hexagon:2610.00527v1

GALOIS GROUPS OF TAYLOR POLYNOMIALS: PRESCRIPTIONS AND ARITHMETIC FAMILIES

KHAI-HOAN NGUYEN-DANG

Abstract. Let $f_n(x) = \sum_{j=0}^{n} a_j x^j$ be the Taylor polynomials of a power series with nonzero rational coefficients. We study the proportions of degrees for which the Galois group over $\mathbb{Q}$ is symmetric, alternating, or neither. We prove that the set of degrees $n \geq 3$ with symmetric group can be chosen arbitrarily, even for an entire function with positive rational coefficients whose Taylor polynomials have distinct negative real roots. More precisely, at each degree $n \geq 3$, f_n has exactly one rational root, and the group on the other roots is the full symmetric group. Thus the proportions need not converge; when they do, the proportion of other groups can be any number in $[0, 1]$. These conclusions answer negatively two questions of Katz and Rivin. Moreover, for fixed $s \in \mathbb{Q} \setminus \mathbb{Z}$, we also give a condition on the prime divisors of rational multipliers of the coefficients $s/(s + j)$ that forces symmetric groups in density one. For the Taylor polynomials of $(1 - x)^{-s}$, we determine the groups in all sufficiently large degrees. The number of exceptions to the symmetric group up to degree X is $c_s\sqrt{X} + O_s(1)$, with an explicit constant $c_s \geq 0$.

We also determine the groups of the central-binomial Taylor polynomials in every degree and prove that every nonconstant Catalan Taylor polynomial has symmetric group. This proves Sun's Catalan group conjecture and his irreducible-reduction criterion for the monic reciprocals of the central-binomial polynomials.

1. Introduction

Let

$$f(x) = \sum_{j\geq 0} a_j x^j \in \mathbb{Q}[[x]], \qquad a_j \neq 0, \qquad f_n(x) = \sum_{j=0}^{n} a_j x^j.$$

We study the Galois group over $\mathbb{Q}$ of the degree-n Taylor polynomial f_n as n varies. In particular, we ask how often this group is the symmetric group $\mathfrak{S}_n$, the alternating group $\mathfrak{A}_n$, or neither.

The classical example is the exponential series. Schur proved in 1930 that

$$E_n(x) = \sum_{j=0}^{n} \frac{x^j}{j!}, \qquad n \geq 1,$$

has Galois group $\mathfrak{A}_n$ when $4 \mid n$ and $\mathfrak{S}_n$ otherwise [40]. Symmetric groups therefore occur in three quarters of the degrees and alternating groups in one quarter. Coleman's proof [11] uses Newton polygons to obtain permutations in the Galois group from the prime divisibility of the factorial denominators. Related arguments apply to generalized Laguerre polynomials [21].

On the other hand, the geometric series gives a different example. Its Taylor polynomial is $(x^{n+1} - 1)/(x - 1)$, so its splitting field is cyclotomic and its group is abelian. For $n \geq 4$ the group is therefore neither $\mathfrak{S}_n$ nor $\mathfrak{A}_n$. In these two examples, all three proportions converge, and the proportion of groups of neither kind is zero or one.

Katz and Rivin [26, Questions 1.1–1.2] ask whether this happens for every power series with nonzero rational coefficients. More precisely, they ask whether the three proportions always converge and, when they all converge, whether the third limit must be zero or one.

Date: 24 October 2026.

2020 *Mathematics Subject Classification.* Primary 11R32, 12F12; Secondary 11N37, 12E05, 30C15, 03D45.

Key words and phrases. Taylor polynomial, Galois group, Hilbert irreducibility, Newton polygon.

Our first result answers both questions negatively. We prove that for any set of degrees $B \subseteq \{3, 4, \ldots\}$, we construct an entire function with positive rational coefficients such that, for $n \geq 3$, its degree-n Taylor polynomial has group $\mathfrak{S}_n$ precisely when $n \in B$. In the remaining degrees $n \geq 3$, it has one rational root and an irreducible factor of degree $n-1$ with group $\mathfrak{S}_{n-1}$. Every Taylor polynomial has distinct negative real roots. Thus even these restrictions on convergence, signs, and zeros leave the set of symmetric degrees arbitrary.

We then give conditions on the prime divisors of the coefficients that force the symmetric group to occur in density one. For nonintegral binomial powers, an exact discriminant formula determines the exceptional degrees and gives their asymptotic number. For the central-binomial and Catalan generating functions, we determine the groups in every degree over $\mathbb{Q}$.

1.1. **Prescribing the degrees with symmetric group.** We call f_n the degree-n *section* of f. For a polynomial $P \in F[X]$, where F is a number field, write $\mathrm{Gal}_F(P)$ for the group of its splitting field over F, acting on its roots. If P is separable of degree n, this gives a subgroup of $\mathfrak{S}_n$, defined up to conjugacy. Put $G_n = \mathrm{Gal}_{\mathbb{Q}}(f_n)$ and

$$\begin{aligned} s_f(N) &= \frac{1}{N}\#\{3 \leq n \leq N : G_n = \mathfrak{S}_n\}, \\ a_f(N) &= \frac{1}{N}\#\{3 \leq n \leq N : G_n = \mathfrak{A}_n\}, \\ o_f(N) &= \frac{1}{N}\#\{3 \leq n \leq N : f_n \text{ is other}\}. \end{aligned}$$

Here a section is called *other* if it has a repeated root, or if it is separable and its group is neither $\mathfrak{S}_n$ nor $\mathfrak{A}_n$. The first two degrees are omitted to avoid small-degree coincidences; omitting them does not affect any limit. When the limits exist, we denote them by $S(f), A(f), O(f)$.

The construction also controls polynomials formed from finite consecutive blocks of coefficients. More precisely, for $0 \leq r < s$, put

$$f_{r,s}(X) = \sum_{j=r}^{s} a_j X^{j-r}, \qquad K_{r,s} = \text{its splitting field over } \mathbb{Q}. \tag{1.1}$$

We call $f_{r,s}$ a *normalized segment*, and a *proper segment* when $r \geq 1$. Normalization removes the initial power X^r, so the segment has nonzero constant term and degree $s - r$. We will require all proper segments to have full symmetric groups. We will also require the splitting fields to be jointly linearly disjoint: for every finite set I of the relevant pairs (r, s),

$$\left[\prod_{(r,s)\in I} K_{r,s} : \mathbb{Q}\right] = \prod_{(r,s)\in I} [K_{r,s} : \mathbb{Q}],$$

where the product of fields means their compositum in a fixed algebraic closure. Finally, $1 \oplus \mathfrak{S}_{n-1}$ denotes the subgroup of $\mathfrak{S}_n$ fixing one root and permuting the other $n-1$ roots arbitrarily.

Theorem A. *Let $B \subseteq \{3, 4, \dots\}$ and let $(\varepsilon_n)_{n\geq 2}$ be positive real numbers. There is an entire function*

$$f(z) = 1 + z + \sum_{n\geq 2} a_n z^n, \qquad a_n \in \mathbb{Q}_{>0},$$

with the following properties.

(i) *We have $G_2 = \mathfrak{S}_2$ and, for $n \geq 3$,*

$$G_n = \begin{cases} \mathfrak{S}_n, & n \in B, \\ 1 \oplus \mathfrak{S}_{n-1}, & n \notin B. \end{cases} \tag{1.2}$$

In the second case, the unique rational root is a negative integer and the remaining factor is irreducible of degree $n - 1$.

(ii) *For every $n \geq 2$,*

$$0 < a_n < \min\{\varepsilon_n, 2^{-n^2}\}, \qquad a_{n-1}^2 > 4a_{n-2}a_n. \tag{1.3}$$

The function has order zero and infinitely many zeros, all simple and negative. Every $f_{r,s}$ has $s - r$ distinct negative real zeros.

(iii) *Every proper segment of degree at least two has full symmetric group:*

$$\mathrm{Gal}(K_{r,s}/\mathbb{Q}) = \mathfrak{S}_{s-r} \qquad (1 \leq r \leq s - 2). \tag{1.4}$$

All fields $K_{r,s}$ with $0 \leq r \leq s - 2$ are totally real and jointly linearly disjoint over $\mathbb{Q}$.

Moreover, if B is decidable, i.e., if an algorithm decides membership at every input, and (ε_n) is a uniformly computable sequence of positive real numbers, the rational coefficients can be computed uniformly from these data.

The coefficients a_n, $n \geq 2$, may thus be required to lie below any prescribed positive bounds. The order of an entire function is $\rho(f) = \limsup_{R\to\infty} \log\log M_f(R)/\log R$, where $M_f(R) = \max_{|z|=R} |f(z)|$.

If B has natural density δ, Theorem A gives

$$(S(f), A(f), O(f)) = (\delta, 0, 1 - \delta).$$

If B has no density, the symmetric groups and other proportions do not converge. This proves both negative answers to Katz and Rivin. More generally, the lower and upper limits of $s_f(N)$ can be any prescribed $0 \leq \alpha \leq \beta \leq 1$; Corollary 7.4 describes all the subsequential limits. The problem of characterizing all series with convergent proportions remains open. The same frequency conclusions hold over every number field, since only finitely many of these segment groups can change after extending the ground field (Corollary 7.5).

A simple example with convergent proportions is the rational function

$$h_2(x) = \frac{1 + x^2}{1 - x} = 1 + x + 2x^2 + 2x^3 + \cdots, \qquad (S(h_2), A(h_2), O(h_2)) = (1/2, 0, 1/2). \tag{1.5}$$

Its even sections have symmetric group, whereas every odd section of degree at least three has the root -1 (Proposition 6.2).

1.2. **An arithmetic condition for density one.** We next consider polynomials obtained from $\sum_{j=0}^{n} sx^j/(s + j)$, with fixed $s \in \mathbb{Q} \setminus \mathbb{Z}$, by multiplying each coefficient by a nonzero rational number. We impose a condition on the prime factors of these multipliers: their numerators and denominators, in lowest terms, have no prime factor larger than $n+C$, where $C \geq 0$ is fixed. The condition preserves the coefficient valuations at primes larger than $n + C$, which are the primes used in the proof.

We state the result over a number field F. Let R_F be the largest rational prime ramified in F, with $R_{\mathbb{Q}} = 1$. The explicit integer $N(a, b, C, F)$ is defined in (4.2). For frequencies over F, we use

the notation $s_{f,F}(N), a_{f,F}(N), o_{f,F}(N)$ and $S_F(f), A_F(f), O_F(f)$, obtained by replacing $\mathbb{Q}$ with F in the definitions above.

Theorem B. *Fix $s = a/b \in \mathbb{Q} \setminus \mathbb{Z}$ in lowest terms, with $b \geq 2$, and a constant $C \geq 0$. For $n \geq 1$, let*

$$R_n(x) = \sum_{j=0}^{n} u_{n,j} \frac{s}{s+j} x^j, \qquad u_{n,j} \in \mathbb{Q}^\times.$$

Suppose that every $u_{n,j}$ is a p-adic unit at every prime $p > n + C$. Over every fixed number field F, the polynomial R_n is irreducible and its Galois group contains $\mathfrak{A}_n$ for every $n \geq N(a, b, C, F)$. For every odd n in this range, its group is $\mathfrak{S}_n$. Moreover, for every $\varepsilon > 0$,

$$\#\{1 \leq n \leq X : \mathrm{Gal}_F(R_n) \neq \mathfrak{S}_n\} \ll_{s,C,F,\varepsilon} X^{1/2+\varepsilon}. \tag{1.6}$$

The threshold and implied constant are uniform in the multipliers.

Thus, beyond the stated threshold, the only possible groups are $\mathfrak{A}_n$ and $\mathfrak{S}_n$, and the alternating degrees have density zero. Allowing the multipliers to depend on n is useful when a change of variable produces a different formula in each degree, as it will for the binomial polynomials below. If the polynomials are sections of one series, that series has frequency triple $(1, 0, 0)$ over F.

For example, the theorem applies to bounded nonzero integer multiples of the coefficients of

$$\sum_{j \geq 0} \frac{s}{(s+j)(j!)^r} x^j, \qquad r \in \mathbb{Z}_{\geq 0}.$$

Section 4.5 gives the resulting Kummer and error-function examples, as well as extensions to polynomial multipliers. A smaller explicit threshold for half-integral s is given in Appendix A.2.

1.3. **Binomial and Catalan polynomials.** We consider certain polynomials to extract more information. Fix $s \in \mathbb{Q} \setminus \mathbb{Z}$. The Taylor polynomials of $(1-x)^{-s}$ are

$$B_{s,n}(x) = \sum_{j=0}^{n} \frac{(s)_j}{j!} x^j, \qquad (s)_0 = 1, \quad (s)_j = s(s+1)\cdots(s+j-1).$$

An affine change of variable puts them in the family of Theorem B. Once the Galois group contains $\mathfrak{A}_n$, the polynomial's discriminant determines whether the group is $\mathfrak{A}_n$ or $\mathfrak{S}_n$: the former occurs exactly when the discriminant is a square in the ground field. We write $F^{\times 2} = \{u^2 : u \in F^\times\}$ for the nonzero squares in F.

Theorem C. *Fix $s = a/b \in \mathbb{Q} \setminus \mathbb{Z}$ in lowest terms, $b \geq 2$, and a number field F. For every $n \geq N(a, b, 0, F)$,*

$$\mathrm{Gal}_F(B_{s,n}) = \begin{cases} \mathfrak{A}_n, & n \text{ even and } (-1)^{n/2} a(a+bn) \in F^{\times 2}, \\ \mathfrak{S}_n, & \text{otherwise.} \end{cases} \tag{1.7}$$

There is an explicitly computable constant $c_{s,F} \geq 0$ such that

$$\#\{1 \leq n \leq X : \mathrm{Gal}_F(B_{s,n}) \neq \mathfrak{S}_n\} = c_{s,F}\sqrt{X} + O_{s,F}(1). \tag{1.8}$$

The constant vanishes exactly when every sufficiently large section has symmetric group. It is positive for every $s > 0$. In all cases, $(1-x)^{-s}$ has triple $(1, 0, 0)$ over F.

For positive nonintegral s, the theorem gives infinitely many alternating degrees, although the symmetric degrees have density one. The square-root count shows that the exponent $1/2$ in the general exceptional bound cannot be decreased. Formula (4.16) computes $c_{s,F}$ from the quadratic subfields of F and finitely many congruences. Over $\mathbb{Q}$, Corollary 4.4 gives a closed formula and determines exactly which negative parameters have infinitely many alternating degrees.

Here the exponent s is fixed and the degree tends to infinity. Filaseta and Moy [18] study the complementary problem in which the degree is fixed and a positive integral exponent varies. The identity (4.14) also expresses $B_{s,n}$ as a Jacobi polynomial with one parameter depending on n; its derivation is given in Section 4 (see also [34]).

For the central-binomial generating function $(1-4x)^{-1/2}$, we obtain a classification in every degree. This proves the group pattern observed by Rabarison, Pazuki, and Molin [36, Section 4.1]. It also proves Sun's criterion for the existence of an irreducible reduction of the monic reciprocal polynomial [45, part (ii)].

Theorem D. *Let $C_n(x) = \sum_{j=0}^{n} \binom{2j}{j} x^j$. For every $n \geq 1$,*

$$\mathrm{Gal}_{\mathbb{Q}}(C_n) = \begin{cases} \mathfrak{A}_n, & n = 2r(r+1) \text{ for an integer } r \geq 1, \\ \mathfrak{S}_n, & \text{otherwise.} \end{cases} \tag{1.9}$$

Over a number field F, for every $n \geq R_F$,

$$\mathrm{Gal}_F(C_n) = \begin{cases} \mathfrak{A}_n, & n \text{ even and } (-1)^{n/2}(2n+1) \in F^{\times 2}, \\ \mathfrak{S}_n, & \text{otherwise.} \end{cases} \tag{1.10}$$

The monic reciprocal $x^n C_n(1/x)$ is irreducible modulo some prime if and only if n is not of the form $2r(r+1)$. In those degrees, such primes have relative natural density $1/n$.

In particular, in the exceptional degrees $2r(r+1)$ the monic reciprocal is irreducible over $\mathbb{Q}$ but reducible modulo every prime. The exceptional degrees come from the square condition on the discriminant. The proof of alternating containment uses the uniform criterion together with explicit arguments for the remaining small degrees.

The Catalan numbers $c_j = \binom{2j}{j}/(j+1)$ have generating function $(1-\sqrt{1-4x})/(2x)$. Seki [41, Theorem 1.1] proved that every nonconstant Taylor polynomial of this function is irreducible over $\mathbb{Q}$. We use his theorem to determine the full Galois group, as conjectured by Sun [45, part (i)].

Theorem E. *For every $n \geq 1$, the polynomial*

$$P_n(x) = \sum_{j=0}^{n} c_j x^j$$

has Galois group $\mathfrak{S}_n$ over $\mathbb{Q}$. For every number field F,

$$\mathrm{Gal}_F(P_n) = \mathfrak{S}_n \qquad (n \geq R_F).$$

In particular, $(1-\sqrt{1-4x})/(2x)$ has triple $(1,0,0)$ over F.

Both the central-binomial and Catalan generating functions are algebraic of degree two. Their Taylor polynomials nevertheless have the full symmetric group over $\mathbb{Q}$, apart from the explicit alternating degrees in Theorem D. Sun's additional bound n^2+n+5 for the least prime at which the monic reciprocal $x^n P_n(1/x)$ has irreducible reduction remains open.

1.4. **Methods and further results.** The construction in Theorem A chooses one coefficient at a time. Reversing the next Taylor polynomial gives

$$X^n f_n(1/X) = g_n(X) + a_n, \qquad g_n(X) = \sum_{j=0}^{n-1} a_j X^{n-j}. \tag{1.11}$$

The coefficients already chosen determine g_n, while a_n is now a constant parameter. We arrange that the relevant polynomials have simple critical points and distinct critical values, with no critical value shared by two of them. A simultaneous version of the linear perturbation argument in [8, Theorem 13] preserves these conditions outside a finite set of choices. These conditions give

the full product of the symmetric groups before specialization. Hilbert irreducibility then gives the required groups for all segments ending at the new degree and makes their splitting fields disjoint from the preceding fields. Adjoining one root before specialization gives the alternative with one rational root. The specializations can be made small and positive, so Hutchinson's coefficient inequalities [23] give the assertions about real zeros.

The simultaneous control of proper segments is related to the conjecture of Bary-Soroker and Ben-Porath [2, Conjecture 1] for proper segments of the exponential series. They prove simultaneous probabilistic results, and Weinbaum [47, Theorem 1.1] proves density-one symmetry for each fixed positive shift. The all-degree problem for proper segments of the fixed exponential series remains open. Earlier questions about irreducibility of Taylor polynomials arose in Katz's 2009 Princeton course; see [9, Introduction]. Chambert-Loir also constructs sections with highly multiple roots [9, Example 3.7].

For Theorem B, suitable primes larger than the degree give a Newton polygon with two primitive edges. The corresponding local factors have degrees j and $n-j$, and inertia supplies a permutation with these two cycles. Using several such primes forces irreducibility and excludes partitions of the roots into nontrivial Galois blocks. Müller's classification [32, Theorem 3.3] then gives containment of $\mathfrak{A}_n$; this step uses the classification of finite simple groups. In even degree, the local discriminant square class at the chosen primes is independent of the allowed multipliers. Heath–Brown's quadratic large sieve [22] bounds the number of degrees in which the discriminant can be a square in the fixed number field. For binomial polynomials, the exact discriminant formula reduces the exceptional count to quadratic congruences.

The Catalan proof begins with the transitivity supplied by Seki's irreducibility theorem. In sufficiently large degree, local inertia rules out all possible block systems except a partition into two blocks. We extend Seki's trace argument from rational factors to possible Galois blocks. The resulting congruences and size bounds force the sums of roots in the two blocks to be distinct rational integers, which is incompatible with transitivity. The classical Jordan–Marggraff theorem [29, Theorem A] then gives the required alternating containment, and an odd inertia permutation gives the symmetric group.

There are also examples with constant term 1 and all other coefficients in $\{1, \dots, 35\}$. Proposition 2.7 gives, after any finite choice of these coefficients, a computable continuation for which $o_f(N)$ has lower limit zero and upper limit one. The proof combines a random-polynomial estimate from [3, Theorems 1(a) and 6] with extensions having many cyclotomic factors. Section 7 gives criteria for convergence and shows that convergence cannot be decided uniformly from a program for the rational coefficients. It also gives a finite test when the Galois labels themselves are generated by an automaton.

Organization. Section 2 proves Theorem A and the bounded-coefficient constructions. Section 3 gives the local Galois criteria. Section 4 proves Theorems B, C, and D; Section 5 proves Theorem E. Section 6 treats further rational and classical families, and Section 7 develops the frequency and computability consequences. The remaining questions are collected in Section 7.6. Appendix A proves the explicit prime estimates.

AI Declaration. OpenAI's ChatGPT was used in the preparation and revision of this paper to assist with mathematical arguments and to prepare and run exact-arithmetic code for the finite certificates. The October 2026 revisions used GPT-6 Astra Pro. Responsibility for the mathematical claims, references, and final text rests with the author.

2. Prescribing all sections and segments

2.1. **Specialization and simultaneous covers.** A polynomial g of degree $d \geq 2$ is *Morse* if g' has $d-1$ distinct zeros and g takes distinct values at them. A finite extension $L/\mathbb{Q}(T)$ is *regular*

over $\mathbb{Q}$ if $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$, in an algebraic closure containing both fields. The following specialization lemma will be applied to products of polynomials, so its formulation allows reducible polynomials.

Lemma 2.1. *Let $P(X, U) \in \mathbb{Q}(U)[X]$ be monic and separable, possibly reducible, and suppose that its splitting field over $\mathbb{Q}(U)$ is regular over $\mathbb{Q}$, with group G. Let $E/\mathbb{Q}$ be a finite extension. There are arbitrarily large positive integers u for which $P(X, u)$ is defined and separable, has Galois group G in its given action on the roots, and has splitting field linearly disjoint from E over $\mathbb{Q}$. Any prescribed finite set of values of u may also be excluded.*

Proof. Let L be the splitting field of P over $\mathbb{Q}(U)$, and let $E^*/\mathbb{Q}$ be a Galois closure of $E/\mathbb{Q}$. Regularity gives

$$\mathrm{Gal}(LE^*/\mathbb{Q}(U)) = G \times \mathrm{Gal}(E^*/\mathbb{Q}).$$

After removing finitely many parameter values, the normalization of the parameter line in LE^* is a finite *étale* Galois cover. At a rational parameter u, each residue field of its fibre is a copy of $L_u E^*$, where L_u is the splitting field of $P(X, u)$. The specialization theorem for Galois covers [42, Proposition 3.3.1] shows that, outside a thin subset of $\mathbb{Q}$, the fibre is a single field of the full generic degree. Hence

$$[L_u E^* : \mathbb{Q}] = |G|[E^* : \mathbb{Q}].$$

The specialization action on the roots identifies $\mathrm{Gal}(L_u/\mathbb{Q})$ with a subgroup of G. The equality of degrees therefore forces this subgroup to be all of G and makes L_u linearly disjoint from E^*, hence from E. This is the disjointness argument of [42, Proposition 3.3.3]; it uses the splitting-field cover and does not require P to be irreducible.

Include the poles of the coefficients, the zeros of the discriminant, and the prescribed finite excluded set among the exceptional values. By the integral thin-set estimate [42, Theorem 3.4.4], the exceptional integers in $[-H, H]$ number $O(H^{1/2} \log H)$. Thus arbitrarily large positive integers satisfy all the required conditions. □

The next lemma makes the induction possible: the conditions for the next degree exclude only finitely many values of the new coefficient. Its one-polynomial form appears in the proof of [8, Theorem 13].

Lemma 2.2. *Let $\ell \geq 1$, and let $h_1, \ldots, h_\ell \in \mathbb{C}[X]$ be pairwise distinct polynomials of degrees at least two. For all but finitely many $c \in \mathbb{C}$, the polynomials $h_i(X) + cX$ are Morse and their sets of critical values are pairwise disjoint.*

Proof. A repeated critical point for the ith polynomial satisfies $h_i''(x) = 0$ and $c = -h_i'(x)$. These equations exclude only finitely many values of c. On a small disk avoiding them, label all critical points holomorphically as $\xi_{i,j}(c)$, and write

$$v_{i,j}(c) = h_i(\xi_{i,j}(c)) + c\xi_{i,j}(c).$$

Since $h_i'(\xi_{i,j}(c)) + c = 0$, differentiation gives

$$v_{i,j}'(c) = \xi_{i,j}(c).$$

Two critical values of the same polynomial cannot agree identically, because their derivatives are distinct critical points. Suppose that critical values belonging to h_i and h_k, with $i \neq k$, agree identically. Their critical points then agree as a holomorphic function $\xi(c)$. If $h_i' - h_k'$ is nonzero, $\xi(c)$ takes values in its finite zero set and is constant, contradicting $h_i'(\xi(c)) + c = 0$. If $h_i' = h_k'$, the polynomial $h_i - h_k$ is a nonzero constant, which also prevents the critical values from agreeing. Hence no two of these critical-value functions agree identically. Their finitely many pairwise differences have a product which is not identically zero. There is consequently a parameter on the disk for which all critical values are distinct.

For a global finite exceptional set, consider

$$D(c,Y)=\prod_{i=1}^{\ell}\operatorname{Res}_X\big(h_i'(X)+c,\ h_i(X)+cX-Y\big).$$

Its leading coefficient in Y is nonzero and independent of c. Away from the already excluded parameters, its roots are all the critical values under consideration. The preceding textbf shows that $\operatorname{Disc}_Y D(c,Y)$ is a nonzero polynomial in c. Its zeros, together with the repeated-critical-point parameters, give the required finite set. A polynomial of degree one in Y has discriminant 1, so that case causes no exception. □

Disjoint critical-value sets make the symmetric groups of the individual covers independent. The same independence remains after one root of one polynomial is adjoined to the base field.

Lemma 2.3. *Let $g_0,\dots,g_k\in\mathbb{Q}[X]$ be pairwise distinct Morse polynomials, with degrees $d_i\ge 2$ and leading coefficients b_i. Suppose their sets of finite critical values are pairwise disjoint.*

(i) *The common splitting field of the polynomials $g_i(X)+T$ over $\mathbb{Q}(T)$ is regular over $\mathbb{Q}$ and has group*

$$\prod_{i=0}^{k}\mathfrak{S}_{d_i} \tag{2.1}$$

in its action on their respective root sets.

(ii) *For an independent variable R, put*

$$Q_{g_0}(X,R)=\frac{g_0(X)-g_0(R)}{X-R}. \tag{2.2}$$

The common splitting field over $\mathbb{Q}(R)$ of

$$Q_{g_0}(X,R),\qquad g_i(X)-g_0(R)\quad(1\le i\le k)$$

is regular over $\mathbb{Q}$ and has group

$$\mathfrak{S}_{d_0-1}\times\prod_{i=1}^{k}\mathfrak{S}_{d_i} \tag{2.3}$$

in the natural action on each displayed factor. In particular, each factor is irreducible over $\mathbb{Q}(R)$.

Dividing the respective polynomials by b_i makes them monic without changing any of these assertions.

Proof. The polynomials $g_i(X)+T$ are separable over $\mathbb{Q}(T)$ and have pairwise disjoint root sets. Indeed, a common root for $i\ne j$ would be algebraic over $\mathbb{Q}$, as a root of the nonzero polynomial g_i-g_j, and would then force T to be algebraic.

For a single polynomial, part (i) is Hilbert's theorem [42, Theorem 4.4.1]. The map $g_i:\mathbb{P}^1_{\mathbb{C}}\to\mathbb{P}^1_{\mathbb{C}}$ has distinct finite branch values, each with one simple ramification point. The corresponding branch permutations are transpositions. They generate the geometric monodromy group: the permutation around infinity is the inverse of their product. The cover is connected, so this group is transitive. A transitive group generated by transpositions is the full symmetric group: the graph joining the two letters of each generating transposition is connected, and its edge transpositions generate all permutations.

Let H be the geometric group of the common splitting field. It embeds in the product in (2.1) and projects onto each factor. The finite branch values in the T-line are the negatives of the critical values of the g_i. A small loop around one belonging only to g_i gives a transposition in the ith factor and the identity in every other factor, since the branch sets are disjoint. Conjugating

this element by H gives all transpositions in the ith factor. Thus H contains each full factor and equals their product. The arithmetic group is contained in the same product and contains H, so it equals H. Its quotient by the geometric group is the Galois group of the constant field over $\mathbb{Q}$; that field is therefore $\mathbb{Q}$. This proves both the group assertion and regularity.

Let L be the common splitting field and let α be a root of $g_0(X) + T$. Its stabilizer in the product is (2.3), and its fixed field is

$$\mathbb{Q}(T)(\alpha) = \mathbb{Q}(\alpha), \qquad T = -g_0(\alpha).$$

Here α is transcendental over $\mathbb{Q}$. Identify this fixed field with $\mathbb{Q}(R)$ by sending α to R. The other roots of $g_0(X) + T$ become the roots of $Q_{g_0}(X, R)$, and the remaining root sets become those of $g_i(X) - g_0(R)$. Together they generate L over $\mathbb{Q}(R)$. The stabilizer acts transitively on each set as the asserted symmetric group, proving (ii). The identity $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$ also proves regularity over this larger base field. The displayed factors remain separable and have disjoint root sets, since they are obtained by extending the base field and removing the root α. □

2.2. **Real zeros.** The analytic condition in the main theorem is a strict form of Hutchinson's criterion [23]; see also the discussion in [27, §1]. We include a proof to record simplicity and the finite-segment assertion explicitly.

Lemma 2.4. *Let $a_j > 0$ for all $j \geq 0$, and suppose*

$$a_j^2 > 4a_{j-1}a_{j+1} \qquad (j \geq 1). \tag{2.4}$$

Then $f(z) = \sum_{j\geq 0} a_j z^j$ is entire of order zero. Every nonconstant normalized finite segment $f_{r,s}$ has only simple negative real zeros. The function f has infinitely many zeros, all simple and negative. The same conclusions hold for every coefficient shift $\sum_{j\geq 0} a_{r+j} z^j$.

Proof. Put $r_k = a_{k-1}/a_k$ for $k \geq 1$. The assumption is $r_{k+1} > 4r_k$, whence

$$a_n \leq a_0 r_1^{-n} 4^{-n(n-1)/2}. \tag{2.5}$$

This proves entire convergence and, by completing the square in the exponent of the majorant, gives $\log M_f(R) = O((\log R)^2)$ as $R \to \infty$. Thus $\rho(f) = 0$.

Set $x_k = 2r_k$ and $x_0 = 0$. Fix $N \geq k \geq 1$. In the sum for $f_N(-x_k)$, divide by $(-1)^k a_k x_k^k$. On either side of the term with index k, the terms alternate and their absolute values strictly decrease as one moves away from that index. The first absolute value on the left is $r_k/x_k = 1/2$; on the right it is $x_k/r_{k+1} < 1/2$, if that side is present. An alternating sum starting with a negative term and decreasing in absolute value is bounded below by its first term. Consequently

$$\frac{(-1)^k f_N(-x_k)}{a_k x_k^k} \geq 1 - \frac{1}{2} - \frac{x_k}{r_{k+1}} > 0, \tag{2.6}$$

where omitting the last term only improves the estimate when $k = N$. Since $f_N(0) > 0$, there is a root in each of the N disjoint intervals

$$(-x_k, -x_{k-1}) \qquad (1 \leq k \leq N).$$

The degree is N, so these are all the roots and each is simple. The same argument applies to a finite consecutive sequence $a_r, \ldots, a_s$, proving the assertion for $f_{r,s}$.

The estimate (2.6) also holds with f in place of f_N, either by absolute convergence of the alternating sums or by taking $N \to \infty$. Thus f has at least one zero in each displayed interval. Hurwitz's theorem, applied off the nonpositive real axis, excludes nonreal zeros, and $f(0) = a_0 > 0$. There can be at most one zero, counted with multiplicity, in any one of these intervals. Otherwise choose a small rectangle around two zeros, counted with multiplicity, whose closure has real part inside that interval and whose boundary contains no zero of f. Local uniform convergence and Rouché's theorem would force f_N to have at least two zeros in the rectangle for large N, contrary

to what was just proved. Finally, $x_k \to \infty$ and $f(-x_k) \neq 0$, so these intervals contain every zero of f. Reindexing the coefficients gives the assertion for every shift. □

The entire functions in Theorem A are locally uniform limits of polynomials with positive coefficients and negative real zeros. They therefore belong to the Laguerre–Pólya class of type I and are section-hyperbolic in the terminology of [27].

2.3. **Main construction.**

Proof of Theorem A. Set $a_0 = a_1 = 1$. At stage $n \geq 2$, the coefficients $a_0, \ldots, a_{n-1}$ have been chosen. For $0 \leq r < n$, put

$$g_{r,n}(X) = \sum_{j=r}^{n-1} a_j X^{n-j}. \tag{2.7}$$

Thus $g_{0,n} = g_n$, and choosing $a_n = t$ gives

$$X^{n-r} f_{r,n}(1/X) = g_{r,n}(X) + t, \qquad g_{r,n+1}(X) = X g_{r,n}(X) + tX. \tag{2.8}$$

We maintain the following condition: the polynomials $g_{r,n}$ for $0 \leq r \leq n-2$ are Morse, and their critical-value sets are pairwise disjoint. At $n = 2$ this holds because the only polynomial is $g_{0,2} = X^2 + X$.

Let E be the compositum of all fields $K_{r,s}$ with $s < n$ and $0 \leq r \leq s-2$, taking $E = \mathbb{Q}$ when $n = 2$. Set

$$\eta_n = \min\left\{\varepsilon_n, 2^{-n^2}, \frac{a_{n-1}^2}{4a_{n-2}}\right\} > 0. \tag{2.9}$$

For $0 \leq r \leq n-1$, the polynomials $X g_{r,n}(X)$ have distinct degrees $n+1, n, \ldots, 2$. Lemma 2.2 therefore excludes only finitely many values of t for which the family $g_{r,n+1}$ fails the next induction condition. Enlarge this finite set to include the values for which

$$\prod_{r=0}^{n-2} (g_{r,n}(X) + t)$$

has a repeated root. This adds only finitely many values, by the separability assertion in Lemma 2.3. Call the resulting finite set F_n. We choose $a_n = t$ in $(0, \eta_n) \cap \mathbb{Q}$ outside F_n.

The symmetric choice. Use this choice when $n = 2$ or $n \in B$. By Lemma 2.3(i), the monic polynomial

$$P_n(X, U) = \prod_{r=0}^{n-2} \frac{g_{r,n}(X) + 1/U}{a_r}$$

has regular splitting field with group

$$H_n = \prod_{r=0}^{n-2} \mathfrak{S}_{n-r},$$

in the indicated actions on its factors. Here the substitution $T = 1/U$ is an isomorphism of rational function fields. Lemma 2.1 gives arbitrarily large positive integers u for which the specialized splitting field has group H_n and is linearly disjoint from E. Take such a u with $1/u < \eta_n$ and $1/u \notin F_n$, and set

$$a_n = \frac{1}{u}.$$

The finite set F_n excludes only finitely many values of u. The full product group means that the individual factor fields are jointly linearly disjoint and have their respective full symmetric groups. Reversal in (2.8) preserves each splitting field, since $a_n \neq 0$. Hence the fields $K_{r,n}$ have

the required groups, are jointly linearly disjoint, and their compositum is linearly disjoint from E.

The choice with one rational root. Use this choice when $n \geq 3$ and $n \notin B$. Apply Lemma 2.3(ii) with $g_0 = g_{0,n}$ and the other polynomials $g_{r,n}$. After putting $R = -1/U$, the product

$$\frac{Q_{g_{0,n}}(X, -1/U)}{a_0} \prod_{r=1}^{n-2} \frac{g_{r,n}(X) - g_{0,n}(-1/U)}{a_r}$$

is monic and separable and has regular splitting field with group

$$H'_n = \mathfrak{S}_{n-1} \times \prod_{r=1}^{n-2} \mathfrak{S}_{n-r}.$$

By Lemma 2.1, for arbitrarily large positive integers u the specialization has this full product group, and its splitting field is linearly disjoint from E. Put

$$\alpha = -\frac{1}{u}, \qquad a_n = -g_{0,n}(\alpha). \tag{2.10}$$

As $u \to \infty$,

$$-g_{0,n}(-1/u) = \frac{a_{n-1}}{u} + O(u^{-2}) > 0,$$

so $0 < a_n < \eta_n$ for all sufficiently large u. The rational function $-g_{0,n}(-1/U)$ is nonconstant. Therefore the condition $a_n \notin F_n$ removes only finitely many values of u. Choose u satisfying all these conditions.

We now have

$$g_{0,n}(X) + a_n = (X - \alpha) Q_{g_{0,n}}(X, \alpha). \tag{2.11}$$

The left side is separable. The other factor is irreducible of degree $n-1$ and has group $\mathfrak{S}_{n-1}$, because the specialized group acts on its roots as the corresponding full symmetric factor of H'_n. Since $n - 1 \geq 2$, α is the unique rational root of (2.11). Reversing the polynomial proves that f_n has unique rational root $-u$, that its remaining factor is irreducible of degree $n-1$, and that $G_n = 1 \oplus \mathfrak{S}_{n-1}$. Each other factor gives $\mathrm{Gal}(K_{r,n}/\mathbb{Q}) = \mathfrak{S}_{n-r}$ for $r \geq 1$. The product group also gives joint disjointness of all fields $K_{r,n}$ at this stage, and their compositum is disjoint from E.

In both cases $a_n \notin F_n$ gives the required Morse and critical-value conditions for every $g_{r,n+1}$, so the induction continues. The bounds in (1.3) hold by (2.9). Lemma 2.4 gives order zero and all the stated assertions about zeros. In particular, all $K_{r,s}$ are totally real. Induction on the last index gives

$$\left[\prod_{\substack{2 \leq s \leq n \\ 0 \leq r \leq s-2}} K_{r,s} : \mathbb{Q} \right] = \prod_{\substack{2 \leq s \leq n \\ 0 \leq r \leq s-2}} [K_{r,s} : \mathbb{Q}].$$

Every finite subfamily occurs for some n, proving joint linear disjointness. The computability assertion is proved in the following proposition. □

2.4. **Effective choices.** A rational sequence is computable if an algorithm returns its nth term exactly from n. A real sequence (ε_n) is uniformly computable if an algorithm, given n, k, returns a rational $q_{n,k}$ with $|q_{n,k} - \varepsilon_n| \leq 2^{-k}$. A set is decidable if an algorithm decides membership at every input. With these conventions, the choices above can be made uniformly from the prescribed data.

Proposition 2.5. *If membership in B is decidable and the positive real bounds ε_n are uniformly computable, the construction in Theorem A can be performed by a terminating exact search at each degree. The resulting entire function can be approximated effectively and uniformly on every closed disk with a given positive rational radius.*

Proof. First replace each ε_n by a computable positive rational number smaller than it. To do this, compute rational approximations $q_{n,k}$ with $|q_{n,k} - \varepsilon_n| \leq 2^{-k}$ until $q_{n,k} > 2^{-k}$, and use $(q_{n,k} - 2^{-k})/2$. Positivity guarantees termination. Thus we may assume that all the bounds are rational.

At a symmetric step, test $u = 1, 2, \ldots$ in order with $t = 1/u$. At a step with one rational root, use the same enumeration with $t = -g_{0,n}(-1/u)$. The inequalities $0 < t < \eta_n$ are decidable in rational arithmetic. Separability of the current product and the next simultaneous Morse condition are decidable by discriminants and the resultant product in Lemma 2.2. Let L be the common splitting field of the new factors. Its compositum with E can be constructed exactly: factor the new polynomials over the current number field, adjoin a root of an irreducible factor of degree greater than one, and repeat until every factor is linear. Each adjunction adds a new root, so the process terminates. Exact factorization and arithmetic in number fields are effective; see [10, §§3.6.2 and 4.2]. The degrees in the resulting tower compute $[EL : E]$. The remaining test is

$$[EL : E] = \begin{cases} \displaystyle\prod_{d=2}^{n} d!, & n = 2 \text{ or } n \in B, \\ \displaystyle(n-1)! \prod_{d=2}^{n-1} d!, & n \geq 3,\ n \notin B. \end{cases}$$

The right side is the largest possible degree, since the group embeds in the corresponding product of symmetric groups. Equality therefore gives the full product group and linear disjointness from E.

Choose the first u passing all tests. Lemma 2.1 and the preceding proof guarantee that this search terminates. This determines each coefficient exactly and uniformly from a program deciding B and a program computing the bounds. Only finitely many membership queries are used for each coefficient. No bound for the running time of the search is asserted. For integers $R, N \geq 1$, the error on $|z| \leq R$ after degree N is at most

$$\sum_{n>N} 2^{-n^2} R^n.$$

Once $R2^{-(2N+3)} \leq 1/2$, the successive terms of this tail decrease by a factor at most $1/2$, so the tail is at most $2 \cdot 2^{-(N+1)^2} R^{N+1}$. This is an effective uniform error bound on every prescribed disk. □

The same exact procedure determines the label of any rational polynomial of degree $n \geq 3$. First test separability; a nonseparable polynomial is other by convention. For a separable polynomial, compute the degree of its splitting field over $\mathbb{Q}$. Degree $n!$ gives label S, degree $n!/2$ gives label A, and all other degrees give label O: the only subgroup of index two in $\mathfrak{S}_n$ is $\mathfrak{A}_n$. Thus the finite label tests used below require only exact algebraic computations.

Two further choices can be incorporated into the induction.

Remark 2.6. The same proof permits a fixed finite extension $E_0/\mathbb{Q}$ to be included in E at every step. For every finite set I of pairs (r, s) with $0 \leq r \leq s - 2$, it then gives

$$\left[E_0 \prod_{(r,s)\in I} K_{r,s} : E_0\right] = \prod_{(r,s)\in I} [K_{r,s} : \mathbb{Q}].$$

Likewise, the negative integer root at a prescribed reducible degree may be required to have absolute value larger than any given bound, since the allowed integers u are arbitrarily large.

2.5. **Bounded positive coefficients.** We now restrict the coefficients to a fixed finite alphabet. The topology and the uniform product measure give different typical behaviour for the other frequency.

Proposition 2.7. *Fix an integer $L \geq 35$, and put $\Omega_L = \{1, \dots, L\}^{\mathbb{N}_{\geq 1}}$, with its product topology. For $a \in \Omega_L$, let*

$$f_a(x) = 1 + \sum_{j \geq 1} a_j x^j.$$

Every finite prefix has a computable continuation such that

$$\liminf_{N \to \infty} o_{f_a}(N) = 0, \qquad \limsup_{N \to \infty} o_{f_a}(N) = 1.$$

The set of all such sequences is a dense G_δ in Ω_L. For the uniform product probability measure, however, $O(f_a) = 0$ almost surely. All these conclusions hold for the same sequences over every fixed number field. Every f_a has radius of convergence exactly one.

A cylinder is the set of sequences beginning with a prescribed finite word. It is both open and closed, and these cylinders form a basis of the product topology on Ω_L.

Proof of Proposition 2.7. Let $I_n(a)$ be the indicator that $f_{a,n}$ is other. Reversal makes $f_{a,n}$ monic with independent uniform coefficients in $\{1, \dots, L\}$. Theorems 1(a) and 6 of [3] give constants $c, K > 0$, depending only on L, such that

$$\mathbb{E} I_n \leq K n^{-c} \qquad (n \geq 3). \tag{2.12}$$

Here the constant term is always nonzero, and the finitely many degrees below the threshold in those theorems are absorbed into K. Fix a prefix $w = (a_1, \dots, a_m)$. Its cylinder has probability L^{-m}, so

$$\mathbb{E}(o_{f_a}(N) \mid w) \leq L^m \mathbb{E} o_{f_a}(N) \longrightarrow 0.$$

Thus, for every $\varepsilon > 0$, there are arbitrarily long finite extensions with $o_{f_a}(N) < \varepsilon$.

There are also arbitrarily long extensions with $o_{f_a}(N) > 1 - \varepsilon$. Choose a squarefree integer k with at least two prime factors and $\varphi(k)/k < \varepsilon/3$. Such integers exist by Euler's product over the primes. Append ones until the number of coefficients, including $a_0 = 1$, is divisible by k. Let S_r be the sum of the assigned coefficients at indices congruent to $r \pmod{k}$, and put $M = \max_r S_r$. Choose an integer $T \geq 0$ with $(L-1)T \geq \max_r S_r - \min_r S_r$. In T further complete blocks of length k, the increment $M + T - S_r$ can be assigned to residue r: it lies in $[T, LT]$, and every integer in this interval is a sum of T members of $\{1, \dots, L\}$. At the resulting endpoint m', all residue sums equal $C = M + T$, and hence

$$k \mid m' + 1, \qquad f_{a,m'}(x) \equiv C(1 + x + \cdots + x^{k-1}) \pmod{x^k - 1}.$$

Continue by appending ones. If $n \geq m'$ and $\gcd(n+1, k) > 1$, choose a prime $q \mid \gcd(n+1, k)$. Evaluation at a primitive qth root of unity shows that Φ_q divides $f_{a,n}$. This factor is proper, since $q < k \leq m' + 1$. These degrees are other, and their periodic density is $1 - \varphi(k)/k$. More explicitly, for $N > m'$,

$$o_{f_a}(N) \geq \frac{(N - m')(1 - \varphi(k)/k) - k}{N}.$$

This exceeds $1 - \varepsilon$ for sufficiently large N.

Alternate the two extensions with rational ε tending to zero. The high extension is explicit. A low extension can be found by enumerating finite words and using the exact label test described after Proposition 2.5; the existence argument ensures termination. This gives a computable continuation of every prefix. For integers $h \geq 2$ and $M \geq 1$, both sets

$$\bigcup_{N \geq M} \{a : o_{f_a}(N) < 1/h\}, \qquad \bigcup_{N \geq M} \{a : o_{f_a}(N) > 1 - 1/h\}$$

are open and dense. Their intersection over h, M is precisely the asserted G_δ, and it is dense by Baire's theorem.

On the other hand, (2.12) gives $\mathbb{E}\sum_{n\geq 3} I_n/n < \infty$, so this series is finite almost surely. For $M < N$,

$$\frac{1}{N}\sum_{3\leq n\leq N} I_n \leq \frac{M}{N} + \sum_{n>M}\frac{I_n}{n},$$

proving $O(f_a) = 0$ almost surely. No independence of the nested sections is used. Proposition 3.7 transfers the other-frequency conclusions pointwise to every number field. In particular, the same probability-one set works for all such fields. Finally, $1 \leq a_j \leq L$ gives radius one. □

For monic degree-n polynomials whose nonleading coefficients are independent and uniform on $\{1, \ldots, L\}$, with $L > e^{12}$, Blachar, Breuillard, and Kozma [6, Corollary 1.2] prove symmetry with probability $1 - O(1/\log n)$.

The estimate (2.12) also gives a computable continuation with zero other frequency. We use conditional expectations to make the choice effective from every prefix.

Proposition 2.8. *For fixed $L \geq 35$, every finite prefix in Ω_L has a uniformly computable continuation with $O(f_a) = 0$.*

Proof. For the fixed alphabet size L, choose a positive rational c and an integer K satisfying (2.12). They are fixed parameters of the algorithm; the asserted uniformity is in the prefix. We do not require an effective choice of these constants from L. Put

$$W(a) = \sum_{n\geq 3}\frac{I_n(a)}{n}, \qquad V(w) = \mathbb{E}(W \mid w).$$

For a prefix w of length m, the real number $V(w)$ is computable uniformly in w. Each finite conditional expectation is rational and can be computed by enumerating finite extensions and their Galois groups. For $N \geq \max\{m, 3\}$, the omitted tail is at most

$$L^m K \sum_{n>N} n^{-1-c} \leq L^m K N^{-c}/c.$$

Also $V(w) = L^{-1}\sum_{b=1}^{L} V(wb)$. Approximate each child value to error less than 2^{-m-3} and choose a child with least approximate value. Its true value is at most $V(w) + 2^{-m-2}$. Along the resulting computable path, the values $V(w)$ are therefore bounded. Each partial sum of W is fixed by a sufficiently long prefix and is at most $V(w)$, since the remaining terms are nonnegative. Hence $W < \infty$, which implies $O(f_a) = 0$ by the estimate in the preceding proof. □

A property is *semidecidable under a promise* if an algorithm halts exactly on the inputs having the property, among inputs satisfying the promise. Here the inputs are programs for total coefficient sequences. The two uniform continuation procedures turn the halting problem into a frequency-convergence problem within the fixed alphabet.

Corollary 2.9. *Under the promise that a program computes coefficients $a_0 = 1$ and $a_j \in \{1, \ldots, L\}$, with fixed $L \geq 35$, neither existence of the other frequency nor its failure is semidecidable. This holds over every fixed number field.*

Proof. Both continuation procedures above are uniform in the prefix. Given a machine, follow a fixed computable maximal-oscillation sequence until it halts; after halting, retain the assigned prefix and use Proposition 2.8. The other frequency then exists exactly when the machine halts, so nonconvergence is not semidecidable. Conversely, follow a fixed computable zero-frequency sequence until the machine halts, and then use the maximal-oscillation continuation of the assigned

prefix. The frequency exists exactly when the machine never halts, so convergence is not semidecidable. At coefficient n, simulating the machine for n steps makes these reductions uniform programs for total sequences. The ground-field assertion again follows from Proposition 3.7. □

3. Local Galois criteria

The arithmetic arguments use two ways to obtain large permutation groups: a single short cycle, or several permutations with two cycles. We first record the group criteria, then explain how local factorizations and ramification determine the group over a number field.

3.1. Permutation group criteria.

For $P \in \mathbb{Q}[x]$ of degree n, choose a nonzero rational multiple $\widetilde{P} \in \mathbb{Z}[x]$. A prime ℓ is *good for* $\widetilde{P}$ if it divides neither its leading coefficient nor its discriminant. If P is separable, multiplying it by a nonzero scalar changes its discriminant by a $(2n-2)$th power, so its square class is unchanged.

A short cycle in a primitive group gives alternating containment. The following form also covers cycles of composite length.

Lemma 3.1. *Let $G \le \mathfrak{S}_n$ be primitive. If G contains a single k-cycle with $2 \le k \le n/2$, then G contains $\mathfrak{A}_n$.*

Proof. The classical Jordan–Marggraff transitivity theorem [29, Theorem A] makes G at least $(n-k+1)$-transitive, hence at least $(k+1)$-transitive. After numbering the points, suppose $\sigma = (1\,2\,\cdots\,k)$ belongs to G. By transitivity on ordered k-tuples, a conjugate of σ is $\tau = (1\,2\,\cdots\,k-1\,k+1)$. Then $\sigma\tau^{-1} = (1\,k+1\,k)$ is a 3-cycle. Since G is 3-transitive, it contains every 3-cycle, and these generate $\mathfrak{A}_n$. □

For the reciprocal families, local ramification gives two cycles whose lengths need not be coprime. Varying these lengths rules out block systems and the exceptional primitive groups.

Lemma 3.2. *Let $G \le \mathfrak{S}_n$ be transitive, with $n > 64$. Suppose that a nonempty set $\mathcal{J}$ of integers satisfies*

$$n/2 < j < n - \sqrt{n} \qquad (j \in \mathcal{J}),$$

and that G contains a permutation of cycle type $(j)(n-j)$ for every $j \in \mathcal{J}$. Suppose also that, for each factorization $n = mr$ with $2 \le m \le r$, some $j \in \mathcal{J}$ is divisible by neither m nor r. Then $\mathfrak{A}_n \subseteq G$.

Proof. If a permutation with exactly two point orbits preserves a block partition with block size m and r blocks, its induced action has either one or two block orbits. In the latter case each point orbit is a union of whole blocks, so $m \mid j$. In the former case each point orbit visits all r blocks, so $r \mid j$. Thus every such block partition would require $m \mid j$ or $r \mid j$ for all $j \in \mathcal{J}$. Interchanging m, r if necessary, the hypothesis rules this out. Hence G is primitive.

Suppose now that G does not contain $\mathfrak{A}_n$. Apply Müller's classification [32, Theorem 3.3] to an element with shorter cycle length $k = n - j$. The affine cases have $k = 1$, $k = 4$, or $k = p$ with $n = p^e$, $e \ge 2$, apart from degrees at most 25. These contradict $\sqrt{n} < k < n/2$. The almost simple cases other than the natural alternating and symmetric groups have $k = 1$ or $k = n/2$, apart from degrees at most 24. These too are excluded. The product actions in part (2) of the classification have $n = r^2$, and both cycle lengths are divisible by r. Applying the classification to every element under consideration would therefore give $r \mid j$ for every $j \in \mathcal{J}$. The hypothesis applied to $n = r \cdot r$ excludes this last case. Thus G contains $\mathfrak{A}_n$. □

We next express alternating containment by irreducibility and one modular factorization. The witness prime and the prime factor degree play different roles.

Definition 3.3. For $P \in \mathbb{Q}[x]$ of degree $n \ge 8$, put $C(P) = 1$ if both conditions hold:

(i) P is irreducible over $\mathbb{Q}$;
(ii) for some good prime ℓ, the reduction of $\widetilde{P}$ has an irreducible factor of prime degree p with $n/2 < p \leq n-3$.

Otherwise put $C(P) = 0$. The other factors modulo ℓ may have arbitrary degrees.

This criterion is exact: allowing the witness prime to vary loses no group containing $\mathfrak{A}_n$.

Proposition 3.4. *If $P \in \mathbb{Q}[x]$ is separable of degree $n \geq 8$, then*

$$C(P) = 1 \quad \Longleftrightarrow \quad \mathrm{Gal}(P/\mathbb{Q}) \supseteq \mathfrak{A}_n.$$

In particular, the definition is independent of the normalization.

Proof. A factor of degree p supplies a Frobenius element with a p-cycle; all its other cycles have total length $n - p < p$. A suitable power kills them and retains a single p-cycle. Irreducibility gives transitivity.

Suppose a nontrivial block system has block size b, where $1 < b \leq n/2$. If a block meeting the support of the p-cycle contains a fixed point, it meets its translate and is invariant. It would contain the whole support, contrary to $b < p$. Thus the support is a union of blocks, and b divides both n and p, contradicting $p < n < 2p$. The action is primitive. Jordan's theorem gives $\mathfrak{A}_n$, since the prime cycle fixes at least three points [25, Theorem 1.1].

Conversely, for $n > 50$, Nagura's theorem supplies a prime $n/2 < p < 3n/5 \leq n-3$ [33]. For $8 \leq n \leq 50$, one of $5, 7, 11, 17, 29$ satisfies $n/2 < p \leq n-3$: the intervals $[p+3, 2p-1]$ cover $[8, 57]$. Every such p is odd. A group containing $\mathfrak{A}_n$ contains a p-cycle. Chebotarev gives good primes with factorization type $(p, 1, \ldots, 1)$; see [44]. Containment also gives transitivity, hence irreducibility. □

Rational irreducibility cannot be replaced by irreducibility modulo some prime. When n is even, $\mathfrak{A}_n$ contains no n-cycle, so an irreducible polynomial with group $\mathfrak{A}_n$ is reducible modulo every good prime. A fixed finite cutoff on the witness prime ℓ is also not part of the criterion.

3.2. **Newton polygons and change of base field.** We use valuations with value group $\mathbb{Z}$ on the local ground field. For a rational prime p unramified in a number field F, the valuation at any place above p therefore satisfies $v(p) = 1$. The denominator of a Newton slope can supply the prime cycle used in Proposition 3.4 without a modular factorization.

Lemma 3.5. *Let $P \in F[X]$ be irreducible of degree n over a number field F. If a lower Newton polygon of P has a slope whose reduced denominator is a prime p with $n/2 < p \leq n-3$, then $\mathrm{Gal}_F(P) \supseteq \mathfrak{A}_n$.*

Proof. A root valuation with denominator p forces the ramification index of its local field to be divisible by p. Thus p divides the order of the splitting-field group. Cauchy's theorem gives an element of order p, necessarily a single p-cycle since $2p > n$. Transitivity, the block argument in Proposition 3.4, and Jordan's theorem give the conclusion. This is the usual Newton-polygon criterion; compare [21, Theorem 2.2]. □

Two local factorizations can also prove global irreducibility if their possible proper factor degrees are disjoint.

Lemma 3.6. *Let $P \in F[X]$ have degree n. Suppose that at two finite places its lower Newton polygons have vertices*

$$(0,0),\ (j_i, -1),\ (n, 0) \qquad (i = 1, 2), \qquad n/2 \leq j_1 < j_2 < n.$$

Then P is irreducible over F. A single lower Newton edge from $(0,0)$ to $(n,-1)$ also implies irreducibility.

Proof. At the ith place, the two slopes have reduced denominators j_i and $n - j_i$. The Newton factorization theorem separates the roots according to slope. Each factor on an edge has degree divisible by its slope denominator, so each entire edge gives one irreducible local factor. A proper factor over F would therefore have degree in both $\{j_1, n - j_1\}$ and $\{j_2, n - j_2\}$. These sets are disjoint. The single-edge assertion follows in the same way. □

Once the degree exceeds that of a fixed base field, alternating containment is unchanged by extending scalars.

Proposition 3.7. *Let $F/\mathbb{Q}$ be a number field and let $P \in \mathbb{Q}[X]$ be separable of degree $n \geq 5$ with $n > [F : \mathbb{Q}]$. Then*

$$\mathrm{Gal}_F(P) \supseteq \mathfrak{A}_n \quad \Longleftrightarrow \quad \mathrm{Gal}_{\mathbb{Q}}(P) \supseteq \mathfrak{A}_n.$$

Consequently, for every series with nonzero rational coefficients, the other-degree labels over F and over $\mathbb{Q}$ agree eventually. In particular, $O_F(f)$ exists if and only if $O(f)$ exists, and the two values are equal.

Proof. Let $L/\mathbb{Q}$ be the splitting field of P, put $G = \mathrm{Gal}(L/\mathbb{Q})$, and identify $H = \mathrm{Gal}(LF/F)$ with $\mathrm{Gal}(L/(L \cap F)) \leq G$. Then $m = [G : H] = [L \cap F : \mathbb{Q}] \leq [F : \mathbb{Q}] < n$. If G contains $\mathfrak{A}_n$, restrict the action on G/H to $\mathfrak{A}_n$. Simplicity of $\mathfrak{A}_n$ makes the kernel either trivial or all of $\mathfrak{A}_n$. The first alternative would embed $\mathfrak{A}_n$ in $\mathfrak{S}_m$, whereas $n!/2 > m!$. Thus $\mathfrak{A}_n$ fixes every coset and lies in H. The reverse implication follows from $H \leq G$. Containment of $\mathfrak{A}_n$ is equivalent to being symmetric or alternating. Repeated-root sections are other over both fields, so the frequency assertion follows as well. □

For small degrees, an unramified prime provides another way to control the change of base field. Odd inertia is particularly useful because it cannot lie in a proper normal subgroup of $\mathfrak{S}_n$.

Lemma 3.8. *Let $L/\mathbb{Q}$ be Galois, and let F be unramified at a rational prime p. Write $\widetilde{F}$ for its Galois closure and $E = L \cap \widetilde{F}$.*

(i) *If $\mathrm{Gal}(L/\mathbb{Q}) = \mathfrak{S}_n$, $n \geq 2$, and inertia at p contains an odd permutation, then $E = \mathbb{Q}$.*
(ii) *If $n \geq 5$, $\mathfrak{A}_n \subseteq \mathrm{Gal}(L/\mathbb{Q}) \leq \mathfrak{S}_n$, and inertia at p is nontrivial, then $\mathfrak{A}_n \subseteq \mathrm{Gal}(L/E)$.*

Proof. Every conjugate of F is unramified at p, and finite composita of unramified extensions of $\mathbb{Q}_p$ are unramified. Thus $\widetilde{F}$, and hence E, is unramified at p. The normal subgroup $\mathrm{Gal}(L/E)$ therefore contains inertia at p. Every proper normal subgroup of $\mathfrak{S}_n$ lies in $\mathfrak{A}_n$; for $n = 2, 3, 4$ this follows from the elementary lists. This proves the first assertion. For $n \geq 5$, every nontrivial normal subgroup of $\mathfrak{A}_n$ or $\mathfrak{S}_n$ contains $\mathfrak{A}_n$, which proves the second. □

4. Reciprocal coefficients and binomial sections

The proof of Theorem B has two parts. We choose primes at which exactly one coefficient has valuation -1; the resulting Newton polygon gives irreducible local factors of complementary degrees. Varying these degrees proves global irreducibility and alternating containment. For even degrees, the same local calculation imposes quadratic character conditions on the discriminant; the quadratic large sieve then bounds the exceptional degrees uniformly in the multipliers. Throughout this section, $s = a/b \in \mathbb{Q} \setminus \mathbb{Z}$ is in lowest terms, with $b \geq 2$. Let $C \geq 0$ and let F be a number field. Write $\mathrm{rad}(b)$ for the product of the primes dividing b, and set

$$M = b\,\mathrm{rad}(b), \qquad Q = \mathrm{lcm}(M, 6), \qquad H = \max\{3, |a|, b, C + 1, R_F\}, \tag{4.1}$$

$$N(a, b, C, F) = \lceil \max\{\exp(\max\{60, Q\}), 100H\} \rceil . \tag{4.2}$$

All logarithms are natural. These bounds are chosen to make the prime selection fully explicit; the half-integral cases admit the sharper thresholds stated in the introduction.

4.1. **Primes avoiding two divisors.** Set

$$c = \begin{cases} 2, & a, b \text{ odd}, \\ 1, & \text{otherwise}. \end{cases}$$

Then $(c, ab) = 1$, $c < b$, and $b/c \geq 3/2$. Choose a reduced residue class $\rho \pmod{Q}$ as follows. First impose

$$c\rho \equiv a + b \pmod{M}. \tag{4.3}$$

If $2 \nmid M$, impose $\rho \equiv 1 \pmod 2$. If $3 \nmid M$, choose $\rho \pmod 3$ in $\{1, 2\}$ so that $c\rho - a \not\equiv 0 \pmod 3$; at most one of these two residues is excluded. These prescriptions are compatible by the Chinese remainder theorem and give $(\rho, Q) = 1$. For any prime $p \equiv \rho \pmod{Q}$, the integer

$$j = \frac{cp - a}{b}$$

is 1 modulo $\mathrm{rad}(b)$ and is coprime to 6. Indeed $3 \nmid j$ by construction. If b is even, the class (4.3) makes j odd. For odd b, either a is even and $c = 1$, or a is odd and $c = 2$; in both cases $cp - a$ is odd.

The next estimate supplies the cycle lengths required by Lemma 3.2. The surplus of primes will also allow us to discard a bounded number of primes excluded by polynomial weights.

Lemma 4.1. *Suppose $n \geq N(a, b, C, F)$, and put*

$$\kappa = \frac{b}{8c}, \qquad U = 6\kappa n, \quad V = 7\kappa n, \quad W = V - U = \kappa n, \qquad L = \log n.$$

Let

$$\mathcal{P} = \{p \text{ prime} : U < p \leq V,\ p \equiv \rho \pmod{Q}\}.$$

Then

$$|\mathcal{P}| > \frac{4W}{5\varphi(Q)L} > \sqrt{n}. \tag{4.4}$$

For every factorization $n = mr$, $2 \leq m \leq r$, more than

$$\frac{W}{10\varphi(Q)L} > \sqrt{n} \tag{4.5}$$

primes in $\mathcal{P}$ satisfy

$$m \nmid \frac{cp - a}{b} \quad \text{and} \quad r \nmid \frac{cp - a}{b}.$$

Every prime in $\mathcal{P}$ exceeds $n + C$ and R_F, and its index satisfies

$$7n/10 < j < 9n/10, \qquad \sqrt{n} < n - j < n/2.$$

The proof is given in Appendix A, where all constants are made explicit.

4.2. **The local discriminant.** One coefficient of valuation -1, between unit constant and leading coefficients, determines the local factor degrees and, when both degrees are odd, the local discriminant class. The remaining coefficients need only be integral. For $z \in \mathbb{Q}_p^\times$, write $[z]_p$ for its class in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.

Lemma 4.2. *Let $p > n$ be an odd prime and let $P(x) = \sum_{i=0}^{n} d_i x^i \in \mathbb{Q}_p[x]$. Suppose that*

$$v_p(d_0) = v_p(d_n) = 0, \qquad v_p(d_j) = -1 \quad (0 < j < n),$$

and $v_p(d_i) \geq 0$ for all other i. Put $k = n - j$. Then P has two irreducible factors over $\mathbb{Q}_p$, of degrees j, k, and their root fields are totally and tamely ramified. Moreover,

$$v_p(\mathrm{Disc}\, P) = -n. \tag{4.6}$$

If j, k are odd, then

$$[\operatorname{Disc} P]_p = [(-1)^{n/2-1} jk]_p. \tag{4.7}$$

Proof. The Newton polygon has vertices $(0,0), (j,-1), (n,0)$. The primitive slopes give one irreducible factor on each edge. The j roots on the first edge have valuation $1/j$; their monic factor A is Eisenstein, since its nonleading coefficients lie in $p\mathbb{Z}_p$ and $v_p(A(0)) = 1$. The other roots have valuation $-1/k$. If B is their monic factor, then $E(x) = x^k B(1/x)/B(0)$ is monic Eisenstein of degree k. Both root fields are totally ramified and tame, since $j, k < p$.

For a monic Eisenstein polynomial H of degree $e < p$, a root α satisfies

$$H'(\alpha) = e\alpha^{e-1}(1+\eta), \qquad v_p(\eta) > 0.$$

Indeed, the leading derivative term has valuation $(e-1)/e$, strictly less than every other term. For $K = \mathbb{Q}_p(\alpha)$, the discriminant–norm identity therefore gives

$$\operatorname{Disc} H = (-1)^{e(e-1)/2} e^e N_{K/\mathbb{Q}_p}(\alpha)^{e-1} N_{K/\mathbb{Q}_p}(1+\eta).$$

Thus $v_p(\operatorname{Disc} H) = e-1$. If e is odd, this also gives

$$[\operatorname{Disc} H]_p = [(-1)^{(e-1)/2} e]_p : \tag{4.8}$$

the norm of $1+\eta$ is a principal unit and hence a square, and the power of the norm of α is even.

Reversal gives $\operatorname{Disc} B = \operatorname{Disc} E/E(0)^{2k-2}$, so $v_p(\operatorname{Disc} B) = -(k-1)$. Every difference between a root of A and a root of B has valuation $-1/k$, whence $v_p(\operatorname{Res}(A,B)) = -j$. The product formula for the discriminant, and the fact that the leading coefficient of P is a unit, now give

$$v_p(\operatorname{Disc} P) = (j-1) - (k-1) - 2j = -n.$$

For square classes the leading-coefficient factor, the resultant squared, and the reversal factor are all squares. Applying (4.8) to A, E proves (4.7). □

4.3. **Alternating containment.** Consider the polynomials R_n in Theorem B. For $p \in \mathcal{P}$ of Lemma 4.1, the unique denominator divisible by p is $a + bj = cp$. Its valuation is one, and all multipliers are units. Lemma 4.2 therefore gives local factors of degrees $j, n-j$. Since $p > R_F$, it is unramified in F. The normalized valuation at any place above p still satisfies $v(p) = 1$, so the same primitive Newton edges give two totally ramified local factors over that completion.

Two distinct primes of $\mathcal{P}$ give distinct $j_1, j_2 > n/2$, so Lemma 3.6 proves irreducibility over F. A generator of tame inertia acts transitively on the roots of each totally ramified local factor, and hence as one cycle on each. It supplies a permutation of cycle type $(j)(n-j)$ for every $p \in \mathcal{P}$. Lemma 4.1 verifies all the hypotheses of Lemma 3.2, which gives alternating containment. If n is odd, this two-cycle permutation has sign $(-1)^{n-2} = -1$, so the group is $\mathfrak{S}_n$.

4.4. **Counting the even exceptions.** For even n, the chosen progression makes both j and $n-j$ odd. This already follows from the class modulo M: use $j \equiv 1 \pmod{\operatorname{rad}(b)}$ for even b and the definition of c for odd b. Put

$$D_n = (-1)^{n/2} a(a+bn). \tag{4.9}$$

Since $j \equiv -a/b$ and $n - j \equiv (a+bn)/b \pmod{p}$, Lemma 4.2 shows that

$$[\operatorname{Disc} R_n]_p = [D_n]_p. \tag{4.10}$$

Here $p > |a|$ and $p \nmid b$. If $p \mid D_n$, the positive integer $n - j < p$ would therefore be divisible by p, a contradiction. The identity is local; no formula for the rational square class of $\operatorname{Disc} R_n$ is being assumed. Coprimality of j, n is unnecessary in this step.

Let

$$W_F = (F^{\times 2} \cap \mathbb{Q}^\times)/\mathbb{Q}^{\times 2}.$$

This is finite, since its nontrivial elements correspond to quadratic subfields of F. Choose signed squarefree integer representatives δ. If $\operatorname{Disc} R_n$ is a square in F, its rational square class is one such δ, and (4.10) implies

$$\left(\frac{\delta D_n}{p}\right) = 1 \tag{4.11}$$

at every prime in the prescribed interval and progression, once n is sufficiently large in terms of a, b, C, F. For this local test, the congruence modulo M suffices: the extra condition $3 \nmid j$ was used only to select cycle lengths for the containment argument.

Fix Y and restrict even n to $Y \le n \le 9Y/8$. The value of c is fixed. The common prime set

$$\mathcal{P}_Y = \left\{p : \frac{27bY}{32c} < p < \frac{7bY}{8c}, \quad p \equiv (a+b)c^{-1} \pmod{M}\right\}$$

lies in the permitted interval for every such n, and has $P_Y \asymp_{a,b} Y/\log Y$ elements by the prime number theorem in arithmetic progressions [28]. For fixed δ, restrict to n whose discriminant has rational square class δ, and let d_n be the signed squarefree part of δD_n. If $d_n \neq 1$, put

$$\Delta(d_n) = \begin{cases} d_n, & d_n \equiv 1 \pmod 4, \\ 4d_n, & d_n \not\equiv 1 \pmod 4. \end{cases}$$

The primitive quadratic character $\chi_{d_n}(m) = (\Delta(d_n)/m)$, with the Kronecker symbol, has conductor $|\Delta(d_n)| \ll_{a,b,F} Y$. This applies to positive and negative d_n alike. Equation (4.11) says that

$$\sum_{p \in \mathcal{P}_Y} \chi_{d_n}(p) = P_Y.$$

Heath–Brown's quadratic large sieve [22, Corollary 1] states that, for positive integers Q_0, Z and coefficients z_m supported on squarefree integers,

$$\sum_{\substack{\chi \text{ real primitive} \\ \operatorname{cond}(\chi) \le Q_0}} \left| \sum_{m \le Z} z_m \chi(m) \right|^2 \ll_\eta (Q_0 Z)^\eta (Q_0 + Z) \sum_{m \le Z} |z_m|^2 \qquad (\eta > 0). \tag{4.12}$$

Take $Q_0, Z \asymp_{a,b,F} Y$ large enough to include all the conductors and all primes in $\mathcal{P}_Y$, and put $z_m = \mathbf{1}_{m \in \mathcal{P}_Y}$. Distinct nontrivial square classes give distinct primitive characters, each contributing P_Y^2. Thus the number of represented nontrivial square classes is $O_{a,b,F,\eta}(Y^{2\eta} \log Y)$. For each fixed signed squarefree d, the equation

$$\delta(-1)^{n/2} a(a + bn) = dt^2$$

has $O_{a,b,F}(\sqrt{Y})$ solutions in the interval: fix n modulo four, then each positive integer $t \ll_{a,b,F} \sqrt{Y}$ determines at most one n. This also bounds the trivial class $d = 1$. Summing over the finite set W_F gives $O_{a,b,F,\eta}(Y^{1/2+2\eta} \log Y)$ exceptions. Choose $\eta = \varepsilon/4$, absorb the logarithm into $Y^{\varepsilon/2}$, and sum over intervals of ratio $9/8$. Together with eventual alternating containment, this proves Theorem B.

4.5. **Series and polynomial weights.** For a fixed sequence (u_j), it suffices that every prime dividing the numerator or denominator of u_j be at most $j + C$. This includes $u_j = v_j/(j!)^r$ for any bounded sequence of nonzero integers v_j and any fixed integer $r \ge 0$. It also includes $u_j = 2^{-j^3}$; for $s > 0$ this gives an entire function of order zero with positive rational coefficients and symmetric frequency one. Finite nonzero coefficient changes preserve the hypothesis after enlarging C. A coefficient shift by h replaces s by $s + h$ and u_j by $su_{j+h}/(s + h)$, so the same conclusions hold after every fixed shift.

For clarity, the classical specializations are

$$H_s(x) = {}_2F_1(1, s; s+1; x) = \sum_{j\ge 0} \frac{s}{s+j} x^j,$$
$$ {}_1F_r(s; s+1, \underbrace{1, \dots, 1}_{r-1}; x) = \sum_{j\ge 0} \frac{s}{(s+j)(j!)^r} x^j \qquad (r \ge 1).$$

The second line includes Kummer's function at $r = 1$. At $s = 1/2$, replacing x by $-x$ where needed, these include

$$\frac{\operatorname{arctanh}\sqrt{x}}{\sqrt{x}}, \qquad \frac{\arctan\sqrt{x}}{\sqrt{x}}, \qquad \frac{\sqrt{\pi}\operatorname{erf}\sqrt{x}}{2\sqrt{x}} = \sum_{j\ge 0} \frac{(-1)^j x^j}{j!(2j+1)}.$$

The quotients have their removable singularities filled in at zero. The identities use the standard hypergeometric and error-function normalizations [14, §§13.2,16.2,7.6]. All these series have triple $(1, 0, 0)$ over every fixed number field.

The local proof allows polynomial weights whose prime divisors need not satisfy the preceding bound.

Corollary 4.3. *Let $r \ge 0$ be an integer and let $P \in \mathbb{Q}[T]$ satisfy $P(-s) \ne 0$. Suppose $a_j \in \mathbb{Q}^\times$ and*

$$a_j = \frac{P(j)}{(s+j)(j!)^r}$$

for all sufficiently large j. Then, over every fixed number field F, the sections of $\sum a_j x^j$ contain $\mathfrak{A}_n$ for all sufficiently large n, have group $\mathfrak{S}_n$ for all sufficiently large odd n, and have group $\mathfrak{S}_n$ outside $O_{s,P,r,F,\varepsilon}(X^{1/2+\varepsilon})$ degrees up to X. The implied constant may also depend on the finitely many changed coefficients. Appendix A.3 gives an explicit degree threshold in terms of these data. In particular, the frequency triple is $(1, 0, 0)$.

Proof. Clear the fixed denominators of P. For sufficiently large selected primes $p > n$, all ordinary coefficients are p-integral, and the constant coefficient is a unit. At the special index $j = (cp-a)/b$, we have $P(j) \equiv P(-a/b) \not\equiv 0 \pmod p$, so the coefficient at index j has valuation -1. Only primes dividing the numerator of $P(n)$ can spoil the unit leading coefficient. Since $|P(n)| \ll_P n^{\deg P}$ and its denominator is bounded, only $O_P(1)$ primes of size comparable to n are lost. The surplus in Lemma 4.1 leaves two local factorizations for irreducibility and a cycle length for each divisor-pair condition in Lemma 3.2. Thus the same proof gives irreducibility and alternating containment. In the large-sieve step the character sum is at least $P_Y - O_P(1)$; its square has the same order as P_Y^2. The previous count applies without change. □

The nonzero-coefficient hypothesis permits the finitely many zeros of $P(j)$ to be replaced by nonzero rationals. It cannot be dropped: $P(T) = T$ gives a permanent factor x. The condition $P(-s) \ne 0$ is also necessary for this conclusion in this generality: $P(T) = T + s$ and $r = 1$ give e^x, with positive alternating frequency. For $r = 0$, the corollary includes $cH_s(x) + R(x)$, where $c \in \mathbb{Q}^\times$, $R \in \mathbb{Q}(x)$ has no finite pole except possibly 1, and all coefficients of the sum are nonzero. Indeed, the eventual coefficients of R are polynomial in the index, and the resulting weight has value $cs \ne 0$ at $-s$.

4.6. **Binomial sections and their exact eventual groups.** Define

$$T_n(y) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{a}{a+bj} y^j, \qquad \gamma_n = \frac{(s+1)_n}{n!}.$$

The affine identity

$$B_{s,n}(1-y) = \gamma_n T_n(y) \tag{4.13}$$

follows by comparing coefficients, since

$$\sum_{i=j}^{n} \frac{(s)_i}{i!}\binom{i}{j} = \frac{(s)_j}{j!}\frac{(s+j+1)_{n-j}}{(n-j)!} = \gamma_n \binom{n}{j}\frac{s}{s+j}.$$

All scalar factors are nonzero. Every prime dividing $\binom{n}{j}$ is at most n, so Theorem B applies to T_n. It proves eventual alternating containment over F, with symmetry in every sufficiently large odd degree.

The standard Jacobi formula [14, Equation 18.5.7], with hypergeometric parameters $-n, s; s+1$, is precisely $\gamma_n T_n(1-x)$. It gives the identity

$$B_{s,n}(x) = P_n^{(s,-n-1)}(2x-1), \tag{4.14}$$

which expresses this family as Jacobi polynomials with one parameter depending on the degree.

To distinguish the two possible groups, write $b_n = (s)_n/n!$. The differential identity

$$(1-x)B'_{s,n}(x) - sB_{s,n}(x) = -(n+s)b_n x^n$$

shows separability: a common zero of $B_{s,n}, B'_{s,n}$ would have to be zero. Evaluating at the roots and using $B_{s,n}(1) = (n+s)b_n/s$ gives

$$\mathrm{Disc}(B_{s,n}) = (-1)^{n(n-1)/2} s(n+s)^{n-1} b_n^{n-2}. \tag{4.15}$$

For completeness, the product of the derivatives at the roots is $s(n+s)^{n-1}$; multiplication by $(-1)^{n(n-1)/2} b_n^{n-2}$ yields the formula. It also follows from the parameter identity in [18, Lemma 3].

For even n, the rational square class in (4.15) is $[D_n]$, with D_n as in (4.9). The already proved containment therefore gives the classification in Theorem C. **The exact exceptional count.** Let $\mathcal{W}_F$ be the set of signed squarefree integer representatives of W_F. For $r \in \{0,2\}$ put $\sigma_r = (-1)^{r/2}$. Whenever $\delta \in \mathcal{W}_F$ satisfies $\delta\sigma_r a > 0$, let $d_{\delta,r}$ be the positive squarefree part of $\delta\sigma_r a$, and set

$$h_{\delta,r} = \#\{v \bmod 4b : d_{\delta,r}v^2 \equiv a + br \pmod{4b}\}.$$

Then the constant in Theorem C is

$$c_{s,F} = \frac{1}{4\sqrt{b}} \sum_{\substack{r\in\{0,2\},\ \delta\in\mathcal{W}_F \\ \delta\sigma_r a>0}} \frac{h_{\delta,r}}{\sqrt{d_{\delta,r}}}. \tag{4.16}$$

In particular, it can be computed from the quadratic subfields of F and finitely many congruences.

To prove the formula, restrict to n large enough that the group classification holds and $a+bn > 0$. On the class $n \equiv r \pmod 4$, an alternating group occurs exactly when δD_n is a rational square for some $\delta \in \mathcal{W}_F$. Its sign requires $\delta\sigma_r a > 0$. Writing $\delta\sigma_r a = d_{\delta,r}t_0^2$, the square condition is then equivalent to

$$a + bn = d_{\delta,r}v^2 \qquad (v \in \mathbb{Z}_{>0}).$$

Here v is integral because $d_{\delta,r}$ is squarefree and $a+bn$ is an integer. The congruence defining $h_{\delta,r}$ expresses exactly that $n = (d_{\delta,r}v^2 - a)/b$ is an integer in the required class modulo four. Positive v give distinct degrees. Counting them in their residue classes gives

$$\frac{h_{\delta,r}}{4b}\sqrt{\frac{bX+a}{d_{\delta,r}}} + O_{s,F}(1) = \frac{h_{\delta,r}}{4\sqrt{bd_{\delta,r}}}\sqrt{X} + O_{s,F}(1).$$

Different pairs (δ, r) give disjoint sets of degrees: r is fixed by n, and the rational discriminant class uniquely determines δ. Summing proves (1.8) and (4.16). The omitted initial degrees contribute only a constant. Every summand is nonnegative. Thus $c_{s,F} = 0$ exactly when all the congruences are insoluble, which is equivalent to symmetry in every sufficiently large degree. If $a > 0$, write $a = dt^2$. The pair $(\delta, r) = (1, 0)$ has the solution $v = t$, so $c_{s,F} > 0$ over every number field.

Over $\mathbb{Q}$, the congruences in (4.16) give the following closed formula.

Corollary 4.4. *Write $|a| = dt^2$ with $d > 0$ squarefree and $t \in \mathbb{Z}_{>0}$, and let $\omega(b)$ count the distinct prime divisors of b. Write v_2 for the 2-adic valuation. Then*

$$c_{s,\mathbb{Q}} = \frac{2^{\omega(b)-1}}{\sqrt{bd}} \tag{4.17}$$

if $a > 0$. For $a < 0$, the same formula holds precisely when b is odd, every prime divisor of b is 1 modulo 4, and $v_2(|a|)$ is zero or odd; otherwise $c_{s,\mathbb{Q}} = 0$. Thus the exponent $1/2$ is sharp for every positive nonintegral parameter. For $a < 0$, the stated conditions are necessary and sufficient for infinitely many alternating degrees.

Proof. Write $|a| = dt^2$, where $d > 0$ is squarefree and $t \in \mathbb{Z}_{>0}$. If $a > 0$, only $r = 0$ contributes, and the congruence is $dv^2 \equiv a \pmod{4b}$. It has exactly $2^{\omega(b)+1}$ solutions modulo $4b$. For odd b, the congruence modulo b is $v^2 \equiv t^2 \pmod{b}$, with $2^{\omega(b)}$ solutions since $(t, b) = 1$. Modulo four it requires v to have the same parity as t, giving two further choices. If b is even, then d, t are odd and the congruence is $v^2 \equiv t^2 \pmod{4b}$. The odd prime powers give two roots each, and the power of 2 in $4b$ gives four. Both cases yield (4.17).

Suppose $a < 0$ and put $A = |a|$. Now only $r = 2$ contributes, with congruence

$$dv^2 \equiv 2b - A \pmod{4b}. \tag{4.18}$$

If b is even, then A is odd and, for $n \equiv 2 \pmod 4$,

$$D_n = A(bn - A) \equiv 2bA - 1 \equiv 3 \text{ or } 7 \pmod 8.$$

There is no square. For odd b, the congruence modulo b is $v^2 \equiv -t^2 \pmod{b}$. Since $(t, b) = 1$, it is soluble exactly when every prime divisor of b is 1 modulo 4; when soluble it has $2^{\omega(b)}$ solutions. Modulo four, (4.18) is soluble exactly when $v_2(A)$ is zero or odd. Indeed, if A is odd it requires v odd; if $v_2(A) = 1$ it requires v even; and if $v_2(A) > 1$ it requires $dv^2 \equiv 2 \pmod 4$, which is possible exactly when d is even, equivalently when $v_2(A)$ is odd. Each soluble case has two residues modulo four. The Chinese remainder theorem therefore gives $2^{\omega(b)+1}$ solutions in precisely the cases stated in Corollary 4.4. This proves the asserted rational constant and the criterion for infinitely many alternating degrees. □

For example, $s = -1/2$ gives eventual symmetry in every degree, whereas $s = -1/5$ has $X^{1/2}/\sqrt{5} + O(1)$ alternating degrees up to X.

A numerical upper bound. Put $N_0 = N(a, b, 0, F)$, or $N_0 = N_2(a, 0, F)$ when $b = 2$, and set $D = |\operatorname{Disc} F|$ and $d = [F : \mathbb{Q}]$. Then, for $X \geq 1$,

$$\#\{1 \leq n \leq X : \operatorname{Gal}_F(B_{s,n}) \neq \mathfrak{S}_n\} \leq N_0 - 1 + 2d(\lfloor\sqrt{D|a|(|a| + bX)}\rfloor + 1). \tag{4.19}$$

Indeed, W_F has at most d elements: their square roots generate a multiquadratic subfield of F of degree $|W_F|$. The squarefree representatives satisfy $|\delta| \leq D$ by the quadratic discriminant formula and the discriminant tower formula. On each of the two even classes modulo four, δD_n is a nonconstant integral affine function with absolute value at most $D|a|(|a|+bX)$. Each nonnegative square value occurs at most once. Summing these counts and adding the degrees below N_0 proves (4.19).

4.7. **Central-binomial and half-integral sections.** The same local witnesses prove the uniform half-integral criterion and the central-binomial classification. We first record the irreducibility argument.

Proposition 4.5. *For every $n \geq 1$, both C_n and $H_{1/2,n}(x) = \sum_{j=0}^{n} x^j/(2j + 1)$ are irreducible over $\mathbb{Q}$.*

Proof. By (4.13), it suffices in the first case to consider $T_n(y) = \sum_{j=0}^{n}(-1)^j\binom{n}{j}y^j/(2j+1)$. If $n \geq 5$, Ramanujan's strengthening of Bertrand's postulate gives two primes in $(n+1/2, 2n+1]$: $\pi(x) - \pi(x/2) \geq 2$ for $x \geq 11$ [38, Section 2]. For either prime, the only coefficient of valuation -1 is at $j = (p-1)/2 \in [n/2, n]$; all others are units. If $j = n$, the single primitive Newton edge proves irreducibility. Otherwise a proper factor has degree j or $n-j$, and two distinct values of $j \in [n/2, n)$ give disjoint possibilities. For $n = 1$ the claim is immediate; for $n = 2, 3$, use $p = 5, 7$, respectively. At $n = 4$, the primes $5, 7$ give incompatible factor degrees $\{2\}$ and $\{1, 3\}$. The same witnesses work for $H_{1/2,n}$, since removing the binomial multipliers leaves these valuations unchanged. □

The irreducibility proof is independent of the multipliers. To obtain the uniform containment result, we combine the preceding prime estimates with finite lists of local witnesses.

Proposition 4.6. *Let*

$$R_n(x) = \sum_{j=0}^{n} \frac{u_{n,j}}{2j+1} x^j, \qquad u_{n,j} \in \mathbb{Q}^\times,$$

where every $u_{n,j}$ is a unit at every prime $p > n$. Over a number field F, the polynomial R_n is irreducible for every $n \geq R_F$. Its Galois group contains $\mathfrak{A}_n$ whenever $n \geq R_F$ and $n \neq 6$. In every odd degree $n \geq R_F$, its group is $\mathfrak{S}_n$.

Proof of Proposition 4.6. The proof of Proposition 4.5 uses only the valuations at primes $p > n$, so it applies to every admissible row. If $n \geq R_F$, these primes are unramified in F, and the primitive Newton edges remain unchanged over its completions. This proves irreducibility over F. At $n < p < 2n$, tame inertia has cycle type $(j)(n-j)$, where $j = (p-1)/2$.

For $n \geq \max\{10^6, R_F\}$, alternating containment follows from (A.5). For $65 \leq n < 10^6$, Table 1 gives three primes $p_i = 2j_i + 1$ whose indices are pairwise coprime and satisfy

$$n/2 < j_i < n - \sqrt{n}.$$

For every factorization $n = mr$ with $m, r > 1$, each of m, r divides at most one j_i. Some index is therefore divisible by neither, so Lemma 3.2 gives alternating containment. To verify a row with degree range $[u, v]$, let j_-, j_+ be its smallest and largest indices and check

$$u > 64, \quad u > j_+, \quad (u - j_+)^2 > u, \quad v < 2j_-.$$

These inequalities persist throughout the interval. The ranges cover every degree from 65 to 1530621. The accompanying verifier checks the endpoints, all primalities by trial division, and the three gcds in each row.

For $5 \leq n \leq 64$, outside $\{6, 10, 12, 24\}$, Table 2 supplies a prime $n + 1 < p \leq 2n - 3$ with $\gcd(n, (p-1)/2) = 1$. The interval rows have prime $j = (p-1)/2$ and $j + 2 \leq n \leq 2j - 1$; the remaining gcds are $\gcd(11, 9) = \gcd(22, 15) = \gcd(23, 21) = 1$. Powers of inertia isolate both cycles of lengths $j, n-j$. The longer cycle forces primitivity. Indeed, a block meeting its support and a fixed point is invariant and would contain all $j > n/2$ support points. Otherwise the support is a union of blocks, so the block size divides both j and n, contrary to coprimality. The shorter cycle has $2 \leq n - j < n/2$; Lemma 3.1 gives alternating containment.

For $n = 10, 12, 24$, the prime $2n-1$ supplies an $(n-1)$-cycle, which makes the transitive action doubly transitive and hence primitive. In degree ten, Müller's classification [32, Theorem 3.2] leaves only $\mathfrak{A}_{10}$ and $\mathfrak{S}_{10}$: 10 is neither a prime power nor $p + 1$ for a prime p, and is neither 12 nor 24. In degrees $12, 24$, the additional primes $19, 41$ give cycle types $(9)(3), (20)(4)$. Neither occurs in a primitive group not containing $\mathfrak{A}_n$: the shorter lengths in the other degree-12 cases are $1, 2, 4, 6$, and those in degree 24 are $1, 3, 12$ [32, Theorem 3.3].

Degrees two and three follow from irreducibility. In degree four, inertia at 7 gives a 3-cycle; a transitive subgroup of $\mathfrak{S}_4$ containing such a cycle contains $\mathfrak{A}_4$. For odd $n \geq 3$, a Bertrand

Range of n	Primes p_1, p_2, p_3
65– 101	$103, 107, 113$
101– 165	$167, 179, 181$
166– 261	$263, 293, 307$
262– 477	$479, 487, 491$
477– 885	$887, 907, 911$
879– 1665	$1667, 1697, 1699$
1666– 3201	$3203, 3229, 3251$
3200– 6267	$6269, 6271, 6287$
6253– 12327	$12329, 12343, 12347$
12322– 24405	$24407, 24419, 24421$
24405– 48485	$48487, 48491, 48497$
48484– 96485	$96487, 96497, 96527$
96484– 192339	$192341, 192343, 192347$
192334– 383757	$383759, 383777, 383791$
383758– 766229	$766231, 766247, 766277$
766230–1530621	$1530623, 1530647, 1530709$

TABLE 1. Three-prime certificates for central-binomial and half-integral reciprocal sections. The indices $(p_i - 1)/2$ are pairwise coprime.

Degrees n	Prime p	$j = (p-1)/2$
5	7	3
7–9	11	5
11	19	9
13–21	23	11
22	31	15
23	43	21
25–45	47	23
43–64	83	41

TABLE 2. Single-prime certificates in the remaining degrees below 65.

prime $n < p < 2n$ gives an odd two-cycle inertia permutation, so the group is $\mathfrak{S}_n$. Degree one is immediate. □

In particular, $\max\{7, R_F\}$ is a uniform threshold for alternating containment. If v_j are nonzero integers with $|v_j| \le B$ and $r \in \mathbb{Z}_{\ge 0}$, the sections of

$$\sum_{j\ge 0} \frac{v_j}{(2j+1)(j!)^r} x^j$$

are irreducible and contain $\mathfrak{A}_n$ for every $n \ge \max\{7, B, R_F\}$, with group $\mathfrak{S}_n$ in odd degree. Indeed, every prime dividing v_j or $j!$ is then at most n.

We can now determine every central-binomial group. Only degree six requires a local witness beyond the uniform criterion.

Proof of Theorem D. We have $C_n(x) = B_{1/2,n}(4x)$. By (4.13), an affine change of variable and a nonzero scalar multiplication give

$$T_n(y) = \sum_{j=0}^{n} \frac{(-1)^j \binom{n}{j}}{2j+1} y^j.$$

Every binomial multiplier is a unit at primes $p > n$. Proposition 4.6 therefore gives alternating containment over F for $n \geq R_F$, $n \neq 6$, and the full symmetric group in odd degree.

For degree six, the prime 11 gives a 5-cycle, so irreducibility implies primitivity. We have

$$C_6(x) \equiv 4(x-1)(x^2+3)(x^3+4x^2+x+2) \pmod 5.$$

The quadratic and cubic factors have no roots in $\mathbb{F}_5$. Thus the reduction is squarefree with factor degrees $(1,2,3)$, and the cube of Frobenius is a transposition. Hence the group over $\mathbb{Q}$ is $\mathfrak{S}_6$. For T_6, the single primitive Newton edge at 13 gives an odd 6-cycle. Lemma 3.8(1) preserves $\mathfrak{S}_6$ over every F with $R_F \leq 6$.

In even degree, (4.15) gives discriminant square class $[(-1)^{n/2}(2n+1)]$. Alternating containment and the discriminant criterion prove (1.10). Over $\mathbb{Q}$ this class is a square precisely when $2n+1 = (2r+1)^2$, equivalently $n = 2r(r+1)$ with $r \geq 1$; such n is automatically divisible by four. This proves (1.9).

A monic polynomial irreducible modulo a prime is squarefree there. Dedekind's theorem therefore forces an n-cycle in its Galois group. When $n = 2r(r+1)$, the group $\mathfrak{A}_n$ contains no n-cycle, so $x^n C_n(1/x)$ has no irreducible reduction. In all other degrees the group is $\mathfrak{S}_n$, and Chebotarev gives relative prime density $(n-1)!/n! = 1/n$ for irreducible reductions [44]. This proves Sun's assertion [45, part (ii)]. □

The exact number of alternating degrees is

$$\#\{3 \leq n \leq X : \mathrm{Gal}_{\mathbb{Q}}(C_n) = \mathfrak{A}_n\} = \left\lfloor \frac{\sqrt{2X+1}-1}{2} \right\rfloor = \sqrt{X/2} + O(1) \qquad (X \geq 1). \tag{4.20}$$

Proposition 4.5 also proves the central-binomial case of Sun's factorial-ratio assertion [46]; the broader assertion remains a separate question.

The excluded degree in the uniform criterion admits only one further group-theoretic possibility.

Remark 4.7. In degree six, the same row hypothesis and $R_F \leq 6$ restrict $\mathrm{Gal}_F(R_6)$ to $\mathfrak{S}_6$ or $\mathrm{PGL}_2(5)$ in its action on six points. Indeed, inertia at 11 gives a 5-cycle and hence primitivity; inertia at 13 gives an odd 6-cycle. Müller's [32, Theorem 3.2] leaves precisely these two possibilities. This does not assert that the smaller group occurs for an admissible row.

For the unweighted reciprocal sections, a second finite-field calculation resolves degree six. The real roots also determine the group in degrees congruent to two modulo four.

Corollary 4.8. *Put $H_n(x) = \sum_{j=0}^{n} x^j/(2j+1)$. For every number field F and every $n \geq R_F$, $\mathrm{Gal}_F(H_n)$ contains $\mathfrak{A}_n$ and is $\mathfrak{S}_n$ when n is odd. Over $\mathbb{Q}$, its group is $\mathfrak{S}_n$ whenever $4 \nmid n$.*

Proof. Only degree six remains. Inertia at 11 gives a 5-cycle, so the group over $\mathbb{Q}$ is primitive. The monic polynomial $13H_6$ satisfies

$$13H_6(x) \equiv (x+4)(x^2+12x+8)(x^3+13x^2+2) \pmod{17}.$$

The quadratic and cubic factors have no roots in $\mathbb{F}_{17}$. The reduction is therefore squarefree with factor degrees $(1,2,3)$, and the cube of Frobenius is a transposition, giving $\mathfrak{S}_6$. The single primitive Newton edge at 13 supplies an odd 6-cycle, so Lemma 3.8 transfers the group to every F with $R_F \leq 6$.

For even n, the identity

$$H_n(x) = \int_0^1 \sum_{j=0}^{n} (xt^2)^j \, dt > 0 \qquad (x \in \mathbb{R})$$

follows from the finite geometric sum: for $x < 0$ the integrand is $(1-(xt^2)^{n+1})/(1-xt^2) > 0$, and for $x \geq 0$ its constant term is one and all other terms are nonnegative. Thus there are no real

roots, and complex conjugation has sign $(-1)^{n/2}$. This proves symmetry when $n \equiv 2 \pmod 4$; odd degrees were already settled by Proposition 4.6. □

For comparison, a fixed integral exponent $s \geq 2$ is outside Theorem B. Formula (4.15) still gives $A((1-x)^{-s}) = 0$: the square classes on n mod 4 are the positive nonsquare polynomials $s(n+s)$ and $s\prod_{j=1}^{s-1}(n+j)/(s-1)!$ on classes zero and one, and negative values on the other two classes, so Proposition 7.3 applies. Also

$$B_{s,n}(x) = \frac{1}{(s-1)!}\frac{d^{s-1}}{dx^{s-1}}\sum_{j=0}^{n+s-1} x^j,$$

and [7, Theorem 2] gives irreducibility in density one. Alternating containment in density one is an additional question. The case $s = 1$ is geometric, with triple $(0, 0, 1)$; nonpositive integral s gives eventually zero coefficients.

5. Catalan sections

Let $c_j = \binom{2j}{j}/(j+1)$ for $j \geq 0$, and write

$$P_n(x) = \sum_{j=0}^{n} c_j x^j, \qquad Q_n(x) = x^n P_n(1/x).$$

Seki proved that P_n is irreducible over $\mathbb{Q}$ for every $n \geq 1$ [41, Theorem 1.1]. To prove Theorem E, we first show that its Galois group is primitive. Local inertia rules out all block systems with at least three blocks. A possible system of two blocks requires a different argument: congruences for the two root sums force their product to have a value incompatible with transitivity. The reduction identities and trace congruences come from Seki's irreducibility argument [41, Section 4]; the step here is to apply them to blocks of the Galois action. Once primitivity is established, the same local cycles give the symmetric group and the stated bound over a number field.

5.1. **Local cycles and discriminants.** The polynomial Q_n is monic integral, has coefficient 1 at x^{n-1}, and all its complex roots satisfy

$$|\alpha| \leq \max_{1\leq j\leq n}\frac{c_j}{c_{j-1}} = 4 - \frac{6}{n+1} < 4 \tag{5.1}$$

by the Eneström–Kakeya bound. Fix a prime $n+1 < p \leq 2n$, and put

$$k = \frac{p-1}{2}, \qquad d = n-k.$$

Then $1 \leq d < n/2$. Since $p > n+1$, the factorial formula for c_j gives $v_p(c_j) = 0$ for $j \leq k$ and $v_p(c_j) = 1$ for $k < j \leq n$. The lower Newton polygon of Q_n therefore consists of the edge from $(0, 1)$ to $(d, 0)$, followed by a horizontal edge. Modulo p we have

$$\overline{Q_n} = x^d\overline{Q_k}, \qquad 2\overline{Q_k}(x) = x^{k+1} - (x-4)^{k+1}. \tag{5.2}$$

The second identity follows by comparing coefficients, using $2c_j \equiv -(-4)^{j+1}\binom{k+1}{j+1} \pmod p$. Consequently

$$\overline{Q_k}(x)\big(x^{k+1} + (x-4)^{k+1}\big) = 2(x^p + x - 4).$$

The polynomial on the right has derivative 2. Thus $\overline{Q_k}$ is squarefree, and its roots satisfy

$$\gamma^p = 4 - \gamma. \tag{5.3}$$

These identities also appear in [41, Section 4.1].

Hensel's lemma gives $Q_n = A_pB_p$ over $\mathbb{Z}_p$, with A_p, B_p monic, $\overline{A_p} = x^d$, and $\overline{B_p} = \overline{Q_k}$. Since $B_p(0)$ is a unit and $v_p(Q_n(0)) = 1$, the constant coefficient of A_p has valuation one. Thus A_p is Eisenstein. A root generates a totally ramified extension of degree $d < p$, and its splitting field

is tame. The squarefree reduction of B_p makes its splitting field unramified. Inertia is therefore cyclic, transitive on the d roots of positive valuation, and trivial on the other roots. A generator acts as a d-cycle on this set and fixes all remaining roots.

We also record the discriminant valuation. Each root α of A_p has valuation $1/d$. In $A_p'(\alpha)$ the leading term $d\alpha^{d-1}$ has valuation $(d-1)/d$, strictly less than that of every other term. Hence $v_p(\mathrm{Disc}(A_p)) = d-1$. The discriminant of B_p and the resultant of A_p, B_p are units. Reversal preserves the discriminant, and therefore

$$v_p(\mathrm{Disc}(P_n)) = v_p(\mathrm{Disc}(Q_n)) = d-1. \tag{5.4}$$

5.2. **Explicit primes in a short interval.** Write $I_n = (n+1, 4n/3]$, and let $\pi(I_n)$ denote the number of primes in this interval. We need primes in specified residue classes, as well as a lower bound that prevents all primes in I_n from lying in one progression of large modulus.

Lemma 5.1. *For $n \geq 1000$, the interval I_n contains a prime in each reduced residue class modulo 4 and modulo 6. For $n \geq 16384$ it also satisfies*

$$\pi(I_n) > \frac{2n}{7\log n}. \tag{5.5}$$

Proof. Put $u = 4n/3$ and $\ell = n+1$, and write $\theta(x;q,a) = \sum_{p\leq x,\ p\equiv a \bmod q} \log p$ and $\theta(x) = \theta(x;1,1)$. Ramaré–Rumely [37, Theorems 1 and 2, p. 398] give, for $q = 1, 4, 6$ and $(a,q) = 1$,

$$\max_{1\leq t\leq x} \left|\theta(t;q,a) - \frac{t}{\varphi(q)}\right| \leq \begin{cases} 2.072\sqrt{x}, & 1 \leq x \leq 10^{10}, \\ \varepsilon_q x/\varphi(q), & x \geq 10^{10}, \end{cases}$$

where $\varepsilon_1 = 0.000213$ and $\varepsilon_4 = \varepsilon_6 = 0.004560$. Applying the maximum bound with the common endpoint $x = u$ handles the transition at 10^{10} as well.

Since $4.144\sqrt{4/3} < 24/5 < 5$, for $q = 4, 6$ the difference $\theta(u;q,a) - \theta(\ell;q,a)$ is at least

$$\begin{cases} n/6 - 1/2 - 5\sqrt{n}, & u \leq 10^{10}, \\ (1/6 - 0.006080)n - 1/2, & u \geq 10^{10}. \end{cases}$$

Both are positive for $n \geq 1000$. For the first, its value at 1000 exceeds $37/6$, since $\sqrt{1000} < 32$, and it increases thereafter. This proves the residue-class assertion.

For $q = 1$ and $n \geq 16384 = 2^{14}$, the same bounds give

$$\frac{\theta(u) - \theta(\ell)}{n} > \frac{1}{3} - \frac{1}{16384} - \frac{3}{80}.$$

Indeed, in the lower range the error is less than $24/(5\sqrt{n}) \leq 3/80$; in the upper range it is $0.000568 < 3/80$. Since $\log n > 9$ and $\log(4/3) < 3/10$, we have $\log n/\log u > 30/31$. It follows that

$$\pi(I_n)\frac{\log n}{n} \geq \frac{\theta(u) - \theta(\ell)}{n}\frac{\log n}{\log u} > \frac{30}{31}\left(\frac{1}{3} - \frac{1}{16384} - \frac{3}{80}\right) = \frac{72689}{253952} > \frac{2}{7}.$$

□

For the finite range we use the prime sets in Table 3. Each row has the following properties: all listed primes belong to I_n throughout the indicated range; their numbers $(p-1)/2$ have gcd one; and both odd residue classes modulo four occur. The overlapping ranges cover every integer $33 \leq n \leq 17325$. The accompanying verifier checks these assertions by integer arithmetic, using trial division for primality.

Range of n	Primes	Range of n	Primes
33–39	41, 43	598–785	787, 797
40–45	47, 53	775–1029	1031, 1033
46–57	59, 61	1030–1365	1367, 1373
55–69	71, 73	1359–1787	1789, 1811
67–81	83, 89	1788–2379	2381, 2383
82–105	107, 109	2377–3165	3167, 3169
105–135	137, 139	3165–4215	4217, 4219
136–177	179, 181	4194–5571	5573, 5591
172–225	227, 229	5514–7347	7349, 7351
220–281	283, 293	7344–9779	9781, 9787, 9791
280–357	359, 373	9757–13005	13007, 13009
348–459	461, 463	13000–17325	17327, 17333
451–597	599, 601		

TABLE 3. Prime sets with $\gcd\{(p-1)/2\} = 1$ and both residue classes modulo four.

5.3. **Excluding smaller blocks.** Suppose a permutation group preserves blocks of size m and contains a single d-cycle with $d > m$. A block meeting both its support and a fixed point would be invariant under the cycle and contain the entire support, a contradiction. Thus the support is a union of whole blocks, and $m \mid d$.

By Seki's theorem the group $G_n = \mathrm{Gal}(Q_n/\mathbb{Q})$ is transitive. Suppose $n \geq 33$ and it preserves blocks of size $2 \leq m \leq n/3$. Then $m \mid n$. Every prime $p \in I_n$ supplies a cycle of length $d = n - (p-1)/2 > n/3 \geq m$, so

$$p \equiv 1 \pmod{2m} \qquad (p \in I_n). \tag{5.6}$$

For $33 \leq n < 16384$, this contradicts the gcd condition in Table 3.

Now let $n \geq 16384$. Lemma 5.1 excludes $m = 2, 3$ by the residue classes 3 mod 4 and 5 mod 6. For $m \geq 4$ we have $\varphi(2m) \geq 4$. Set $y = (n-3)/3$ and $M = y/(2n^{3/5})$. If $m \leq M$, the Brun–Titchmarsh inequality for short intervals [31, Theorem 2, (1.10)] gives

$$\pi(I_n) < \frac{2y}{\varphi(2m)\log(y/(2m))} \leq \frac{5y}{6\log n} < \frac{5n}{18\log n} < \frac{2n}{7\log n},$$

contrary to (5.5). Here $y/(2m) \geq n^{3/5} > 1$, as required by that inequality. If $m > M$, the progression in (5.6) contains at most $y/(2m) + 1 < n^{3/5} + 1$ integers in I_n. For $n \geq 16384$,

$$(n^{-2/5} + n^{-1})\log n < \frac{2}{7},$$

since the left side decreases on this range, and at the left endpoint it is less than $10(1/40 + 1/16384) = 2053/8192 < 2/7$. We used $\log 16384 < 10$ and $16384^{2/5} > 40$. This again contradicts (5.5). The only proper divisor of n larger than $n/3$ is $n/2$; it remains to exclude a system of two blocks.

5.4. **Excluding two blocks by their traces.** Suppose now that $n \geq 33$ and there are two blocks of size $n/2$. Let A, B be their root sums. The group permutes the blocks, so

$$A + B = -1, \qquad T = AB \in \mathbb{Z}, \qquad |T| < 4n^2.$$

The integrality follows because T is a Galois-invariant algebraic integer; the bound follows from (5.1).

Let L be the splitting field, fix a prime $n+1 < p \leq 2n$, and choose a prime $\mathfrak{p}$ of L above p. Let R be the set of d roots with positive $\mathfrak{p}$-adic valuation. If $d > 1$, the inertia cycle has fixed roots

and hence cannot interchange the two blocks. Its orbit R is therefore contained in one block; the same conclusion is immediate for $d = 1$. The decomposition group preserves the nonempty set R, so it fixes the block containing R and consequently both blocks.

An arithmetic Frobenius lift thus permutes the unit roots in each block. If a block has h such roots and S is the sum of their reductions modulo $\mathfrak{p}$, this permutation gives $S^p = S$, while (5.3) gives $S^p = 4h - S$. Thus $S = 2h$. The two blocks have $n/2$ and $n/2 - d$ unit roots, and all other roots reduce to zero. Consequently A, B reduce to n and $n - 2d$, in some order. Since $T \in \mathbb{Z}$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, we obtain

$$T \equiv n(n - 2d) = n(p - 1 - n) \equiv -n(n + 1) \pmod{p}.$$

For $n \geq 24$, three applications of Nagura's theorem [33, Theorem, p. 180] give distinct primes

$$n + 1 < p_1 < p_2 < p_3 < (6/5)^3(n + 1) < 2n.$$

Consequently

$$\prod_{n+1<p\leq 2n} p > (n + 1)^3 > 5n^2 + n.$$

This product divides the integer $T + n(n+1)$, whose absolute value is less than $5n^2 + n$. Therefore $T = -n(n + 1)$, and A, B are the two distinct rational roots $n, -n - 1$ of $Z^2 + Z - n(n + 1)$. Transitivity requires an element interchanging the two blocks and hence their sums, which is impossible for distinct rational numbers. Thus G_n is primitive for every $n \geq 33$.

5.5. **The symmetric group in every degree.** For every $n \geq 33$, Table 3 and Lemma 5.1 supply a prime $p \in I_n$ with $p \equiv 2n+1 \pmod 4$. The associated cycle has even length $d = (2n+1-p)/2$, with $2 \leq d < n/2$. Lemma 3.1 yields $\mathfrak{A}_n \subseteq G_n$. An even-length cycle is an odd permutation, so $G_n = \mathfrak{S}_n$.

For $3 \leq n \leq 32$, Table 4 gives two squarefree reductions of Q_n. The factor degrees modulo p are $(1, n - 1)$. The partition λ_q modulo q contains exactly one quadratic factor, with all other factors of odd degree. Dedekind's theorem [30, Theorem 8.23] therefore supplies an $(n - 1)$-cycle and an element with an odd power equal to a transposition. A transitive group containing an $(n-1)$-cycle is primitive: the block containing its fixed point must either be a singleton or contain the entire support. A primitive group containing a transposition is symmetric. Indeed, the graph whose edges are its conjugate transpositions has components forming a block system; it is connected, and its edge transpositions generate $\mathfrak{S}_n$. Degrees one and two follow directly from irreducibility.

For a squarefree polynomial $f \in \mathbb{F}_p[x]$, successive gcds with $x^{p^j} - x$, removing the factors already found, determine the number of irreducible factors of degree j. The accompanying verifier implements this procedure with integer arithmetic and checks squarefreeness separately.

5.6. **An explicit bound over a number field.** We claim that for every $n \geq 2$ there is a prime $p > n$ with odd inertia in the splitting field of P_n. For $n \geq 33$ we already have a prime $n+1 < p < 2n$ with $p \equiv 2n+1 \pmod 4$; its inertia cycle has even length. For $7 \leq n \leq 32$, primes with these properties are:

p	n odd	p	n even
11	$7, 9$	13	$8, 10$
19	$11, 13, 15, 17$	17	$12, 14$
23	$19, 21$	29	$16, 18, 20, 22, 24, 26$
31	$23, 25, 27, 29$	37	$28, 30, 32$
43	31		

n	p	q	λ_q	n	p	q	λ_q
3	5	5	$(1,2)$	18	53	7	$(1^2,2,3,11)$
4	2	7	$(1^2,2)$	19	59	13	$(1,2,3,13)$
5	3	53	$(2,3)$	20	191	13	$(1^2,2,3,13)$
6	5	19	$(1,2,3)$	21	73	7	$(1,2,9^2)$
7	23	53	$(2,5)$	22	139	59	$(1,2,5,7^2)$
8	47	29	$(1^3,2,3)$	23	83	97	$(1^2,2,5,7^2)$
9	41	23	$(1^2,2,5)$	24	73	79	$(2,7,15)$
10	61	7	$(1,2,7)$	25	127	83	$(1^2,2,21)$
11	37	7	$(1^2,2,7)$	26	13	59	$(1^3,2,21)$
12	103	37	$(2,5^2)$	27	421	5	$(1,2,3,21)$
13	53	37	$(1^4,2,7)$	28	281	5	$(1^2,2,3,21)$
14	53	37	$(1,2,11)$	29	97	13	$(1^2,2,25)$
15	47	107	$(1,2,3,9)$	30	379	179	$(2,9,19)$
16	211	127	$(1,2,13)$	31	113	149	$(2,29)$
17	53	7	$(1,2,3,11)$	32	311	97	$(1,2,29)$

TABLE 4. Squarefree factorizations of Q_n modulo two primes. The factor degrees modulo p are $(1, n-1)$; exponents in λ_q count distinct irreducible factors of the indicated degree.

At $n = 5$, take $p = 7$, which gives a 2-cycle. The remaining degrees have the following exact discriminants and odd-valuation prime divisors:

n	$\mathrm{Disc}(P_n)$	p
2	-7	7
3	-543	181
4	533489	4409
6	-1318026434480736	181

In each row $p > n$ and $v_p(\mathrm{Disc}(P_n)) = 1$. The quadratic extension defined by the discriminant is consequently ramified at p, so the sign character is nontrivial on inertia. These small discriminants are also checked by the accompanying integer-arithmetic verifier.

For $n \geq \max\{2, R_F\}$, the chosen prime $p > n$ is unramified in F, so Lemma 3.8(1) gives $\mathrm{Gal}_F(P_n) = \mathfrak{S}_n$. The degree-one case is immediate. Hence

$$\mathrm{Gal}_F(P_n) = \mathfrak{S}_n \qquad (n \geq R_F). \tag{5.7}$$

This completes the proof of Theorem E.

6. Arithmetic families

We begin with a family of rational functions whose coefficients are eventually constant. Their sections are quotients of trinomials, and their Galois groups can be determined by the classical inertia and transposition argument; compare [42, Section 4.4, Remark 2]. The following consequence of Minkowski's bound will control ramification at 2.

Lemma 6.1. *A number field unramified at every odd prime and tamely ramified at* 2 *is* $\mathbb{Q}$.

Proof. Suppose the field has degree $d \geq 2$, discriminant D, and r_2 conjugate pairs of nonreal embeddings. The tame discriminant formula gives $|D| \leq 2^{d-1}$, whereas Minkowski's bound [30, Theorem 4.3] gives

$$|D| \geq (\pi/4)^{2r_2}(d^d/d!)^2 \geq (\pi/4)^d(d^d/d!)^2 \geq \pi^d/4 > 2^{d-1}.$$

The inequality $d^d/d! \geq 2^{d-1}$ follows by induction, since the successive ratio is $(1+1/d)^d \geq 2$. The last inequality holds at $d = 2$ and becomes stronger thereafter. □

For the family below, parity detects the reducible sections. In the remaining degrees, the preceding lemma allows us to recover the whole group from inertia at odd primes.

Proposition 6.2. *Let $k = 2^a$, where a is a positive integer, and put $h_k = (1 + x^k)/(1 - x)$. For every $n \geq k$,*

$$\mathrm{Gal}((h_k)_n/\mathbb{Q}) = \mathfrak{S}_n \quad \textit{if } n \textit{ is even}, \qquad (h_k)_n(-1) = 0 \quad \textit{if } n \textit{ is odd}.$$

Consequently $(S(h_k), A(h_k), O(h_k)) = (1/2, 0, 1/2)$.

Proof. Put $N = n + 1$ and $m = N - k$. Reversal gives

$$x^n(h_k)_n(1/x) = Q(x) := \frac{x^N + x^m - 2}{x - 1}. \tag{6.1}$$

If n is odd, N, m are even and $Q(-1) = 0$. Suppose n is even. Then N, m are odd and $\gcd(N, m) = 1$.

The polynomial $R = x^N + x^m - 2$ has no root of modulus less than one. On the unit circle, equality in the triangle inequality forces $x^N = x^m = 1$, hence $x = 1$. This root is simple, since $R'(1) = N + m > 0$. All roots of the monic integral polynomial Q therefore have modulus greater than one. Since $Q(0) = 2$, a nontrivial monic integral factorization would give two constant coefficients of absolute value at least two, with product two. Gauss's lemma gives a contradiction. Thus Q is irreducible.

Fix an odd prime p, and let $\alpha \in \overline{\mathbb{F}_p}$ be a multiple root of the reduction of R. Then $\alpha \neq 0$ and

$$\alpha^N + \alpha^m = 2, \qquad N\alpha^N + m\alpha^m = 0.$$

No such root exists if $p \mid Nm(N - m)$. Otherwise

$$\alpha^N = -2m/(N - m), \qquad \alpha^m = 2N/(N - m).$$

Coprimality of N, m makes it unique if it exists, and $\alpha^2 R''(\alpha) = -2Nm \neq 0$. Thus the only possible repeated root is double. The same holds after division by $x - 1$. Inertia can only permute roots with the same reduction. Thus each inertia group at an odd prime is trivial or generated by a single transposition on the roots of Q.

At 2,

$$Q(x) \equiv x^m(x + 1)^{k-1} \pmod 2.$$

Hensel factorization gives $Q = AB$ in $\mathbb{Z}_2[x]$, with A, B monic of degrees $m, k - 1$ and reductions $x^m, (x + 1)^{k-1}$. Since $Q(0) = 2$ and $B(0)$ is odd, A is Eisenstein. Its odd degree makes its root field tame. For $k = 2$, B is linear. For $k \geq 4$, $v_2(Q(1)) = v_2(2N - k) = 1$, and $A(1)$ is odd. Thus $B(x + 1)$ is Eisenstein of odd degree. Tame local extensions remain tame under conjugacy and compositum [12, Theorem 2.1]. Hence the splitting field L of Q is tame at 2.

Let H be the normal subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by all inertia groups at odd primes. Its fixed field is unramified outside 2 and tame at 2, so Lemma 6.1 makes it $\mathbb{Q}$. The whole group is generated by transpositions. Irreducibility makes it transitive, so it is $\mathfrak{S}_{N-1}$. Reversal preserves the splitting field and its root action. □

The case $k = 2$, which is the example in (1.5), also shows that the coefficient tail does not determine the frequencies.

Corollary 6.3. *Neither the frequency triple nor the zero–one property is invariant under changes to finitely many coefficients.*

Proof. The series $2/(1 - x)$ has cyclotomic splitting fields and triple $(0, 0, 1)$, whereas $2/(1 - x) - h_2 = 1 + x$. □

6.1. **Further exact rational families.** For every fixed even $k \geq 2$, set $u_k = (2x^k - 1)/(1 - x)$. Then

$$(S(u_k), A(u_k), O(u_k)) = (\varphi(k)/k, 0, 1 - \varphi(k)/k). \tag{6.2}$$

Its coefficients are -1 before degree k and 1 afterwards. We combine Schinzel's irreducibility theorem with the preceding inertia argument. For $N = n + 1 > k$, put $R(x) = x^N - 2x^k + 1 = (x-1)(u_k)_n(x)$. If $d = \gcd(N, k) > 1$, the section has the proper cyclotomic factor $(x^d - 1)/(x - 1)$. Suppose instead that $\gcd(N, k) = 1$. Schinzel's theorem [39] makes the quotient by $x-1$ irreducible except when $(N, k) = (7, 2)$ or $(7, 5)$; see [19, p. 5]. We may therefore assume $N > 7$. Since k is even, N is odd, so the reduction modulo 2 is squarefree. At an odd prime dividing $Nk(N - k)$, the reductions of R and R' have no common root. For an odd prime $p \nmid Nk(N - k)$, a common root $\alpha \in \overline{\mathbb{F}_p}$ satisfies

$$\alpha^k = \frac{N}{2(N-k)}, \quad \alpha^N = \frac{k}{N-k}, \quad R''(\alpha) = 2k(N-k)\alpha^{k-2} \neq 0.$$

Since $\gcd(N, k) = 1$, the first two identities determine at most one α, and the third makes it a double root. All finite inertia groups are therefore trivial or generated by a transposition. Their normal closure is the whole group, since $\mathbb{Q}$ has no nontrivial extension unramified at all finite primes [30, Theorem 4.9]. Transitivity gives $\mathfrak{S}_n$. Counting $\gcd(n + 1, k) = 1$ proves (6.2).

For the positive family $h_k = (1 + x^k)/(1 - x)$, Garmi's trinomial theorem [20, Theorem 1.1], in its $|ab| = 2$ case, gives the analogous formula for every integer $k \geq 1$:

$$(S(h_k), A(h_k), O(h_k)) = (\varphi(k)/k, 0, 1 - \varphi(k)/k). \tag{6.3}$$

Indeed, for $n \geq k$ and $N = n + 1$, (6.1) applies. When $\gcd(N, k) = 1$, the only unit-circle root of $x^N + x^{N-k} - 2$ is 1, and Garmi's theorem gives $\mathfrak{S}_{N-1}$ for $N > 8$. If the gcd exceeds one, a proper cyclotomic factor remains. For general k, this calculation uses Garmi's preprint; Proposition 6.2 gives an independent proof for powers of two, including every degree $n \geq k$.

The ratios $\varphi(k)/k$ are dense in $[0, 1]$, a classical fact going back to Euler [16, Introduction]. Indeed, products of $1 - 1/p$ over successive primes beyond any fixed threshold tend to zero, with each downward step at most $1/p$. Stopping at the first crossing of a target in $(0, 1)$ proves density. Thus (6.3) gives a dense set of triples on the edge $(t, 0, 1 - t)$ for rational functions with positive bounded integer coefficients. Within this family, $O(h_k) \in \{0, 1\}$ holds exactly when $k = 1$.

For an integer $r \geq 0$, write $f^{[r]} = \sum_{j \geq 0} a_{j+r} x^j$. Then

$$h_k^{[r]} = \begin{cases} h_{k-r}, & r < k, \\ 2/(1 - x), & r \geq k. \end{cases}$$

Consequently, deleting a finite prefix need not preserve the frequency triple.

6.2. **A rational family with other frequency one.** A different mechanism occurs for coefficients with a geometric progression on each parity class. Odd sections factor, while even sections have a reciprocal symmetry that preserves pairs of roots.

Proposition 6.4. *For $a, b, c \in \mathbb{Q}^\times$,*

$$f(x) = \frac{a + bx}{1 - cx^2} \quad \Longrightarrow \quad (S(f), A(f), O(f)) = (0, 0, 1).$$

Proof. Odd sections factor as $(a + bx) \sum_{j=0}^{m} (cx^2)^j$. Even sections satisfy $c^m x^{2m} f_{2m}(1/(cx)) = f_{2m}(x)$. If one is irreducible of degree at least four, the involution $\alpha \mapsto 1/(c\alpha)$ has no fixed root, since a fixed root has degree at most two. Its root pairs form a nontrivial Galois-invariant block system, excluding $\mathfrak{A}_{2m}$ and $\mathfrak{S}_{2m}$. Reducible sections and sections with repeated roots are already other. □

This includes every nonzero two-periodic rational coefficient sequence. For period $d \geq 3$, only a weaker conclusion is immediate. If $f = P(x)/(1-x^d)$, with $\deg P = d-1$ and nonzero coefficients, every large section of degree $d-1$ mod d factors as $P(x)\sum_{j=0}^{m} x^{dj}$. Its lower other frequency is at least $1/d$. The remaining classes require further Galois information.

6.3. **Exponential and logarithm.** Schur's theorem gives

$$G_n(e^x) = \begin{cases} \mathfrak{A}_n, & 4 \mid n, \\ \mathfrak{S}_n, & 4 \nmid n, \end{cases} \qquad (S(e^x), A(e^x), O(e^x)) = (3/4, 1/4, 0).$$

See [40, 11] and [36, Theorem 1.1]. With $e_n(x) = \sum_{j=0}^{n} x^j/j!$, the exact discriminants are

$$\mathrm{Disc}(n!e_n) = (-1)^{n(n-1)/2}(n!)^n, \qquad \mathrm{Disc}(e_n) = (-1)^{n(n-1)/2}(n!)^{2-n}.$$

The separate frequencies can change after extending the ground field. For every fixed number field F,

$$(S_F(e^x), A_F(e^x), O_F(e^x)) = \begin{cases} (1/2, 1/2, 0), & i \in F, \\ (3/4, 1/4, 0), & i \notin F. \end{cases} \tag{6.4}$$

Indeed, Proposition 3.7 gives alternating containment in all large degrees. For even n, the discriminant class is $[(-1)^{n/2}]$. For odd n, a Bertrand prime $n/2 < p < n$ has $v_p(n!) = 1$, so the discriminant has odd valuation. For large n this prime is unramified in F, excluding an F-square. This proves (6.4) and illustrates why the invariant other frequency does not force the separate frequencies to be invariant.

For every fixed integer $a > 0$, Weinbaum's preprint [47, Theorem 1.1] proves the density-one result

$$E_a(x) = \sum_{j \geq 0} \frac{x^j}{(a+j)!}, \qquad (S(E_a), A(E_a), O(E_a)) = (1, 0, 0).$$

For $L(x) = 1 - \log(1-x)$, Shokri et al. proved irreducibility and alternating containment in every degree [43]; see also [13, Section 1]. Hence $O(L) = 0$. Yamamura conjectured that every section has group $\mathfrak{S}_n$. The symmetric group is known for every $n \equiv 0, 2, 3 \pmod 4$ [13, Theorem 1], so

$$\liminf_{N\to\infty} s_L(N) \geq 3/4, \qquad \limsup_{N\to\infty} a_L(N) \leq 1/4.$$

Convergence of the first two frequencies is equivalent to the existence of a square-discriminant density. Cullinan and Gajek-Leonard also prove symmetry in degree mq for each fixed m and all sufficiently large primes q [13, Theorem 3]. These families do not by themselves determine a density in the degree variable.

6.4. **Factorial denominators and bounded multipliers.** The next result combines Allen–Filaseta's irreducibility theorems with explicit Newton polygons. It includes two Mittag–Leffler families and permits arbitrary bounded nonzero integer multipliers.

Proposition 6.5. *Let $B \geq 1$ be an integer, let (b_j) be nonzero integers with $|b_0| = 1$ and $|b_j| \leq B$, and let F be a number field of degree d_F. Put $B_F = \min\{d_F + 1, 2R_F\}$. For an integer $m \geq 1$, set*

$$N_1 = \max\{50, 4m, 2B, B_F\}.$$

The degree-n section of $\sum_{j\geq 0} b_j x^j/(mj)!$ has Galois group containing $\mathfrak{A}_n$ over F for every $n \geq N_1$.

For $m \geq 2$, put

$$N_2 = \left\lceil \max\left\{179386, 4m+1, 2B, 2\exp((2m)^{1/3}), B_F\right\}\right\rceil.$$

Write $u_{(r)}$ for the largest divisor of a positive integer u coprime to r, and define

$$\mathcal{E}_{m,B} = \{n \geq 1 : (mn+1)_{(2)} \leq B \text{ or } (mn(mn+1))_{(6)} \leq B\}.$$

The degree-n section of $\sum_{j\ge 0} b_j x^j/(mj+1)!$ has Galois group containing $\mathfrak{A}_n$ over F whenever $n \ge N_2$ and $n \notin \mathcal{E}_{m,B}$. Moreover, for $X \ge 1$, writing $\log_r x = (\log x)/(\log r)$, we have

$$\#(\mathcal{E}_{m,B} \cap [1, X]) \le B(1 + \lfloor \log_2(mX+1) \rfloor) + 2B(1 + \lfloor \log_3(mX+1) \rfloor).$$

For $m = 2, 3$, one may instead take $N_2 = \max\{50, 4m+1, 2B, B_F\}$. If $B = 1$ and m is even, the second conclusion holds for every $n \ge N_2$. In particular, both families have $O_F = 0$.

Proof. Let P_n denote the relevant section and set $D = mn$. Write $P_n(x^m) = \sum_{i=0}^{D} a_i x^i/i!$ in the first family and $P_n(x^m) = \sum_{i=0}^{D} a_i x^i/(i+1)!$ in the second. In both cases, $a_{mj} = b_j$, and the remaining a_i are zero. Thus Allen–Filaseta's theorems apply without a restriction on the internal multipliers [1, Theorems 1 and 2]. For the first family, $D \ge 50$ and $|b_n| \le B < D$, so their first theorem gives irreducibility. Its only exceptional total degrees are 6 and 10. For the second family, their second theorem gives irreducibility whenever $n \notin \mathcal{E}_{m,B}$. In both cases, irreducibility of $P_n(x^m)$ implies that of P_n.

For $n \ge N_1$, Nagura's theorem supplies a prime $n/2 < p < 3n/5 < n-2$; at $n = 50$ one may take $p = 29$. Our bounds imply $p > m, B$ and $p^2 > mn$. Since $p > B$, all b_j are p-adic units. The coefficient valuations in the first family are therefore $-\lfloor mj/p \rfloor$. The line $y = -mx/p$ lies below all coefficient points, with equality precisely at the indices $j = 0, p$. It gives a Newton edge of slope $-m/p$, whose reduced denominator is p.

For the second family, Dusart's explicit prime interval [15, Proposition 5.4] supplies, for every $x \ge 89693$, a prime $x < p \le x(1 + 1/\log^3 x)$. At $x = n/2$ our choice of N_2 gives

$$\frac{n}{2} < p \le \frac{n}{2}\left(1 + \frac{1}{2m}\right) < \frac{mn}{2m-1} < n - 2.$$

Also $p > m, B$ and $p^2 > mn + 1$. Choose $t \in \{1, \dots, m-1\}$ with $tp \equiv 1 \pmod m$ and put $j_0 = (tp-1)/m$. The coefficient valuations are $-\lfloor (mj+1)/p \rfloor$. The line $y = -(mx+1)/p$ lies below the coefficient points, with equality exactly when $j \equiv j_0 \pmod p$. Since $0 \le j_0 < p$, $2p > n$, and $j_0 + p < (2m-1)p/m < n$, its contact indices are precisely $j_0, j_0 + p$. Thus it gives another Newton edge of slope $-m/p$ and reduced denominator p. For $m = 2, 3$, Nagura gives $n/2 < p < 3n/5 \le mn/(2m-1)$, so the same argument applies with the smaller stated threshold.

Lemma 3.5 now gives alternating containment over $\mathbb{Q}$ in each irreducible degree under consideration. If $n > d_F$, Proposition 3.7 gives the same conclusion over F. If $n \ge 2R_F$, the prime $p > n/2$ is unramified in F. Its Newton edge forces p to divide the inertia-group order, and an element of order p is a single p-cycle because $2p > n$. Lemma 3.8(2) then gives alternating containment over F. This proves the stated minimum B_F.

For the exceptional count, the first condition has the form $mn + 1 = \delta 2^u$ with $1 \le \delta \le B$. Under the second, the odd member of $mn, mn+1$ equals $\delta 3^v$ for some $1 \le \delta \le B$, so $mn = \delta 3^v$ or $\delta 3^v - 1$. Counting the possible exponents gives the displayed bound. Finally, when $|b_n| = 1$ and $D > 8$, the discussion following [1, Theorem 2] leaves only $D+1$ a power of two as a possible failure. For even m, the number $D + 1 > 1$ is odd, so this case does not occur. □

In particular,

$$E_{m,1}(x) = \sum_{j\ge 0} \frac{x^j}{(mj)!}, \qquad E_{m,2}(x) = \sum_{j\ge 0} \frac{x^j}{(mj+1)!}$$

have $O_F = 0$ for $m \ge 1$ and $m \ge 2$, respectively. Their separate symmetric and alternating frequencies reduce to a square-discriminant density. The folded trigonometric series $\cos\sqrt{x} = E_{2,1}(-x)$ and $\sin\sqrt{x}/\sqrt{x} = E_{2,2}(-x)$, with value 1 at $x = 0$, are examples; folding removes the zero coefficients of sine and cosine. The case $m = 1$ of $E_{m,2}$ is the proper exponential shift already discussed.

6.5. **Reciprocal factorial powers.** For a fixed integer $k \geq 1$, put

$$F_k(x) = \sum_{j\geq 0} \frac{x^j}{(j!)^k} = {}_0F_{k-1}(;1,\ldots,1;x).$$

For $n \geq \max\{50, 2k\}$, irreducibility of its section over $\mathbb{Q}$ implies alternating containment over $\mathbb{Q}$. Nagura's theorem gives $n/2 < p < 3n/5 < n-2$ with $p > k$. Its Newton polygon has the edge $(0,0)$ to $(p,-k)$, whose reduced slope denominator is p. Lemma 3.5 proves the assertion. Over a number field F, the same containment follows for $n \geq \max\{50, 2k, B_F\}$, where $B_F = \min\{[F:\mathbb{Q}]+1, 2R_F\}$, by the same index or ramification argument. Consequently, for every fixed F, the other degrees eventually coincide with the degrees in which the section is reducible over $\mathbb{Q}$. Thus $O_F(F_k)$ exists if and only if these reducible degrees have a natural density, and it equals that density. In particular, $O_F(F_k)$ exists and lies in $\{0,1\}$ precisely when that density is zero or one. The full triple converges if and only if, in addition, the irreducible sections whose discriminant is a square in F have a density in the set of all degrees. For $k = 2$ the series is the modified Bessel function $I_0(2\sqrt{x})$. The remaining arithmetic input is the density of its irreducible sections.

The same exact reduction applies to $1 + \mathrm{Li}_k(x) = 1 + \sum_{j\geq 1} x^j/j^k$, with fixed integer $k \geq 1$. For $n/2 < p < n-2$ and $p > k$, its coefficient valuations are $-k$ at $j = p$ and zero elsewhere. The edge $(0,0)$ to $(p,-k)$ again supplies the prime cycle, with the same explicit degree bounds. Here $k = 1$ is the logarithm discussed above.

7. Frequencies and effective constructions

We first express the frequency problem through alternating containment and discriminant square classes. We then draw the consequences of simultaneous prescription and consider effective questions.

7.1. **Two arithmetic means.** Put $\iota_n = C(f_n)$ for $n \geq 8$, and $\iota_n = 0$ for smaller n. For a number field F, define

$$D_{n,F} = \mathbf{1}_{\{\mathrm{Disc}(f_n)\in F^{\times 2}\}}, \qquad \theta_N = \frac{1}{N}\sum_{n\leq N} \iota_n, \qquad \alpha_{F,N} = \frac{1}{N}\sum_{n\leq N} \iota_n D_{n,F}.$$

The sums start at $n = 1$, and zero is excluded from $F^{\times 2}$. Write $\alpha_N = \alpha_{\mathbb{Q},N}$. The first mean measures alternating containment; the second measures the square-discriminant degrees among those sections.

Proposition 7.1. *For any fixed number field F, all three frequencies over F exist if and only if θ_N and $\alpha_{F,N}$ converge. If their limits are θ, α, then*

$$(S_F(f), A_F(f), O_F(f)) = (\theta - \alpha, \alpha, 1 - \theta). \tag{7.1}$$

Independently of the other limits, $O_F(f)$ exists if and only if θ_N converges.

Proof. By Propositions 3.4 and 3.7, for all sufficiently large n,

$$\mathbf{1}_{\{\mathrm{Gal}_F(f_n)=\mathfrak{S}_n\}} = \iota_n(1 - D_{n,F}), \qquad \mathbf{1}_{\{\mathrm{Gal}_F(f_n)=\mathfrak{A}_n\}} = \iota_n D_{n,F}.$$

For a separable section, a subgroup containing $\mathfrak{A}_n$ is $\mathfrak{A}_n$ or $\mathfrak{S}_n$, and its discriminant is a square in F exactly when the root action is even. For a nonseparable section, both displayed indicators and ι_n are zero. Thus the other indicator is $1 - \iota_n$ in either case. Averaging and discarding the finitely many initial degrees proves the result. □

The criterion replaces full group determination by irreducibility, a modular factorization witness, and a square test. The existence of the resulting means still requires information about the family. At the endpoints, convergence can be tested by comparing pairs of containment indicators.

Corollary 7.2. *Put $H_N = N^{-2}\sum_{1\le m,n\le N}|\iota_m - \iota_n|$. For any fixed number field F,*

$$O_F(f) \text{ exists and lies in } \{0,1\} \quad\Longleftrightarrow\quad H_N \longrightarrow 0.$$

Moreover, all three frequencies exist with $O_F(f)\in\{0,1\}$ if and only if $H_N\to 0$ and $\alpha_{F,N}$ converges.

Proof. Counting unequal ordered pairs gives $H_N = 2\theta_N(1-\theta_N)$. If $H_N\to 0$, then eventually $\theta_N\in[0,1/4)\cup(3/4,1]$. Since $|\theta_{N+1}-\theta_N|\le 1/(N+1)$, it cannot keep switching between these components. It stays in one and tends to its endpoint. The converse and the last assertion follow from Proposition 7.1. □

In particular, if alternating containment holds in density one, then $O_F(f)=0$, and the other two frequencies converge exactly when the F-square discriminant degrees have a density δ. The triple is then $(1-\delta,\delta,0)$. More generally, if irreducibility over F implies alternating containment over F outside a density-zero set, the other degrees over F agree, up to density zero, with the degrees reducible over F. This reduces existence and the endpoint property of O_F to the corresponding reducibility density. Full convergence also requires the density of F-square discriminants among sections irreducible over F.

When the discriminant square class is a rational function on each of finitely many progressions, quantitative Hilbert irreducibility reduces its square values to the progressions on which that function is itself a square.

Proposition 7.3. *Fix $q\ge 1$. Suppose, outside a density-zero set and finitely many zeros or poles, that*

$$[\mathrm{Disc}(f_n)] = [R_r(n)] \quad (n\equiv r \pmod q), \qquad R_r(T)\in\mathbb{Q}(T)^\times,$$

where brackets denote rational square classes. Put $I=\{r \bmod q : R_r\in\mathbb{Q}(T)^{\times 2}\}$. Then

$$\alpha_N - \frac{1}{N}\sum_{\substack{n\le N\\ n \bmod q\in I}}\iota_n \longrightarrow 0.$$

If alternating containment holds in density one, the triple over $\mathbb{Q}$ is $(1-|I|/q,|I|/q,0)$. If I is empty, then $A(f)=0$ without a containment hypothesis.

Proof. A square rational function has square values wherever defined and nonzero. Otherwise $Y^2-R_r(qT+r)$ is irreducible over $\mathbb{Q}(T)$, and its integer specializations with a rational root form a thin set of size $O(\sqrt{N}\log N)$ up to N, by quantitative Hilbert irreducibility [42, Theorem 3.4.4]. Summing over the finitely many classes and applying the indicator identities proves the result. □

7.2. **Cluster sets and coefficient shifts.** The prescription theorem reduces the frequency questions to the counting function of the set of symmetric degrees.

Corollary 7.4. *For every $0\le\alpha\le\beta\le 1$, a function in Theorem A can be chosen so that the set of subsequential limits of $(s_f(N),a_f(N),o_f(N))$ is exactly*

$$\{(t,0,1-t) : \alpha\le t\le\beta\}. \tag{7.2}$$

For rational α,β and computable coefficient bounds, the coefficients can be chosen computably. In particular, every $(\delta,0,1-\delta)$, $0\le\delta\le 1$, occurs as a frequency triple, and computable examples have lower symmetric frequency zero and upper symmetric frequency one.

Proof. For the function associated with B, the group prescription gives, for $N\ge 3$,

$$s_f(N) = \frac{\#(B\cap[3,N])}{N}, \qquad a_f(N)=0, \qquad o_f(N) = \frac{N-2}{N} - s_f(N). \tag{7.3}$$

Indeed, $(n-1)! < n!/2$ for $n \geq 3$, so the point stabilizer is neither $\mathfrak{S}_n$ nor $\mathfrak{A}_n$, even as an abstract group.

When $\alpha = \beta = \delta$, take

$$B = \{n \geq 3 : \lfloor \delta n \rfloor - \lfloor \delta(n-1) \rfloor = 1\}.$$

Its counting function is $\delta N + O(1)$. When $\alpha < \beta$, put $\Delta = \beta - \alpha$ and start a binary sequence with a single zero. At stage $j \geq 1$, append ones until its running average is at least $u_j = \beta - \Delta/(j+2)$, then append zeros until that average is at most $\ell_j = \alpha + \Delta/(j+2)$. Since $0 < \ell_j < u_j < 1$, every stage terminates. Both runs are nonempty at every stage, so their endpoint indices tend to infinity. Each change of average has absolute value at most $1/N$ at index N, so the overshoots at these endpoints tend to zero. The averages within a run lie between its endpoint averages. Their lower and upper limits are therefore α and β, and every intermediate value is a subsequential limit. Let B consist of the indices at least three at which the sequence equals one. Removing its first two entries does not change these limits. Equation (7.3) proves (7.2).

For rational endpoints the construction decides membership in B using rational arithmetic. The computable assertion follows from Theorem A. Taking $\alpha = \beta = 1/2$ disproves the zero–one assertion, and taking $(\alpha, \beta) = (0, 1)$ disproves universal convergence. □

For $r \geq 1$, the degree-d Taylor polynomial of $f^{[r]}$ is $f_{r,r+d}$. Thus every positive shift has full symmetric groups in all degrees $d \geq 2$, order zero, and simple negative zeros.

Joint linear disjointness gives a uniform bound on how many segment groups can change after extending the ground field.

Corollary 7.5. *Fix a function from Theorem A. For every number field F, the root permutation group of $f_{r,s}$ over F equals its group over $\mathbb{Q}$ for all but at most*

$$\lfloor \log_2 [F : \mathbb{Q}] \rfloor$$

pairs (r, s) with $0 \leq r \leq s-2$. In particular, the same function gives the same limiting frequencies, or the same failure of convergence, over every number field.

Proof. Put $D_{r,s} = K_{r,s} \cap F$. Since $K_{r,s}/\mathbb{Q}$ is Galois, restriction identifies its group over F with $\mathrm{Gal}(K_{r,s}/D_{r,s})$. The group changes exactly when $D_{r,s}$ is larger than $\mathbb{Q}$. For any finite collection I of affected pairs, joint linear disjointness of the $K_{r,s}$ implies joint linear disjointness of their subfields $D_{r,s}$. All these subfields lie in F, and therefore

$$2^{|I|} \leq \prod_{(r,s)\in I} [D_{r,s} : \mathbb{Q}] = \left[\prod_{(r,s)\in I} D_{r,s} : \mathbb{Q} \right] \leq [F : \mathbb{Q}].$$

This proves the bound. Only finitely many Taylor-polynomial groups change, so all the frequency conclusions are preserved. □

7.3. **Preserving finite initial data.** The initial normalization $a_0 = a_1 = 1$ is convenient but is not needed for the Galois prescription. In particular, no finite initial list of positive rational coefficients forces limiting Galois frequencies in the unrestricted class.

Proposition 7.6. *Let $m \geq 1$, and fix $a_0, \ldots, a_m \in \mathbb{Q}_{>0}$. Let $B \subseteq \{m+2, m+3, \ldots\}$, and let $\varepsilon_n > 0$ for $n > m$. There is an entire extension*

$$f(z) = \sum_{j=0}^{m} a_j z^j + \sum_{n>m} a_n z^n, \qquad a_n \in \mathbb{Q}_{>0},$$

of order zero, with $0 < a_n < \min\{\varepsilon_n, 2^{-n^2}\}$ for $n > m$, such that (1.2) holds for every $n \geq m+2$. These Taylor polynomials are separable, and in the point-stabilizer case their unique rational root

is a negative integer. Moreover,

$$\mathrm{Gal}(K_{r,n}/\mathbb{Q}) = \mathfrak{S}_{n-r} \qquad (n \geq m+2,\ 1 \leq r \leq n-2).$$

The whole family $\{K_{r,n} : n \geq m+2,\ 0 \leq r \leq n-2\}$ *is jointly linearly disjoint and may be required to be jointly disjoint from any fixed finite extension of* $\mathbb{Q}$.

If the prefix satisfies $a_j^2 > 4a_{j-1}a_{j+1}$ *for* $1 \leq j < m$, *the extension can satisfy these inequalities for every* $j \geq 1$; *then all the zero assertions of Theorem A hold. For decidable* B *and computable positive bounds the extension can be chosen computably.*

Proof. For $0 \leq r \leq m$, form $g_{r,m+1}(X) = \sum_{j=r}^{m} a_j X^{m+1-j}$. Choose $a_{m+1} = t > 0$ rational, as small as required, such that

$$g_{r,m+2}(X) = Xg_{r,m+1}(X) + tX \qquad (0 \leq r \leq m)$$

are Morse and have pairwise disjoint critical-value sets. The polynomials $Xg_{r,m+1}$ have distinct degrees, so Lemma 2.2 excludes only finitely many values of t. We may also exclude the finitely many values for which $g_{0,m+1} + t$ has a repeated root. Starting at $n = m+2$, the construction in Subsection 2.3 now applies. Its normalization by the leading coefficient a_r in each factor accommodates the arbitrary initial coefficient a_0.

At every new degree, the product specialization gives the asserted groups for all proper segments. Include the fixed extension and all preceding segment splitting fields in E at each stage. This gives joint disjointness for the entire new family. The coefficient bound gives order zero, since a finite initial polynomial does not affect the estimate $\log M_f(R) = O((\log R)^2)$. If the prefix satisfies the strict coefficient inequalities, impose also $a_n < a_{n-1}^2/(4a_{n-2})$ at every new step, including the choice of a_{m+1}. Lemma 2.4 then applies. The first coefficient t can be found by an exact search using the resultant tests in Lemma 2.2; subsequent coefficients are computable by Proposition 2.5. □

The extra degree in Proposition 7.6 is sometimes necessary. For a composite integer $d \geq 4$, take the positive prefix for which

$$g_d(X) = (X+1)^d - 1.$$

For every parameter t giving a separable polynomial, $g_d(X) + t$ is, after translation, a binomial $Y^d - (1-t)$. If it is irreducible, the Galois action preserves the nontrivial partition of its roots into fibers of $Y \mapsto Y^a$, where $d = ab$ with $a, b > 1$; if it is reducible, the action is intransitive. In either case it cannot be the natural action of $\mathfrak{S}_d$. Thus an arbitrary positive prefix need not admit a full symmetric group at the very next degree.

Preserving a sufficiently long prefix also gives approximation on any fixed disk, with an arbitrary frequency cluster set of the form (7.2).

Corollary 7.7. *Let* $\Phi(z) = \sum_{j\geq 0} b_j z^j$ *be entire with* $b_j \in \mathbb{Q}_{>0}$. *Given* $R > 0$, $\epsilon > 0$, *and* $0 \leq \alpha \leq \beta \leq 1$, *there is an entire function* f *with positive rational coefficients and order zero such that*

$$\max_{|z|\leq R} |f(z) - \Phi(z)| < \epsilon$$

and the frequency-triple cluster set of f *is* (7.2). *Any prescribed finite number of the initial coefficients of* Φ *may be retained.*

Proof. Choose a sufficiently long Taylor polynomial of Φ so that its omitted tail on $|z| \leq R$ is smaller than $\epsilon/2$, and so that it contains all the coefficients to be retained. Apply Proposition 7.6 to this prefix, choosing the new bounds so that $\sum_{n>m} \varepsilon_n R^n < \epsilon/2$. Use a set B with lower and upper densities α and β as in the proof of Corollary 7.4. The finitely many initial degrees do not change the cluster set. □

7.4. **Uniform computability and decision problems.** We use the promise convention of Subsection 2.5. The inputs below are programs returning exact rational coefficients; the constructions always produce total programs satisfying the stated analytic and arithmetic promises. Uniformity in the prescribed set B gives the following undecidability statements.

Proposition 7.8. *There is no algorithm which, from a program computing the exact rational coefficients of a series, decides whether all three frequencies converge. This remains true under the promise of strictly positive coefficients and an entire function of order zero. Neither convergence nor nonconvergence is semidecidable under this promise.*

Even under the additional promise that all three frequencies exist, the property $O(f) \in \{0, 1\}$ is undecidable, and neither this property nor its complement is semidecidable. All these assertions remain valid within the functions supplied by Theorem A, retaining all its real-zero, proper-segment, and disjointness properties. They also hold over every fixed number field.

Proof. Use the uniform algorithm of Proposition 2.5 with fixed computable bounds. Put $M_j = 2^{2^j}$ and

$$B_0 = \bigcup_{j\geq 0} ([M_{2j}, M_{2j+1}) \cap \mathbb{Z}_{\geq 3}).$$

This set is computable. Since $M_{j+1}/M_j \to \infty$, its lower and upper densities are zero and one. Given a machine e, at input $n \geq 3$ run it for n steps. If it has not halted, use the label of B_0; if it has halted, include n. This defines a computable set B_e, uniformly in e. Its density exists exactly when e halts. Interchanging the two rules makes its density exist exactly when e never halts. Theorem A transfers both reductions to the three frequencies. The halting problem is undecidable and its complement is not semidecidable, proving all assertions in the first textbf.

For the second textbf, use all degrees until the machine halts and even degrees thereafter. The resulting triples are $(1, 0, 0)$ if it never halts and $(1/2, 0, 1/2)$ if it halts. Every constructed series has all three limits. Reversing the two rules reverses the endpoint property. The same two halting reductions prove the claims. Corollary 7.5 preserves the frequency conclusions over every fixed number field. □

A real number is *limit-computable*, or Δ^0_2, if it is a limit of a computable sequence of rational numbers. Those in $[0, 1]$ are exactly the densities of computable sets [24, Theorem 2.21]. The prescription theorem transfers this description to Galois frequencies, while retaining its analytic and field-theoretic conclusions. For completeness, we include the elementary density construction.

Proposition 7.9. *For $\delta \in [0, 1]$, the following are equivalent:*

(i) *δ is a limit of a computable sequence of rational numbers;*
(ii) *$\delta = S(f)$ for some series with computable rational coefficients for which this limit exists;*
(iii) *there is a function satisfying every conclusion of Theorem A, with computable coefficients, whose triple is $(\delta, 0, 1 - \delta)$.*

Proof. Condition (iii) implies (ii). For (ii) implies (i), the exact label procedure following Proposition 2.5 computes each rational average $s_f(N)$. For (i) implies (iii), choose computable $q_n \in [0, 1]$ tending to δ, put $K_0 = 0$, and set

$$b_n = \mathbf{1}_{\{K_{n-1} < nq_n\}}, \qquad K_n = K_{n-1} + b_n.$$

Then $K_n/n \to \delta$. Indeed, fix $\varepsilon > 0$, put $l = \max(0, \delta - \varepsilon)$ and $u = \min(1, \delta + \varepsilon)$, and take n_0 after which $l \leq q_n \leq u$. Choose $K \geq 1$ covering the initial discrepancy. Induction gives $ln - K \leq K_n \leq un + K$. If $b_n = 0$, the lower bound follows from $K_n \geq nq_n \geq ln$, and the upper bound follows by induction. If $b_n = 1$, the upper bound follows from $K_n < nq_n + 1 \leq un + 1$, and the lower bound follows by induction and $l \leq 1$. Divide by n and then let $\varepsilon \downarrow 0$. Apply Theorem A, with fixed computable bounds, to $B = \{n \geq 3 : b_n = 1\}$. □

This gives an exact description of attainable limits on the edge $A = 0$. Prescribing arbitrary ternary degree patterns, or arbitrary frequency triples, remains a separate problem.

7.5. **Automatic Galois labels.** Assume an automaton for the *Galois labels* $\lambda(n) \in \{S, A, O\}$. Automatic coefficients alone do not give this hypothesis. Density criteria for automatic sets are classical [35, 4]; the following matrix version is convenient here.

Extend the labels arbitrarily to $n = 0, 1, 2$; finite modifications preserve automaticity. Let $q \geq 2$, and let a finite deterministic automaton with output read base-q digits from most significant to least significant. We may adjoin a new initial state s_0 with a loop on digit zero and, on each nonzero digit, the same transition as the old initial state. Thus leading zeros do not change the output at positive integers; give s_0 the output assigned to zero. Delete unreachable states. These operations are effective and preserve all the chosen labels. If there are s states, let

$$P_{ij} = \frac{\#\{d \in \{0, \ldots, q-1\} : \delta(i, d) = j\}}{q},$$

and let V be the s by 3 output-indicator matrix, with columns S, A, O. Write $\mathbf{e}$ for the all-ones column vector of length s. Put $d = \operatorname{lcm}(1, \ldots, s)$ and $L = \lim_{k\to\infty} P^{dk}$. Each recurrent class of P has period dividing d, so the recurrent classes of P^d are aperiodic and the limit exists. Its entries are computable rational numbers: solve the rational linear systems for the stationary distribution in each recurrent class of P^d and for the probabilities of reaching those classes from transient states. These matrices give a finite, exact test for convergence.

Proposition 7.10. *All three natural label frequencies exist if and only if every row of LV is the same vector v. That vector is their triple. The other frequency exists and is zero or one if and only if its column in LV is constantly zero or constantly one.*

Proof. A prefix reaching state i represents an integer a. Appending all q^k suffixes gives the interval $[aq^k, (a+1)q^k)$, whose average is $(P^kV)_i$. Global prefix counts $Nv + o(N)$ imply, by subtraction at the two endpoints, convergence of this average to v. The initial state uses $[0, q^k)$. Necessity follows.

If $LV = \mathbf{e}v$, then $P^{dk+t}V \to P^t\mathbf{e}v = \mathbf{e}v$ for each $0 \leq t < d$. Thus every row of P^kV tends to v. Decompose $[0, N)$ into base-q prefix intervals, at most $q-1$ per scale. For fixed K, intervals shorter than q^K have total length at most q^K; larger intervals have averages uniformly close to v once K is large. Divide by N. The single-column argument proves the endpoint statement. □

The endpoint condition says, respectively, that no reachable recurrent state has output O, or every reachable recurrent state does. When $O = 0$, the first two columns still need their convergence test. Periodic labels give the proportions of residue classes. Automatic labels need not converge: positive integers of even binary length have lower density $1/3$ and upper density $2/3$ [4]. The prescribed-pattern theorem realizes this as the symmetric-degree set of an order-zero entire function.

7.6. **Further questions.** The prescription theorem and bounded-coefficient construction settle the universal convergence and zero–one assertions in the Katz–Rivin questions. A structural description of the series with convergent frequencies remains open. Section 7 reduces the problem to two arithmetic means, while the undecidability results rule out a uniform algorithm on programs for arbitrary nonzero rational coefficients, and even for the existence of the other frequency over a fixed finite alphabet. Specific coefficient families can nevertheless admit precise answers, as Theorems B–E show.

Classical sections and smaller thresholds. Theorems D and E determine the central-binomial and Catalan groups in every degree. Sun's additional bound n^2+n+5 for the least prime at which the monic reciprocal $x^nP_n(1/x)$ has irreducible reduction remains open [45, part (i)]. For

general nonintegral binomial exponents, the degrees below the threshold remain to be classified uniformly in the parameter. It would also be useful to sharpen the bounds (4.2) and (A.5) and to obtain a two-cycle criterion adapted to these inertia elements without using the classification of finite simple groups. Another quantitative question is to make the implied constant in (1.6) numerical. An explicit containment threshold alone does not supply a numerical constant in the quadratic-large-sieve estimate.

The logarithmic discriminant. Yamamura's conjecture asks for symmetry in every degree for $1+x+x^2/2+\cdots+x^n/n$. Since alternating containment is known, proving that square discriminants occur in density zero would already determine the frequency triple as $(1,0,0)$. The results of [13] for degrees $n = mq$ with fixed m and q prime do not by themselves give density one among all degrees. Theorem B uses a nonintegral parameter to obtain a unique denominator divisible by a prime $p > n$; this argument does not apply to the logarithm. Square-discriminant densities also remain to be determined in general for the factorial-denominator families of Proposition 6.5.

Rational functions. Do all three frequencies converge for every rational function with nonzero Taylor coefficients? The examples in Section 6 show that the other frequency need not be an endpoint. Even the class $f(x) = P(x)/(1-x)$ is a natural general problem: if $n \geq \deg P$ and $P(1) \neq 0$, then

$$(1-x)f_n(x) = P(x) - P(1)x^{n+1}.$$

This connects the question to sparse polynomials with a growing exponent. The finite-alphabet construction varies the coefficients in long blocks and does not decide convergence for a fixed rational generating function.

Irreducible nonconvergence and alternating prescriptions. Can the frequencies fail to converge when every sufficiently large section is irreducible? Our nonconvergent examples obtain other degrees through rational or cyclotomic factors. An irreducible example would require compatible alternating groups or other proper transitive groups in a suitable collection of degrees; oscillation between symmetric and alternating groups would already suffice. More generally, can one prescribe alternating groups as well as symmetric and other groups in one Taylor sequence?

There is a concrete limitation to the one-parameter method in Section 2. If $g \in \mathbb{Q}[X]$ is Morse of degree n, then $D(T) = \mathrm{Disc}_X(g(X)+T)$ is squarefree of degree $n-1$: its simple zeros are the negatives of the distinct critical values. The smooth projective model of $Y^2 = D(T)$ has genus $\lfloor (n-2)/2 \rfloor$. For $n \geq 6$, Faltings's theorem [17] therefore leaves only finitely many rational parameters with square discriminant. Thus, for a fixed Morse prefix, the argument cannot supply alternating specializations at arbitrarily small nonzero parameters. An alternating prescription may require additional parameters or a different generic group.

Appendix A. Explicit prime estimates

We give the explicit estimates used in Lemma 4.1 and then prove the smaller threshold for half-integral parameters. The argument first counts primes in one progression and then subtracts the primes for which a prescribed divisor divides the special index. We use φ for Euler's totient function and

$$\theta(x;q,a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \log p.$$

The inputs are an explicit prime estimate in a fixed progression and the interval Brun–Titchmarsh inequality.

A.1. **The general bound.**

Proof of Lemma 4.1. We have

$$L \geq \max\{60, Q\}, \qquad \frac{3}{16} \leq \kappa \leq \frac{Q}{8}.$$

The explicit prime estimate of Bennett, Martin, O'Bryant, and Rechnitzer [5, Theorem 1.2 and equations (1.10)–(1.11)] gives, in a weakened form valid for every $Q \geq 3$,

$$\left|\theta(x; Q, \rho) - \frac{x}{\varphi(Q)}\right| < \frac{x}{160 \log x} \tag{A.1}$$

for $x \geq x_0(Q)$, where

$$x_0(Q) = \begin{cases} 8 \cdot 10^9, & Q \leq 10^5, \\ \exp(0.03\sqrt{Q}\,\log^3 Q), & Q > 10^5. \end{cases}$$

Our lower bound on n ensures $U > x_0(Q)$. For $Q \leq 10^5$, use $U > n \geq e^{60}$. For $Q > 10^5$, the function $(\log Q)^3/\sqrt{Q}$ decreases, and

$$\frac{0.03 \log^3(10^5)}{\sqrt{10^5}} < \frac{0.03 \cdot 12^3}{300} < 1,$$

so $0.03\sqrt{Q}\log^3 Q < Q \leq L$.

For $L \geq 60$ and $Q \leq L$, elementary monotonicity gives

$$\log Q \leq L/10, \qquad \log(600Q) \leq L/4, \qquad \log(6Q) \leq L/8. \tag{A.2}$$

Each follows by replacing Q with L and checking the endpoint $L = 60$; the corresponding linear function minus the logarithm increases thereafter. Since $\log U > L$, $\log V \leq L + \log Q \leq 11L/10$, and $U + V = 13W$, we obtain

$$\begin{aligned} |\mathcal{P}| &\geq \frac{\theta(V; Q, \rho) - \theta(U; Q, \rho)}{\log V} \\ &> \frac{W}{\varphi(Q)\log V}\left(1 - \frac{13\varphi(Q)}{160 \log U}\right) \\ &> \frac{147}{176}\frac{W}{\varphi(Q)L} > \frac{4}{5}\frac{W}{\varphi(Q)L}. \end{aligned}$$

Here we used $\varphi(Q) \leq Q \leq L$.

Put $T = W/(\varphi(Q)L)$. If a divisor d of n has a prime factor in common with aQ, no prime in $\mathcal{P}$ has $d \mid j$. For primes dividing Q this follows from the congruences preceding the lemma. If a prime $q \mid a$ also divided j, it would divide cp; this is impossible because $(c, a) = 1$ and $p > |a|$. If $(d, aQ) = 1$, the condition $d \mid j$ imposes one reduced residue class modulo Qd, since then $p \equiv ac^{-1} \pmod{d}$ and $(Q, d) = 1$.

For $d = m \leq \sqrt{n}$ with $(m, aQ) = 1$, the interval Brun–Titchmarsh inequality [31, Theorem 2, equation (1.10)] therefore gives

$$\#\{p \in \mathcal{P} : m \mid j\} \leq \frac{2W}{\varphi(Q)\varphi(m)\log(W/(Qm))}. \tag{A.3}$$

Here $(m, 6) = 1$, so $m \geq 5$. If $m \leq 100$, then $\varphi(m) \geq 4$, and

$$\log\frac{W}{Qm} \geq L - \log\frac{100Q}{\kappa} > L - \log(600Q) \geq \frac{3L}{4}.$$

Thus (A.3) is at most $2T/3$. If $m > 100$, then m is odd and $\varphi(m) \geq \sqrt{m} > 10$. The last elementary inequality follows by multiplying $p^{e-1}(p-1) \geq p^{e/2}$ over odd prime powers dividing

m. Since $\varphi(m)$ is even, it is at least 12. Also

$$\log \frac{W}{Qm} \geq \frac{L}{2} - \log \frac{Q}{\kappa} > \frac{L}{2} - \log(6Q) \geq \frac{3L}{8}.$$

Hence (A.3) is at most $4T/9$. These positive lower bounds for the logarithm also verify the hypothesis $W > Qm$ of Brun–Titchmarsh.

For $d = r \geq \sqrt{n}$, a direct count in its residue class gives

$$\#\{p \in \mathcal{P} : r \mid j\} \leq \frac{W}{Qr} + 1.$$

Dividing by T and using $Q/\kappa < 6Q \leq 6L$ bounds this by

$$Le^{-L/2} + 6L^2 e^{-L} < \frac{1}{100} \qquad (L \geq 60).$$

Both terms decrease, and their values at 60 prove the inequality. Subtracting the two forbidden sets from (4.4) leaves more than

$$\left(\frac{4}{5} - \frac{2}{3} - \frac{1}{100}\right) T = \frac{37}{300} T > \frac{T}{10}$$

primes. Finally,

$$\frac{T}{10\sqrt{n}} = \frac{\kappa\sqrt{n}}{10\varphi(Q)L} \geq \frac{3e^{L/2}}{160L^2} > 1.$$

The last expression increases for $L \geq 60$, and the inequality at 60 follows already from $e^{30} > 2^{30}$.

Since $b/c \geq 3/2$, we have $p > U \geq 9n/8 > n + C$. Also $p > R_F$ and $p > |a|, b$. The bound $n \geq 100|a|$ gives $|a|/b \leq n/200$, whence

$$\frac{3n}{4} - \frac{n}{200} < j \leq \frac{7n}{8} + \frac{n}{200}.$$

These inequalities imply all the asserted bounds on j. □

A.2. **The half-integral case.** For an odd integer a, choose the reduced residue class $\rho = \rho(a) \pmod{12}$ by

$$\rho \equiv a + 2 \pmod 4, \qquad \rho \equiv \begin{cases} -a \pmod 3, & 3 \nmid a, \\ 1 \pmod 3, & 3 \mid a. \end{cases}$$

Then $(p-a)/2$ is coprime to 6 whenever $p \equiv \rho \pmod{12}$. For $a = 1$, this is the class $11 \pmod{12}$. The small modulus permits a much sharper numerical bound than (4.2).

Lemma A.1. *Let $n \geq 10^6$ and let a be an odd integer with $|a| \leq n/100$. Put*

$$\mathcal{P} = \{p \text{ prime} : 3n/2 < p \leq 7n/4,\ p \equiv \rho(a) \pmod{12}\}.$$

Then

$$|\mathcal{P}| > \frac{547n}{10000 \log n} > 2.$$

For every factorization $n = mr$ with $2 \leq m \leq r$, there is a prime $p \in \mathcal{P}$ for which

$$m \nmid (p-a)/2 \quad \text{and} \quad r \nmid (p-a)/2.$$

Proof. Write $L = \log n > 13.8$, $U = 3n/2$, and $V = 7n/4$. Ramaré–Rumely [37, Theorems 1 and 2, p. 398] give

$$\max_{1 \leq y \leq x} \left| \theta(y; 12, \rho) - \frac{y}{4} \right| \leq \begin{cases} 2.072\sqrt{x}, & x \leq 10^{10}, \\ 0.004560x/4, & x \geq 10^{10}. \end{cases}$$

Apply this maximum bound with the common endpoint V, which also handles the transition at 10^{10}. Since $4.144\sqrt{7/4} < 5.5$, we obtain

$$\frac{\theta(V;12,\rho)-\theta(U;12,\rho)}{n} \geq \begin{cases} 1/16 - 5.5/\sqrt{n}, & V \leq 10^{10}, \\ 1/16 - 0.003990, & V \geq 10^{10}. \end{cases}$$

Both lower bounds are at least 0.057 for $n \geq 10^6$. As $\log(7/4) < 0.56$, it follows that

$$|\mathcal{P}| \geq \frac{0.057n}{\log V} > \frac{n}{L}\,0.057\frac{13.8}{13.8+0.56} = \frac{n}{L}\,\frac{57}{1000}\frac{345}{359} > \frac{547n}{10000L}.$$

Put $j = (p-a)/2$. If a positive integer d has a prime factor in common with $6a$, then no $p \in \mathcal{P}$ has $d \mid j$. For factors $2, 3$ this follows from $(j, 6) = 1$; if an odd prime $q \mid a, d$, then $d \mid j$ would imply $q \mid p$, whereas $q \leq |a| < p$. For $(d, 6a) = 1$, the condition $d \mid j$ imposes one reduced class modulo $12d$ on p.

It remains to consider $(d, 6a) = 1$. First suppose $d = m \leq \sqrt{n}$. The interval Brun–Titchmarsh inequality [31, Theorem 2, equation (1.10)] gives

$$\#\{p \in \mathcal{P} : m \mid j\} \leq \frac{n}{8\varphi(m)\log(n/(48m))}. \tag{A.4}$$

Its hypothesis $12m < n/4$ holds because $\sqrt{n} > 48$. Since $(m, 6) = 1$, either $m = 5$ or $m \geq 7$. If $m = 5$, the right side is

$$\frac{n}{32\log(n/240)} < \frac{0.052n}{L},$$

because $\log 240 < 5.49$ and $13.8/[32(13.8-5.49)] < 0.052$. If $7 \leq m \leq 100$, then $\varphi(m) \geq 6$, so the bound is at most

$$\frac{n}{48\log(n/4800)} < \frac{0.0541n}{L},$$

using $\log 4800 < 8.48$ and $13.8/[48(13.8-8.48)] < 0.0541$. If $m > 100$, then m is odd and $\varphi(m) \geq \sqrt{m} > 10$, as in the general bound. Since $\varphi(m)$ is even, it is at least 12. Thus (A.4) is at most

$$\frac{n}{96(\frac{1}{2}L - \log 48)} < \frac{0.048n}{L},$$

using $\log 48 < 3.88$ and $13.8/[96(6.9-3.88)] < 0.048$.

For $d = r \geq \sqrt{n}$, the direct count in a residue class gives

$$\#\{p \in \mathcal{P} : r \mid j\} \leq \frac{n}{48r} + 1 \leq \frac{\sqrt{n}}{48} + 1 < \frac{0.00031n}{L}.$$

The last inequality holds at $n = 10^6$ because

$$\frac{L}{48\sqrt{n}} + \frac{L}{n} < \frac{14}{48\cdot 1000} + \frac{14}{10^6} < 0.00031,$$

and the left side decreases thereafter. The union of the two excluded sets therefore has fewer than $(0.0541 + 0.00031)n/L < 0.0547n/L$ primes. This is smaller than $|\mathcal{P}|$, and proves the lemma. □

The preceding estimate gives the following smaller threshold when $b = 2$:

$$N_2(a, C, F) = \left\lceil \max\{10^6, 100|a|, 2C, R_F\} \right\rceil, \tag{A.5}$$

where a is odd and R_F is the largest rational prime ramified in F, with $R_F = 1$ when none is ramified. Indeed, every prime in $\mathcal{P}$ exceeds $n + C$ and R_F, and its special index $j = (p-a)/2$ satisfies

$$7n/10 < j < 9n/10, \qquad \sqrt{n} < n - j < n/2.$$

The local factors are tame and have degrees $j, n-j$. Two distinct primes prove irreducibility. For every factorization $n = mr$, the lemma supplies a prime for which neither factor divides j; Lemma 3.2 therefore gives alternating containment. Odd degrees have an odd inertia permutation. The same threshold with $C = 0$ applies to the exact binomial classification for $s = a/2$.

A.3. **Polynomial weights.** For Corollary 4.3, suppose the nonzero coefficients agree for all $i \geq J$ with

$$a_i = \frac{P(i)}{(s+i)(i!)^r}, \qquad s = a/b, \quad r \in \mathbb{Z}_{\geq 0}, \quad P(-s) \neq 0.$$

Write $P = A/D$, where $A \in \mathbb{Z}[T]$ and D is a positive integer. Put

$$d = \deg A, \qquad h = \max_i |[T^i]A|, \qquad K = b^d A(-a/b) \in \mathbb{Z} \setminus \{0\}.$$

Write each modified coefficient $a_i = m_i/\ell_i$, $0 \leq i < J$, in lowest terms, with $\ell_i > 0$. In (4.2), take $C = 0$ and enlarge H to include

$$J,\ D,\ |K|,\ (d+2)^2,\ (d+1)h, \quad \max_{0 \leq i < J} \{|m_i|, \ell_i\},$$

where the last maximum is omitted if $J = 0$. Then the same threshold gives irreducibility and alternating containment over F, and full symmetry for odd n.

Indeed the special index j lies beyond the modified prefix. Every coefficient away from j is integral at p. The choice of H also makes the constant coefficient a unit, whether it lies in the modified prefix or comes from $A(0)$. At j, we have $A(j) \equiv A(-a/b) \not\equiv 0 \pmod{p}$ because $p > |K|$, so its coefficient has valuation -1. Only primes dividing $A(n)$ can prevent the leading coefficient from being a unit. Since

$$0 < |A(n)| \leq (d+1)hn^d \leq n^{d+1},$$

at most d distinct primes above n divide $A(n)$. Discard them. More than $\sqrt{n} \geq 10(d+2)$ primes were available both in total and for each divisor-pair condition in Lemma 4.1. Thus at least two primes remain for irreducibility, and at least one remains for every factor pair, including the square-degree pair used in Müller's theorem. The same group proof applies. No extra dependence on r is needed, since $p > n$ makes every $i!$ a unit at p.

References

[1] M. Allen and M. Filaseta, *A generalization of a second irreducibility theorem of I. Schur*, Acta Arith. **109** (2003), 65–79. doi:10.4064/aa109-1-3.

[2] L. Bary-Soroker and O. Ben-Porath, *On the Galois theory of generalized Laguerre polynomials and trimmed exponential*, Acta Arith. **200** (2021), no. 2, 183–196. doi:10.4064/aa200825-7-3. arXiv:2008.05165.

[3] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), 1041–1120. doi:10.1007/s00222-023-01193-6.

[4] J. P. Bell, *The upper density of an automatic set is rational*, J. Théor. Nombres Bordeaux **32** (2020), 585–604. doi:10.5802/jtnb.1135.

[5] M. A. Bennett, G. Martin, K. O'Bryant, and A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois J. Math. **62** (2018), 427–532. doi:10.1215/ijm/1552442669.

[6] G. Blachar, E. Breuillard, and G. Kozma, *Galois groups of random polynomials of large degree*, preprint (2026), arXiv:2609.40123v1.

[7] A. Borisov, M. Filaseta, T. Y. Lam, and O. Trifonov, *Classes of polynomials having only one non-cyclotomic irreducible factor*, Acta Arith. **90** (1999), 121–153. doi:10.4064/aa-90-2-121-153.

[8] D. Brink, *On alternating and symmetric groups as Galois groups*, Israel J. Math. **142** (2004), 47–60. doi:10.1007/BF02771527.

[9] A. Chambert-Loir, *The theorem of Jentzsch–Szegő on an analytic curve: application to the irreducibility of truncations of power series*, Int. J. Number Theory **7** (2011), no. 7, 1807–1823. doi:10.1142/S1793042111004691. arXiv:1004.3813.

[10] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. doi:10.1007/978-3-662-02945-9.

[11] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, Enseign. Math. (2) **33** (1987), 183–189. doi:10.5169/seals-87891.

[12] B. Conrad, *Math 248A: Tame ramification and composite fields*, course handout, Stanford University, Theorem 2.1. https://virtualmath1.stanford.edu/~conrad/248APage/handouts/tamecomp.pdf.

[13] J. Cullinan and R. Gajek-Leonard, *On the discriminants of truncated logarithmic polynomials*, Integers **25** (2025), Paper A39. doi:10.5281/zenodo.15283716.

[14] *NIST Digital Library of Mathematical Functions*, Chapters 7, 13, 16, and 18, accessed 23 October 2026. https://dlmf.nist.gov/.

[15] P. Dusart, *Explicit estimates of some functions over primes*, Ramanujan J. **45** (2018), 227–251. doi:10.1007/s11139-016-9839-4.

[16] P. Erdős, F. Luca, and C. Pomerance, *On the proportion of numbers coprime to a given integer*, in *Anatomy of Integers*, CRM Proceedings & Lecture Notes, vol. 46, American Mathematical Society, 2008, 47–64.

[17] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. doi:10.1007/BF01388432; erratum, **75** (1984), 381. doi:10.1007/BF01388572.

[18] M. Filaseta and R. Moy, *On the Galois group over $\mathbb{Q}$ of a truncated binomial expansion*, Colloq. Math. **154** (2018), 295–308. doi:10.4064/cm7474-3-2018.

[19] M. Filaseta and I. Solan, *An extension of a theorem of Ljunggren*, Math. Scand. **84** (1999), 5–10. doi:10.7146/math.scand.a-13928.

[20] H. Garmi, *Galois Groups of Trinomials with Small Coefficients*, preprint (2026), arXiv:2610.22764v2.

[21] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 517–525. doi:10.5802/jtnb.505.

[22] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275. doi:10.4064/aa-72-3-235-275.

[23] J. I. Hutchinson, *On a remarkable class of entire functions*, Trans. Amer. Math. Soc. **25** (1923), no. 3, 325–332. doi:10.1090/S0002-9947-1923-1501248-1.

[24] C. G. Jockusch, Jr., and P. E. Schupp, *Generic computability, Turing degrees, and asymptotic density*, J. London Math. Soc. (2) **85** (2012), 472–490. doi:10.1112/jlms/jdr051.

[25] G. A. Jones, *Primitive permutation groups containing a cycle*, Bull. Aust. Math. Soc. **89** (2014), 159–165. doi:10.1017/S000497271300049X.

[26] N. M. Katz and I. Rivin, *Speculations in Galois theory*, to appear in *Algebraic Geometry and the Langlands Program: A Volume in Honour of Gérard Laumon*, Simons Symposia, Springer, Cham. Author manuscript, version kGalois_11bis, https://web.math.princeton.edu/~nmk/kGalois_11bis.pdf (consulted 24 October 2026).

[27] V. P. Kostov and B. Shapiro, *Hardy–Petrovitch–Hutchinson's problem and partial theta function*, Duke Math. J. **162** (2013), no. 5, 825–861. doi:10.1215/00127094-2087264. arXiv:1106.6262.

[28] D. Koukoulopoulos, *The Distribution of Prime Numbers*, Graduate Studies in Mathematics, vol. 203, American Mathematical Society, Providence, RI, 2019. doi:10.1090/gsm/203.

[29] R. Levingston and D. E. Taylor, *The theorem of Marggraff on primitive permutation groups which contain a cycle*, Bull. Austral. Math. Soc. **15** (1976), 125–128. doi:10.1017/S0004972700036832.

[30] J. S. Milne, *Algebraic Number Theory*, version 3.08, 19 July 2020. https://www.jmilne.org/math/CourseNotes/ANT.pdf.

[31] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134. doi:10.1112/S0025579300004708.

[32] P. Müller, *Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), 369–438. doi:10.2422/2036-2145.201012_002.

[33] J. Nagura, *On the interval containing at least one prime number*, Proc. Japan Acad. **28** (1952), 177–181. doi:10.3792/pja/1195570997.

[34] K.-H. Nguyen-Dang, *Arithmetic of Jacobi polynomials*, preprint, 22 October 2026, hexagon:2610.00468v1.

[35] M. Peter, *The asymptotic distribution of elements in automatic sequences*, Theoret. Comput. Sci. **301** (2003), 285–312. doi:10.1016/S0304-3975(02)00587-X.

[36] P. Rabarison, F. Pazuki, and P. Molin, *Exponentielle tronquée et autres contes galoisiens*, Publ. Math. Besançon Algèbre Théorie Nombres (2024), 105–117. doi:10.5802/pmb.57.

[37] O. Ramaré and R. Rumely, *Primes in arithmetic progressions*, Math. Comp. **65** (1996), no. 213, 397–425. doi:10.1090/S0025-5718-96-00669-2.

[38] S. Ramanujan, *A proof of Bertrand's postulate*, J. Indian Math. Soc. **11** (1919), 181–182. https://ramanujan.sirinudi.org/Volumes/published/ram24.html.

[39] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*, Colloq. Math. **9** (1962), no. 2, 291–296. doi:10.4064/cm-9-2-291-296; correction, **12** (1964), 289. doi:10.4064/cm-12-2-289.

[40] I. Schur, *Gleichungen ohne Affekt*, Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl. (1930), 443–449; reprinted in *Gesammelte Abhandlungen*, vol. III, Springer-Verlag, Berlin, 1973, 191–197.

[41] S. Seki, *Irreducibility of truncations of the Catalan generating function*, preprint (2026), arXiv:2609.10526v1.

[42] J.-P. Serre, *Topics in Galois Theory*, second ed., notes written by H. Darmon, Research Notes in Mathematics, vol. 1, A K Peters, Wellesley, MA, 2008. doi:10.1201/b10588.

[43] K. M. Shokri, J. Shaffaf, and R. Taleb, *Galois groups of Taylor polynomials of some elementary functions*, Int. J. Number Theory **15** (2019), 1127–1141. doi:10.1142/S1793042119500623.

[44] P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37. doi:10.1007/BF03027290.

[45] Z.-W. Sun, entry A224416, *The On-Line Encyclopedia of Integer Sequences*, created 6 April 2013, consulted 24 October 2026. https://oeis.org/A224416.

[46] Z.-W. Sun, comment dated 23 March 2013 on entry A000984, *The On-Line Encyclopedia of Integer Sequences*, accessed 24 October 2026. https://oeis.org/A000984.

[47] S. Weinbaum, *Galois groups of shifted exponential polynomials*, preprint, 2026, arXiv:2610.26873v2.

Morningside Center of Mathematics, Chinese Academy of Sciences, Beijing, China