $\mathrm{End}(h^i(X))$ should carry a positive involution, hence be semisimple, hence the motives form a semisimple abelian category (folder 12, p. 158; folder 16, p. 48); and one line proposes « Positivité à la Hodge en se ramenant à des questions de diviseurs » by induction (folder 15, p. 169).

Where it stops. The letter of 1965 misses a way of moving a cycle to infinity in the affine complement $X \smallsetminus Y$, which the weak-to-full step needs. The letter to Coates says of the induction: « Thus the main problems arise already for 1-cycles on threefolds » (folder 16, p. 46). The 1965 conditions are stated modulo algebraic equivalence, and in that form they are false (Griffiths), as the modernised reading notes. For positivity there is only the one line of folder 15.

Today. Open in general. The Lefschetz type is known for curves, surfaces and abelian varieties [27], and the Hodge type in characteristic 0 by the Hodge–Riemann relations. Over $\mathbb{C}$, Arapura proves the Lefschetz type for every variety motivated by curves or surfaces in André's sense, among them uniruled threefolds and unirational fourfolds [2, Cor. 4.3], and for Hilbert schemes of points on a surface and moduli spaces of stable bundles on a curve, under the conditions stated there [2, Cor. 7.2, 7.5]. Beilinson shows that in characteristic 0 the standard conjectures follow from the existence of a motivic t-structure [4, §1.4–1.5], and that over $\mathbb{C}$ they are equivalent to a weak form of Suslin's conjecture on Lawson homology [4, §2.2, Prop.]. One step of his proof, over $\mathbb{C}$ with rational coefficients, is the reduction of the letter to Coates: if for each $i > 0$ some correspondence c induces an isomorphism $H^{n+i} \to H^{n-i}$, the Lefschetz type holds, the inverse of L^i being $f(A)\,c$ for $A = c \circ L^i$ and a polynomial f with $f(A)A = 1$ on H^{n-i} [4, §2.3, proof of (b)]. Deligne proved the Weil conjectures without them. An OpenAI preprint of

6 October 2026, not peer-reviewed and not formalised, announces the Hodge conjecture for complex abelian varieties with complex multiplication and deduces the Hodge type for abelian varieties in every characteristic [37].

Conjecture 2 (The generalised Hodge conjecture, in its ℓ-adic form)**.** For X smooth projective, the coniveau filtration $\mathrm{Filt}^j H^i(\bar{X}, \mathbb{Q}_\ell)$, made of the classes that vanish on the complement of a closed subset of codimension $\geq j$, is the realisation of the largest sub-motive of $h^i(X)$ of level $\leq i - 2j$.

Source. folder 12, pp. 2–3, 41–42, 52–54, inventory dating 1964–[c. 1971]; folder 36, pp. 12, 16. The pages do not name the conjecture; the name is the reading's.

The route. Page 3 states the expected equality and draws its consequence, granting resolution of singularities and the standard conjectures « (conséquence de la résolution et des conjectures standard) »: the dimensions of the $\mathrm{Filt}^j H^i$ are independent of ℓ, since traces of motivic endomorphisms are rational and independent of ℓ (pp. 29–30). One inclusion comes from the coniveau spectral sequence, read at E_1: for X smooth projective the classes supported in codimension p are Gysin images, of level $\leq n - 2p$ (p. 41). For the level itself, pp. 52–54 read weight and effectivity on the eigenvalues of Frobenius, and folder 36 applies this after reduction to a finite field: a piece of level 1 has eigenvalues divisible by q^{n-1}, so a p-adic unit eigenvalue shows that a piece is not of level 1 (p. 16).

Where it stops. The reverse inclusion, that the largest sub-motive of low level lies in the coniveau filtration, is never argued, and the Frobenius characterisation of p. 54 is struck. In folder 36 he cannot show, even granting the standard conjectures, that the level of a motive can only drop under specialisation: « la triste vérité est que je ne sais pas » (p. 16).

Today. Open. Grothendieck's 1969 paper corrected Hodge's general conjecture of 1950, which is false, into this form. In its Hodge-theoretic form, that the coniveau filtration equals the largest Hodge substructures of bounded level, it holds for all powers of the Jacobian of a very general complex curve of genus ≥ 2 [2, Prop. 6.5]. The OpenAI preprint on abelian varieties with complex multiplication deduces it for them, not beyond [37].

Conjecture 3 (The period conjecture)**.** Over $\overline{\mathbb{Q}}$, the functor that sends a motive to its de Rham realisation, its Betti realisation and the comparison isomorphism between them is fully faithful. In the form of Bost and Charles, the comparison isomorphism is Zariski-dense in the torsor of motivic periods, so that the periods of a motive generate a field of transcendence degree equal to the dimension of its motivic Galois group [6, Conj. 2.12]; with the standard conjectures, this form implies the first [6, Prop. 2.13].

Source. folder 13, *Groupe de Galois motivique*, pp. 30–34, 47–51, dated 1965; folder 18, pp. 10–12, 41–50, inventory dating 1969–[c. 1972]. An undated plan headed « Motifs » (IHÉS, fonds Grothendieck–Illusie, 2ILL5, p. 8) states an arithmetic variant, marked « (de Groth.) », perhaps in another hand: for X of finite type over $\mathbb{Z}$, the functor that sends a motive to its de Rham realisation on $X_{\mathbb{Q}}$ and its crystalline realisations with Frobenius at every p, in place of the Betti realisation, is fully faithful.

The route. Folder 13 starts from a negative observation: the algebraic data of a realisation do not say which Hodge data come from motives, and must be completed by conditions of the type « arg. de transcendance » (p. 31). Pages 33–34 prove an abstract lemma: if g places the second lattice and H is the group generated by the closure of the elements ts^{-1}, then $V \cap T'(V) = V^H$, so full faithfulness becomes $V^H = V^G$ for every representation V. Page 47 asks the question without filtration or Hodge structure, reduces it at once to $\overline{\mathbb{Q}}$ and to V simple, and settles rank one: « c'est une puissance de Tate, et ça marche ». Folder 18 turns it into transcendence: the field generated by a generic period point has transcendence degree $\dim G - 1$ for a group G attached to the motive (p. 11), which « contient le th. de Schneider » for elliptic curves without complex multiplication; elliptic curves are the test case (p. 12), and pp. 46–50 sketch an adelic analogue.

Where it stops. No non-Tate motive is treated. For a product of two non-isogenous elliptic curves without complex multiplication his bound gives at most 5 against the expected 6 (folder 18, p. 44). Over a field of finite type the functor is not fully faithful, and the page breaks off on « idiot ! » before hoping for a weaker result (folder 13, p. 48).

Today. Open. For a Weierstrass function with algebraic invariants, two of $\omega_1, \omega_2, \eta_1, \eta_2$ are algebraically independent, and so are π/ω and η/ω for any period ω and its quasi-period η [11, §2 A, Th. 1 and 3]. For an elliptic curve with complex multiplication this proves the conjecture, the periods and quasi-periods having transcendence degree 2; Bost and Charles cite it as the main known case [6, §2.2.2]. Without complex multiplication, the expected degree 4 is open. The conjecture's consequence for classes, that a class of degree $2k$ rational in both the Betti and the de Rham structure (up to $(2\pi i)^k$) is algebraic, is proved in codimension 1 for products of curves, abelian varieties and K3 surfaces, and in codimension 2 for cubic fourfolds [6, Cor. 3.9, 3.10, Th. 5.6]. A Lean statement of the elliptic case is in the Tau Ceti roadmap on elliptic periods.

Conjecture 4 (The homotopy hypothesis)**.** n-groupoids, up to n-equivalence, are the same as homotopy n-types, and ∞-groupoids the same as homotopy types.

Source. folder 134-2, pp. 42–46, postscript of a letter to Breen of 5 February 1975; pp. 48–51, letter of 17 February; pp. 145–149 and 167–170, French original of the letter of July 1975; folder 134-1, p. 6, letter to Deligne of 27 August 1974.

The route. To a Kan complex K he attaches an n-category $C_n(K)$ of points, paths and homotopies, the top level taken up to homotopy, and notes that $\pi_i(K) \cong \pi_i(C_nK)$ for $i \leq n$ almost by definition (pp. 42–43); the two localised categories should then be equivalent. He uses the hypothesis to choose the definitions: the yoga « pourrait constituer un fil d'Ariane » for defining non-strict n-categories, their functors and their equivalences (p. 43). He checks the dictionary on familiar constructions (p. 45): loops and $\mathrm{Hom}(x, x)$, mapping spaces and functor categories, homotopy fibres and fibre products, $K(\pi, n)$ and n-gerbes, truncation and classes of top arrows. The abelian case comes first: strict Picard n-categories should be complexes of length n, and the correspondence between simplicial sets and ∞-groupoids a set-theoretic Dold–Puppe (pp. 146–147); for groups in n-categories he wants a « non-commutative chain complex », and for $n = 1$ gives crossed modules with their invariant in H^3 (pp. 148–149). The functor from simplicial sets to n-groupoids is not negotiable: a theory without it « me semblerait

canularesque » (p. 146). On the topos side, locally constant stacks on X should be functors on $\Pi_n(X)$, and Π_n recovered from them as in Galois theory (pp. 48–51, 167–170).

Where it stops. Nothing is proved: the definition of non-strict n-categories is the missing piece, and he writes of the « inquiétant mirage » of n-limits (p. 169, reading uncertain). He cannot define the classifying topos of an n-gerbe for $n \geq 2$ (p. 45), and asks Breen for candidates for the non-abelian complexes. *Pursuing Stacks* (1983), not transcribed in the edition, takes the programme up with coherators and test categories.

Today. The answer depends on the model. It is false for strict n-groupoids from $n = 3$: for any realisation functor that preserves homotopy groups, no strict 3-groupoid realises the 3-type of S^2, and no strict ∞-groupoid realises S^2 [46, Prop. 5.1, Cor. 6.1]. Simpson conjectured that strictly associative composition with weak units suffices [46, §7, Conj. 1]; Henry proves a form of this for ∞-groupoids in which only the « regular » compositions are strict [20, §§6.1–6.3]. For Grothendieck's globular ∞-groupoids in Maltsiniotis's formulation it is open. Henry reduced it, for a fixed coherator, to one statement: on a finitely cellular ∞-groupoid, freely adding a cell parallel to an n-cell and an $(n+1)$-cell between them is a weak equivalence [19, Conj. 5.3.3, Cor. 5.3.13]. An OpenAI preprint of 24 September 2026, not peer-reviewed, announces a proof for the Ara–Henry coherators, of which only the elementary-expansion step is formalised in Lean [37].

Conjecture 5 (The section conjecture)**.** For a hyperbolic curve U over a field K of finite type over $\mathbb{Q}$, every section of $\pi_1(U) \to \mathrm{Gal}(\bar{K}/K)$ comes, up to conjugacy, from a rational point of U or from a rational point at infinity.

Source. folder 149, pp. 26–127, undated: Theorem 3 (pp. 31–33), the « Conjecture fondamentale » (p. 47), Conjectures A, B and B′ (pp. 55–62), relative curves (pp. 63–64, where « Nos conjectures impliquent donc qu'il y a exactement deux sortes de telles sections »), specialisation (pp. 69–98), the birational form (pp. 123–127); folder 142, pp. 79–81.

The route. Only injectivity is proved, and arithmetically: he first tried a geometric proof, « Finalement, je n'arrive pas à le prouver par voie géométrique » (p. 26). He reduces to a semi-abelian variety and the Kummer sequences for all n; a point with trivial class is infinitely divisible, hence zero since the group of rational points is finitely generated (pp. 31–33), and one prime ℓ is not enough (p. 33). The section conjecture is the case « V a point » of his conjecture on morphisms (p. 48). The rest of the folder reformulates the conjecture. Sections at a cusp are told from rational points by filling the hole (p. 54). Conjecture B recasts the statement as a fixed point: the action of the Galois group on the universal cover completed by its cusps has « un pt fixe et un seul » (p. 58). Over a model the sections become lifts to $\pi_1(S)$, and a local criterion says that a rational point extends over a discrete valuation ring exactly when its section kills the inertia (p. 73); this compares sections over K and over the residue fields. Pages 98–103 try to build counterexamples from bad reduction, without success.

Where it stops. No route to surjectivity appears. Mordell's conjecture, which Faltings proved in 1983, is never used; the only arithmetic input is the Mordell–Weil theorem, for injectivity. The case of the thrice-punctured sphere at a cusp rests on a relation the page calls « hautement plausible » (p. 60). On reduction he writes that he has no idea for the moment (p. 102), and the explicit cocycle of a point is called fascinating work not yet begun (folder 142, p. 81).

Today. Open. Injectivity is known, as are a birational p-adic form (Koenigsmann) and the real analogue. An OpenAI preprint (24 September and 6 October 2026), not peer-reviewed and not formalised, announces the local p-adic conjecture for curves of genus at least 2, and the global one over number fields when a descent locus equals the rational points, which covers $X_0(N)$ and $X_1(N)$ of genus at least 2 over $\mathbb{Q}$; the affine, cuspidal form of folder 149 is not claimed [37].

Conjecture 6 (Ihara's question: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the Teichmüller tower)**.** The outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the profinite fundamental groups of the moduli spaces $M_{g,\nu}$ identifies it with the automorphisms of the tower that respect its structure; in Drinfeld's form, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{GT}$ is an isomorphism.

Source. folder 142, pp. 12–16, 21–41, 86–100, inventory dating [from 1978]; folder 143, pp. 28–30; folder 145, pp. 4–37; folder 147, pp. 59, 103, 148–151; folder 144, p. 4; folder 146; folder 67, p. 49, January 1984.

The route. The target is stated in folder 143: « On aimerait » that $\pi_1(M_{g,\nu})$ map isomorphically onto the outer automorphisms of the profinite surface group that satisfy the loop condition, which would describe the Galois group through them (p. 29). Folder 142 reduces the action on any curve to the thrice-punctured sphere, by Belyi and a Lefschetz-type curve (pp. 86–88), and lists the necessary conditions for an automorphism of the profinite groupoid to come from Galois: it lifts to the covers, stabilises the kernels of morphisms, is compatible with morphisms between covers, and satisfies the loop condition, « sûrement la plus importante de toutes, de très loin ! » (p. 99). He conjectures them sufficient for one curve (pp. 94–95, Problem 12). Since the first conditions cannot be written down directly in the parameters (p. 98), he turns to the moduli spaces, with a conjecture tied to $M_{0,4}$ and $M_{0,5}$ that the page announces and that is nearly illegible (pp. 98–99). The low levels are computed: automorphisms commuting with $\mathfrak{S}_3$ as triples satisfying one relation (folder 142), pairs (p, g) with a marginal « $= \chi(u)$ » (folder 145), presentations in modular dimension 0 and 1 (folder 146). Folder 147 then plans the discrete tower: a more or less complete understanding of the cases of modular dimension at most 2 « donnera la clef pour une compréhension complète dans le cas général » (p. 59), a programme to present all the groups and their maps by generators and relations (p. 103), and a gluing theorem at infinity over the strata of codimension 1 and 2 (pp. 149–151, Problem 13).

Where it stops. The sufficiency of the conditions, the $M_{0,4}$–$M_{0,5}$ conjecture, the programme of folder 147 and the gluing theorem are announced, not proved. Page 59 of folder 147 speaks of the discrete groups, in the analytic setting; reading it as the two-level principle for the Galois action is the edition's. The last step, that an automorphism satisfying the relations of the tower comes from Galois, is not attempted anywhere in the notes.

Today. Open; the map is injective by Belyi's theorem. Hatcher, Lochak and Schneps add to the relations of $\widehat{GT}$ with $\lambda = 1$ one relation in the profinite mapping class group of genus 1 with two boundary components, and show that the subgroup Λ it defines acts on every $\widehat{\Gamma}^m_{g,n}$, compatibly with the homomorphisms induced by the inclusions of subsurfaces, and injects into the special outer automorphisms of that tower [21, Th. A–C]. The relations defining Λ live in modular dimension 1 and 2, so relations on the first two levels already give an action on the whole tower, in all genera. On the motivic side, Brown proved that the motivic Galois group of

mixed Tate motives over $\mathbb{Z}$ acts faithfully on the motivic fundamental group of $\mathbb{P}^1 \smallsetminus \{0,1,\infty\}$, and notes that this implies the Deligne–Ihara conjecture on the outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on its pro-ℓ fundamental group [9, §1, Conj. 1, Th. 1.1]. An OpenAI preprint of 23 September 2026, not peer-reviewed, announces the Deligne–Drinfeld conjecture, that the rational Grothendieck–Teichmüller Lie algebra is free on one generator in each odd weight ≥ 3; it does not touch Ihara's question [37].

Conjecture 7 (The p-curvature conjecture)**.** Let S be integral, of finite type and dominant over $\operatorname{Spec}\mathbb{Z}$, X/S smooth, and E a vector bundle on X with an integrable connection. If the p-curvature of E vanishes at almost all closed points of S, then E has finite monodromy at the generic point.

Source. folder 93, pp. 188–212, *Connexions de Gauss–Manin et équations de Picard–Fuchs*, inventory dating [1972]–1981. No other folder has it.

The route. Page 194 notes, without proof, that finite monodromy forces vanishing p-curvature at almost all closed points, and asks: « La réciproque est-elle vraie ? » It then splits rank one: « La question précédente se décompose en deux ». First, is the class of E in the Picard group torsion? If so, $E = \mathcal{O}_X$ with connection $d + \omega$, and the question becomes whether a closed form that is locally logarithmic at almost all primes has a multiple that is logarithmic. In characteristic 0 the target is explicit: the logarithmic forms are a group $\mathbb{Z}^r$ by Rosenlicht, so the integrable classes form $(\mathbb{Q}/\mathbb{Z})^r$ (pp. 191–192). Pages 195–197 extend the question to torsors under group schemes, and for an abelian scheme rewrite it on the universal vector extension of the dual: a section that is divisible by p at every closed point, is it of finite order? He reduces it to a local-global statement about connected subgroups, and the case of unipotent rank 0 is the one on which, « si ce résultat était acquis », everything reduces to the semi-abelian case. Pages 198–212 compute the condition $\tilde{C}\omega = \tilde{\omega}$ on the Cartier operator and the Verschiebung of the Picard functor with connection; that these serve the question is our reading, not the page's.

Where it stops. The converse and each of its reductions stay questions. There is no Gauss–Manin case, no Chebotarev argument and no reduction to curves in the notes.

Today. Open. Katz proved it for Gauss–Manin connections (1972), and it holds for connections with solvable monodromy, rank one included (Chudnovsky for curves, André, Bost).

Q10 How the list was made, and its limits

The thirteen problems were chosen from the register of findings among the rows still open and outside what Lean reached, and with a statement precise enough to be proved or refuted. Rows whose only interest is a slip on the page, a dating, or a statement now known to be in print were left out, as were the conjectures already in the published record, which §Q9 treats from the side of the routes the notes take, and the companion paper from the side of their first appearance [24].

Three limits apply to every entry. The transcriptions are first passes by a language model, and doubtful readings are marked but not all checked against the facsimile; a statement may rest on a misread word, and the entries say where we know this. The literature searches were

made by the same means, with full texts where they were open and abstracts otherwise; an entry that says « not found » reports a search, not an absence. And the steps marked « ours » have not been checked by a specialist.

Corrections, references and proofs are welcome at the address above. The Lean files are in the repository `https://github.com/Commutator-IO/grothendieck-project`, directory `lean/`.

Changes

26 October 2026: the pseudoline dichotomy of folder 80 proved (§Q7); the count of Kostant quadruples derived, and Problem 7 replaced by the question Grothendieck asked Kostant; Problem 4 narrowed after Breen's 1975 theorem; references corrected after a citation check. 29 October 2026: §Q9 added, on the routes the notes take to seven published conjectures; the arguments for Problems 5 and 6 written out step by step, with what a specialist should check; Problem 5 narrowed to the condition $A^0(Y_T)$, after a Lean proof of the two cases of the splitting; the OpenAI preprints on four of the seven conjectures noted. 31 October 2026: the problem on bigon-free arrangements answered for every bigon-free arrangement, three pencils included, by a sign argument on chirotopes and the Folkman–Lawrence theorem; the sign argument and its rank-2 step proved in Lean, Folkman–Lawrence left outside; the sources of §Q9 completed from the texts read (issue #102). 1 November 2026: Problem 10 updated after Grothendieck's letter to Breen of 5 February 1975 (IHÉS, 1ILL21), which withdraws the « universal » argument of 1974, and what would settle it restated; the letter to Giraud of 1969 added to the source of Problem 4; the full-faithfulness conjecture of the IHÉS plan « Motifs » (2ILL5) added to the source of Conjecture 3. The Buffalo problem added (§Q8), from the recording of his Buffalo lecture of 11 July 1973, with its first statement in print (1961). 5 November 2026: the problem on bigon-free arrangements and their skeleton removed (it was Problem 14 in the earlier versions); the Buffalo problem is now Problem 14.

Declaration

This note was drafted with a language model (Claude Opus 5.5, Anthropic) from the edition's registers: the findings, the modernised readings and the Lean files. The transcriptions and the modernised readings it relies on were also made with language models (Claude Opus 5 and Opus 5.5). The author received no funding for this work.

References to the second part

[Q1] Y. André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthèses 17, SMF, 2004.

[Q2] D. Arapura, Motivation for Hodge cycles, *Adv. Math.* 207 (2006), 762–781; statements numbered as in arXiv:math/0501348v3.

[Q3] H.-J. Baues, *Homotopy Type and Homology*, Oxford Mathematical Monographs, 1996.

[Q4] A. Beilinson, Remarks on Grothendieck's standard conjectures, in *Regulators*, Contemp. Math. 571, AMS, 2012, 25–32, arXiv:1006.1116.

[Q5] J. Bokowski, P. Pokora, On the Sylvester–Gallai and the orchard problem for pseudoline arrangements, *Period. Math. Hungar.* 77 (2018), 164–174, arXiv:1607.05864.

[Q6] J.-B. Bost, F. Charles, Some remarks concerning the Grothendieck period conjecture, *J. reine angew. Math.* 714 (2016), 175–208; statements numbered as in arXiv:1307.1045v2.

[Q7] L. Breen, Un théorème d'annulation pour certains Ext^i de faisceaux abéliens, *Ann. Sci. ÉNS* (4) 8 (1975), 339–352.

[Q8] L. Breen, Monoidal categories and multiextensions, *Compositio Math.* 117 (1999), 295–335, arXiv:math/9809104.

[Q9] F. Brown, Mixed Tate motives over $\mathbb{Z}$, *Ann. of Math.* 175 (2012), 949–976, arXiv:1102.1312.

[Q10] O. Caramello, De Morgan classifying toposes, *Adv. Math.* 222 (2009), 2117–2144, arXiv:0808.1519.

[Q11] G. V. Chudnovsky, Algebraic independence of values of exponential and elliptic functions, in *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, vol. 1, Acad. Sci. Fennica, 1980, 339–350.

[Q12] D. Clausen, A. Mathew, Hyperdescent and étale K-theory, *Invent. Math.* 225 (2021), 981–1076, arXiv:1905.06611.

[Q13] B. Collas, Anabelian perspectives in Galois-Teichmüller theory, arXiv:2603.02848, 2026.

[Q14] A. H. Durfee, Mixed Hodge structures on punctured neighborhoods, *Duke Math. J.* 50 (1983), 1017–1040.

[Q15] P. T. Johnstone, *Sketches of an Elephant: A Topos Theory Compendium*, 2 vols, Oxford Logic Guides 43–44, Oxford, 2002.

[Q16] R. Friedman, R. Laza, The higher Du Bois and higher rational properties for isolated singularities, *J. Algebraic Geom.* 33 (2024), 493–520, arXiv:2207.07566.

[Q17] O. Gabber, F. Orgogozo, Sur la p-dimension des corps, *Invent. Math.* 174 (2008), 47–80, arXiv:0706.0671.

[Q18] O. Gabber, B. Zavyalov, Algebraization techniques and rigid-analytic Artin–Grothendieck vanishing, *Ann. Sci. ÉNS* 59 (2026), 387–436, arXiv:2402.08741.

[Q19] S. Henry, Algebraic models of homotopy types and the homotopy hypothesis, preprint, 2016, arXiv:1609.04622.

[Q20] S. Henry, Regular polygraphs and the Simpson conjecture, preprint, 2018, arXiv:1807.02627.

[Q21] A. Hatcher, P. Lochak, L. Schneps, On the Teichmüller tower of mapping class groups, *J. reine angew. Math.* 521 (2000), 1–24.

[Q22] P. Deligne, Théorie de Hodge III, *Publ. Math. IHÉS* 44 (1974), 5–77.

[Q23] A. Grothendieck, Techniques de construction et théorèmes d'existence en géométrie algébrique III : préschémas quotients, Séminaire Bourbaki 6 (1960/61), exp. 212, 99–118, `http://www.numdam.org/item/SB_1960-1961__6__99_0`.

[Q24] M. Hua, Formalising a mathematician's working notes: Lean proofs from the Grothendieck archive, preprint, 2026.

[Q25] L. Illusie, Revisiting deformations of truncated Barsotti–Tate groups, talk notes, Chicago, 6 March 2023, `https://www.imo.universite-paris-saclay.fr/~luc.illusie/Illusie-Chicago-2023-1.pdf`.

[Q26] L. M. Kelly, R. Rottenberg, Simple points in pseudoline arrangements, *Pacific J. Math.* 40 (1972), 617–622.

[Q27] S. L. Kleiman, Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. 3, North-Holland, 1968, 359–386.

[Q28] A. Kock, I. Moerdijk, Every étendue comes from a local equivalence relation, *J. Pure Appl. Algebra* 82 (1992), 155–174.

[Q29] A. Kock, I. Moerdijk, Spaces with local equivalence relations, and their monodromy, *Topology Appl.* 72 (1996), 47–78.

[Q30] J. Kollár, Quotients by finite equivalence relations, with an appendix by C. Raicu, in *Current Developments in Algebraic Geometry*, MSRI Publ. 59, Cambridge University Press, 2012, 227–256, arXiv:0812.3608.

[Q31] C. Raicu, Affine toric equivalence relations are effective, *Proc. Amer. Math. Soc.* 138 (2010), 3835–3847, doi:10.1090/S0002-9939-2010-10416-1, arXiv:0905.4805.

[Q32] B. Kostant, The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math.* 81 (1959), 973–1032.

[Q33] A. Mathew, On $K(1)$-local TR, *Compositio Math.* 157 (2021), 1079–1119, arXiv:2005.08744.

[Q34] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006.

[Q35] I. Moerdijk, Foliations, groupoids and Grothendieck étendues, *Rev. Acad. Cienc. Zaragoza* (2) 48 (1993), 5–33.

[Q36] S. Mukai, Duality between $D(X)$ and $D(\hat{X})$ with its application to Picard sheaves, *Nagoya Math. J.* 81 (1981), 153–175.

[Q37] OpenAI, `openai/math`, repository of manuscripts and Lean files, `https://github.com/openai/math`, folder `preprints`, read on 17 and 26 October 2026; none of the manuscripts is peer-reviewed.

[Q38] A. Philippe, Morphisme net d'anneaux, et descente, *Bull. Sci. Math. (2)* 97 (1973), 57–64.

[Q39] B. Poonen, M. Stoll, The Cassels–Tate pairing on polarized abelian varieties, *Ann. of Math.* 150 (1999), 1109–1149.

[Q40] F. Pop, Finite tripod variants of I/OM: on Ihara's question/Oda–Matsumoto conjecture, *Invent. Math.* 216 (2019), 745–797.

[Q41] K. I. Rosenthal, Sheaves and local equivalence relations, *Cahiers Top. Géom. Diff.* 25 (1984), 179–206.

[Q42] M. Saito, Mixed Hodge modules, *Publ. RIMS* 26 (1990), 221–333.

[Q43] C. Scheiderer, *Real and Étale Cohomology*, Lecture Notes in Math. 1588, Springer, 1994.

[Q44] M. Demazure, A. Grothendieck (eds.), *Schémas en groupes* (SGA 3), LNM 151, 152, 153, Springer, 1970.

[Q45] M. Artin, A. Grothendieck, J.-L. Verdier (eds.), *Théorie des topos et cohomologie étale des schémas* (SGA 4), LNM 269, 270, 305, Springer, 1972–1973.

[Q46] C. Simpson, Homotopy types of strict 3-groupoids, preprint, 1998, arXiv:math/9810059.

[Q47] T. A. Springer, Regular elements of finite reflection groups, *Invent. Math.* 25 (1974), 159–198.

[Q48] F. Tonini, Stacks of ramified Galois covers, PhD thesis, 2013, arXiv:1307.1116.

[Q49] F. Tonini, Ramified Galois covers via monoidal functors, *Transform. Groups* 22 (2017), 845–868, arXiv:1507.05309.

[Q50] J. Venken, Non effectivité de la descente de modules plats par un morphisme fini d'anneaux locaux artiniens, *C. R. Acad. Sci. Paris Sér. A* 272 (1971), A1553–A1554.