The Watermark and Double Ladder Theorems

The discriminant group of the Néron–Severi lattice of a Fermat surface of prime degree

Rafael Amichis Luengo

Madrid, Spain · tretoef@gmail.com · ORCID 0009-0008-6252-675X · 25 November 2026

Abstract

Let $S_p \subset \mathbb{P}^3$ be the complex Fermat surface $x_0^p + x_1^p + x_2^p + x_3^p = 0$ of prime degree $p \geq 5$. Its Néron–Severi lattice $\mathrm{NS}(S_p)$ is generated by the classes of the $3p^2$ lines on S_p (Schütt–Shioda–van Luijk, Degtyarev). We prove that

$$|\operatorname{disc} \mathrm{NS}(S_p)| = p^{3(p-3)^2} \qquad \text{(the Watermark Theorem)},$$

which answers formula (7.10) of Shioda's Question 7.4 (1987) for every prime $p \geq 5$, and we determine the discriminant group itself:

$$\mathrm{NS}(S_p)^* / \mathrm{NS}(S_p) \;\cong\; \begin{cases} (\mathbb{Z}/p)^{3p^2-24p+59} \times (\mathbb{Z}/p^2)^{3p-16}, & p \geq 7, \\ (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25, & p = 5 \end{cases}$$

(the Double Ladder Theorem). The transcendental lattice of S_p has the same discriminant group. The proofs work with the explicit integer intersection matrix G of the lines and use elementary lattice arithmetic. For the order, G acts by multiples of p on functions pulled back along the $p+1$ pencils of parallel lines of $\mathbb{F}_p^2$, its kernel contains an explicit sublattice of index p^{12}, and two index computations conclude. For the group, an identity $GYG = 6p^2G$ with an explicit integer matrix Y bounds the exponent by p^2, and G modulo p factors through twelve functions of one variable, which gives its rank $12(p-3)$ (26 at $p=5$). On the level $\nu \leq 3$ of a filtration by vanishing moments of degree $< \nu$, the rank of the form modulo p is $12(p-3) - 3\nu(\nu+1)$ for $p \geq 7$; this is not needed in the proofs. The lattice statements of both theorems are checked in Lean 4 with Mathlib; the identification of G with the intersection matrix of the lines is proved by hand.

hexagon:2610.00231v2

1 Introduction

The Néron–Severi lattice of the Fermat surface has been a test case for the theory of algebraic cycles since Shioda's work on Fermat varieties [8, 18, 20]. For $m \geq 1$ let $S_m \subset \mathbb{P}^3(\mathbb{C})$ be the Fermat surface $x_0^m + x_1^m + x_2^m + x_3^m = 0$; for $m \geq 3$ it contains exactly $3m^2$ lines. For $m \leq 4$ or $\gcd(m,6) = 1$ their classes span $\mathrm{NS}(S_m) \otimes \mathbb{Q}$ [19] (see [15, §3]), and for $\gcd(m,6) = 1$ they generate $\mathrm{NS}(S_m)$ over $\mathbb{Z}$: Schütt, Shioda and van Luijk proved this for $m \leq 100$ [15], and Degtyarev for every such m [10]. Shimada and Takahashi gave a general method for the primitive closure of the lattice generated by given curves on a surface, motivated by Shioda's question whether the lines generate $\mathrm{NS}(S_m)$, and applied it to cyclic coverings of $\mathbb{P}^2$ branched along four lines [17, Theorems 1.2 and 1.4]. From now on $p \geq 5$ is a prime; then $\rho(S_p) = 3(p-1)(p-2)+1$ [8, 19].

At the end of [20] (§7, pp. 133–134) Shioda asked whether $|\det \mathrm{NS}| = p^{3(p-3)^2}$ for the Fermat surface of prime degree p: in Question 7.2 for the surface over a field of characteristic $r \equiv 1 \pmod p$, and in Question 7.4, formula (7.10), for the complex surface. Schütt, Shioda and van Luijk computed the determinant of the intersection form on their basis of lines for every odd $m \leq 81$ and found $m^{3(m-3)^2}$ [15, end of §4]. In 2015 Shioda still used the formula as expected, inside Conjecture 23 of [21]. Aljovin, Movasati and Villaflor computed by machine the elementary divisors of the lattice of the lines for $3 \leq m \leq 14$ [1, Table 1]; for $p = 5, 7, 11, 13$ their rows are

$$1^{26}\,5^{10}\,25, \qquad 1^{48}\,7^{38}\,49^{5}, \qquad 1^{96}\,11^{158}\,121^{17}, \qquad 1^{120}\,13^{254}\,169^{23},$$

whose products are $p^{3(p-3)^2}$. We did not find a proof of the formula for general prime p, nor a description of the group for general p, in the works we consulted; in particular Degtyarev [10], who proves that the lines generate, and Degtyarev–Shimada [11], who study the same primitivity question for the standard subspaces of Fermat varieties of higher dimension by a different method (Pham polyhedra), do not compute the discriminant (§11).

Theorem 1 (Watermark Theorem: the order of the discriminant)**.** *For every prime $p \geq 5$, the lattice V spanned by the classes of the $3p^2$ lines of S_p, with the intersection form, is free of rank $3(p-1)(p-2)+1$ and the Gram matrix of every $\mathbb{Z}$-basis of V has determinant $p^{3(p-3)^2}$. Hence $|\operatorname{disc} \mathrm{NS}(S_p)| = p^{3(p-3)^2}$.*

Theorem 2 (Double Ladder Theorem: the discriminant group)**.** *For every prime $p \geq 7$,*

$$V^*/V \;\cong\; (\mathbb{Z}/p)^{3p^2-24p+59} \times (\mathbb{Z}/p^2)^{3p-16},$$

and $V^*/V \cong (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25$ for $p = 5$. Here $V^* = \operatorname{Hom}(V, \mathbb{Z})$, and $V \subset V^*$ through the form.

Since $V = \mathrm{NS}(S_p)$, Theorem 2 is the discriminant group of the Néron–Severi lattice; Theorem 1 gives its order. The sign of the determinant in Theorem 1 is $+$: the form has signature $(1, \rho-1)$ and $\rho - 1 = 3(p-1)(p-2)$ is even.[1] The four rows of [1, Table 1] quoted above are Theorem 2 at $p = 5, 7, 11, 13$.

Scope. Theorem 1 answers Shioda's Question 7.4, formula (7.10), for every prime $p \geq 5$. We do not treat Question 7.2, in characteristic $r \equiv 1 \pmod{p}$: it would require that the lines generate the Néron–Severi group of the reduction of S_p modulo r, which we do not prove; the lines of the reduction have the same intersection matrix G, so Theorem 1 gives the discriminant of the lattice they span. (For $p = 3$ formula (7.10) is classical, $|\det \mathrm{NS}(S_3)| = 1$; formulas (7.12)–(7.13), on the product of two Fermat curves, are not treated.)

Corollary 3. *For every prime $p \geq 5$ the transcendental lattice $T_p = \mathrm{NS}(S_p)^\perp \subset H^2(S_p, \mathbb{Z})$ has rank $(p-1)(p-3)^2$ and $T_p^*/T_p \cong V^*/V$; in particular $|\operatorname{disc} T_p| = p^{3(p-3)^2}$.*

Proof. $H^2(S_p, \mathbb{Z})$ is torsion free and unimodular, since S_p is simply connected (Lefschetz) and by Poincaré duality, and $\mathrm{NS}(S_p) = H^2(S_p, \mathbb{Z}) \cap H^{1,1}$ is a primitive sublattice, so the discriminant groups of $\mathrm{NS}(S_p)$ and of its orthogonal complement are isomorphic: for a primitive sublattice M of a unimodular lattice L the projections give $M^*/M \cong L/(M \oplus M^\perp) \cong (M^\perp)^*/M^\perp$ (cf. [14, Prop. 1.6.1], stated there for even lattices; $\mathrm{NS}(S_p)$ is odd, since a line has self-intersection $2-p$). The second Betti number of a smooth surface of degree p in $\mathbb{P}^3$ is $p^3 - 4p^2 + 6p - 2$, and $p^3 - 4p^2 + 6p - 2 - (3p^2 - 9p + 7) = (p-1)(p-3)^2$. □

The proofs. Everything is proved for an explicit integer matrix G of size $3p^2$, defined in §2; that G is the intersection matrix of the lines is the classical configuration, proved in §3.[2] Theorem 1 is proved in §§4–8. The kernel K of G contains an explicit sublattice K_0 with $pK \subseteq K_0$ and $[K : K_0] = p^{12}$ (the number 12 counts the relations modulo p among the

[1] The row $(2, 7)$ of [1, Table 1] (arXiv:1711.02628v2) prints the sign $-$; the signature argument and a direct computation of the determinant both give the sign $+$, that is, the value 7^{48}. The composite rows $(2, 6)$, $(2, 9)$ and $(2, 12)$ of the same table also print the sign opposite to $(-1)^{r-1}$, r the rank, which is the sign forced by the signature $(1, r-1)$ of the lattice of lines (it contains the class of a plane section); all the other rows $(2, m)$ of the table print the sign $(-1)^{r-1}$.

[2] Both theorems were first obtained in June 2026 by a different route, through the characters of $(\mathbb{Z}/p)^3$ [2, 6]. Two steps of the June argument for Theorem 1 (an inclusion of lattices and a rank) and four steps of the June argument for Theorem 2 were checked by computer only, the latter at a few primes; the proof printed here does not use them. The proof printed here is the integral route along which the theorems were formalized in Lean. Earlier versions of this paper are in [4] (version 2, 14 October 2026) and on Hexagon, hexagon:2610.00231v1.

functions that build K_0, Lemma 12); and $A = \mathbb{Z}^{3p^2}$ contains an explicit sublattice F, the orthogonal direct sum of N_0 (the indicator vector of the lines of one family) and $3(p-2)$ blocks, whose image in V has index $p^{3(p^2+p+2)/2-12}$. Theorem 2 is proved in §9: the order is Theorem 1, the exponent divides p^2 by an identity $GYG = 6p^2G$ with an explicit integer matrix Y (§9.1), and the rank of G modulo p is $12(p-3)$ (26 at $p=5$). Proposition 29 computes the same rank on the levels of a filtration by vanishing moments.

Lean. The lattice statements of Theorems 1 and 2, for the matrix G of §2, are checked in Lean 4 with Mathlib (§10). The geometric identification of §3, the equality $V = \mathrm{NS}(S_p)$ [10,15] and Corollary 3 are not formalized.

The names. *Watermark.* The degree is pressed into the whole intersection form: every non-zero eigenvalue of G is a multiple of p (they are $-p$, $-2p$ and $3p$; see the paragraph after Lemma 24), and so is every entry of the Gram matrix of the sublattice of full rank used in §8. The rank of V does not show it; the form does, as a watermark is seen only when the sheet is held against the light. Shioda knew that the mark is there, since the discriminant divides a power of the degree [20, Added in proof]; Theorem 1 reads how much of it the lattice keeps, $p^{3(p-3)^2}$, from the degree alone. *Double Ladder.* The rank of G modulo p, which with the order and the exponent fixes the group of Theorem 2, is the bottom rung of a ladder. On the subspace M_ν of the combinations modulo p whose coefficient function in each family has vanishing moments of total degree $< \nu$, the form $x^{\mathsf{T}}Gy$ modulo p has rank $12(p-3)-3\nu(\nu+1)$ for $p \geq 7$ and $0 \leq \nu \leq 3$, and also for $\nu = 4$ when $p \geq 11$ (Proposition 29). Each rung imposes 3ν new conditions and lowers the rank by twice that number, 6ν: the image of M_ν under the shadow map of §9.2 loses 3ν dimensions and the radical of the form gains 3ν. The name records this doubling, read on a ladder. The ladder is not used in the proof of Theorem 2; in the first proof [2] the rung $\nu = 2$, of rank $12p-54$, entered the count of the factors $\mathbb{Z}/p^2$, and it was checked there by computer only, at a few primes.

Notation. Throughout, $p \geq 5$ is prime, $\mathbb{F}_p = \mathbb{Z}/p$, and $P = \mathbb{F}_p^2$; its elements are written (k,l). For a function $u : \mathbb{F}_p \to \mathbb{Z}$ write $\Sigma u = \sum_{x \in \mathbb{F}_p} u(x)$; Z_0 is the group of u with $\Sigma u = 0$, free of rank $p-1$. For a commutative ring R and $u : \mathbb{F}_p \to R$ put $u^{\pm}(x) = u(x \pm 1)$; for $c \in \mathbb{F}_p$, $\delta_c : \mathbb{F}_p \to \mathbb{Z}$ is the indicator of c.

2 The configuration and the lattice

The set of *lines* is $I = \{0,1,2\} \times P$, so $|I| = 3p^2$; the first coordinate is the *family*. Let $A = \mathbb{Z}^I$ and define the symmetric matrix $G \in \mathbb{Z}^{I \times I}$ by the following entries, for lines $\ell = (j,k,l)$ and $\ell' = (j',k',l')$:

- same family ($j = j'$): $G_{\ell\ell} = 2-p$; for $(k,l) \neq (k',l')$, $G_{\ell\ell'} = 1$ if $k = k'$ or $l = l'$, and 0 otherwise;
- families 0 and 1 ($j = 0$, $j' = 1$): $G_{\ell\ell'} = 1$ if $k - l = k' - l'$, else 0;
- families 1 and 2 ($j = 1$, $j' = 2$): $G_{\ell\ell'} = 1$ if $k + l = k' + l'$, else 0;
- families 0 and 2 ($j = 0$, $j' = 2$): $G_{\ell\ell'} = 1$ if $k' - l' = k + l + 1$, else 0;
- the remaining entries by symmetry, $G_{\ell'\ell} = G_{\ell\ell'}$.

All equalities are in $\mathbb{F}_p$. Let $K = \ker G \subseteq A$ and $V = A/K$, with the form induced by $B(x,y) = x^{\mathsf{T}}Gy$ (by Corollary 6 this is the lattice V of Theorem 1); it is well defined because G is symmetric. The group V is torsion free (if $cx \in K$ with $c \neq 0$ then $x \in K$), hence free.

For $j \in \{0,1,2\}$ let $N_j \in A$ be the indicator of family j, and $\mathbf{1} = N_0 + N_1 + N_2$. For $x \in A$ write $x_j : P \to \mathbb{Z}$ for its restriction to family j and $\mathrm{aug}(x_j) = \sum_{z \in P} x_j(z)$.

Rows of G. The row of G at $\ell = (j,k,l)$ has $2-p$ at ℓ, 1 at the $2(p-1)$ lines of family j that share k or l with ℓ, and, in each other family j', the value 1 exactly on an *incidence set* $S_{j'}(\ell) \subset P$:

family of ℓ		
0 :	$S_1(\ell) = \{k' - l' = k - l\}$,	$S_2(\ell) = \{k' - l' = k + l + 1\}$,
1 :	$S_0(\ell) = \{k' - l' = k - l\}$,	$S_2(\ell) = \{k' + l' = k + l\}$,
2 :	$S_0(\ell) = \{k' + l' = k - l - 1\}$,	$S_1(\ell) = \{k' + l' = k + l\}$.

Each incidence set is a "$-$ set" $\{k' - l' = c\}$ or a "$+$ set" $\{k' + l' = c\}$; it has p points.

Lemma 4. *$GN_j = p\mathbf{1}$ for every j, and $G\mathbf{1} = 3p\mathbf{1}$.*

Proof. At a line of family j the row sum over family j is $(2-p) + 2(p-1) = p$. At a line of another family the row meets family j in an incidence set, of p points. □

3 The geometry

This section identifies G with the intersection matrix of the lines on S_p and V with $\mathrm{NS}(S_p)$. It is not used in §§4–9.

Put $\eta = e^{\pi i/p}$ and $\zeta = \eta^2 = e^{2\pi i/p}$, so that $\eta^p = -1$. For $(a,b) \in \mathbb{F}_p^2$ the following lines lie on S_p:

$$\begin{array}{ll} \text{family 0}: & x_0 = \eta\zeta^a x_1, \quad x_2 = \eta\zeta^b x_3; \\ \text{family 1}: & x_0 = \eta\zeta^a x_2, \quad x_1 = \eta\zeta^b x_3; \\ \text{family 2}: & x_0 = \eta\zeta^a x_3, \quad x_1 = \eta\zeta^b x_2. \end{array}$$

For instance on a line of family 0, $x_0^p + x_1^p = (\eta^p + 1)x_1^p = 0$ and likewise $x_2^p + x_3^p = 0$. These are the $3p^2$ lines of S_p [15]; the line of family j with parameters (a,b) is the line $(j,a,b) \in I$.

Proposition 5. *The intersection number of the lines (j,a,b) and (j',c,d) on S_p is the entry of G.*

Proof. By adjunction a line L on S_p has $L^2 = -2 - K_{S_p} \cdot L = -2 - (p-4) = 2-p$. Two distinct lines on a smooth surface meet in at most one point, transversally, so their intersection number is 1 if they meet and 0 otherwise; they meet if and only if their four linear equations have a common non-zero solution. Two lines of one family meet if and only if they share a or b: for instance the lines of family 0 with the same a and different b meet at $(\eta\zeta^a : 1 : 0 : 0)$, and if $a \neq a'$ and $b \neq b'$ the equations force $x = 0$. For families 0 and 1, with parameters (a,b) and (c,d), a common point has $x_3 \neq 0$ (otherwise all coordinates vanish) and $x_0 = \eta\zeta^a x_1 = \eta^2\zeta^{a+d}x_3$, $x_0 = \eta\zeta^c x_2 = \eta^2\zeta^{c+b}x_3$; so the lines meet if and only if $a - b = c - d$. In the same way families 1 and 2, with (c,d) and (e,f), meet if and only if $c + d = e + f$. For families 0 and 2, with (a,b) and (e,f), again $x_3 \neq 0$ and $x_0 = \eta\zeta^a x_1 = \eta^2\zeta^{a+f}x_2 = \eta^3\zeta^{a+f+b}x_3$ and $x_0 = \eta\zeta^e x_3$, so the lines meet if and only if $\eta^2\zeta^{a+b+f} = \zeta^e$, that is, $e - f = a + b + 1$. These are the entries of G; the $+1$ of the last case is $\eta^2 = \zeta$. □

Corollary 6. *The lattice spanned by the classes of the lines in $H^2(S_p, \mathbb{Z})$, with the intersection form, is isometric to V. For prime $p \geq 5$ it is $\mathrm{NS}(S_p)$.*

Proof. The classes of the lines span $\mathrm{NS}(S_p) \otimes \mathbb{Q}$ for $\gcd(p,6) = 1$ [19] (see [15, §3]), $H^2(S_p, \mathbb{Z})$ is torsion free, as S_p is simply connected, and the intersection form on $\mathrm{NS}(S_p)$ is non-degenerate (Hodge index theorem). So a combination $x \in A$ of lines has class 0 if and only if it pairs to zero with every line, that is, $Gx = 0$, by Proposition 5. Hence the lattice of the lines is $A/\ker G = V$ with the form of G. For $\gcd(p,6) = 1$ the lines generate $\mathrm{NS}(S_p)$ [10, 15]. □

The proof of Proposition 5 was also checked by computer: for $p = 5, 7, 11$ the lines were built numerically and every pair of distinct lines was tested for a common point (rank of a 4×4 complex matrix); all 2 775, 10 731 and 65 703 such pairs agree with G (the diagonal entries $2-p$ come from adjunction), and the same test with $k + l - 1$ in place of $k + l + 1$ in the last case disagrees on 250, 686 and 2 662 pairs.

4 Pencils and pullbacks

For $t \in \mathbb{F}_p$ let $\pi_t(k, l) = k + tl$, and let $\pi_\infty(k, l) = l$. These are the $p+1$ *pencils*: the linear forms on P up to scalars. We call $\pi_0 = k$ and $\pi_\infty = l$ the *axis* pencils, $\pi_1 = k + l$ and $\pi_{-1} = k - l$ the *overlap* pencils, and the $p-3$ others the *live* pencils. For a family j, a pencil π and $u : \mathbb{F}_p \to \mathbb{Z}$, the *pullback* $\mathrm{pb}_j^\pi(u) \in A$ is $u \circ \pi$ on family j and 0 elsewhere. For $y : P \to \mathbb{Z}$ the *fibre sums* are $\mathrm{fib}_\pi(y)(v) = \sum_{\pi(z)=v} y(z)$.

Lemma 7. *Let $\pi \neq \pi'$ be pencils and $u, v : \mathbb{F}_p \to \mathbb{Z}$. Then $\sum_{z \in P} u(\pi(z))v(\pi'(z)) = (\Sigma u)(\Sigma v)$ and $\sum_{z \in P} u(\pi(z))v(\pi(z)) = p \sum_x u(x)v(x)$. In particular every fibre of π meets every fibre of π' in exactly one point.*

Proof. Two non-proportional linear forms on $\mathbb{F}_p^2$ give a bijection $z \mapsto (\pi(z), \pi'(z))$ of P onto $\mathbb{F}_p^2$; every fibre of one pencil has p points. □

Lemma 8 (Fibre decomposition)**.** *For every $y : P \to \mathbb{Z}$ and every family j,*

$$p \cdot y|_{\text{family } j} \;=\; \sum_\pi \mathrm{pb}_j^\pi\left(\mathrm{fib}_\pi(y)\right) - \Big(\sum_z y(z)\Big) N_j,$$

the sum running over the $p + 1$ pencils (here $y|_{\text{family } j} \in A$ is y on family j and 0 elsewhere).

Proof. At (j, z) the right side is $\sum_\pi \sum_{\pi(z')=\pi(z)} y(z') - \sum_{z'} y(z')$. A point $z' \neq z$ lies on the same fibre as z for exactly one pencil, the one containing the direction $z' - z$; the point z does so for all $p + 1$. So the double sum is $(p + 1)y(z) + \sum_{z' \neq z} y(z')$. □

Lemma 9 (G on pullbacks)**.** *Let $u \in Z_0$.*

(a) Axis pencils: $G\ \mathrm{pb}_j^{\pi_0}(u) = G\ \mathrm{pb}_j^{\pi_\infty}(u) = 0$ for every j.

(b) Live pencils: $G\ \mathrm{pb}_j^{\pi_t}(u) = -p\ \mathrm{pb}_j^{\pi_t}(u)$ for $t \notin \{0, 1, -1\}$ and every j.

(c) Overlap pencils:

$$\begin{aligned}
G\ \mathrm{pb}_0^{\pi_{-1}}(u) &= -p\ \mathrm{pb}_0^{\pi_{-1}}(u) + p\ \mathrm{pb}_1^{\pi_{-1}}(u), & G\ \mathrm{pb}_1^{\pi_{-1}}(u) &= -p\ \mathrm{pb}_1^{\pi_{-1}}(u) + p\ \mathrm{pb}_0^{\pi_{-1}}(u),\\
G\ \mathrm{pb}_1^{\pi_1}(u) &= -p\ \mathrm{pb}_1^{\pi_1}(u) + p\ \mathrm{pb}_2^{\pi_1}(u), & G\ \mathrm{pb}_2^{\pi_1}(u) &= -p\ \mathrm{pb}_2^{\pi_1}(u) + p\ \mathrm{pb}_1^{\pi_1}(u),\\
G\ \mathrm{pb}_0^{\pi_1}(u) &= -p\ \mathrm{pb}_0^{\pi_1}(u) + p\ \mathrm{pb}_2^{\pi_{-1}}(u^-), & G\ \mathrm{pb}_2^{\pi_{-1}}(u) &= -p\ \mathrm{pb}_2^{\pi_{-1}}(u) + p\ \mathrm{pb}_0^{\pi_1}(u^+).
\end{aligned}$$

Proof. Let $v = \mathrm{pb}_j^\pi(u)$ and look at $(Gv)(\ell')$.

Lines $\ell' = (j, k, l)$ of family j. If π is an axis pencil, say $\pi = \pi_0$, the entry is $(2-p)u(k) + (p-1)u(k) + \sum_{k' \neq k} u(k') = \Sigma u = 0$; likewise for π_∞. If $\pi = \pi_t$ with $t \neq 0$, the row $\{k' = k\}$ and the column $\{l' = l\}$ each meet every fibre of π once, so with $x = \pi(k, l)$ the entry is $(2-p)u(x) + 2(\Sigma u - u(x)) = -pu(x)$.

Lines ℓ' of another family. The entry is the sum of $u \circ \pi$ over an incidence set S. On a $-$ set $\{k' - l' = c\}$, π_t takes the values $(1 + t)l' + c$, a bijection onto $\mathbb{F}_p$ unless $t = -1$; on a $+$ set $\{k' + l' = c\}$, π_t takes the values $(1 - t)k' + tc$, a bijection unless $t = 1$; $\pi_0 = k'$ and $\pi_\infty = l'$ are bijections on both kinds. A bijection gives $\Sigma u = 0$. In the two remaining cases (π_{-1} on a $-$ set, π_1 on a $+$ set) π is constant on S and the entry is $p\,u(\text{value})$. Reading the value off the table of incidence sets gives the six formulas; for example, for $v = \mathrm{pb}_0^{\pi_1}(u)$ and $\ell' = (2, k, l)$ the set is $S_0(\ell') = \{k' + l' = k - l - 1\}$, so the entry is $p\,u(k - l - 1) = p\,u^-(k - l)$; for $v = \mathrm{pb}_2^{\pi_{-1}}(u)$ and $\ell' = (0, k, l)$ it is $S_2(\ell') = \{k' - l' = k + l + 1\}$, giving $p\,u^+(k + l)$. □

The three *overlap pairs* are $(\mathrm{pb}_0^{\pi^{-1}}, \mathrm{pb}_1^{\pi^{-1}})$, $(\mathrm{pb}_1^{\pi_1}, \mathrm{pb}_2^{\pi_1})$ and $(\mathrm{pb}_0^{\pi_1}, \mathrm{pb}_2^{\pi^{-1}})$, the last one with a shift by one.

5 An explicit sublattice of the kernel

Definition 10. Let R be a commutative ring. A *datum* over R consists of functions $a_j, b_j : \mathbb{F}_p \to R$ $(j = 0, 1, 2)$, $w_0, w_1, w_2 : \mathbb{F}_p \to R$, and scalars $\varepsilon_1, \varepsilon_2 \in R$. It is *admissible* if each of the nine functions a_j, b_j, w_i has sum zero; the admissible data form a free R-module Src_R of rank $9(p-1)+2 = 9p-7$. The map $s_R : \mathrm{Src}_R \to R^I$ sends a datum to the vector with values

$$\begin{aligned}(0,k,l) &\mapsto a_0(k) + b_0(l) + w_0(k-l) + w_2(k+l) + \varepsilon_1,\\ (1,k,l) &\mapsto a_1(k) + b_1(l) + w_0(k-l) + w_1(k+l) + \varepsilon_2 - \varepsilon_1,\\ (2,k,l) &\mapsto a_2(k) + b_2(l) + w_1(k+l) + w_2(k-l-1) - \varepsilon_2.\end{aligned}$$

Put $K_0 = s_{\mathbb{Z}}(\mathrm{Src}_{\mathbb{Z}}) \subseteq A$.

In terms of pullbacks, $s_{\mathbb{Z}}$ of a datum is

$$\sum_j \big(\mathrm{pb}_j^{\pi_0}(a_j) + \mathrm{pb}_j^{\pi_\infty}(b_j)\big) + \big(\mathrm{pb}_0^{\pi^{-1}} + \mathrm{pb}_1^{\pi^{-1}}\big)(w_0) + \big(\mathrm{pb}_1^{\pi_1} + \mathrm{pb}_2^{\pi_1}\big)(w_1) + \mathrm{pb}_0^{\pi_1}(w_2) + \mathrm{pb}_2^{\pi^{-1}}(w_2^-) + \varepsilon_1(N_0 - N_1) + \varepsilon_2(N_1 - N_2).$$

Lemma 11. $K_0 \subseteq K$.

Proof. By Lemma 9(a), G kills the axis pullbacks. For the first overlap pair, Lemma 9(c) gives

$$G\big(\mathrm{pb}_0^{\pi^{-1}} + \mathrm{pb}_1^{\pi^{-1}}\big)(w_0) = (-p+p)\ \mathrm{pb}_0^{\pi^{-1}}(w_0) + (p-p)\ \mathrm{pb}_1^{\pi^{-1}}(w_0) = 0,$$

and likewise for the second. For the third, $G\,\mathrm{pb}_0^{\pi_1}(w_2) = -p\,\mathrm{pb}_0^{\pi_1}(w_2) + p\,\mathrm{pb}_2^{\pi^{-1}}(w_2^-)$ and $G\,\mathrm{pb}_2^{\pi^{-1}}(w_2^-) = -p\,\mathrm{pb}_2^{\pi^{-1}}(w_2^-) + p\,\mathrm{pb}_0^{\pi_1}(w_2)$, since $(w_2^-)^+ = w_2$; the sum is 0. Finally $G(N_0 - N_1) = G(N_1 - N_2) = 0$ by Lemma 4. □

Lemma 12 (Relations modulo p)**.** *The kernel of $s_{\mathbb{F}_p} : \mathrm{Src}_{\mathbb{F}_p} \to \mathbb{F}_p^I$ has dimension 12; hence its image has dimension $9p-19$.*

Proof. Let Θ be an admissible datum over $\mathbb{F}_p$ with $s_{\mathbb{F}_p}(\Theta) = 0$, so that the three displayed functions of (k,l) vanish identically. For $\Phi : P \to \mathbb{F}_p$ put $(\Box\Phi)(k,l) = \Phi(k+1,l+1) - \Phi(k+1,l) - \Phi(k,l+1) + \Phi(k,l)$, and for $w : \mathbb{F}_p \to \mathbb{F}_p$ put $(\Delta^2 w)(z) = w(z+2) - 2w(z+1) + w(z)$. The operator $\Box$ kills functions of k alone, of l alone, and constants, and a direct computation gives $\Box[w(k-l)] = -(\Delta^2 w)(k-l-1)$ and $\Box[w(k+l)] = (\Delta^2 w)(k+l)$.

Applying $\Box$ to the three identities gives, for all k, l:

$$(\Delta^2 w_2)(k+l) = (\Delta^2 w_0)(k-l-1), \qquad (\Delta^2 w_1)(k+l) = (\Delta^2 w_0)(k-l-1),$$
$$(\Delta^2 w_1)(k+l) = (\Delta^2 w_2)(k-l-2).$$

Since p is odd, $(k,l) \mapsto (k+l, k-l)$ is a bijection of P, so each of these says that both sides are one and the same constant. Hence $\Delta^2 w_0 = \Delta^2 w_1 = \Delta^2 w_2 = 2c$ for one $c \in \mathbb{F}_p$. As $\Delta^2(x^2) = 2$, the function $w_i - cx^2$ has zero second difference, so its first difference is a constant α_i and $w_i(x) = cx^2 + \alpha_i x + \beta_i$ for all $x \in \mathbb{F}_p$.

With these w_i the cross terms cancel, $(k-l)^2 + (k+l)^2 = 2k^2 + 2l^2$ and $(k+l)^2 + (k-l-1)^2 = 2k^2 + 2l^2 - 2k + 2l + 1$, so each identity reads $a_j(k) + b_j(l) = \phi_j(k) + \psi_j(l)$ with explicit polynomials ϕ_j, ψ_j of degree ≤ 2 (the constants β_i and $\pm\varepsilon_1, \pm\varepsilon_2$ are absorbed into ϕ_j and ψ_j). Its solutions are exactly $a_j = \phi_j + t_j$, $b_j = \psi_j - t_j$ with $t_j \in \mathbb{F}_p$ (put $l = 0$, then $k = 0$).

Conversely every such choice is admissible: each of $a_j = \phi_j + t_j$, $b_j = \psi_j - t_j$ and w_i is a polynomial function of degree ≤ 2 on $\mathbb{F}_p$, and such a function has sum zero (for the constant t_j, $\Sigma t_j = pt_j = 0$), because $\sum_x 1 = p$, $\sum_x x = p(p-1)/2$ and $\sum_x x^2 = (p-1)p(2p-1)/6$ vanish in $\mathbb{F}_p$ ($\gcd(p,6) = 1$). So the kernel is the image of the injective linear map from $\mathbb{F}_p^{12}$ sending $(c, \alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2, \varepsilon_1, \varepsilon_2, t_0, t_1, t_2)$ to the datum just described. Injectivity: c, α_i, β_i are read off the w_i, t_j off $a_j(0)$, and $\varepsilon_1, \varepsilon_2$ are coordinates of the datum. □

Remark 13. At $p = 3$ the count drops to 11 because $\sum_{x \in \mathbb{F}_3} x^2 \neq 0$; this is one of the places where $p \ge 5$ is used.

Lemma 14. *Reduction modulo p maps* $\mathrm{Src}_{\mathbb{Z}}$ *onto* $\mathrm{Src}_{\mathbb{F}_p}$*, and* $s_{\mathbb{F}_p}(\Theta \bmod p) = s_{\mathbb{Z}}(\Theta) \bmod p$ *for* $\Theta \in \mathrm{Src}_{\mathbb{Z}}$.

Proof. The second statement holds because reduction is a ring map. For the first, lift a sum-zero $f : \mathbb{F}_p \to \mathbb{F}_p$ to any $y : \mathbb{F}_p \to \mathbb{Z}$; p divides Σy, and $y - (\Sigma y)\,\delta_0$ is a sum-zero lift of f (it changes y only at 0, by a multiple of p). The scalars $\varepsilon_1, \varepsilon_2$ lift trivially. □

6 The kernel

Lemma 15 (Augmentations on the kernel)**.** *For $x \in K$:* $\mathrm{aug}(x_0) + \mathrm{aug}(x_1) + \mathrm{aug}(x_2) = 0$*, and p divides each* $\mathrm{aug}(x_j)$.

Proof. By Lemma 4, $0 = N_0^{\mathsf{T}} G x = (GN_0)^{\mathsf{T}} x = p \sum_\ell x(\ell)$, which is the first statement. For the second, let y be the indicator of the fibre $\{\pi_t = c\}$ of family 0, so that $py = \mathrm{pb}_0^{\pi_t}(p\delta_c - 1) + N_0$ with $p\delta_c - 1 \in Z_0$. By Lemmas 9 and 4:

$$\begin{aligned} Gy &= 2N_0 + N_1 + N_2 - py && (t \notin \{0, \pm 1\}),\\ Gy &= 2N_0 + N_1 + p\chi - py && (t = 1),\\ Gy &= 2N_0 + N_2 + p\chi' - py && (t = -1), \end{aligned}$$

with $\chi, \chi' \in A$ fibre indicators. Pairing with $x \in K$ gives $0 = y^{\mathsf{T}} G x$, hence, with $s_j = \mathrm{aug}(x_j)$: $2s_0 + s_1 + s_2 \equiv 0$, $2s_0 + s_1 \equiv 0$ and $2s_0 + s_2 \equiv 0 \pmod p$. A live pencil exists because $p \ge 5$. Subtracting, $s_1 \equiv s_2 \equiv 0$ and $2s_0 \equiv 0$, so $s_0 \equiv 0$ as p is odd. □

Lemma 16 (Fibre sums on the kernel)**.** *Let $x \in K$ and write $f_{j,\pi} = \mathrm{fib}_\pi(x_j)$. Then f_{j,π_t} is constant for every j and every live t, and the functions $f_{0,\pi_{-1}} - f_{1,\pi_{-1}}$, $f_{1,\pi_1} - f_{2,\pi_1}$ and $v \mapsto f_{0,\pi_1}(v) - f_{2,\pi_{-1}}(v+1)$ are constant.*

Proof. For every $w \in A$, $x^{\mathsf{T}} G w = (Gx)^{\mathsf{T}} w = 0$, and $x^{\mathsf{T}} \mathrm{pb}_j^\pi(u) = \sum_v u(v) f_{j,\pi}(v)$. A function $f : \mathbb{F}_p \to \mathbb{Z}$ with $\sum_v u(v) f(v) = 0$ for every $u \in Z_0$ is constant (take $u = \delta_a - \delta_b$). Apply this with $w = \mathrm{pb}_j^{\pi_t}(u)$ for live t, and with $w = \mathrm{pb}_0^{\pi_{-1}}(u)$, $\mathrm{pb}_1^{\pi_1}(u)$, $\mathrm{pb}_0^{\pi_1}(u)$, using Lemma 9; in the last case $\sum_z u(z-1) f_{2,\pi_{-1}}(z) = \sum_v u(v) f_{2,\pi_{-1}}(v+1)$. □

Proposition 17. $pK \subseteq K_0$.

Proof. Let $x \in K$, put $\mu_j = \mathrm{aug}(x_j)/p \in \mathbb{Z}$ (Lemma 15, which also gives $\mu_0 + \mu_1 + \mu_2 = 0$), and $\tilde f_{j,\pi} = f_{j,\pi} - \mu_j$; since $\Sigma f_{j,\pi} = \mathrm{aug}(x_j)$, each $\tilde f_{j,\pi}$ has sum zero. By Lemma 8,

$$p \cdot x_j\big|_{\text{family } j} = \sum_\pi \mathrm{pb}_j^\pi(\tilde f_{j,\pi}) + (p+1)\mu_j N_j - p\mu_j N_j = \sum_\pi \mathrm{pb}_j^\pi(\tilde f_{j,\pi}) + \mu_j N_j.$$

By Lemma 16, $\tilde f_{j,\pi_t}$ is constant with sum zero, hence 0, for every live t; and the three overlap differences, constant with sum zero, vanish: $\tilde f_{0,\pi_{-1}} = \tilde f_{1,\pi_{-1}}$, $\tilde f_{1,\pi_1} = \tilde f_{2,\pi_1}$, $\tilde f_{2,\pi_{-1}} = \tilde f_{0,\pi_1}^{-}$. Hence $px = s_{\mathbb{Z}}(\Theta)$ for the admissible datum Θ: $a_j = \tilde f_{j,\pi_0}$, $b_j = \tilde f_{j,\pi_\infty}$, $w_0 = \tilde f_{0,\pi_{-1}}$, $w_1 = \tilde f_{1,\pi_1}$, $w_2 = \tilde f_{0,\pi_1}$, $\varepsilon_1 = \mu_0$, $\varepsilon_2 = -\mu_2$ (note $\varepsilon_2 - \varepsilon_1 = \mu_1$). □

7 The sublattice F and two indices

Let $F \subseteq A$ be spanned by N_0 and by the $3(p-2)$ *blocks*: the $3(p-3)$ blocks $\mathrm{pb}_j^{\pi_t}(Z_0)$ for $j \in \{0,1,2\}$ and t live, and the three blocks $\mathrm{pb}_0^{\pi_{-1}}(Z_0)$, $\mathrm{pb}_1^{\pi_1}(Z_0)$ and $\mathrm{pb}_0^{\pi_1}(Z_0)$ (one member of each overlap pair).

Lemma 18. *Distinct blocks are B-orthogonal, and N_0 is B-orthogonal to every block. Inside a block, $B(\mathrm{pb}\,u, \mathrm{pb}\,v) = -p^2 \sum_x u(x)v(x)$; and $B(N_0, N_0) = p^3$.*

Proof. By Lemma 9, G applied to a block vector is $-p$ times it, plus, for the three overlap members, p times a pullback along an overlap pencil of another family: of family 1 along π_{-1}, of family 2 along π_1, and of family 2 along π_{-1}. None of these three is a block of F, so that term pairs with a block of F either through disjoint supports or through two different pencils of one family, which gives $(\Sigma u)(\Sigma v) = 0$ by Lemma 7. Two blocks of one family and different pencils are orthogonal for the same reason, and blocks of different families have disjoint supports. Inside a block, Lemma 7 gives $-p \cdot p \sum_x u(x)v(x)$. Finally $B(N_0, w) = (GN_0)^{\mathsf{T}} w = p \sum_\ell w(\ell)$, which is 0 on pullbacks of sum-zero functions, and $p \cdot p^2$ for $w = N_0$. □

Corollary 19. *$F \cap K = 0$, and F is free of rank $3(p-2)(p-1)+1$.*

Proof. Write $x \in F$ as $cN_0 + \sum_\beta \mathrm{pb}(u_\beta)$, one term per block. If $x \in K$ then $0 = B(x, \mathrm{pb}(u_\beta)) = -p^2 \sum u_\beta^2$, so every $u_\beta = 0$, and $0 = B(x, N_0) = cp^3$. The same argument shows that the blocks and N_0 are independent; each block is isomorphic to Z_0 because π is surjective. □

Let $L_{\mathrm{fam}} \subseteq \mathbb{Z}^P$ be spanned by the constant 1 and all $u \circ \pi$, $u \in Z_0$, π a pencil; and let $L \subseteq A$ consist of the x with $x_j \in L_{\mathrm{fam}}$ for every j.

Lemma 20. *L_{fam} has full rank in $\mathbb{Z}^P$ and $[\mathbb{Z}^P : L_{\mathrm{fam}}] = p^{(p^2+p+2)/2}$; hence $[A : L] = p^{3(p^2+p+2)/2}$.*

Proof. The $(p+1)(p-1)+1 = p^2$ vectors $(\delta_x - \delta_0) \circ \pi$ ($x \neq 0$, π a pencil) and 1 span L_{fam}. By Lemma 7 their Gram matrix for the standard inner product is block diagonal: inside one pencil it is $p(I+J)$ of size $p-1$, with determinant $p^{p-1} \cdot p$; and $\langle 1, 1\rangle = p^2$. The Gram determinant is $(p^p)^{p+1} p^2 = p^{p^2+p+2} \neq 0$; so the vectors form a basis, and the index of the lattice they span is the square root of the Gram determinant ($p^2 + p$ is even). □

Lemma 21. *$F + K_0 = L$, and $F \cap K_0 = 0$.*

Proof. Both F and K_0 lie in L. Conversely L is spanned by the vectors $\mathrm{pb}_j^{\pi}(u)$, $u \in Z_0$, and N_0, N_1, N_2. Live blocks lie in F; axis pullbacks lie in K_0; for an overlap pair, one member lies in F and the sum of the pair lies in K_0 (with a datum having one non-zero w_i; for the third pair, the vector $\mathrm{pb}_2^{\pi_{-1}}(v)$ is reached with $w_2 = v^+$). Finally $N_0 \in F$, and $N_0 - N_1$, $N_1 - N_2 \in K_0$. The intersection is 0 because $F \cap K = 0$ and $K_0 \subseteq K$. □

Proposition 22. *K_0 and K are free of rank $9p-7$, and $[K : K_0] = p^{12}$.*

Proof. By Lemmas 20 and 21, $F \oplus K_0$ has finite index in A, so $\operatorname{rank} K_0 = 3p^2 - \operatorname{rank} F = 9p-7$. Since $K_0 \subseteq K$ and $F \cap K = 0$, also $9p - 7 \leq \operatorname{rank} K \leq 3p^2 - \operatorname{rank} F = 9p - 7$.

By Proposition 17, K/K_0 is killed by p, so $[K : K_0] = |K/pK|/|K_0/pK| = p^{9p-7}/|K_0/pK|$. Since $K = \ker G$, $K \cap pA = pK$, so K/pK embeds in $A/pA = \mathbb{F}_p^I$; it maps K_0/pK onto the reduction of K_0 modulo p, which by Lemma 14 is the image of $s_{\mathbb{F}_p}$, of dimension $9p - 19$ (Lemma 12). Hence $[K : K_0] = p^{(9p-7)-(9p-19)} = p^{12}$. □

Corollary 23. $[A : F + K] = p^{3(p^2+p+2)/2-12}$.

Proof. $L = F + K_0 \subseteq F + K \subseteq A$. The map $K \to (F+K)/(F+K_0)$ is onto with kernel $K \cap (F + K_0) = K_0$: if $k = f + s$ then $f = k - s \in F \cap K = 0$. So $[F + K : L] = [K : K_0] = p^{12}$, and $[A : F + K] = [A : L]/p^{12}$. □

8 Proof of Theorem 1

$V = A/K$ is free of rank $3p^2 - (9p-7) = 3(p-1)(p-2)+1$ (§2 and Proposition 22). The quotient map $\varphi : A \to V$ is injective on F (Corollary 19) and $V/\varphi(F) \cong A/(F+K)$, so $\varphi(F)$ is a sublattice of full rank and index $N = p^{3(p^2+p+2)/2-12}$ (Corollary 23).

Let c be the basis of $\varphi(F)$ formed by $\varphi(N_0)$ and, for each block, the images of $\mathrm{pb}(\delta_x - \delta_0)$, $x \neq 0$. By Lemma 18 its Gram matrix is block diagonal, with $3(p-2)$ blocks $-p^2(I+J)$ of size $p-1$ and the block (p^3); since $p-1$ is even,

$$\det \mathrm{Gram}_c = \left(p^{2(p-1)} \cdot p\right)^{3(p-2)} \cdot p^3 = p^{3(p-2)(2p-1)+3}.$$

For any basis b of V, $\mathrm{Gram}_c = M^{\mathsf{T}} \mathrm{Gram}_b M$ with $|\det M| = N$, so

$$\det \mathrm{Gram}_b = p^{3(p-2)(2p-1)+3-3(p^2+p+2)+24} = p^{3p^2-18p+27} = p^{3(p-3)^2}.$$

With Corollary 6 this proves Theorem 1. □

9 Proof of Theorem 2

By Theorem 1, $D = V^*/V$ is a finite group of order $p^{3(p-3)^2}$. Its structure is fixed by two more facts: its exponent divides p^2 (§9.1), and the rank of G modulo p (§9.2) is known.

9.1 The exponent

For a pencil π let $P_\pi \in \mathbb{Z}^{I \times I}$ be the block-diagonal matrix with $(P_\pi)_{\ell\ell'} = 1$ if ℓ, ℓ' lie in one family and $\pi(\ell) = \pi(\ell')$, and 0 otherwise. Put

$$Y = P_{\pi_0} + P_{\pi_\infty} + 3P_{\pi_{-1}} + 3P_{\pi_1} - 6p\, I.$$

Lemma 24. *$GYG = 6p^2 G$.*

Proof. By Lemma 8 (applied to the indicator of one point), $\mathbb{Q}^I$ is spanned over $\mathbb{Q}$ by the pullbacks $\mathrm{pb}_j^\pi(u)$, $u \in Z_0$, and the vectors N_j (write $\delta_{\pi(z)} = (\delta_{\pi(z)} - \frac{1}{p}) + \frac{1}{p}$); we check the identity on these. By Lemma 7, $P_\pi \,\mathrm{pb}_j^{\pi'}(u)$ is $p\,\mathrm{pb}_j^\pi(u)$ if $\pi' = \pi$ and 0 otherwise, and $P_\pi N_j = pN_j$. So Y acts by $-5p$ on axis pullbacks, by $-3p$ on overlap pullbacks, by $-6p$ on live pullbacks, and by $2p$ on the N_j. Now use Lemma 9. Axis: both sides vanish. Live: $(-p)(-6p)(-p) = -6p^3 = 6p^2 \cdot (-p)$. Each overlap pair spans a G-stable plane on which $G = pE$, $E = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ (for the third pair use the vectors $\mathrm{pb}_0^{\pi_1}(u)$ and $\mathrm{pb}_2^{\pi_{-1}}(u^-)$), and $Y = -3p$; as $E^2 = -2E$, $pE(-3p)pE = 6p^3E = 6p^2 \cdot pE$. On the span of N_0, N_1, N_2, $G = pJ_3$ (Lemma 4) and $Y = 2p$; as $J_3^2 = 3J_3$, $pJ_3 \cdot 2p \cdot pJ_3 = 6p^3 J_3$. □

The proof shows that G is diagonalizable over $\mathbb{Q}$ with eigenvalues $-p$ (multiplicity $3(p-1)(p-3)$: the live pullbacks), $-2p$ (multiplicity $3(p-1)$: one in each overlap plane), $3p$ (multiplicity 1: the vector $\mathbf{1}$) and 0 (multiplicity $9p-7$), so its minimal polynomial is $x(x+p)(x+2p)(x-3p)$; and Y acts as $6p^2/\lambda$ on the λ-eigenspace for every $\lambda \neq 0$; the integer 6 is the least common denominator of p^2/λ over $\lambda \in \{-p, -2p, 3p\}$.

Corollary 25. *$p^2 V^* \subseteq V$: the exponent of D divides p^2.*

Proof. A functional on V is given by a vector $f \in \mathbb{Z}^I$ orthogonal to $K = \ker G$; as G is symmetric, $f = Gy$ with $y \in \mathbb{Q}^I$. By Lemma 24, $6p^2 f = GYGy = G(Yf)$, which is the functional of the class of the integer vector Yf. So $6p^2 V^* \subseteq V$. The order of D is a power of p and $\gcd(6, p) = 1$, so $p^2 V^* \subseteq V$. □

9.2 The rank of G modulo p

Use the four pencils $\pi_0, \pi_\infty, \pi_{-1}, \pi_1$ (that is, k, l, $k-l$, $k+l$). For each family j and each of them let $\mathrm{push}_{j,\pi} : \mathbb{F}_p^P \to \mathbb{F}_p^{\mathbb{F}_p}$ be the fibre sum, and let $\mathcal{S} : \mathbb{F}_p^I \to U = (\mathbb{F}_p^{\mathbb{F}_p})^{12}$ collect these twelve *shadows*. Let Γ be the symmetric matrix on U that pairs each of the six axis slots $(j, \pi_0), (j, \pi_\infty)$ with itself by the identity, pairs $(0, \pi_{-1})$ with $(1, \pi_{-1})$ and $(1, \pi_1)$ with $(2, \pi_1)$ by the identity, and pairs $(0, \pi_1)$ with $(2, \pi_{-1})$ by the shift (the value v of the first slot with the value $v+1$ of the second). Then $\Gamma^2 = I$.

Lemma 26. *$G = \mathcal{S}^\mathsf{T}\Gamma\mathcal{S} - pI$ over $\mathbb{Z}$ (with $\mathcal{S}$ and Γ read as integer matrices). Hence $G \equiv \mathcal{S}^\mathsf{T}\Gamma\mathcal{S}$ (mod p) and $\mathrm{rank}_{\mathbb{F}_p}(G \bmod p) = \dim W - \dim(W \cap W^{\perp_\Gamma})$, where $W = \mathrm{im}\,\mathcal{S}$ and $W^{\perp_\Gamma} = \{w : \langle \Gamma w, W\rangle = 0\}$.*

Proof. The entry of $\mathcal{S}^\mathsf{T}\Gamma\mathcal{S}$ at two lines of one family is $[k = k'] + [l = l']$ (only the axis slots pair inside a family), which is 2 on the diagonal; at a line of family 0 and one of family 1 it is $[k - l = k' - l']$; at families $1, 2$ it is $[k + l = k' + l']$; at families $0, 2$ it is $[k' - l' = k + l + 1]$. Subtracting pI gives G. For the rank: $\mathcal{S}^\mathsf{T}\Gamma\mathcal{S}x = 0$ if and only if $\Gamma\mathcal{S}x \perp W$, i.e. $\mathcal{S}x \in W \cap W^{\perp_\Gamma}$, so $\dim\ker = \dim\ker\mathcal{S} + \dim(W \cap W^{\perp_\Gamma})$. □

Lemma 27. $\dim W = 12p - 18$. *The annihilator $\mathcal{R}$ of W (for the standard pairing) has dimension 18; family by family it is spanned by the elements placing $c_\pi x^s$ in the slot (j, π), with $s \in \{0, 1, 2\}$ and $\sum_\pi c_\pi \pi^s = 0$ as a form on P.*

Proof. $W = \bigoplus_j W_j$. A tuple $(h_\pi)_\pi$ of functions annihilates W_j if and only if $\sum_\pi h_\pi(\pi(k, l)) = 0$ as a function on P. Write each h_π as a polynomial of degree $\le p - 1$; the sum is a polynomial of total degree $\le p - 1$, which vanishes as a function on $\mathbb{F}_p^2$ if and only if it vanishes as a polynomial, i.e. if and only if $\sum_\pi c_{\pi,s}\pi^s = 0$ for each s, where $c_{\pi,s}$ is the coefficient of x^s in h_π. For $3 \le s \le p - 1$ the four forms π^s are linearly independent: writing $\pi = ak + bl$, the coefficient of $k^t l^{s-t}$ in π^s is $\binom{s}{t} a^t b^{s-t}$, the binomial coefficients are units ($s < p$), and the matrix $(a_\pi^t b_\pi^{s-t})_{\pi,t}$ has rank 4 because evaluation of binary forms of degree $s \ge 3$ at the four distinct points $(1:0), (0:1), (1:-1), (1:1)$ of $\mathbb{P}^1(\mathbb{F}_p)$ is surjective onto $\mathbb{F}_p^4$: since $s \ge 3$, for each of the four points the product of three linear forms vanishing at the other three points and of the $(s-3)$-th power of a linear form not vanishing at it has degree s, vanishes at the other three points and does not vanish at the given one. For $s \le 2$ the four forms π^s span all binary forms of degree s (here char $\ne 2$), a space of dimension $s + 1$, so the relations have dimension $3, 2, 1$ for $s = 0, 1, 2$; the relation in degree 2 is $(k + l)^2 + (k - l)^2 = 2k^2 + 2l^2$. So $\dim \mathcal{R}_j = 6$ and $\dim W_j = 4p - 6$. □

Proposition 28. *For every prime $p \ge 7$, $\mathrm{rank}_{\mathbb{F}_p}(G \bmod p) = 12(p - 3)$.*

Proof. $W^{\perp_\Gamma} = \Gamma(W^\perp) = \Gamma\mathcal{R}$. The slot functions of an element of $\Gamma\mathcal{R}$ are polynomials of degree ≤ 2, possibly translated by ± 1. Such an element lies in $W = \mathcal{R}^\perp$ if it pairs to zero with $\mathcal{R}$; each pairing is $\sum_{x \in \mathbb{F}_p} f(x)g(x)$ with $\deg(fg) \le 4$, and $\sum_{x \in \mathbb{F}_p} x^e = 0$ for $0 \le e \le p - 2$. As $4 \le p - 2$ for $p \ge 7$, $\Gamma\mathcal{R} \subseteq W$, so $W \cap W^{\perp_\Gamma} = \Gamma\mathcal{R}$ has dimension 18 and the rank is $(12p - 18) - 18$. □

At $p = 5$ the pairings of degree 4 survive, because $\sum_{x \in \mathbb{F}_5} x^4 = -1$. Only the three relations of degree 2 pair non-trivially (every other product has degree $\le 3 = p - 2$): the relation r_j places $-2x^2, -2x^2, x^2, x^2$ in the slots $(j, \pi_0), (j, \pi_\infty), (j, \pi_{-1}), (j, \pi_1)$, and $\langle \Gamma r_j, r_{j'} \rangle$ is $8\sum_x x^4$ for $j = j'$ (the two axis slots) and $\sum_x x^4$ for $j \ne j'$ (one overlap slot; the shift changes only terms of lower degree). The matrix $-(7I + J_3) \equiv 3I + 4J_3 \pmod 5$ has rank 2. So the 18×18 matrix of Γ-pairings between the relations has rank 2, $\dim(W \cap W^{\perp_\Gamma}) = 16$ and $\mathrm{rank}(G \bmod 5) = 26$. This value is also checked in Lean (lemma `rank_gram_map_five`, §10), and it agrees with [1, Table 1, row $(2, 5)$].

9.3 The rank on a filtration by moments

For $\nu \geq 0$ let $M_\nu \subseteq \mathbb{F}_p^I$ be the subspace of the x such that $\sum_{(k,l)\in P} x_j(k,l)\, k^a l^b = 0$ for every family j and all $a, b \geq 0$ with $a + b < \nu$ (here and below $0^0 = 1$); so $M_0 = \mathbb{F}_p^I$. Let $U_{<\nu} \subseteq U$ be spanned by the elements with the function $x \mapsto x^s$ in one slot, $0 \leq s < \nu$, and 0 in the other slots.

Proposition 29 (Rank on the moment filtration)**.** *Let $p \geq 7$ be prime, and let $0 \leq \nu \leq 3$, or $\nu = 4$ and $p \geq 11$. The restriction of the bilinear form $(x, y) \mapsto x^{\mathsf{T}} G y$ over $\mathbb{F}_p$ to M_ν has rank $12(p-3) - 3\nu(\nu+1)$.*

For $\nu = 0$ this is Proposition 28.

Proof. Put $W_\nu = \mathcal{S}(M_\nu)$. For a family j, a pencil π and $x \in \mathbb{F}_p^I$, the shadow $h = \mathrm{push}_{j,\pi}(x_j)$ has moments $\sum_v h(v) v^s = \sum_{z\in P} x_j(z)\pi(z)^s$, and π^s is a binary form of degree s; so $W_\nu \subseteq W \cap U_{<\nu}^\perp$.

The dimension of W_ν. If the four shadows of x_j vanish, then $\sum_z x_j(z)\pi(z)^s = 0$ for the four pencils and every s. For $s \leq 3$ the four forms π^s span all binary forms of degree s: for $s \leq 2$ by the proof of Lemma 27, and for $s = 3$ because they are four independent forms in a space of dimension 4. So all moments of x_j of degree ≤ 3 vanish, and $\ker \mathcal{S} \subseteq M_4 \subseteq M_\nu$. Hence $\dim W_\nu = \dim M_\nu - \dim \ker \mathcal{S}$. The monomials $k^a l^b$ with $a + b < \nu \leq 4 < p$ are linearly independent functions on P, so $\dim M_\nu = 3p^2 - 3\nu(\nu+1)/2$, and $\dim \ker \mathcal{S} = 3p^2 - (12p - 18)$ by Lemma 27. Thus $\dim W_\nu = 12p - 18 - 3\nu(\nu+1)/2$.

The annihilator of W_ν. It contains $\mathcal{R}$ and $U_{<\nu}$. Family by family, $\mathcal{R}_j$ is the direct sum of its parts of degree $s = 0, 1, 2$, of dimensions $3, 2, 1$ (Lemma 27), and $\mathcal{R}_j \cap U_{<\nu,j}$ is the sum of the parts with $s < \nu$, of dimension $0, 3, 5, 6, 6$ for $\nu = 0, \ldots, 4$; and $\dim U_{<\nu,j} = 4\nu$, since $1, x, \ldots, x^{\nu-1}$ are independent functions on $\mathbb{F}_p$. So $\dim(\mathcal{R}_j + U_{<\nu,j}) = 6 + 4\nu - \dim(\mathcal{R}_j \cap U_{<\nu,j}) = 6 + \nu(\nu+1)/2$, and $\dim(\mathcal{R} + U_{<\nu}) = 18 + 3\nu(\nu+1)/2 = 12p - \dim W_\nu$. Hence $W_\nu^\perp = \mathcal{R} + U_{<\nu}$, and $W_\nu = W \cap U_{<\nu}^\perp$.

The rank. The form on M_ν is $(x, y) \mapsto \langle \mathcal{S}x, \Gamma\mathcal{S}y\rangle$ (Lemma 26), so its rank is the rank of $(w, w') \mapsto \langle w, \Gamma w'\rangle$ on W_ν, that is, $\dim W_\nu - \dim(W_\nu \cap \Gamma(W_\nu^\perp))$, as Γ is a symmetric involution. The slot functions of an element of $\Gamma(\mathcal{R} + U_{<\nu})$ are polynomials of degree $\leq d = \max(2, \nu - 1)$, possibly translated by ± 1. Its pairings with $\mathcal{R}$ and with $U_{<\nu}$ are sums $\sum_{x\in\mathbb{F}_p} f(x)g(x)$ with $\deg(fg) \leq d + \max(2, \nu - 1)$, that is, ≤ 4 for $\nu \leq 3$ and ≤ 6 for $\nu = 4$; they vanish because $\sum_{x\in\mathbb{F}_p} x^e = 0$ for $0 \leq e \leq p - 2$, and $4 \leq p - 2$ for $p \geq 7$, $6 \leq p - 2$ for $p \geq 11$. So $\Gamma(\mathcal{R} + U_{<\nu}) \subseteq W \cap U_{<\nu}^\perp = W_\nu$, and the rank is $\dim W_\nu - (12p - \dim W_\nu) = 2\dim W_\nu - 12p = 12(p-3) - 3\nu(\nu+1)$. □

The proof also shows why the rank drops by 6ν at each step: passing from $M_{\nu-1}$ to M_ν imposes 3ν conditions, the image W_ν loses 3ν dimensions and the radical $\Gamma(W_\nu^\perp)$ gains 3ν, so the rank drops by 6ν. The proposition is not used in the proof of Theorem 2. In the first proof [2] these ranks were found and checked at a few primes; we checked the five levels $\nu = 0, \ldots, 4$ by computer at $p = 7$, 11 and 13: the ranks are $48, 42, 30, 12, 0$, then $96, 90, 78, 60, 36$, then $120, 114, 102, 84, 60$, where the value 0 at $p = 7$, $\nu = 4$ lies outside the range of the proposition.

9.4 Assembly

K is a direct summand of A (it is saturated), so in a basis of A adapted to $A = K \oplus C$ the matrix G becomes $0 \oplus \mathrm{Gram}(V)$. Hence the non-zero elementary divisors of G are those of $\mathrm{Gram}(V)$, whose cokernel is D. All of them are powers of p (the order of D is), and by Corollary 25 none has valuation ≥ 3. Let n_0, n_1, n_2 be the numbers of non-zero elementary divisors 1, p, p^2. Then $D \cong (\mathbb{Z}/p)^{n_1} \times (\mathbb{Z}/p^2)^{n_2}$ and

$$n_0 + n_1 + n_2 = \mathrm{rank}\, V = 3p^2 - 9p + 7, \qquad n_1 + 2n_2 = 3(p-3)^2, \qquad n_0 = \mathrm{rank}(G \bmod p).$$

For $p \geq 7$, $n_0 = 12(p-3)$, so $n_1 + n_2 = 3p^2 - 21p + 43$, and $n_2 = 3p - 16$, $n_1 = 3p^2 - 24p + 59$. For $p = 5$: $n_0 = 26$, $n_1 + n_2 = 11$, $n_1 + 2n_2 = 12$, so $n_2 = 1$ and $n_1 = 10$. This proves Theorem 2. □

Remark 30. The proof also explains the exceptional prime: $p = 5$ is the only prime ≥ 5 with $4 > p - 2$, that is, the only one for which $\sum_x x^4 \neq 0$ in $\mathbb{F}_p$ enters the count. The integer 6 in Lemma 24 is harmless because $\gcd(p, 6) = 1$. (The same condition appears, for reasons unrelated to the present proof, in the classical fact that the lines generate $\mathrm{NS}(S_m)$ if and only if $m \leq 4$ or $\gcd(m, 6) = 1$ [10, 19].)

10 Verification in Lean

The lattice statements of Theorems 1 and 2 are proved in Lean 4 [9] with the Mathlib library [13], toolchain `leanprover/lean4:v4.28.0`. The Lean definitions of the lines, of G (as the case analysis of §2), of $K = \ker G$, of $V = A/K$ with the induced form, and of $D = V^*/V$ (the dual of V modulo the range of the form) are printed verbatim in the two certificates [3, 7] and compared there, line by line, with the June papers [2,6], whose definitions are those of §2. The final theorems are:

- `Watermark.watermark_theorem`: for every prime $p \geq 5$, V is free of rank $3(p-1)(p-2)+1$, and for every $\mathbb{Z}$-basis b of V the Gram determinant is $p^{3(p-3)^2}$;
- `DoubleLadder.double_ladder_theorem`: for every prime $p \geq 7$, $D \cong (\mathbb{Z}/p)^{3p^2-24p+59} \times (\mathbb{Z}/p^2)^{3p-16}$ as abelian groups;
- `DoubleLadder.double_ladder_five`: $D \cong (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25$ at $p = 5$.

(The Lean namespaces carry the names of the two theorems, which are also the titles of the June papers [2,6].) The definitions on which the final theorems rest are the following (verbatim from the project, with comments and two line breaks removed; Lean's quotient sign, the big solidus U+29F8, is printed as /; Lean's `m` is our p, and its families `0`, `1`, `2` are those of §2):

```
abbrev Point (m : ℕ) : Type := ZMod m × ZMod m
abbrev Line (m : ℕ) : Type := Fin 3 × Point m

def gramUpper (m : ℕ) (p q : Line m) : ℤ :=
  if p.1 = q.1 then
    (if p.2 = q.2 then 2 - (m : ℤ)
     else if p.2.1 = q.2.1 ∨ p.2.2 = q.2.2 then 1 else 0)
  else if p.1 = 0 ∧ q.1 = 1 then
    (if p.2.1 - p.2.2 = q.2.1 - q.2.2 then 1 else 0)
  else if p.1 = 1 ∧ q.1 = 2 then
    (if p.2.1 + p.2.2 = q.2.1 + q.2.2 then 1 else 0)
  else if p.1 = 0 ∧ q.1 = 2 then
    (if q.2.1 - q.2.2 = p.2.1 + p.2.2 + 1 then 1 else 0)
  else 0

def gram (m : ℕ) : Matrix (Line m) (Line m) ℤ :=
  Matrix.of fun p q => if p.1 ≤ q.1 then gramUpper m p q else gramUpper m q p

abbrev A (m : ℕ) : Type := Line m → ℤ
noncomputable def gramLin (m : ℕ) [NeZero m] : A m →ₗ[ℤ] A m := (gram m).mulVecLin
noncomputable def K (m : ℕ) [NeZero m] : Submodule ℤ (A m) := LinearMap.ker (gramLin m)
abbrev V (m : ℕ) [NeZero m] : Type := A m ⧸ K m
abbrev D (m : ℕ) [NeZero m] : Type := Module.Dual ℤ (V m) ⧸ LinearMap.range (formV m)
```

This is the case analysis of §2: the four cases are the four bullet points there, and for families 0 and 2 the condition is `q.2.1 - q.2.2 = p.2.1 + p.2.2 + 1`; `gram` fills in the cases with $j > j'$ by symmetry. Here `formV m` is the form that $B(x, y) = x^{\mathsf{T}} G y$ induces on V. The

three final statements are (proofs omitted; - on $\mathbb{N}$ is truncated subtraction, which agrees with ordinary subtraction in the range of the theorems):

```
theorem watermark_theorem [Fact m.Prime] (hm : 5 ≤ m) :
    Module.Free ℤ (V m) ∧ Module.finrank ℤ (V m) = 3 * (m - 1) * (m - 2) + 1 ∧
      ∀ {ι : Type*} [Fintype ι] [DecidableEq ι] (b : Module.Basis ι ℤ (V m)),
        (LinearMap.BilinForm.toMatrix b (formV m)).det = (m : ℤ) ^ (3 * (m - 3) ^ 2)

theorem double_ladder_theorem (m : ℕ) [Fact m.Prime] (hm : 7 ≤ m) :
    Nonempty (D m ≃+ ((Fin (3 * m ^ 2 + 59 - 24 * m) → ZMod m) ×
      (Fin (3 * m - 16) → ZMod (m ^ 2))))

theorem double_ladder_five : Nonempty (D 5 ≃+ ((Fin 10 → ZMod 5) × ZMod 25))
```

They depend only on the axioms `propext`, `Classical.choice` and `Quot.sound`; the project contains no `sorry`, no `admit` and no `native_decide`. At $p = 5$ the rank 26 of G modulo 5 (lemma `rank_gram_map_five`) is proved from two identities between explicit matrices modulo 5, `hBC` and `hXY`: $G \equiv \texttt{matB} \cdot \texttt{matC}$, where `matB` has size 75×26 and `matC` has size 26×75, so the rank is at most 26; and $G_{\mathrm{rows}} \cdot \texttt{matY} \equiv I_{26}$, where G_{rows} is the 26×75 matrix of the 26 rows of G listed in `fiveRows` and `matY` has size 75×26, so the rank is at least 26. Every entry of both identities is checked by `decide +kernel`. The Lean proof follows §§4–9 with a few differences of detail recorded in the certificates: for instance, the inclusion $K_0 \subseteq K$ is proved there for every positive integer in place of p by a direct computation, the relations of Lemma 27 are identified by mixed second differences instead of polynomials, and the structure of D is obtained from $|D|$ and $|D/pD|$ instead of a Smith form. In the Lean project Lemmas 8, 15 and 12 are called R.1, R.2 and C, and K_0 is called `SAT`. Proposition 29 is not formalized. The Lean proofs were written by the system Aristotle (Harmonic) [12] from statements and proofs prepared by the author, then compiled and checked again on the author's machine, including a clean rebuild of the whole project. The project, the certificates and the logs are in the Zenodo record [4] and the repository `https://github.com/tretoef-estrella/watermark-theorem`.

Not formalized: the geometry of §3 (Mathlib has no complex algebraic surfaces and no singular cohomology of them), the equality $V = \mathrm{NS}(S_p)$, which is cited [10,15], and Corollary 3, which uses the unimodularity of $H^2(S_p, \mathbb{Z})$ and [14].

11 What was known before, and what is new

We consulted [1, 10, 11, 15–17, 20, 21] in the original; a search cannot prove that nothing else exists: it only records what we looked at.

- Shioda [20], §7, pp. 133–134, asks for the order of the discriminant, not for the group (Question 7.2, formula (7.8), and Question 7.4, formula (7.10), prime degree); Question 7.4 also asks, in (7.11), whether the lines generate NS. In "Added in proof" he notes that the discriminant divides a power of m for every degree m. Theorem 1 answers (7.10) for prime $p \geq 5$; Question 7.2 is not treated here. Degtyarev [10] answers (7.11) (the lines generate NS).
- Schütt, Shioda and van Luijk [15, end of §4]: for every odd $m \leq 81$ the Gram determinant of their rational basis $\mathcal{B}$ of lines is $m^{3(m-3)^2}$, by computer, "with exponent as conjectured"; $\mathcal{B}$ spans $\mathrm{NS}(S_m)$ when $\gcd(m, 6) = 1$ and $m < 100$ (equivalently $m \leq 100$, as in §1, since 100 is even) [15, Remark 4.5 and the proof of Theorem 1.1]; so Theorem 1 was known, by computer, for $5 \leq p \leq 79$.
- Shioda [21, §6.5, Conjecture 23] still uses the formula as expected in 2015, for every m prime to 6; the present paper proves it for prime degree only.
- Aljovin, Movasati and Villaflor [1, Table 1]: the elementary divisors for $3 \leq m \leq 14$,

by machine; for prime degree these are the rows quoted in §1, that is, Theorem 2 at $p = 5, 7, 11, 13$. They give no formula for general degree.

- Shimada [16, Theorem 1.1]: in positive characteristic ℓ, for the Fermat hypersurface of dimension $2n$ and degree $q+1$ (q a power of ℓ), the linear n-subspaces span the numerical lattice up to finite index, and the discriminant of the lattice they generate is a power of ℓ. That setting is supersingular and of degree $q + 1$, and no formula for the exponent is given there (for $\ell = q = 2$ the primitive part of the lattice, that is, its part orthogonal to the class of a linear section, is Λ_{22} in dimension 4 and has discriminant $2^{16} \cdot 3$ in dimension 6 [16, Theorems 1.5 and 1.6]).

11.1 Degtyarev and Degtyarev–Shimada

Degtyarev proves that the quotient of $\mathrm{Pic}(S_m)$ by the subgroup generated by the lines has no torsion, for every m [10, Theorem 1.3]; with the rational statement [19] this gives generation for $m \leq 4$ and for $\gcd(m, 6) = 1$ [10, Theorem 1.2]. The proof is topological. For a reduced curve C on a simply connected surface X, [10, Theorem 2.2] identifies the torsion of $H_1(X \smallsetminus C)$ with the dual of the torsion of $\mathrm{NS}(X)$ modulo the components of C, and $H_1(X \smallsetminus C)$ modulo torsion with the dual of $\ker[H_2(C) \to H_2(X)]$, the lattice of relations among the components; Degtyarev applies this to $C = \bar{L}$, the union of the lines and of the plane section $\{x_0 = 0\}$; its lattice of relations has rank $9m - 6$ for odd m and contains our K, the relations among the lines alone (of rank $9p - 7$ for prime p), with corank one. The torsion vanishes because the length of $H_1(S_m \smallsetminus \bar{L})$, computed through an Alexander module of the covering $S_m \to \mathbb{P}^2$, $(x_i) \mapsto (x_i^m)$, does not exceed that rank [10, (3.21), Lemma 4.4, §4.2]. The intersection form plays no role in the argument, which uses only an upper bound for the rank of the group generated by the lines [10, Remark 4.15]; Degtyarev notes that his theorem gives "a complete description of $\mathrm{Pic}\,\Phi_m = \mathrm{NS}(\Phi_m)$, including the intersection form" [10, §1] (his Φ_m is our S_m), but no invariant of that form, determinant or discriminant group, is computed there.

Degtyarev and Shimada [11] study the lattice $L(X)$ spanned by the standard d-dimensional subspaces of the Fermat variety of dimension $2d$. They reduce the torsion of $H_{2d}(X)/L(X)$ to the torsion of explicit modules over group rings [11, Theorem 1.1], compute the rank of $L(X)$ [11, Theorem 1.4], show that only primes dividing the degree can occur in that torsion [11, Corollary 1.5], and conjecture that $L(X)$ is primitive [11, Conjecture 1.2], which they verify by computer in dimension 4 for $3 \leq m \leq 12$ and in the cases $(2d, m) = (6, 3), (6, 4), (6, 5), (8, 3)$ [11, §5]; for $d = 1$ this is [10]. The order and the structure of the discriminant group of $L(X)$ are not determined there.

So what these works give about the discriminant of $\mathrm{NS}(S_p)$ is what we use: the lines generate $\mathrm{NS}(S_p)$, so that its discriminant is that of V. Its order and its group are the content of Theorems 1 and 2.

11.2 What is standard and what is new

Standard: the counting in the affine plane $\mathbb{F}_p^2$ behind Lemmas 7 and 8; the index of a sublattice from a Gram determinant; the isomorphism between the discriminant groups of a primitive sublattice of a unimodular lattice and of its orthogonal complement (cf. [14]); the vanishing of power sums over $\mathbb{F}_p$; and the assembly of a finite abelian p-group from its order, its exponent and the rank of a presentation matrix modulo p. New, as far as we could determine: the explicit sublattice K_0 of the kernel, with $pK \subseteq K_0$ and $[K : K_0] = p^{12}$ read off from the relations modulo p (Lemma 12, Proposition 22); the integral form, over $\mathbb{Z}$ and pencil by pencil, of the orthogonal decomposition of the lattice of lines: the pullbacks along the pencils (Lemma 9) and the vectors N_j, on which G has eigenvalues $-p$, $-2p$, $3p$ and 0, give the orthogonal block lattice F and the exact index of Corollary 23; the identity $GYG = 6p^2G$, which bounds the exponent;

and the factorization of G modulo p through twelve shadows, with the rank of Proposition 28 and the ranks of Proposition 29. Over $\mathbb{Z}[\zeta]$ the decomposition is in Schütt, Shioda and van Luijk [15, §3, (4)–(6)], who sketch there the argument of [19]: the character sums $w_j(\alpha)$ of the lines of one family are orthogonal to the plane section, $w_j(\alpha) \cdot w_j(\beta) = 0$ for $\beta \neq -\alpha$, and $w_j(\alpha) \cdot w_j(-\alpha) = -p^3$ (there for every degree m, with $-m^3$), which shows that the discriminant divides a power of p [15, Corollary 3.2]; since $w_j(-\alpha)$ is the complex conjugate of $w_j(\alpha)$, the decomposition is orthogonal for the Hermitian form $x \cdot \bar{y}$ (for the symmetric form, the planes spanned by $w_j(\alpha)$ and $w_j(-\alpha)$ are mutually orthogonal). A pullback $\mathrm{pb}_j^{\pi}(u)$ with $u \in Z_0$ is a linear combination, with coefficients in $\frac{1}{p}\mathbb{Z}[\zeta]$, of the $p-1$ character sums of its family that are constant on the fibres of the pencil; for the two axis pencils these sums are not among the $w_j(\alpha)$, and they vanish in $\mathrm{NS}(S_p) \otimes \mathbb{Z}[\zeta]$ by Lemma 9(a). The results new here are the formula $p^{3(p-3)^2}$ for every prime $p \geq 5$ (known before, by computer, for $p \leq 79$ [15], and with the group for $p \leq 13$ [1]), the structure of the discriminant group for every prime $p \geq 5$ with the exceptional value at $p = 5$, and the verification of both lattice statements in Lean.

Not done here: the discriminant bilinear form $b_V \colon D \times D \to \mathbb{Q}/\mathbb{Z}$ (we determine the group only; V is an odd lattice, and the argument of Corollary 3 would give $b_{T_p} \cong -b_V$), Question 7.2, and composite degrees. The determinant of the lattice of linear cycles of Fermat varieties of prime degree in every even dimension is treated, by other methods and modulo cited results, in [5].

Acknowledgements

The author thanks an anonymous referee for a careful preliminary report, which led to several improvements of this paper.

Use of AI

This work was developed with extensive use of AI systems: Claude (Anthropic) for exploration, computation, writing and auditing, and Aristotle (Harmonic) for writing the Lean proofs. The first version of this text was read before release by a separate reader, also an AI system, and this revised version by further separate readers, also AI systems, working from the sources and the Lean files; their reports led to corrections, all of which are included here. The statements, the choice of what to claim and the responsibility for errors are the author's.

References

[1] E. Aljovin, H. Movasati, R. Villaflor Loyola, *Integral Hodge conjecture for Fermat varieties*, J. Symbolic Comput. **95** (2019), 177–184, doi:10.1016/j.jsc.2019.02.006. arXiv:1711.02628.

[2] R. Amichis Luengo, *The Double Ladder Theorem*, version 4 (30 September 2026), in [4].

[3] R. Amichis Luengo, *The Double Ladder Theorem — Lean certificate*, version 2 (30 September 2026), in [4].

[4] R. Amichis Luengo, *The Watermark and Double Ladder Theorems (Verified in Lean)*, Zenodo (2026), doi:10.5281/zenodo.23062529 (all versions).

[5] R. Amichis Luengo, *The Watermark in Every Even Dimension: the Discriminant of the Hodge Lattice of a Fermat Variety of Prime Degree*, Zenodo (2026), doi:10.5281/zenodo.23091046.

[6] R. Amichis Luengo, *The Watermark Theorem*, 4 June 2026, with the version note of 30 September 2026, in [4].

[7] R. Amichis Luengo, *The Watermark Theorem — Lean certificate*, version 2 (30 September 2026), in [4].

[8] N. Aoki, T. Shioda, *Generators of the Néron–Severi group of a Fermat surface*, in: Arithmetic and Geometry, Vol. I, Progr. Math. **35**, Birkhäuser, Boston (1983), 1–12.

[9] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer (2021), 625–635.

[10] A. Degtyarev, *Lines generate the Picard groups of certain Fermat surfaces*, J. Number Theory **147** (2015), 454–477. arXiv:1305.3073.

[11] A. Degtyarev, I. Shimada, *On the topology of projective subspaces in complex Fermat varieties*, J. Math. Soc. Japan **68** (2016), no. 3, 975–996. arXiv:1405.4683.

[12] Harmonic, *Aristotle* (automated theorem prover), `https://aristotle.harmonic.fun`, accessed September 2026.

[13] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM (2020), 367–381.

[14] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izv. **14** (1980), 103–167.

[15] M. Schütt, T. Shioda, R. van Luijk, *Lines on Fermat surfaces*, J. Number Theory **130** (2010), no. 9, 1939–1963. arXiv:0812.2377.

[16] I. Shimada, *Lattices of algebraic cycles on Fermat varieties in positive characteristics*, Proc. London Math. Soc. (3) **82** (2001), no. 1, 131–172.

[17] I. Shimada, N. Takahashi, *Primitivity of sublattices generated by classes of curves on an algebraic surface*, Comment. Math. Univ. St. Pauli **59** (2010), no. 2, 77–95.

[18] T. Shioda, *The Hodge conjecture for Fermat varieties*, Math. Ann. **245** (1979), 175–184.

[19] T. Shioda, *On the Picard number of a Fermat surface*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 725–734 (1982).

[20] T. Shioda, *Some observations on Jacobi sums*, in: Galois Representations and Arithmetic Algebraic Geometry, Adv. Stud. Pure Math. **12**, Kinokuniya / North-Holland (1987), 119–135.

[21] T. Shioda, *Mordell–Weil lattice of higher genus fibration on a Fermat surface*, J. Math. Sci. Univ. Tokyo **22** (2015), 443–468.