IRREDUCIBILITY AND GALOIS GROUPS OF RANDOM RECIPROCAL POLYNOMIALS OF LARGE DEGREE

DAVID HOKKEN AND DIMITRIS KOUKOULOPOULOS

ABSTRACT. Let $A = a_0T^m + \sum_{j=1}^{m-1} a_j(T^{m-j} + T^{m+j}) + T^{2m} + 1 \in \mathbf{Z}[T]$ be a monic reciprocal polynomial of degree $2m$ sampled randomly by selecting its coefficients $a_0, a_1, \dots, a_{m-1}$ independently according to a given probability measure μ on $\mathbf{Z}$. For a wide range of measures μ, we prove that A is irreducible with probability $\geqslant 1 - Cm^{-c}$ for some absolute constants $c, C > 0$. In addition, we prove that with the same probability the Galois group of A is either the full hyperoctahedral group $C_2 \wr \mathcal{S}_m$ or one of two of its index-2 subgroups. The main condition that μ must satisfy is of Fourier-theoretic nature, and holds for example when μ is the uniform measure on a set of at least 35 consecutive integers, or on an arbitrary, sufficiently large subset of an interval $[-H, H]$, with H larger than some absolute constant. Our most general result allows for each a_j to be sampled by its own probability measure μ_j.

Our approach builds on earlier work of Bary-Soroker, Kozma and the second author, who proved for essentially the same μ_j that the 'standard' monic polynomial $a_0 + \cdots + a_{m-1}T^{m-1} + T^m$ is irreducible and has as Galois group either the symmetric group $\mathcal{S}_m$ or the alternating group $\mathcal{A}_m$ with high probability, conditioning on $a_0 \neq 0$. In our setting of reciprocal polynomials, we can rule out (all subgroups of) the maximal alternating subgroup $(C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}$ of the hyperoctahedral group as likely Galois group of A by analyzing its discriminant.

CONTENTS

Date: October 21, 2025.
2020 *Mathematics Subject Classification.* Primary: 11R09, 11R32, 11T55, 12F10. Secondary: 60G50, 20B30.
Key words and phrases. Random polynomial, reciprocal polynomial, irreducibility, Galois theory, discriminant.

1. Introduction

Factoring polynomials as well as understanding symmetries between their zeros is a classical subject in number theory. Both of these aspects are captured by the Galois group of the polynomial. Here, we focus on polynomials with integer coefficients, say $A(T) \in \mathbf{Z}[T]$, and we will denote by $\mathcal{G}_A$ the Galois group of (the splitting field of) A over $\mathbf{Q}$. If A is of degree n, we may view $\mathcal{G}_A$ as a subgroup of $\mathcal{S}_n$, the symmetric group on n letters. Regarding the size of the Galois group, the general philosophy is that $\mathcal{G}_A$ is "almost always as large as it can be for a typical choice of A". In other words, if we select A randomly among all polynomials of degree n, then we expect that $\mathcal{G}_A = \mathcal{S}_n$ almost surely. Of course, we must specify what *random* means. A classical case is the following: we fix a finite set $\mathcal{N}$ of integers and we select all coefficients of A independently and uniformly at random from $\mathcal{N}$. Following Van der Waerden's pioneering work [34, 35], a lot of literature (see, e.g., [1, 4, 10, 14, 15, 21]) focuses on the *large box model*, where the degree n is fixed and we take a growing set of coefficients, usually $\mathcal{N} = [-H, H] \cap \mathbf{Z}$ with $H \to \infty$. The state-of-the-art in this direction is Bhargava's result [10] that $\mathbb{P}(\mathcal{G}_A \neq \mathcal{S}_n) = \mathbb{P}(A \text{ is reducible}) + \mathbb{P}(\mathcal{G}_A = \mathcal{A}_n) + O(H^{-2})$ and that $\mathbb{P}(\mathcal{G}_A = \mathcal{A}_n) = O(H^{-1})$, where $\mathcal{A}_n$ is the alternating group on n letters.

Instead, here we will focus on the *restricted coefficient model* where $\mathcal{N}$ is fixed and the degree n tends to infinity. This was first considered by Odlyzko and Poonen [27]. Taking $\mathcal{N} = \{0, 1\}$ in the uniform measure, they stated as a folklore conjecture that the probability that A is irreducible tends to 1 as $n \to \infty$, conditioning on $A(0) = 1$. Konyagin [25] showed that the probability is $\gg 1/\log n$. Breuillard and Varjú [11] proved the folklore conjecture under the Riemann hypothesis for Dedekind zeta functions. In 2020, Bary-Soroker, Kozma and the second author [7] improved Konyagin's unconditional lower bound to $\gg 1$, a result that continues to hold when we instead sample the coefficients of A independently according to *any* fixed probability measure μ on $\mathbf{Z}$ with finite support that is not a Dirac mass, conditioning on $A(0) \neq 0$. Furthermore, again under a wide range of choices of μ, they proved that $\mathcal{G}_A$ contains $\mathcal{A}_n$ with high probability. When μ is the uniform measure on $\{\pm 1\}$, Bary-Soroker, Kozma, Poonen and the first author [6] showed that $\limsup_{n\to\infty} \mathbb{P}(A \text{ is irreducible}) = 1$.

In the present paper, we study the irreducibility and Galois group of polynomials A in the restricted coefficient model with an additional constraint: we shall assume that A is *reciprocal*.

Definition 1.1 (Reciprocal polynomial)**.** Let A be a polynomial over a field K. We say that A is *reciprocal* if either $A = 0$ or if A has even degree and satisfies the relation

$$A(T) = T^{\deg A} A(1/T). \tag{1.1}$$

Equivalently, A is reciprocal if there are $m \in \mathbf{Z}_{\geqslant 0}$ and $a_0, a_1, \dots, a_m \in K$ such that

$$A(T) = a_m + a_{m-1}T + \cdots + a_1 T^{m-1} + a_0 T^m + a_1 T^{m+1} + \cdots + a_{m-1}T^{2m-1} + a_m T^{2m}. \tag{1.2}$$

Remark 1.2. If A has odd degree and satisfies (1.1), then we may write $A(T) = (T + 1)B(T)$ with B a reciprocal polynomial.

The Galois group of A as in (1.2) is always smaller than $\mathcal{S}_{2m}$, because of the relations between the zeros of A implied by (1.1). In fact, $\mathcal{G}_A$ is contained in the *hyperoctahedral group* $C_2 \wr \mathcal{S}_m$, whose construction we recall in §14. The following is one of our results about random reciprocal polynomials.

Theorem A. *Let $\mathcal{N}$ be a set of at least 35 consecutive integers and let m be a positive integer. Let $a_m = 1$ and sample integers $a_0, a_1, \dots, a_{m-1}$ independently and uniformly at random from $\mathcal{N}$ and let these be the coefficients of the monic reciprocal polynomial A as in (1.2). Then*

$$\lim_{m\to\infty} \mathbb{P}\big(A \text{ is irreducible in } \mathbf{Z}[T]\big) = 1.$$

Moreover, if $\mathcal{G}_A$ denotes the Galois group of A over $\mathbf{Q}$, then

$$\lim_{m\to\infty} \mathbb{P}\Big(\mathcal{G}_A \in \big\{C_2 \wr \mathcal{S}_m, C_2 \wr \mathcal{A}_m, G_2\big\}\Big) = 1,$$

where G_2 denotes the group defined in (14.3).

This introductory section is dedicated to presenting our main results (see Theorem B and the general Theorem C below) and comparing our study to the literature. A detailed discussion of our proof strategy and of the structure of the paper are given in §2. The proofs of the main theorems can be found in §3; they are based on a set of propositions that are stated in §2 and proved in §§4–16.

Reciprocal polynomials are ubiquitous in number theory and related areas: for example, they are the 'optimisers' for Lehmer's longstanding conjecture regarding the minimal Mahler measure of a polynomial, and they appear as the characteristic polynomials of symplectic matrices. In the large box model, Bhargava's theorem [10] mentioned in the first paragraph has already been adapted to the reciprocal setting by Anderson, Bertelli and O'Dorney [1] (see also the earlier paper [15] in this direction). They obtained the following: if $m \geqslant 2$ is fixed and A is sampled uniformly at random from the set of monic reciprocal polynomials in $\mathbf{Z}[T]$ all of whose coefficients are at most H in absolute value, then

$$\mathbb{P}\Big(\mathcal{G}_A \neq C_2 \wr \mathcal{S}_m\Big) = \mathbb{P}\Big(\mathcal{G}_A = (C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}\Big) + O\big(H^{-1}\big) \asymp_m \frac{\log H}{H}, \qquad H \to \infty.$$

Here, the implicit constants depend on m. Notably, the leading term of the asymptotic for $\mathbb{P}(\mathcal{G}_A \neq C_2 \wr \mathcal{S}_m)$ comes from the maximal alternating subgroup $(C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}$ and contains no contribution of reducible polynomials. In contrast, it is originally a conjecture by Van der Waerden [35] that in Bhargava's result about 'standard' polynomials (where there are no further relations between the coefficients), the alternating group should not appear and instead $\mathbb{P}(\mathcal{G}_A \neq \mathcal{S}_n) = \mathbb{P}(A \text{ is reducible}) + o(H^{-1})$ as H goes to infinity. From the examples mentioned so far, one already observes that the alternating group plays a special role in probabilistic Galois theory. In the large box model, this is discussed in more detail in work by Bary-Soroker, Ben-Porath and Matei [4]. Bary-Soroker and Goldgraber [5] proved that the alternating group can be ruled out in a hybrid model where both the degree and the coefficient box grows; in the setting of polynomials over $\mathbf{F}_q[t]$, Entin [19] similarly showed that the Galois group over $\mathbf{F}_q(t)$ is the alternating group with low probability only.

Other than reciprocal polynomials discussed in [1] and here, polynomials with dependent coefficients have been considered from the Galois-theoretic perspective in a few other studies. In the model of fixed degree polynomials, Pham and Xu [29] generalised known results regarding irreducibility of polynomials over $\mathbf{Q}$ to a setting of significantly relaxed independence, uniformity and support assumptions. Another perspective is that of random polynomials coming from random matrices: Eberhard [18] considered the characteristic polynomial ϕ of an $n \times n$ matrix with entries drawn independently according to a nontrivial measure μ on $\mathbf{Z}$ with finite support. He showed that ϕ is irreducible with high probability if μ is uniform modulo the product of four primes, generalising an earlier paper by Bary-Soroker and Kozma [8]. In addition, assuming the Riemann hypothesis for Dedekind zeta functions, Eberhard proved that $\mathcal{G}_\phi$ contains $\mathcal{A}_n$ with high probability, generalising the result of Breuillard and Varjú [11]. The latter result has been extended to the setting of symmetric matrices as well [20]. In [24], the authors give an application in quantum chaos — related to the support of semiclassical measures for quantum cat maps — of the following result they prove: when ordered by any norm, 100% of the symplectic $2m \times 2m$ matrices M have the property that the (reciprocal) characteristic polynomials of M^k with $k \geqslant 1$ all have maximal Galois group.

Our approach builds on the aforementioned work of Bary-Soroker, Kozma and the second author [7], who employed rather different methods than those utilized in the large box model

or in a setting where the extended Riemann hypothesis is assumed, drawing instead ideas from the anatomy of integers, permutations and polynomials, from p-adic Fourier analysis, and from asymptotic group theory. They showed analogues of Theorem A and the other results presented below for standard monic polynomials (again, where all coefficients are drawn independently). Our proofs, outlined in §2, follow the same line of reasoning. We mention the main novelties in our work. In the Fourier-analytic part of the paper (§§9–12), the dependencies between the coefficients of A form a serious technical obstacle. We use character theory of finite abelian groups to address this (see §9). To obtain the Galois group results, we combine [7] with an analysis of (1) the asymptotic subgroup structure of $C_2 \wr \mathcal{S}_m$ by means of group cohomology, part of which was already described in [1] (see §14); (2) the discriminant of random reciprocal polynomials to handle the group $(C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}$, building on the first author's earlier paper [23] (see §7); and (3) the Frobenius automorphism to handle the group $C_2 \times \mathcal{S}_m$ (see §16).

Let us now discuss our other results. First, we state some conventions and introduce some notation, mostly following [7]. In general, by saying that the polynomial A in (1.2) is a *random monic reciprocal polynomial* we mean that $a_m = 1$ and that the coefficients $a_0, a_1, \dots, a_{m-1}$ are independent random variables, with each a_j selected according to a fixed probability measure μ_j on the integers.

Definition 1.3. We denote by $\mathcal{R}(m)$ the set of monic reciprocal polynomials $A \in \mathbf{Z}[T]$ of degree $2m$. In other words, $\mathcal{R}(m)$ is the set of polynomials as in (1.2) with integer coefficients and $a_m = 1$. Similarly, if p is prime, then the set of such polynomials A in the ring $\mathbf{F}_p[T]$ will be denoted by $\mathcal{R}_p(m)$.

Any sequence $\mu_0, \mu_1, \dots, \mu_{m-1}$ of probability measures on the integers induces a probability measure on $\mathcal{R}(m)$ via

$$\mathbb{P}_{\mathcal{R}(m)}(A) := \prod_{j=0}^{m-1} \mu_j(a_j), \tag{1.3}$$

where it is understood that the a_j refer to the coefficients of A in (1.2). We will prove results as those in Theorem A for a wide range of varying measures μ_j, subject to certain Fourier-analytic conditions. Our most general result, Theorem C below, also specifies a lower bound for the rate of convergence, that applies (for example) in the setting of Theorem A.

Since our general Theorem C discussed below is so similar to the case $s = 1$ in [7, Theorem 7], our other results are, minor details aside, the exact analogues of results in [7] — such as Theorem B below. To state this result, we first introduce the following standard notation. Given a probability measure μ, we denote by $\mathrm{supp}(\mu)$ its support. Furthermore, when μ is supported on the integers, we set

$$\|\mu\|_q := \begin{cases} (\sum_{a \in \mathbf{Z}} \mu(a)^q)^{1/q} & \text{if } 1 \leqslant q < \infty, \\ \sup_{a \in \mathbf{Z}} \mu(a) & \text{if } q = \infty. \end{cases} \tag{1.4}$$

Given a prime p and a measure μ, we will sometimes consider its projection $\overline{\mu}_p$ to $\mathbf{F}_p$, i.e., the measure

$$\overline{\mu}_p \colon \mathbf{F}_p \to [0,1], \quad \overline{\mu}_p(a) = \sum_{\substack{b \in \mathbf{Z} \\ b \equiv a \bmod p}} \mu(b). \tag{1.5}$$

When the measure is $\mu = \mu_j$, we write $\overline{\mu}_{j,p}$ instead to avoid confusion. The norms $\|\overline{\mu}_p\|_q$ for $q \in [1, \infty]$ are defined as in (1.4), with the domain of the sum and of the supremum equal to $\mathbf{F}_p$ instead of $\mathbf{Z}$.

Theorem B. *Let $H \geqslant 3$ and $m \geqslant 3$ be integers and suppose $\mu_j = \mu$ is a fixed probability measure for all $j = 0, 1, \dots, m-1$, with the following properties:*

(1) (bounded support) $\mathrm{supp}(\mu) \subset [-H, H]$;

(2) (support not too sparse) $\|\mu\|_2^2 \leqslant \min\{H^{-4/5}, m^{1/16}/H\}/(\log H)^2$.

Then there are absolute constants $c, C, H_0 > 0$ *such that* $H \geqslant H_0$ *implies*

$$\mathbb{P}_{\mathcal{R}(m)}(A \text{ is irreducible}) \geqslant 1 - Cm^{-c}.$$

Theorems A and B are both consequences of Theorem C, which is our most general result. (We will refrain from rehashing other results of [7], such as their Theorems 3 and 4, in the setting of reciprocal polynomials; the interested reader could derive them from the general Theorem C below in the same way as Theorems 3 and 4 in [7] follow from their Theorem 7.) For this, define the function $e(x) := \exp(2\pi i x)$ and recall that the Fourier transform of a measure μ on the integers is defined as

$$\hat{\mu}\colon \mathbf{R}/\mathbf{Z} \to \mathbf{C}, \qquad \hat{\mu}(\theta) = \sum_{a \in \mathbf{Z}} \mu(a) e(a\theta).$$

Our most general result is then the following.

Theorem C. *Let* P *be the product of four distinct primes. Consider an integer* $m \geqslant P^4$ *and probability measures* $\mu_0, \mu_1, \dots, \mu_{m-1}$ *on the integers, all supported in* $[-H, H]$ *with* $H \geqslant 2$. *Let* $\alpha > 0$ *and* $B \geqslant 1$ *be two constants. Suppose that the following hold:*

(1) (bounded support) $H \leqslant Bm^{1/2-\alpha}$;

(2) (controlled Fourier transform modulo four primes) We have

$$\frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \left|\hat{\mu}_j(k/Q + \ell/R)\right| \leqslant 1 - m^{-1/10}$$

for all $j = 0, \dots, m-1$ *and all integers* Q, R, ℓ *such that* $QR = P$ *and* $Q > 1$.

Then there are constants $c, C > 0$ *depending at most on* α *and* B *such that*

$$\mathbb{P}_{A \in \mathcal{R}(m)}(A \text{ is irreducible}) \geqslant 1 - Cm^{-c}. \tag{1.6}$$

Moreover, there are constants $c', C' > 0$ *depending at most on* α *and* B *such that*

$$\mathbb{P}_{A \in \mathcal{R}(m)}\Big(\mathcal{G}_A \in \{C_2 \wr \mathcal{S}_m, C_2 \wr \mathcal{A}_m, G_2\}\Big) \geqslant 1 - C'm^{-c'}, \tag{1.7}$$

where G_2 *denotes the group defined in* (14.3).

A more precise bound, given specific choices of the μ_j, on the probability that A is irreducible and $\mathcal{G}_A \leqslant (C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}$ can be derived using Proposition 2.8. The probability that A is irreducible and $\mathcal{G}_A \leqslant C_2 \times \mathcal{S}_m$ is bounded in Lemma 16.3.

Surprisingly, our irreducibility results are of virtually the same strength as those in [7], despite concerning only a sparse subsequence of all polynomials of degree n. This is thanks to the rigid divisor structure of reciprocal polynomials (see Lemma 2.1 below), which dictates that a reducible reciprocal polynomial either has a nontrivial reciprocal divisor or factors in an exceptional, structured way that occurs only rarely[1] (see §7). On the other hand, all our results are "all or (almost) nothing": for a given sequence of measures $\mu_0, \mu_1, \dots, \mu_{m-1}$ we can either show that A is irreducible with high probability, or we can only rule out divisors of degree $\ll m^{1/10}$, following Konyagin's classical argument [25]. In contrast, [7, Theorem 7] shows that in the standard polynomial case, divisors of degree $\leqslant \theta m$ for some constant $\theta > 0$ (depending on the measures) can also be precluded in many cases. The source of this difference lies in a trick employed in the proof of the L^1 bounds in [7, Lemma 6.3], the analogue of which fails to hold in our setting. This is explained in more detail in Remark 12.6.

Remark 1.4. Reciprocal polynomials, sometimes with slightly different definitions, are occasionally called palindromic, self-reciprocal, (self-)inversive or symmetric polynomials.

[1] This is markedly different from the direct analogue over the integers: the divisors of a *palindromic integer* are typically not palindromic themselves.

Acknowledgements. Many thanks to Gunther Cornelissen for helpful conversations and feedback on earlier versions of this manuscript.

D. H. is supported by the Dutch Research Council (NWO) through the grant OCENW.M20.233. This project was originally conceived during a visit of D. H. to Université de Montréal in October 2023, supported by the Courtois Chair. He would like to thank his hosts for the pleasant stay.

D. K. is supported by the Courtois Chair II in fundamental research, by the Natural Sciences and Engineering Research Council of Canada (RGPIN-2024-05850), by the Fonds de recherche du Québec - Nature et technologies (2025-PR-345672) and by the Simons Foundation.

Notation. We utilize the standard Vinogradov and big-O asymptotic notation, with $f \ll g, g \gg f$ and $f = O(g)$ on some domain X all meaning that there exists a constant $C = C(f, g, X) > 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. If the constant depends on more than just the datum f, g and X, this is indicated by a subscript such as $f \ll_\delta g$. The notation $f \asymp g$ means both $f \ll g$ and $g \ll f$ hold.

2. Overview and proof strategy

Overview and structure of the paper. Globally, we follow the same strategy as in the work of Bary-Soroker, Kozma and the second author [7] . We will borrow their notation unless stated explicitly. We shortly summarise their approach to prove irreducibility for 'standard' monic random polynomials $A(T) = a_0 + a_1T + \cdots + a_{m-1}T^{m-1} + T^m$:

(1) The first step is to show that A cannot have a divisor of small degree, say smaller than $n^{1/10}$, using a classical approach due to Konyagin [25]. This approach combines the random walk-type properties of the polynomial A to exclude cyclotomic divisors, with an analysis based on the Mahler measure for the noncyclotomic divisors. The result is then obtained with a union bound.

(2) Next, for the divisors of degree $k > n^{1/10}$, they start with the basic observation that if A has a divisor of degree k, then so does $A_p \coloneqq (A \bmod p) \in \mathbf{F}_p[T]$. They then show that A_p is approximately uniformly distributed among the polynomials of degree n in $\mathbf{F}_p[T]$, in the sense that, for $D \in \mathbf{F}_p[T]$, the approximation $\mathbb{P}(D \text{ divides } A_p) \approx p^{-\deg D}$ holds very well *on average*.

(3) The divisor structure of polynomials over $\mathbf{F}_p$ is well-understood: the probability that a 'typical' random polynomial of degree n in $\mathbf{F}_p[T]$ has a divisor of degree k is approximately $k^{-1+\log 2} \approx k^{-0.3}$. Since A_p is approximately uniform, this also holds for A_p. However, the probability is too large to simply sum over all $k > n^{1/10}$.

(4) To circumvent this problem, they use not just one, but multiple primes as in the predecessor paper of Bary-Soroker and Kozma [8]. (Indeed, naively one would expect the factorisations of A_p, as p varies, to be independent; this indeed holds by the Chinese remainder theorem for the primes p dividing H when the coefficients of A are selected uniformly at random from the set $\{1, 2, \dots, H\}$.) Thus one needs to control the *joint* distribution of $(A_p)_{p\in\mathcal{P}}$ for some set $\mathcal{P}$ of four primes, as $k^{4(-1+\log 2)} \approx k^{-1.2}$; summing this over all $k > n^{1/10}$ yields a quantity that goes to 0 as n goes to infinity.

To adjust this strategy in our context, let us first introduce two pivotal concepts. First, the *trace polynomial* of A, denoted A_{R}, is the unique polynomial of degree m with the property

$$A(T) = T^m A_{\mathsf{R}}(T + T^{-1}).$$

The mapping $A \mapsto A_{\mathsf{R}}$ is linear and multiplicative, setting up a correspondence between the divisors of A_{R} and the *reciprocal* divisors of A; see §5 below. The *reversal polynomial* of a polynomial F is

$$F_{\mathsf{rev}}(T) \coloneqq T^{\deg F} F(T^{-1}),$$

so that $F = F_{\mathsf{rev}}$ when F is reciprocal. (The notation comes from [13].)

A fundamental fact, proved in §4, is the following: if A is reducible, then either A has a reciprocal divisor of degree $\leqslant m$, or $A = \pm I \cdot I_{\mathsf{rev}}$ for some monic irreducible nonreciprocal polynomial I. We deal with small-degree reciprocal divisors (step 1) in §6, and with the 'exceptional factorisation' $A = \pm I \cdot I_{\mathsf{rev}}$ in §7. The Fourier analysis (steps 2 and 4) is carried out in §§8–12, and §13 concerns the anatomy of reciprocal polynomials (step 3). These sections cover the proof of irreducibility of A with high probability. Sections §§14–16 cover the Galois group. Some preliminary Galois-theoretic work is done in §7, where we study the discriminant of A.

We compare our proof of irreducibility with that in [7], other than the exceptional factorisation that we already mentioned. Let $D \in \mathcal{R}(k)$ be a reciprocal polynomial of degree $2k$. We handle the case $k \leqslant m^{1/10}$ with a simple adaptation of the approach in [7]. Step 2, where $k > m^{1/10}$, requires considerable effort: it turns out that the main contribution to $\mathbb{P}(D \text{ divides } A_p)$ does not come from just the zero residue as in [7], but rather from a linear subspace of $\mathbf{F}_p[T]/(D)$ of dimension k, which is of character-theoretic origin. This happens because of the dependencies between the coefficients of reciprocal polynomials, and is a significant hurdle in establishing the L^1 bounds (§12). The main results that help overcome this are covered in §§8–9. The proof of the L^∞ bounds (§11) is also quite different, with out approach boiling down to linear algebra and some classical results about Chebyshev polynomials. For the anatomy of reciprocal polynomials (step 3), we can rely — after a trick — on the work carried out in [7, §§8-10].

For the Galois theory, we have a different approach than in the paper [7], although we do require the result of their work. Starting in §14 we carry out an analysis of the subgroup structure of the *hyperoctahedral group* $C_2 \wr \mathcal{S}_m$, which is the largest Galois group A can have. We then show in §15 that the Galois group of A is either one of five 'large' groups — those that are compatible with the results of [7] and have bounded index in $C_2 \wr \mathcal{S}_m$ as m goes to infinity — or is contained in one 'small' group: $C_2 \times \mathcal{S}_m$. We can exclude two of the five large groups by using our results on the discriminant, which we already consider in §7. Lastly, in §16, we use an idea about the modulo p factorisation of reciprocal polynomials that we believe is new to preclude the small group $C_2 \times \mathcal{S}_m$ and its subgroups as possible Galois groups.

As mentioned in the introduction, the present section provides the precise statements proved in §§4–16. From these statements, we deduce in the remaining section §3 the main Theorems A, B and C that were presented in §1.

Preliminaries. A preliminary result that greatly facilitates the analysis carried out in this paper, is the following basic proposition regarding the divisor structure of a reciprocal polynomial.

Lemma 2.1 (Divisors of reducible reciprocal polynomials)**.** *Suppose that $A \in \mathbf{Z}[T]$ is a monic reducible reciprocal polynomial of degree $2m$. Then either A has a monic reciprocal divisor in $\mathbf{Z}[T]$ of degree $2k \leqslant m$, or there exists a monic irreducible polynomial $I \in \mathbf{Z}[T]$ of degree m and a sign $u \in \{\pm 1\}$ such that $A = uI \cdot I_{\mathsf{rev}}$.*

Lemma 2.1 is a direct consequence of the following more general proposition.

Proposition 2.2 (Prime factorization of reciprocal polynomials)**.** *Let K be a field. Suppose that $A(T) \in K[T]$ is a nonzero reciprocal polynomial. Then there exist irreducible polynomials $I_1, \dots, I_r$ and $J_1, \dots, J_s$ over K, integers $a, b \geqslant 0$ and an element $u \in K^\times$ such that:*

(a) each I_j is reciprocal;
(b) each J_j is coprime to $J_{j,\mathsf{rev}}$;
(c) $A(T) = u \cdot (T-1)^{2a}(T+1)^{2b} \prod_{i=1}^{r} I_i(T) \prod_{j=1}^{s} J_j(T) J_{j,\mathsf{rev}}(T)$.

Proposition 2.2 and Lemma 2.1 are shown in §4.

Small degree reciprocal factors and the exceptional factorisation. As explained in the first subsection, we will proceed by showing that A is unlikely to have a divisor of degree k, for any $k \in \{1, 2, \dots, m\}$. Since only p^k of the p^{2k} monic polynomials in $\mathbf{F}_p[T]$ of degree $2k$ are reciprocal, Proposition 2.2 allows us to consider a much smaller set of possible factors.

We start by proving that A is unlikely to have a reciprocal factor of small degree.

Proposition 2.3 (Small degree factors)**.** *Let $m \in \mathbf{Z}_{\geqslant 1}$ and $\mu_0, \dots, \mu_{m-1}$ a sequence of probability measures on the integers. Suppose*

(1) (bounded support) $\operatorname{supp}(\mu_j) \subset [-\exp(m^{1/3}), \exp(m^{1/3})]$ *for all* $j \geqslant 0$,

(2) (anti-concentration) $\|\mu_j\|_\infty \leqslant 1 - m^{-1/10}$ *for all* $j \geqslant 0$.

Then

$$\mathbb{P}_{A \in \mathcal{R}(m)}\Big(A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k \leqslant m^{1/10}\Big) \ll m^{-7/20}.$$

The proof of Proposition 2.3 is given in §6. The method goes back to Konyagin [25]. Here, we closely follow the adaptation of Konyagin's ideas laid out in [7, §7].

Next, we show that A is unlikely to have the *exceptional factorisation* $A = \pm I \cdot I_{\mathsf{rev}}$, where $I \in \mathbf{Z}[T]$ is a monic, irreducible, nonreciprocal polynomial.

Proposition 2.4 (Exceptional factorisation)**.** *Let $m \in \mathbf{Z}_{\geqslant 2}$. Let $\mu_0, \dots, \mu_{m-1}$ be a sequence of probability measures supported on $[-H, H]$ for some $H \geqslant 2$. Let $\varepsilon > 0$ such that $\|\mu_j\|_\infty \leqslant 1 - \varepsilon$ for all $j = 0, 1, \dots, m-1$. Then*

$$\mathbb{P}_{A \in \mathcal{R}(m)}\left(\begin{array}{l}\exists \text{ monic, irreducible, nonreciprocal } I \in \mathbf{Z}[T] \\ \text{such that } A = \pm I \cdot I_{\mathsf{rev}}\end{array}\right) \ll \frac{H(\log m)^{3/2}}{\varepsilon\sqrt{m}}. \tag{2.1}$$

Proposition 2.4 is shown in §7. In a nutshell, the proof proceeds by observing that the expression $A(1)A(-1)$ is a square up to sign if A factors as $A = \pm I \cdot I_{\mathsf{rev}}$, and then showing that this is unlikely to occur by writing $A(1)A(-1)$ as the difference of two (squared) random walks, with steps given by the coefficients of A.

Large degree reciprocal factors: approximate equidistribution and the anatomy of reciprocal polynomials.

Perfect equidistribution modulo four primes. Let us see how what we laid out so far helps to prove irreducibility in a particularly 'fair' setting. Let $\mathcal{P} = \{p_1, \dots, p_r\}$ be a set of $r \geqslant 4$ primes. Let H be a positive integer divisible by each of the p_j, and suppose A has coefficients drawn independently and uniformly at random from $\{1, \dots, H\}$. Fix $p \in \mathcal{P}$ and write $A_p \coloneqq (A \bmod p) \in \mathbf{F}_p[T]$. Then A_p is perfectly equidistributed among the reciprocal polynomials of degree $2m$ in $\mathbf{F}_p[T]$. By the details of the correspondence between reciprocal polynomials and their trace polynomials (Lemma 5.3 below), the trace polynomial $(A_p)_{\mathsf{R}} = (A_{\mathsf{R}})_p$ is then perfectly equidistributed among the polynomials of degree m in $\mathbf{F}_p[T]$. But then one can leverage the earlier work [8] to prove that the polynomial A_{R} is irreducible with high probabilty. As a result, by Lemma 2.1 and the reciprocal polynomial-trace polynomial correspondence, we conclude that, with high probability, the polynomial A is irreducible or factors as $A = \pm I \cdot I_{\mathsf{rev}}$. But this last option is unlikely by Proposition 2.4, thus concluding the proof that A is irreducible with probability. In this approach, note that it is essential that $r \geqslant 4$: this is an intrinsic limit to the method of both [8] and [7], and will thus remain essential in this paper as well.

Approximate equidistribution and independence. Before proceeding, we will first introduce some notation, borrowing from [7] whenever possible. We denote by boldface letters tuples of polynomials in $\mathbf{F}_{\mathcal{P}}[T] \coloneqq \prod_{p \in \mathcal{P}} \mathbf{F}_p[T]$. For example, the tuple $\boldsymbol{D} = (D_p)_{p \in \mathcal{P}}$ consists of

polynomials $D_p \in \mathbf{F}_p[T]$, for each $p \in \mathcal{P}$. In the case of boldface $\boldsymbol{A}$, this will typically denote the specific tuple $(A \bmod p)_{p\in\mathcal{P}}$. We then set

$$\|D_p\|_p := p^{\deg D_p}, \qquad \|\boldsymbol{D}\|_{\mathcal{P}} := \prod_{p\in\mathcal{P}} \|D_p\|_p.$$

The phrase '$\boldsymbol{D}$ divides $\boldsymbol{A}$' will mean that D_p divides A_p in $\mathbf{F}_p[T]$, for all $p \in \mathcal{P}$. Suppose $\boldsymbol{D}$ is a *reciprocal* tuple, that is, each D_p is a reciprocal polynomial. Furthermore, assume that each D_p is of degree $\leqslant 2m$. In the setting of perfect equidistribution outlined above, observe that

$$\mathbb{P}\big(D_p \text{ divides } A_p\big) = \mathbb{P}\big((D_p)_{\mathsf{R}} \text{ divides } (A_p)_{\mathsf{R}}\big) = \frac{1}{\|(D_p)_{\mathsf{R}}\|_p} = \frac{1}{\|D_p\|_p^{1/2}}$$

for each $p \in \mathcal{P}$. In other words,

$$\mathbb{P}(\boldsymbol{D} \text{ divides } \boldsymbol{A}) = \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}}.$$

The power $1/2$ in the preceding line is somewhat surprising at first sight, but it stems from the correspondence between the reciprocal polynomial A and its trace polynomial A_{R}, which is of half the degree of A and has a divisor if and only if A has a reciprocal divisor.

Now, in order to establish irreducibility results in a setting away from perfect equidistribution, we follow the ways of Fourier analysis — as in [7]. Let us first sketch an, at this point, tempting route that however fails. In [7], Bary-Soroker, Kozma and the second author established for *standard polynomials* $B = b_0 + \cdots + b_{m-1}T^{m-1} + T^m$ the following. If

$$\mathbb{P}(\boldsymbol{G} \text{ divides } \boldsymbol{B}) \approx \frac{1}{\|\boldsymbol{B}\|_{\mathcal{P}}}$$

on average over all tuples $\boldsymbol{G} = (G_p)_{p\in\mathcal{P}}$ with $\deg G_p \leqslant m$ for all p, and the measures according to which the b_j are selected are not too concentrated modulo each p, then B is unlikely to have a factor of large degree. (The precise conditions are not important at this point.) Thus, in our setting, it seems reasonable to first pass to the trace polynomial by 'setting' $\boldsymbol{B} = \boldsymbol{A}_{\mathsf{R}}$, and then import the results of [7]. However, there is one major problem: the coefficients of A_{R} are not independent (see Lemma 5.7), that is, there exist a choice of measures $\mu_0, \dots, \mu_{m-1}$ such that the induced probability distribution on the trace polynomial $\boldsymbol{A}_{\mathsf{R}}$ cannot be realised by selecting the coefficients of $\boldsymbol{A}_{\mathsf{R}}$ independently according to some other sequence of measures $\mu_0', \dots, \mu_{m-1}'$. But the independence assumption on the coefficients of the polynomial B underlying $\boldsymbol{B}$ is indispensable in [7]. More precisely, the approach taken in [7] fails without this assumption at the very start of the Fourier-analytic approach, in their Lemma 4.1.

Thus, instead of *first* passing to the trace polynomial and then carrying out the Fourier analysis, here we perform the Fourier analysis on the reciprocals immediately. Of course, dependence between the coefficients cannot be avoided, since the coefficients of A are already dependent by the reciprocity assumption. Overcoming this (comparatively mild) dependency is the main technical novelty in this work, with the core of it described in §9. As a consequence, we show that

$$\mathbb{P}(\boldsymbol{D} \text{ divides } \boldsymbol{A}) \approx \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}}$$

holds on average over all vectors $\boldsymbol{D} = (D_p)_{p\in\mathcal{P}}$ with $\deg D_p \leqslant m$ for all p, under the assumption that the Fourier transforms of the measures μ_j are sufficiently well-behaved. Since

$$\mathbb{P}(\boldsymbol{D} \text{ divides } \boldsymbol{A}) = \mathbb{P}(\boldsymbol{D}_{\mathsf{R}} \text{ divides } \boldsymbol{A}_{\mathsf{R}}) \quad \text{and} \quad \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} = \frac{1}{\|\boldsymbol{D}_{\mathsf{R}}\|_{\mathcal{P}}}$$

this implies

$$\mathbb{P}(\boldsymbol{D}_{\mathsf{R}} \text{ divides } \boldsymbol{A}_{\mathsf{R}}) \approx \frac{1}{\|\boldsymbol{D}_{\mathsf{R}}\|_{\mathcal{P}}}$$

on average as well, allowing us to import the results from [7] — which at this point *is* possible (see §13).

In fact, we show that $\boldsymbol{A}$ is approximately equidistributed among the 'admissible' residue classes modulo $\boldsymbol{D}$. The precise result is the following. Let $\mathbb{P}_{\mathcal{R}_p(m)}$ denote the probability measure induced by $\mathbb{P}_{\mathcal{R}(m)}$ after reduction modulo p, that is

$$\mathbb{P}_{\mathcal{R}_p(m)}(A) := \prod_{j=0}^{m-1} \overline{\mu}_{j,p}(a_j),$$

where we recall that $\overline{\mu}_{j,p}$ is defined in (1.5). Similarly, set

$$\mathbb{P}_{\mathcal{R}_{\mathcal{P}}(m)}(\boldsymbol{A}) := \prod_{j=0}^{m-1} \Big(\sum_{\substack{a \in \mathbf{Z} \\ a \equiv a_{j,p} \bmod p \ \forall p \in \mathcal{P}}} \mu_j(a) \Big)$$

where we write $a_{j,p}$ for the coefficient of the monomial T^j of A_p. We shall denote $\boldsymbol{A} \equiv \boldsymbol{C} \bmod \boldsymbol{D}$ to mean that D_p divides $A_p - C_p$ for all $p \in \mathcal{P}$. By $R_m(\boldsymbol{D}) \subset \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D}) := \prod_{p \in \mathcal{P}} \mathbf{F}_p[T]/(D_p)$ we denote the set of all possible residues that *could* occur as the residue of a tuple of reciprocal polynomials $\boldsymbol{A} \in \mathcal{R}_{\mathcal{P}}(m) := \prod_{p \in \mathcal{P}} \mathcal{R}_p(m)$ modulo a reciprocal polynomial $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k}) := \prod_{p \in \mathcal{P}} \mathcal{R}_p(k_p)$, where $\boldsymbol{k} = (k_p)_{p \in \mathcal{P}}$; the more precise definition requires some work and is given in (9.1). Lastly, set

$$\Delta^{\mathsf{R}}_{\mathcal{P}}(m; k) := \sum_{\substack{\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}} \\ \deg \boldsymbol{D} \leqslant 2k \\ 2 \in \mathcal{P} \implies T^2+1 \nmid D_2}} \max_{\boldsymbol{C} \in R_m(\boldsymbol{D})} \Big| \mathbb{P}_{\boldsymbol{A} \in \mathcal{R}_{\mathcal{P}}(m)}\big(\boldsymbol{A} \equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) - \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \Big|, \tag{2.2}$$

where

$$\deg \boldsymbol{D} := \max_{p \in \mathcal{P}} \deg(D_p).$$

We also adopt the convention $\Delta^{\mathsf{R}}_p(m; k) := \Delta^{\mathsf{R}}_{\{p\}}(m; k)$. The quantity $\Delta^{\mathsf{R}}_{\mathcal{P}}$ measures the extent to which the probability measure $\mathbb{P}_{\mathcal{R}(m)}$ fails to be equidistributed modulo the primes in $\mathcal{P}$ for reciprocal moduli up to a given degree. The requirement that $T^2 + 1$ does not divide D_2 whenever $2 \in \mathcal{P}$ is technical; see §11. It is equivalent to the condition that T does not divide the trace polynomial of D_2. This is reminiscent of the (stronger) condition that T does not divide D_p for *any* $p \in \mathcal{P}$, which is stipulated in [7, (2.6)].

We then show that $\Delta^{\mathsf{R}}_{\mathcal{P}}$ is very small when the measures $\mu_0, \mu_1, \ldots$ have good Fourier-theoretic properties.

Proposition 2.5 (Controlled Fourier transform implies approximate equidistribution)**.** *Let $\mathcal{P} = \{p_1, \ldots, p_r\}$ be a set of distinct primes, and set $P = p_1 \cdot \ldots \cdot p_r$. In addition, consider an integer $m \geqslant P^4$ and a sequence $\mu_0, \ldots, \mu_{m-1}$ of probability measures on the integers for which there is $\gamma \geqslant 1/2$ such that*

$$\sum_{k=0}^{Q-1} \big|\hat{\mu}_j(k/Q + \ell/R)\big| \leqslant \big(1 - m^{-1/10}\big) \cdot Q^{1-\gamma}$$

for all $j = 0, \ldots, m-1$ and all integers Q, R, ℓ such that $QR = P$ and $Q > 1$. Then

$$\Delta^{\mathsf{R}}_{\mathcal{P}}\big(m; \gamma m + m^{0.88}\big) \ll_r e^{-m^{1/10}}.$$

Proposition 2.5 will be proved in §12; the proof combines results from §§8–12.

Conclusion: precluding large degree reciprocal factors. As in [7], we define the constant

$$\lambda_0 := \frac{1}{4 - 4\log 2} = 0.81\ldots.$$

The final step in the proof of irreducibility is to rule out reciprocal factors of large degree under the assumption of approximate equidistribution. We prove the following analogue of [7, Proposition 2.2].

Proposition 2.6 (Large degree factors)**.** *Let $m \in \mathbf{Z}_{\geqslant 1}$ and $\varepsilon \in (0, 1/100]$. Let $\mathcal{P}$ be a set of four primes. Suppose $\mu_0, \ldots, \mu_{m-1}$ a sequence of probability measures on the integers satisfying the following:*

(1) (mod-$\mathcal{P}$ approximate equidistribution) $\Delta^{\mathsf{R}}_{\mathcal{P}}(m; m/2 + m^{\lambda_0+\varepsilon}) \leqslant m^{-30}$.

(2) (mod-$\mathcal{P}$ anti-concentration) $\sup_{0\leqslant j<m} \|\overline{\mu}_{j,p}\|_\infty \leqslant 1 - m^{-\varepsilon/200}$ for all $p \in \mathcal{P}$.

Then there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{A\in\mathcal{R}(m)}\Big(A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k \in [m^{1/10}, m/2]\Big) \leqslant Cm^{-c}.$$

Proposition 2.6 is proved in §13. The idea behind the proof is anatomy of polynomials: an analysis of the typical multiplicative structure of the polynomial A reduced modulo the primes in $\mathcal{P}$. As alluded to above, at this stage we *can* use the work of [7], because the anatomical part of their argument is insensitive to the dependencies between the coefficients of A_{R}. In this way, we bypass almost all of the hard work that had to be carried out in [7] at this point (their §§8-9) and swifly prove irreducibility after translating their results to our setting.

It is not always clear in the anatomy part of [7] that the coefficients could be dependent variables. For example, their Proposition 2.2 explicitly mentions the sequence of measures $\mu_0, \mu_1, \ldots$, implying that the coefficients are chosen independently. In §13, we state a version of that proposition for a general probability measure $\mathbb{P}_{\mathcal{M}(m)}$ on the set $\mathcal{M}(m)$ of monic polynomials of degree m. In similar vein, even though the probability measure $\mathbb{P} = \mathbb{P}_{\mathcal{R}(m)}$ in our Proposition 2.6 is induced by the sequence $\mu_0, \ldots, \mu_{m-1}$, this is not necessary. A more general version of Proposition 2.6, where condition (2) is replaced by a suitable alternative, is given in Proposition 13.3.

Galois theory. In §§14–16, we study the Galois group $\mathcal{G}_A$ of A over $\mathbf{Q}$. In the last part of this paper, we study the typical Galois group of A. Some preparatory work is already done in §7, where bound the probability that the polynomial discriminant $\Delta(A)$ of A is a nonzero square.

The Galois group. The zeros of a reciprocal polynomial A come in pairs: if α is a zero of A, then α^{-1} is also a zero of A. Any element τ of the Galois group $\mathcal{G}_A$ of A over $\mathbf{Q}$, being a field automorphism, must respect this property as $\tau(\alpha^{-1}) = \tau(\alpha)^{-1}$. Let $\alpha_1, \alpha_1^{-1}, \ldots, \alpha_m, \alpha_m^{-1}$ denote the zeros of A. The above shows that $\mathcal{G}_A$ permutes the *blocks* $\{\alpha_j, \alpha_j^{-1}\}$. In general, the group of symmetries of the set $\{-m, \ldots, -2, -1, 1, 2, \ldots, m\}$ that permutes the pairs $\{k, -k\}$ is the *hyperoctahedral group* $C_2 \wr \mathcal{S}_m$. Thus the Galois group of A is contained in $C_2 \wr \mathcal{S}_m$. This group is realised as a *permutational wreath product*, and its construction is explained in §14.

Our main result states that under the condition of approximate equidistribution modulo *one* prime, with high probability A is irreducible and the Galois group of A almost certainly contains at least one of two index-2 subgroups of the hyperoctahedral group. More precisely, we have the following.

Proposition 2.7. *Consider probability measures $\mu_0, \mu_1, \ldots, \mu_{m-1}$ on the integers, all supported on $[-H, H]$ with $H \geqslant 2$. Fix a prime p and real numbers $B \geqslant 1$, $\alpha \in (0, 1/2)$ and $\varepsilon \in (0, 1/100]$. Suppose the following hold:*

(1) (bounded support) $H \leqslant Bm^{1/2-\alpha}$.

(2) (mod-p approximate equidistribution) $\Delta_p^{\mathsf{R}}(m, m/2 + m^{\lambda_0+\varepsilon}) \leqslant m^{-10}$,

(3) (mod-p anti-concentration) $\sup_{0\leqslant j<m} \|\overline{\mu}_{j,p}\|_\infty \leqslant 1 - (\log m)^{-2}$,

Then there are constants $c, C > 0$ depending at most on B, α and ε such that

$$\mathbb{P}_{A\in\mathcal{R}(m)}\Big(\mathcal{G}_A \notin \{C_2 \wr \mathcal{A}_m, C_2 \wr \mathcal{S}_m, G_2\} \text{ and } A \text{ is irreducible}\Big) \leqslant Cm^{-c}.$$

Here, the group G_2 is defined in (14.3).

Proposition 2.7 is proved in §16. We use the results from [7] to prove in §15 that A_{R} has, with high probability, either the symmetric group $\mathcal{S}_m$ or the alternating group $\mathcal{A}_m$ as Galois group. Then we need to understand what the possibilities for $\mathcal{G}_A$ are given that $\mathcal{G}_{A_{\mathsf{R}}} \in \{\mathcal{S}_m, \mathcal{A}_m\}$. In §14, we use group cohomology to show that $\mathcal{G}_A$ is either one of five 'large' groups (of index at most 4 in $C_2 \wr \mathcal{S}_m$) or is contained in the 'small' group $C_2 \times \mathcal{S}_m$. Two of the five large groups can be excluded by studying the discriminant of A (see below), and the small group can be excluded by analyzing the factorisation pattern of A modulo a suitable prime.

The discriminant: ruling out alternating subgroups. In [7], the authors show that the typical Galois group of a standard, monic polynomial $B = b_0 + \ldots + b_{m-1}T^{m-1} + T^m$ is $\mathcal{S}_m$ or $\mathcal{A}_m$ with high probability, when the b_j are sampled independently according to measures satisfying Fourier-theoretic conditions that are essentially the same as ours in Proposition 2.5. The group $\mathcal{S}_m$ is maximal possible; to rule out the alternating group and its subgroups as possible Galois groups of some polynomial $F \in \mathbf{Z}[T]$ of degree m, one can consider its discriminant $\Delta(F)$, since

$$\Delta(F) \in \mathbf{Z} \text{ is a nonzero square if and only if } \mathcal{G}_F \leqslant \mathcal{A}_m.$$

For a standard random polynomial B, it is an open problem to quantify the probability that $\Delta(B)$ is a square; it is believed to be a highly unlikely event. For reciprocal polynomials however, the discriminant is a much more accessible invariant, and we prove the following:

Proposition 2.8. *Let $\varepsilon > 0$. Suppose the probability measures $\mu_0, \ldots, \mu_{m-1}$ have support contained in $[-H, H]$ with $H \geqslant 2$ and satisfy $\|\mu_j\|_\infty \leqslant 1 - \varepsilon$ for all $j \in [0, m-1] \cap \mathbf{Z}$. Then*

$$\mathbb{P}_{A\in\mathcal{R}(m)}\big(\Delta(A) \text{ is a nonzero square}\big) \ll \frac{H(\log m)^{3/2}}{\varepsilon\sqrt{m}}. \tag{2.3}$$

The proof of Proposition 2.8 is given in §7. Observe that the right-hand side of (2.3) is the same as the right-hand side of (2.1). Both bounds follow from a bound on the probability that $\pm A(1)A(-1)$ is a square.

Remark 2.9. To establish this bound we follow [23], in which the first author considered the case where $\mu_j = \mu$ for all j with the law $\mu(1) = \mu(-1) = 1/2$; these are known as *Littlewood polynomials* or *random Rademacher polynomials*. When $m \equiv 0, 3 \bmod 4$, then [23, Corollary 1.2] implies the asymptotic $\mathbb{P}_{\mathcal{R}(m)}(\Delta(A) \text{ is a nonzero square}) \sim c\log(m)/\sqrt{m}$ for an explicit constant $c > 0$, whereas the probability is 0 when $m \equiv 1, 2 \bmod 4$ due to arithmetic effects [23, Lemma 7.1]. In particular, the bound (2.3) cannot be sharpened in general by more than a factor of $\sqrt{\log m}$, and a lower bound must take arithmetic effects into account.

3. From Propositions 2.2–2.8 to Theorems A–C

In this section, we deduce Theorems A–C from Propositions 2.2–2.8. We commence by proving Theorem C, which we then show implies the other main theorems. The proofs of Propositions 2.2–2.8 will take up the remaining sections of this paper.

Proof of Theorem C. Define the events

$$\mathcal{E}_1 := \{A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k < m^{1/10}\},$$
$$\mathcal{E}_2 := \{A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k \in [m^{1/10}, m/2]\},$$
$$\mathcal{E}_3 := \{\exists \text{ monic, irreducible, nonreciprocal } I \in \mathbf{Z}[T] : A = \pm I \cdot I_{\mathsf{rev}}\}.$$

To show (1.6), by Lemma 2.1 it suffices to show that $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}_3$ occur with very small probability. Possibly after adjusting C, we may assume m is sufficiently large throughout. As in the proof of [7, Theorem 7], we have the following: for any j, any divisor $Q \mid P$ with $Q > 1$, and any $b \in \mathbf{Z}/Q\mathbf{Z}$, Fourier inversion and condition (2) imply

$$\sum_{a \equiv b \bmod Q} \mu_j(a) \leqslant \frac{1}{Q} \sum_{k=0}^{Q-1} \left|\hat{\mu}_j(k/Q)\right| \leqslant \frac{1 - m^{-1/10}}{\sqrt{Q}} < \frac{1}{\sqrt{2}}.$$

In particular, for any j and any prime divisor $p \mid P$ we have

$$\|\mu_j\|_\infty \leqslant \|\overline{\mu}_{j,p}\|_\infty < \frac{1}{\sqrt{2}}. \tag{3.1}$$

All this implies the following. For $\mathcal{E}_1$, condition (1) of Theorem C implies condition (1) of Proposition 2.3 as m can be taken sufficiently large. Condition (2) of Proposition 2.3 holds by (3.1). Thus there exists an absolute constant $C_1 > 0$ such that $\mathbb{P}(\mathcal{E}_1) \leqslant C_1 m^{-7/20}$. For $\mathcal{E}_2$, we may first apply Proposition 2.5 with $\mathcal{P}$ the set of prime divisors of P and $\gamma = 1/2$ to find that condition (1) of Proposition 2.6 holds for any $\varepsilon_{\text{Proposition 2.6}} \in (0, 1/100]$. Pick $\varepsilon_{\text{Proposition 2.6}} = 1/100$. Condition (2) of Proposition 2.6 is also satisfied by (3.1). Thus there are absolute constants $c_2, C_2 > 0$ for which $\mathbb{P}(\mathcal{E}_2) \leqslant C_2 m^{-c_2}$. For $\mathcal{E}_3$, we again employ (3.1) to apply Proposition 2.4 with $\varepsilon_{\text{Proposition 2.4}} = 1 - 1/\sqrt{2}$. By condition (1) of Theorem C, this implies there exists $C_3 = C_3(\alpha) > 0$ such that $\mathbb{P}(\mathcal{E}_3) \leqslant C_3 m^{-\alpha/2}$. We conclude that

$$\mathbb{P}_{A \in \mathcal{R}(m)}(A \text{ is reducible}) = \mathbb{P}(\mathcal{E}_1) + \mathbb{P}(\mathcal{E}_2) + \mathbb{P}(\mathcal{E}_3) \leqslant C m^{-c}$$

for some constants $c, C > 0$ depending at most on α.

To go from irreducibility to the Galois group, we require Proposition 2.7. Its condition (1) holds by condition (1) of Theorem C, its condition (2) by condition (2) of Theorem C combined with Proposition 2.5 and the choice $\varepsilon_{\text{Proposition 2.7}} = 1/100$, and its condition (3) by (3.1). Thus, combining the conclusion of Proposition 2.7 with the already proved (1.6), the result follows. □

Remark 3.1. (a) Our Theorem C is quite similar to Theorem 7 in [7]. However, observe that our condition on the support of the measures μ_j is more strict, which is needed to preclude the exceptional factorisation (in Proposition 2.4) and show that the discriminant is unlikely to be a square (in Proposition 2.8). Furthermore, in the notation of [7, Theorem 7], we do not cover the case $s > 1$, for technical reasons explained in Remark 12.6.

(b) The conclusion of Theorem 7 in [7] contains a typo: it should say that A is unlikely to have divisors of small degree, not that it is unlikely not to have divisors of small degree.

Proof of Theorem A. We will deduce this from Theorem C. As $H = \max_{a \in \mathcal{N}} |a|$ is bounded, condition (1) of Theorem C is satisfied for any $\alpha \in (0, 1/2)$. To prove that the Fourier condition (2) of Theorem C is satisfied when all measures μ_j equal the fixed, uniform measure μ on a set $\mathcal{N}$ of at least 35 consecutive integers, we refer to [7, §3.1]. □

Proof of Theorem B. Again, we deduce this from Theorem C. Possibly after adjusting C, we may assume that m is sufficiently large. Since $\mu_j = \mu$ is fixed, this also implies that we may assume that condition (1) of Theorem C is satisfied. To prove that condition (2) of Theorem C holds as well, we refer to [7, §3.6]. □

4. Prime factorization of reciprocal polynomials

In this section, we prove Proposition 2.2. We begin with the following simple lemma.

Lemma 4.1. *Let K be a field and let I be a monic irreducible polynomial over K.*

(a) If $I = I_{\mathrm{rev}}$, then either I is reciprocal or $I(T) = T + 1$.

(b) If $I \neq I_{\mathrm{rev}}$, then either I and I_{rev} are coprime, or $I(T) = T - 1$ and $\mathrm{char}(K) \neq 2$.

Proof. We start with (a). The only monic polynomial I of degree 1 satisfying the relation $I = I_{\mathrm{rev}}$ is the polynomial $I(T) = T + 1$. Let us assume now that $\deg I \geqslant 2$. Since $I = I_{\mathrm{rev}}$, we will have that I is reciprocal as long as we can show that $\deg I$ is even. Indeed, according to Remark 1.2, if $\deg I$ is odd, then the relation $I = I_{\mathrm{rev}}$ implies that I can be factored as $I(T) = (T + 1)J(T)$ for some reciprocal polynomial J. This is impossible because we have assumed that I is irreducible and has degree $\geqslant 2$. We have thus established our claim that $\deg I$ is even. This completes the proof of part (a) of the lemma.

For (b), let us assume that I and I_{rev} are not coprime; otherwise there is nothing to prove. Since both of these polynomials are irreducible, we must have that $I_{\mathrm{rev}} = uI$ for some $u \in K^\times$. Since I is monic, we have $I(T) = T^m + c_{m-1}T^{m-1} + \cdots + c_0$ for some $c_j \in K$. The relation $I_{\mathrm{rev}} = uI$ then implies that $c_0 = u$ and that $1 = uc_0$. We thus find that $u = c_0 = \pm 1$. Since we have assumed that $I \neq I_{\mathrm{rev}}$, we must have $u = -1 \neq 1$. In particular, K has characteristic different than 2, and thus the relation $I = -I_{\mathrm{rev}}$ implies that $I(1) = 0$. Since I is monic irreducible, we must have $I(T) = T - 1$. This completes the proof of the lemma. □

Proof of Proposition 2.2. Let J be an irreducible factor of A such that $J \neq J_{\mathrm{rev}}$. The polynomial J_{rev} is also irreducible. Since J divides A, the polynomial J_{rev} divides $A_{\mathrm{rev}} = A$ as well. Moreover, since A is reciprocal, J and J_{rev} must divide A to the exact same power. If J and J_{rev} are coprime, we thus find that there exists an integer $\nu \geqslant 0$ such that

$$A = (JJ_{\mathrm{rev}})^\nu B.$$

The polynomial B must be reciprocal because A and $(JJ_{\mathrm{rev}})^\nu$ are reciprocal. These observations together with Lemma 4.1 readily imply that we may write

$$A(T) = u \cdot (T-1)^k (T+1)^\ell \prod_{i=1}^{r} I_i(T) \prod_{j=1}^{s} J_j(T) J_{j,\mathrm{rev}}(T), \tag{4.1}$$

where each I_i is reciprocal irreducible, each J_j is irreducible and coprime to $J_{j,\mathrm{rev}}$, and $k, \ell \in \mathbf{Z}_{\geqslant 0}$ and $u \in K^\times$. It remains to check that k and ℓ are even. For the former claim, we may assume that $\mathrm{char}(K) \neq 2$ (as otherwise $T - 1 = T + 1$ and we may take $k = 0$). If $B(T)$ denotes the polynomial on the right-hand side of (4.1), then $B_{\mathrm{rev}} = (-1)^k B$. Since $B = A$ is reciprocal, and we also know here that $\mathrm{char}(K) \neq 2$, we conclude that k must be even. Finally, we must have that ℓ is even because A and the I_i are all reciprocal polynomials and thus have even degrees (cf. Definition 1.1). □

Proof of Lemma 2.1. Since A is monic and has integer coefficients here, the polynomials I_i and J_j in Proposition 2.2 can be assumed to be monic and to lie in $\mathbf{Z}[T]$. Comparing leading coefficients, and using again our assumption that A is monic, we find that the u of Proposition 2.2 satisfies $u = \pm 1$.

If $a + b + r + s \geqslant 2$, the result follows by selecting a factor of minimal degree among

$$\underbrace{(T-1)^2, \ldots, (T-1)^2}_{a \text{ times}}, \quad \underbrace{(T+1)^2, \ldots, (T+1)^2}_{b \text{ times}}, \quad I_1, \ldots, I_r, \quad \text{and} \quad J_1 J_{1,\mathrm{rev}}, \ldots, J_s J_{s,\mathrm{rev}}.$$

Let us now examine the case $a + b + r + s = 1$. The subcase when $r = 1$ and $a = b = s = 0$ can be discarded, because A would then be irreducible. In each of the remaining subcases, we

may easily check that we may write $A = uI \cdot I_{\mathsf{rev}}$ for some monic irreducible polynomial I: we take $I = T - 1$, $I = T + 1$ or $I = J_1$, according to whether $a = 1$, $b = 1$ or $s = 1$. This completes the proof. □

We will also make use of the following notion — a reciprocal version of the greatest common divisor.

Definition 4.2. For two (not-necessarily reciprocal) polynomials $A, B \in K[T]$, let $(A, B)_{\boldsymbol{r}}$ denote the *greatest common reciprocal divisor* of A and B: that is, the monic reciprocal polynomial of maximal degree dividing both A and B.

Remarks. (a) The polynomial $(A, B)_{\boldsymbol{r}}$ is unique by the requirement that it is monic, just as the usual greatest common divisor (A, B) is unique if it is required to be monic.

(b) Using Proposition 2.2, we find that $(A, B)_{\boldsymbol{r}} = (A, B)$ if A and B are reciprocal. However, this relation is not true in general.

5. The trace polynomial

Let K be a field. In this preliminary section, we define the *trace polynomial* A_{R} of a reciprocal polynomial $A \in K[T]$. When viewing A as an element of a particular vector space defined below, the correspondence $A \mapsto A_{\mathsf{R}}$ defines a linear bijection that is also multiplicative. Under this map, the divisors of A_{R} correspond to the *reciprocal* divisors of A. We will use this correspondence in several places, in particular when studying the *anatomy* of reciprocal polynomials in §13.

We start by observing that the set of polynomials of degree $\leqslant \ell$ in $K[T]$ is a vector space over K, whereas the set of reciprocal polynomials of degree $\leqslant 2\ell$ is not: it is not closed under addition. For this reason, we introduce the following notion:

Definition 5.1 (Shifted reciprocal polynomials)**.** Let K be a field.

(a) We write $\mathcal{R}_K^{\mathsf{sh}}(\ell)$ for the set of *ℓ-shifted reciprocal polynomials*, which are defined to be all polynomials of the form

$$C(T) = c_\ell + c_{\ell-1}T \cdots + c_1T^{\ell-1} + c_0T^\ell + c_1T^{\ell+1} + \cdots + c_{\ell-1}T^{2\ell-1} + c_\ell T^{2\ell} \in K[T].$$

(b) We write $\mathcal{R}_K^{\mathsf{sh}} = \bigcup_{\ell \geqslant 0} \mathcal{R}_K^{\mathsf{sh}}(\ell)$ for the set of *shifted reciprocal polynomials*.

Remarks. (a) If $C(T) \in \mathcal{R}_K^{\mathsf{sh}}$ is nonzero, then there exists a unique integer $\ell \geqslant 0$ such that $C(T) \in \mathcal{R}_K^{\mathsf{sh}}(\ell)$.

(b) $\mathcal{R}_K^{\mathsf{sh}}(\ell)$ is a K-vector space of dimension $\ell + 1$. A basis for it is given by

$$\{T^\ell, T^{\ell-1} + T^{\ell+1}, \dots, T + T^{2\ell-1}, 1 + T^{2\ell}\}. \tag{5.1}$$

(c) For any integers $0 \leqslant i \leqslant j \leqslant \ell$ we have the inclusions

$$T^{\ell-i}\mathcal{R}_K(i) \subset T^{\ell-j}\mathcal{R}_K^{\mathsf{sh}}(j) \subset \mathcal{R}_K^{\mathsf{sh}}(\ell),$$

where the last inclusion is one of vector spaces.

Let $K[T]_\ell$ denote the set of monic polynomials in $K[T]$ of degree ℓ and write $K[T]_{\leqslant \ell}$ for the set of (not-necessarily monic) polynomials in $K[T]$ of degree $\leqslant \ell$, the latter including the zero polynomial. Also denote by $\mathcal{R}_K$ the set of all reciprocal polynomials over K. We construct a correspondence between $K[T]_{\leqslant \ell}$ and $\mathcal{R}_K^{\mathsf{sh}}(\ell)$.

Definition 5.2 (Reciprocal maps)**.** Let K be a field.

(a) For each integer $\ell \geqslant 0$, we define the map $(-)^{\mathsf{R},\ell} \colon K[T]_{\leqslant \ell} \to \mathcal{R}_K^{\mathsf{sh}}(\ell)$ by

$$G(T) \mapsto G^{\mathsf{R},\ell}(T) := T^\ell G(T + T^{-1}).$$

(b) We define the *reciprocal mapping* $(-)^{\mathsf{R}}\colon K[T] \to \mathcal{R}_K$ by

$$G(T) \mapsto G^{\mathsf{R}}(T) := \begin{cases} G^{\mathsf{R},\deg G}(T) = T^{\deg G} G(T + T^{-1}) & \text{if } G \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.3. *The map $(-)^{\mathsf{R},\ell}$ is an isomorphism of K-vector spaces. Moreover, for any $j \leqslant \ell$, it restricts to an isomorphism between the K-vector spaces $K[T]_{\leqslant j}$ and $T^{\ell-j}\mathcal{R}_K^{\mathsf{sh}}(j)$, and to a bijection between the sets $K[T]_j$ and $T^{\ell-j}\mathcal{R}_K(j)$.*

Proof. The map $(-)^{\mathsf{R},\ell}$ is a linear isomorphism because it is an injective, linear homomorphism between vector spaces of the same dimension. The claims made in the last sentence of the lemma statement are immediate consequences of the statement made in the first sentence, so we are done. □

Definition 5.4. The inverse of $(-)^{\mathsf{R},\ell}$ is denoted by $(-)_{\mathsf{R},\ell}$.

Next, we define the trace polynomial of a reciprocal polynomial.

Definition 5.5 (The trace polynomial)**.** Let K be a field. Let $(-)_{\mathsf{R}}$ denote the inverse function of $(-)^{\mathsf{R}}$. Given $A \in \mathcal{R}_K$, we call A_{R} the *trace polynomial* of A.

From Definitions 5.2 and 5.5, it follows immediately that the reciprocal mapping and its inverse commute with multiplication, that is $(FG)^{\mathsf{R}} = F^{\mathsf{R}}G^{\mathsf{R}}$ and $(AB)_{\mathsf{R}} = A_{\mathsf{R}}B_{\mathsf{R}}$.

The trace polynomials of the polynomials of the form $T^{2j} + 1$ are the *Chebyshev polynomials*.

Definition 5.6 (Chebyshev polynomials)**.** Let K be a field and $j \geqslant 0$. We then define the j-th *Chebyshev polynomial* $C_j(T) \in K[T]$ through the recursion

$$C_0(T) := 2, \quad C_1(T) := T, \quad \text{and} \quad C_{j+1}(T) := TC_j(T) - C_{j-1}(T) \text{ for } j \geqslant 1.$$

We extend this definition to negative indices by setting

$$C_{-j} := C_j.$$

Remarks. (a) For reference, when the characteristic of K is not 2, our Chebyshev polynomials are a common rescaling of the standard Chebyshev polynomials T_j, defined as the unique polynomial satisfying $\mathrm{T}_j(\cos x) = \cos(jx)$; they are related through $C_j(2T) = 2\mathrm{T}_j(T)$.

(b) A simple inductive argument yields

$$C_j(T + T^{-1}) = T^j + T^{-j} \quad \text{for } j = 0, 1, 2, \ldots$$

In other words, we indeed have $C_j^{\mathsf{R}} = T^{2j} + 1$ for nonnegative j.

(c) The set $\{1, C_1(T), C_2(T), \ldots, C_\ell(T)\}$ is a basis of $K[T]_{\leqslant \ell}$ and maps to the basis (5.1) of $\mathcal{R}_K^{\mathsf{sh}}(\ell)$ under $(-)^{\mathsf{R},\ell}$.

(d) We may easily check that

$$TC_j(T) = C_{j+1}(T) + C_{j-1}(T) \text{ for all } j \in \mathbf{Z}. \tag{5.2}$$

One can spell out explicitly how the coefficients of A_{R} depend on those of A:

Lemma 5.7. *Given $A(T) = 1 + a_{m-1}T + \cdots + a_0T^m + \cdots + a_{m-1}T^{2m-1} + T^{2m} \in \mathcal{R}_K(m)$ with trace polynomial $A_{\mathsf{R}}(T) = b_0 + \cdots + b_{m-1}T^{m-1} + T^m$, the coefficients of A and A_{R} satisfy the relations*

$$b_i = a_i + \sum_{j=1}^{\lfloor \frac{m-i}{2} \rfloor} (-1)^j \frac{i+2j}{i+j} \binom{i+j}{j} a_{i+2j} \tag{5.3}$$

and

$$a_i = \sum_{j=0}^{\lfloor \frac{m-i}{2} \rfloor} b_{i+2j} \binom{i+2j}{i+j}.$$

The proof is elementary but lengthy; we omit it here.

A consequence of the relation between the coefficients of A and A_{R}, described by Lemma 5.7, is that the probability measure $\mathbb{P}_{\mathcal{R}(m)}$ on the set of monic reciprocal polynomials in $\mathbf{Z}[T]$ of degree $2m$ induces a probability measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$ on the set $\mathcal{M}(m)$ of monic polynomials in $\mathbf{Z}[T]$ of degree m:

Definition 5.8. If $B \in \mathbf{Z}[T]$ is a monic polynomial of degree m, then we define

$$\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}(B) \coloneqq \mathbb{P}_{\mathcal{R}(m)}\left(B^{\mathsf{R}}\right).$$

If P is some property, then we will further use the notation

$$\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\Big(B \text{ has property } P\Big) \coloneqq \mathbb{P}_{A\in\mathcal{R}(m)}\Big(A_{\mathsf{R}} \text{ has property } P\Big).$$

By (5.3), the coefficients of B are not independent random variables, so we cannot apply the results of [7] directly to show that the trace polynomial of A is irreducible with high probability.

Definition 5.9 (Semi-irreducibility)**.** Let K be a field and let $A \in \mathcal{R}_K$. We say that A is *semi-irreducible* if it has no nontrivial reciprocal factors (of even degree, cf. Definition 1.1).

Lemma 5.10. *Let K be a field and let $A \in \mathcal{R}_K$. The following are equivalent:*

(a) A is semi-irreducible;
(b) A_{R} is irreducible;
(c) either A is irreducible, or $A = uI \cdot I_{\mathsf{rev}}$ for a nonreciprocal irreducible polynomial I and for some $u \in K^\times$.

Proof. It is easy to see that (a) and (b) are equivalent: if we have a factorization of the trace polynomial $A_{\mathsf{R}} = BC$, then we obtain a factorization $A = B^{\mathsf{R}}C^{\mathsf{R}}$ into two reciprocal factors of even degree. The converse is also true.

Let us now prove that (a) and (c) are equivalent. Clearly, (c) implies (a). Hence, it remains to show that (a) implies (c). Recall Proposition 2.2 and the notation therein. Since A has no nontrivial reciprocal factors, we must have that $a+b+r+s = 1$. If $a = 1$, we can take $I = T-1$. If $b = 1$, we can take $I = T+1$. If $r = 1$, then A is irreducible. Lastly, if $s = 1$, we can take $I = J_1$. This completes the proof. □

Lemma 5.11. *Let K be a field and let $A, B \in K[T] \setminus \{0\}$. Then A and B are coprime if, and only if, A^{R} and B^{R} are coprime.*

Proof. Assume that A and B are coprime, and let $D = \gcd(A^{\mathsf{R}}, B^{\mathsf{R}})$. Using Proposition 2.2, we find that D is reciprocal. In particular D_{R} is a common factor of A and B, and hence $D_{\mathsf{R}} = 1$. We thus also find that $D = 1$.

Conversely, if D is a nontrivial common factor of A and B, then D^{R} is a nontrivial common factor of A^{R} and B^{R}. This completes the proof. □

6. Small degree factors

In this section, we prove Proposition 2.3, which states that A is unlikely to have reciprocal factors of degree $\leqslant 2m^{1/10}$. The proof is a direct analogue of [7, Proposition 2.1]; we will thus skip some details. Both proofs follow the work of Konyagin [25], who considered polynomials with coefficients in $\{0,1\}$. He presented two arguments, of which we follow the first and simpler one. The argument proceeds in two steps, bounding cyclotomic and non-cyclotomic divisors separately.

As in the other results in [7] and in the present work, we must assume that the probability measures are contained in some bounded interval $[-H, H]$, but here we may take the comparatively large $H := \lfloor \exp(m^{1/3}) \rfloor$. If A has a reciprocal factor of degree $\leqslant 2k_0$, then it must have a semi-irreducible factor of degree $\leqslant 2k_0$ (see Definition 5.9). Hence it suffices to control the probability that the latter event occurs with $k_0 = m^{1/10}$.

Definition 6.1. We let $\mathcal{D}(k_0)$ denote the set of monic semi-irreducible reciprocal polynomials $1 + d_1 T + \cdots + d_1 T^{2k-1} + T^{2k}$ of degree $\leqslant 2k_0$ for which each d_j is bounded by $(H+1)^{2k}$ in absolute value.

An analogous argument to the one leading up to [7, Equation 7.2] implies that if A has a factor of degree $\leqslant 2k_0$, then it must have a factor in $\mathcal{D}(k_0)$.

We start by bounding the probability that A has a cyclotomic divisor of small degree. Here and elsewhere in the paper we will use the following inequality, due to Kolmogorov and Rogozin [31, Theorem 2].

Lemma 6.2 (Kolmogorov–Rogozin inequality)**.** *Suppose $X_1, \dots, X_\ell$ are discrete, independent random variables. Write $X = X_1 + X_2 + \cdots + X_\ell$. Then*

$$\sup_a \mathbb{P}(X = a) \ll \Big(\sum_{j=1}^{\ell} \big(1 - \sup_b \mathbb{P}(X_j = b)\big) \Big)^{-1/2}. \tag{6.1}$$

In particular, if there is an $\varepsilon > 0$ such that $\sup_b \mathbb{P}(X_j = b) \leqslant 1 - \varepsilon$ for all j, then

$$\sup_a \mathbb{P}(X = a) \ll \frac{1}{\sqrt{\varepsilon \ell}}. \tag{6.2}$$

Remark. When $\sup_b \mathbb{P}(X_j = b) = 1$ for all j, the right-hand side of (6.1) is understood as 1.

Lemma 6.3. *Fix $\varepsilon > 0$. For each $j \in [0, m-1] \cap \mathbf{Z}$, let μ_j be a probability measure such that $\|\mu_j\|_\infty \leqslant 1 - \varepsilon$. Then for fixed $z \in \mathbf{C}$, we have*

$$\mathbb{P}_{A \in \mathcal{R}(m)}(A(z) = 0) \ll \frac{1}{\sqrt{\varepsilon m}}.$$

In particular, given some positive integer k_0, we find

$$\sum_{d \,:\, \phi(d) \leqslant 2k_0} \mathbb{P}_{A \in \mathcal{R}(m)}(\Phi_d \mid A) \ll \frac{k_0}{\sqrt{\varepsilon m}}.$$

Proof. We follow [7, Lemma 7.3]. Note that $A(0) \neq 0$ for a reciprocal polynomial, so we may assume $z \neq 0$. For integers j in the interval $[1, m-1]$, define the random variable $X_j = a_{m-j}(z^{m-j} + z^{m+j})$. Set $X_0 = a_m z^m$. Then $X_0, X_1, \dots, X_{m-1}$ is a sequence of discrete random variables. Let J denote the set of values of $j \in [0, m-1] \cap \mathbf{Z}$ for which $z^{m-j} + z^{m+j}$ is nonzero. Since z is nonzero, the cardinality of J is strictly smaller than m only if z is a root of unity, say $z = e(\theta)$ for some $\theta \in \mathbf{Q}$. In that case, the relation $z^{m-j} + z^{m+j} = 0$ is equivalent to $\cos(2\pi j\theta) = 0$, i.e. to $j\theta \in \{1/4, 3/4\} \bmod 1$. In particular, the denominator of θ must be a multiple of 4, and J must have cardinality at least $m/2$ (with equality if $\theta \in \{1/4, 3/4\}$ and m is even).

Now, let $X = \sum_{j \in J} X_j$. Then

$$\begin{aligned} \mathbb{P}\big(A(z) = 0\big) = \mathbb{P}\big(X = -(1 + z^{2m})\big) &\leqslant \sup_{u \in \operatorname{supp}(X)} \mathbb{P}(X = u) \\ &\ll \Big(\sum_{j \in J} \big(1 - \sup_{b \in \operatorname{supp} X_j} \mathbb{P}(X_j = b)\big) \Big)^{-1/2}, \end{aligned}$$

by Lemma 6.2. Hence

$$\mathbb{P}(A(z) = 0) \ll \frac{1}{\sqrt{\varepsilon \cdot \#J}} \ll \frac{1}{\sqrt{\varepsilon m}}.$$

Since Φ_d is irreducible for all d, we have $\Phi_d \mid A$ if and only if $A(e(1/d)) = 0$. There are $\ll k_0$ values of d with $\phi(d) \leqslant 2k_0$ by [9], which concludes the proof. □

For the noncyclotomic divisors, we proceed by means of the *Mahler measure*: if $F \in \mathbf{Z}[T]$ is a polynomial of degree d with leading coefficient f_0 and zeros $z_1, \dots, z_d$ (listed with multiplicity), then the (exponential) Mahler measure of F is the quantity

$$M(F) \coloneqq |f_0| \prod_{j=1}^{d} \max\{1, |z_j|\}.$$

Choose $C > 0$ such that $\log(x)/\log\log x$ is strictly increasing and larger than 1 on $x > C$. Let $c \geqslant 1200$ be minimal such that $M(F) \geqslant 1 + 1/c$ for all irreducible, noncyclotomic polynomials of degree $\leqslant C$ with leading coefficient ± 1; it is a classical result that such c exists, see e.g. [12, Lemma 1.3]. Now define

$$L(x) = \begin{cases} c & \text{if } x \leqslant C, \\ c(\log(x)/\log\log x)^3 & \text{if } x > C, \end{cases}$$

and observe that L is a nondecreasing function on $x > 0$. In particular, the work of Dobrowolski [16] implies that

$$M(D) \geqslant 1 + 1/L(2k) \tag{6.3}$$

for all semi-irreducible reciprocal polynomials D of degree $2k$ that are noncyclotomic. Indeed, if D is irreducible, this follows directly by [16]. On the other hand, if $D = \pm I \cdot I_{\mathsf{rev}}$, then we have $M(D) = M(I)M(I_{\mathsf{rev}}) \geqslant (1 + 1/L(k))^2 > 1 + 1/L(2k)$ since L is nondecreasing.

Fix a noncyclotomic polynomial $D \in \mathcal{D}(k_0)$ of degree $2k$ other than $(T+1)^2$ or $(T-1)^2$. By semi-irreducibility, the polynomial D has distinct zeros $z_1, \dots, z_{2k}$. Following [7], pick a prime number

$$p = p_D \in ((1 + L(2k))\log(4Hm), 2(1 + L(2k))\log(4Hm)]$$

for which z_1^p has algebraic degee $2k$. That such p exists follows from [16, Lemma 3]. The conjugates of z_1^p are $z_2^p, \dots, z_{2k}^p$, which must thus be distinct.

Lemma 6.4. *Let $m, k \in \mathbf{Z}_{\geqslant 1}$. Let $D \in \mathcal{D}(k_0)$ be distinct from $(T+1)^2$ and $(T-1)^2$, and let $p = p_D$ be as above. Consider integers c_j for each $j \in [0, m] \cap \mathbf{Z}$ with $j \not\equiv 0 \pmod p$. Then there exists at most one reciprocal polynomial $A(T) = T^{2m} + a_{m-1}T^{2m-1} + \cdots + a_0 T^m + \cdots + a_{m-1}T + 1$ such that $D \mid A$, $|a_j| \leqslant H$ for all j, and $a_j = c_j$ for all $j \not\equiv 0 \pmod p$.*

Proof. Assume A and B are two distinct polynomials as in the lemma statement. The $2m$ coefficients of $A - B$ are bounded by $2H$ in absolute value, and the Mahler measure of $A - B$ is bounded above by the sum of these coefficients [12, Lemma 1.7], so that $M(A - B) < 4Hm$. However, we will prove that $M(A - B) \geqslant M(D)^p$, which is $> 4Hm$ by definition of p and by (6.3). This yields a contradiction.

To prove the claim that $M(A - B) \geqslant M(D)^p$, observe that D divides

$$A(T) - B(T) = T^m \left(g_0 + \sum_{0 < j < m/p} g_j (T^{-pj} + T^{pj}) \right).$$

The Mahler measure of $A - B$ is the same as that of $G(T) = T^{(p-1)m}(A(T) - B(T))$, which is still divisible by D and is a polynomial in T^p. Let ζ be a primitive p-th root of unity. Observe

that there are no integers $i \neq j$ and a such that $\zeta^a z_i = z_j$, as then we would have $z_i^p = z_j^p$. It follows that G is divisible by $\prod_{\ell=1}^{2k} \prod_{j=0}^{p-1} (T - \zeta^j z_\ell)$. Hence

$$M(A-B) \geqslant \prod_{\ell=1}^{2k} \prod_{j=0}^{p-1} \max\left\{1, |\zeta^j z_\ell|\right\} = \prod_{\ell=1}^{2k} \max\left\{1, |z_\ell|\right\}^p = M(D)^p. \qquad \square$$

This brings us to the proof of Proposition 2.3, which is again very similar to the proof of [7, Proposition 2.1].

Proof of Proposition 2.3. Set $k_0 := \lfloor m^{1/10} \rfloor$. By Lemma 6.3, which we may apply with $\varepsilon = m^{-1/10}$, the probability that $\Phi_d \mid A$ for some cyclotomic $\Phi_d \in \mathcal{D}(k_0)$ is $\ll m^{1/10}/\sqrt{m^{9/10}} = m^{-7/20}$. The probability that $(T+1)^2$ or $(T-1)^2$ divides A is equals the probability that $A(1)$ or $A(-1)$ vanishes, which is $\ll m^{-9/20}$, again by invoking Lemma 6.3.

It remains to bound the probability of A having a noncyclotomic divisor $D \in \mathcal{D}(k_0)$. Let $\mathcal{E}$ denote this event. Then $\mathbb{P}(\mathcal{E}) \leqslant \#\mathcal{D}(k_0) \cdot \sup_{D \in \mathcal{D}(k_0)} \mathbb{P}(D \mid A)$. Observe that the primes $p = p_D$ in the proof of Lemma 6.4 all satisfy $p \leqslant 2(1 + L(2m)) \log(4Hm) \ll (\log m)^3 m^{1/3}$. By Lemma 6.4, we then find

$$\sup_{D \in \mathcal{D}(k_0)} \mathbb{P}(D \mid A) \leqslant \sup_{0 \leqslant j \leqslant m-1} \|\mu_j\|_\infty^{\lfloor m/p \rfloor} \leqslant (1 - m^{-1/10})^{\lfloor m/p \rfloor} \leqslant \exp(-m^{0.55}).$$

Lastly, since each coefficient of D is bounded by $(H+1)^{2k_0}$ in absolute value, a straightforward count shows that $\#\mathcal{D}(k_0) \ll \exp(m^{0.54})$. This completes the proof. $\square$

7. Exceptional factors and the discriminant

Lemma 5.10 shows that A may be reducible even if its trace polynomial is not — that is, even if it has no nontrivial reciprocal divisor. In this case, we have the factorization

$$A = \pm I \cdot I_{\mathsf{rev}}$$

for some monic nonreciprocal irreducible polynomial $I \in \mathbf{Z}[T]$ of degree m. In this section, we show that this is unlikely to occur by studying the quantity $A(1)A(-1)$. If $A = \pm I \cdot I_{\mathsf{rev}}$, then $A(1) = \pm I(1) I_{\mathsf{rev}}(1) = \pm I(1)^2$ and $A(-1) = \pm I(-1) I_{\mathsf{rev}}(-1) = \pm I(-1)^2$. Thus

$$\mathbb{P}_{\mathcal{R}(m)}(A = \pm I I_{\mathsf{rev}} \text{ for some } I) \leqslant \mathbb{P}_{\mathcal{R}(m)}(A(1)A(-1) \neq 0 \text{ is a square up to sign}). \tag{7.1}$$

Bounding the right-hand side of (7.1) is also useful when ruling out subgroups of the alternating group $\mathcal{A}_{2m}$ as possible Galois group of A, as we will do in §16. Let us first explain this. Recall that if $F \in \mathbf{Z}[T]$ is of degree d and has zeros $\alpha_1, \dots, \alpha_d$ (listed with multiplicities) and leading coefficient c, then the *(polynomial) discriminant* $\Delta(F)$ of F is the integer

$$\Delta(F) := c^{2d-2} \prod_{1 \leqslant i < j \leqslant d} (\alpha_i - \alpha_j)^2. \tag{7.2}$$

We then have the following basic lemma from Galois theory.

Lemma 7.1. *Let $F \in \mathbf{Z}[T]$ be a squarefree polynomial of degree d. Then $\Delta(F) \in \mathbf{Z}$ is a square if and only if $\mathcal{G}_F \leqslant \mathcal{A}_d$.*

For general polynomials $F \in \mathbf{Z}[T]$, the quantity $\Delta(F)$ is difficult to analyze. However, reciprocal polynomials have the following neat property.

Lemma 7.2. *Let $A \in \mathcal{R}(m)$. Then $\Delta(A) = (-1)^m A(1)A(-1)\Delta(A_{\mathsf{R}})^2$.*

Proof. See e.g. [17, p. 85]. $\square$

A consequence of Lemma 7.2 is that

$$\mathbb{P}_{\mathcal{R}(m)}\big(\Delta(A) \neq 0 \text{ is a square}\big) \leqslant \mathbb{P}_{\mathcal{R}(m)}\big(A(1)A(-1) \neq 0 \text{ is a square up to sign}\big), \tag{7.3}$$

which is the same as the right-hand side of (7.1).

Thus our task is to analyze the product $A(1)A(-1)$. In the spirit of [23], our approach will be to write $A(1)A(-1)$ as the difference of two squares, say $X^2 - Y^2$, by splitting the even and odd part of the polynomial A. Moreover, the random variables X and Y are both sums of mutually independent random variables. Our main auxiliary result, then, is the following.

Lemma 7.3. *Fix $c, \varepsilon \in (0,1)$. Let $m, m_1, m_2 \in \mathbf{Z}_{\geqslant 1}$ be positive integers with $m = m_1 + m_2$ and $m_1, m_2 \geqslant cm$. Suppose $X_1, X_2, \dots, X_{m_1}$ and $Y_1, Y_2, \dots, Y_{m_2}$ are integer-valued, independent random variables supported in $[-H, H]$. Assume that $\sup_{k\in\mathbf{Z}} \mathbb{P}(X_j = k) \leqslant 1-\varepsilon$ and $\sup_{k\in\mathbf{Z}} \mathbb{P}(Y_j = k) \leqslant 1-\varepsilon$ hold for all j. Write $X = X_1 + X_2 + \cdots + X_{m_1}$ and $Y = Y_1 + Y_2 + \cdots + Y_{m_2}$. Then*

$$\mathbb{P}(X^2 - Y^2 \neq 0 \text{ is a square}) \ll \frac{H(\log m)^{3/2}}{\varepsilon c\sqrt{m}}. \tag{7.4}$$

Before proving Lemma 7.3, let us see how it implies Proposition 2.4 and Proposition 2.8.

Proof of Proposition 2.4 and of Proposition 2.8. By (7.3), and (7.1), it suffices to bound the probability that $A(1)A(-1)$ is nonzero and square up to sign. Write $A(T) = A_e(T^2) + TA_o(T^2)$ for the decomposition of A into its even and odd parts. Then we have $A(1)A(-1) = A_e(1)^2 - A_o(1)^2$. Furthermore, note that $A_e(1) = 2 + 2a_{m-2} + 2a_{m-4} + \cdots$ and $A_o(1) = 2a_{m-1} + 2a_{m-3} + 2a_{m-5} + \cdots$ are both sums of $\geqslant -1 + m/2$ discrete, independent random variables V_j with support contained in $[-3H, 3H]$ and with $\sup_{k\in\mathbf{Z}} \mathbb{P}(V_j = k) \leqslant 1-\varepsilon$ for all j. Thus (2.3) and Proposition 2.4 both follow by applying Lemma 7.3 twice: first with $X = A_e(1)$ and $Y = A_o(1)$, and then with $X = A_o(1)$ and $Y = A_e(1)$. □

Apart from the Kolmogorov–Rogozin inequality (Lemma 6.2), our main probabilistic tool for the proof of Lemma 7.3 is Hoeffding's inequality [22, Theorem 2].

Lemma 7.4 (Hoeffding's inequality)**.** *Let $X_1, \dots, X_\ell$ be discrete and independent random variables with support contained in $[-H, H]$. Write $X = X_1 + \cdots + X_\ell$. If $t > 0$, then*

$$\mathbb{P}\Big(\big|X - \mathbb{E}X\big| \geqslant t\Big) \leqslant 2\exp\left(-\frac{t^2}{2H^2\ell}\right).$$

We are now ready to prove Lemma 7.3.

Proof of Lemma 7.3. We may assume that m is sufficiently large and that $H \leqslant \sqrt{m}$, as otherwise the conclusion of the lemma is trivial. Recall that the set of Pythagorean triples $a^2 + b^2 = c^2$ with $abc \neq 0$ is in bijective correspondence with the set

$$S = \{(k, r, s) \in \mathbf{Z}^3 : k \neq 0 \text{ and } r,\ s \text{ coprime and of opposite parity}\}$$

through the assignment $a = k(r^2 - s^2)$, $b = 2krs$, and $c = k(r^2 + s^2)$. In other words, if $X^2 - Y^2$ is a square, then $X = k(r^2 + s^2)$ and $Y \in \{2krs, k(r^2 - s^2)\}$ for some tuple $(k, r, s) \in S$. Write $p(k, r, s) \coloneqq \mathbb{P}(X = k(r^2 + s^2))\mathbb{P}(Y \in \{2krs, k(r^2 - s^2)\})$. Then

$$\mathbb{P}(X^2 - Y^2 = \square \neq 0) = \sum_{(k,r,s)\in S} p(k, r, s). \tag{7.5}$$

Set $t \coloneqq H\sqrt{m \log m}$. By Lemma 7.4, we have

$$\mathbb{P}\Big(\big|X - \mathbb{E}X\big| \geqslant t\Big) \leqslant 2\exp\left(-\frac{m \log m}{2m_1}\right) \ll \frac{1}{\sqrt{m}} \tag{7.6}$$

since $m_1 \geqslant cm$ and $c \in (0,1)$. The right-hand side of (7.6) is small compared to the right-hand side of (7.4). Moreover, if we let S_t be the set of triples in S for which $\big|k(r^2+s^2) - \mathbb{E}X\big| < t$, then

$$\sum_{(k,r,s)\in S_t} p(k,r,s) \leqslant 2|S_t| \sup_{a\in\mathbf{Z}} \mathbb{P}(X=a) \sup_{b\in\mathbf{Z}} \mathbb{P}(Y=b) \ll \frac{\#S_t}{\varepsilon\sqrt{m_1 m_2}} \ll \frac{\#S_t}{\varepsilon cm} \tag{7.7}$$

by Lemma 6.2 and by our assumption that $m_1 + m_2 = m$ and that $m_1, m_2 \geqslant cm$.

It remains to bound the size of S_t. Let us denote by $S_t' \subset S$ the set of triples with the property $\big|k(r^2+s^2)\big| \leqslant t$. By the work of Stronina [32], we have

$$\#S_t' = c_1 t \log t + c_2 t + o\left(\sqrt{t}\right) \tag{7.8}$$

for explicit nonzero constants c_1, c_2. Let $x = |\mathbb{E}X|$ and note that $x \leqslant Hm$ since X is the sum of $\leqslant m$ random variables, each of which is supported in $[-H, H]$. If now $x < 2t$, then $S_t \subset S_{3t}'$, which is of size $\ll t\log t \ll H\sqrt{m(\log m)^3}$ by (7.8) and the assumption $H \leqslant \sqrt{m}$. On the other hand, if $x \geqslant 2t$, then again by (7.8) and by the Mean Value Theorem, we find

$$\#S_t \leqslant \#S_{x+t}' - \#S_{x-t}' \ll t\log(x+t) + \sqrt{x+t}.$$

Since $2t \leqslant x \leqslant Hm$ here, we conclude that $\#S_t \ll H\sqrt{m(\log m)^3}$. Combining these results with (7.7) yields

$$\sum_{(k,r,s)\in S_t} p(k,r,s) \ll \frac{H(\log m)^{3/2}}{\varepsilon c\sqrt{m}}$$

which, together with (7.6) and (7.5), proves the lemma. □

8. Interlude: Euclidean division

In §6 and §7, we ruled out reciprocal divisors of small degree and the exceptional factorisation $A = \pm I \cdot I_{\mathsf{rev}}$. The goal of §§8–13 is to rule out reciprocal divisors of large degree. We follow the proof methods of [7], and in many cases our arguments are direct analogues of those presented there. However, the lack of independence of the coefficients does mean that more work is required in many places.

First off, in this short, intermediate section, we prove a fundamental result regarding division with remainder of a (shifted) reciprocal polynomial C by a nonzero reciprocal polynomial D over $\mathbf{F}_p[T]$. By classical Euclidean division, there exist a quotient $Q \in \mathbf{F}_p[T]$ and a remainder $R \in \mathbf{F}_p[T]$ such that $R = 0$ or $\deg R < \deg D$; typically, R is not a reciprocal polynomial, and it is not immediately clear how many distinct R may occur as such a residue. However, in Definition 8.4 we describe an explicit, complete set $R_m(D)$ of remainders that are shifted reciprocal polynomials. The set $R_m(D)$ is of size $p^{\deg(D)/2}$. Proofs of the results in subsequent sections rely heavily on the description of $R_m(D)$.

Lemma 8.1 (Euclidean division for shifted reciprocal polynomials)**.** *Let p be a prime, $k \in \mathbf{Z}_{\geqslant 1}$ and $m \in \mathbf{Z}_{\geqslant 0}$. In addition, let $C \in \mathcal{R}_p^{\mathsf{sh}}(m)$ and $D \in \mathcal{R}_p(k)$. There are unique polynomials $Q \in \mathbf{F}_p[T]$ and $R \in T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1) \cap \mathbf{F}_p[T] \subset \mathcal{R}_p^{\mathsf{sh}}(m)$ such that $C = QD + R$.*

Remark. If $\ell = \min\{k-1, m\}$, then a simple computation shows that $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1) \cap \mathbf{F}_p[T] = T^{m-\ell}\mathcal{R}_p^{\mathsf{sh}}(\ell)$. The reason why we state Lemma 8.1 in this way is to motivate Definition 8.4, whose precise shape will be crucial in §§9-12.

At any rate, for the purposes of establishing Proposition 2.5, we only need to control $D \in \mathcal{R}_p(k)$ with k at most slightly larger than $m/2$. Hence, we will always have that $k \leqslant m+1$. However, in certain auxiliary results we will consider products of the form DD' with $D \in \mathcal{R}_p(k)$, $D' \in \mathcal{R}_p(k')$, in which case $k + k'$ can exceed $m+1$.

Proof of Lemma 8.1. Let $\ell = \min\{k-1, m\}$. By the above remark, we must show there are unique polynomials $Q \in \mathbf{F}_p[T]$ and $R \in T^{m-\ell}\mathcal{R}_p^{\mathsf{sh}}(\ell)$ such that $C = QD + R$. If such Q and R exist, their uniqueness is immediate, because if $C = QD + T^{m-\ell}R_1 = Q'D + T^{m-\ell}R_1'$ with $R_1, R_1' \in \mathcal{R}_p^{\mathsf{sh}}(\ell)$, then $T^{m-\ell}R_1 \equiv T^{m-\ell}R_1' \mod D$. We also know that $T \nmid D$ because $D \in \mathcal{R}_p(k)$. Thus $R_1 \equiv R_1' \mod D$. Since R_1 and R_1' are either 0 or have degrees $\leqslant 2\ell < \deg(D)$, we conclude that $R_1 = R_1'$ as needed.

Let us now prove the existence of Q and R. If $k > m$, we may trivially take $R = C$ and $Q = 0$. Now suppose $k \leqslant m$. Recall from Definition 5.4 that $(-)_{\mathsf{R},m}$ denotes the inverse of the map $(-)^{\mathsf{R},m}$, which by Lemma 5.3 is an isomorphism between the K-vector spaces $K[T]_{\leqslant m}$ and $\mathcal{R}_K^{\mathsf{sh}}(m)$. Hence by Euclidean division, there exist Q', R' with $C_{\mathsf{R},m} = Q'D_{\mathsf{R}} + R'$ and $\deg R' < \deg D_{\mathsf{R}} = k \leqslant m$ or $R' = 0$. Moreover, if $Q' \neq 0$, then $\deg(Q') \leqslant m - k$. Multiplying by T^m, we find that

$$\begin{aligned} C(T) = T^m C_{\mathsf{R},m}(T + T^{-1}) &= T^m Q'(T + T^{-1})D_{\mathsf{R}}(T + T^{-1}) + T^m R'(T + T^{-1}) \\ &= T^{m-k}Q'(T + T^{-1})D(T) + T^m R'(T + T^{-1}). \end{aligned}$$

Hence the claim holds with $Q = (Q')^{\mathsf{R},m-k}$ and $R = (R')^{\mathsf{R},m}$. □

Definition 8.2. In the notation of Lemma 8.1, we say that R is the *reciprocal remainder* of C modulo D, and write $R \coloneqq C \operatorname{rmod} D$.

As $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1) \subset \mathcal{R}_p^{\mathsf{sh}}(m)$ when $m \geqslant k-1$, Lemma 8.1 has the following immediate consequence.

Lemma 8.3. *Let p be a prime, let $k \in \mathbf{Z}_{\geqslant 1}$, let $D \in \mathcal{R}_p(k)$ and let $m \geqslant k-1$ be an integer. Then the images of $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$ and $\mathcal{R}_p^{\mathsf{sh}}(m)$ in $\mathbf{F}_p[T]/(D)$ coincide.*

Definition 8.4. Let p be a prime, let $k \in \mathbf{Z}_{\geqslant 0}$, let $D \in \mathcal{R}_p(k)$ and let $m \in \mathbf{Z}_{\geqslant 0}$. If $k \geqslant 1$, we denote by $R_m(D)$ the image of $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$ in $\mathbf{F}_p[T]/(D)$. If $k = 0$, we let $R_m(D) = \{0\}$.

Remark. Since T and any (reciprocal) D are coprime, there exists a multiplicative inverse of T in $\mathbf{F}_p[T]/(D)$, so Definition 8.4 also makes sense when $m \leqslant k-2$.

We will also need to prove the technical Lemma 8.6 below, which we will use in §11. First, we need an auxiliary result concerning the Chebyshev polynomials C_j (see Definition 5.6).

Lemma 8.5. *Let p be a prime and let $a, b \in \mathbf{Z}_{>0}$.*

(a) Suppose p is odd, and $t/s \neq p^\lambda$ for all $\lambda \in \mathbf{Z}$ and for all positive integers t and s satisfying $t \mid 4a$, $t \nmid 2a$, $s \mid 4b$ and $s \nmid 2b$. Then the Chebyshev polynomials C_a and C_b are coprime in $\mathbf{F}_p[T]$. In particular, if a and b have a different 2-valuation, then C_a and C_b are coprime in $\mathbf{F}_p[T]$.

(b) Suppose $p = 2$. Then C_a/T and C_b/T are coprime in $\mathbf{F}_p[T]$ if $2|(a+1)(b+1)$ and $\gcd(a, b) = 1$. In particular, C_a/T and C_{a+1}/T are coprime.

Proof. (a) If $T^{2a} + 1$ and $T^{2b} + 1$ are coprime, then their trace polynomials C_a and C_b are also coprime: indeed, if the latter have a common factor I, then I^{R} divides both $T^{2a} + 1$ and $T^{2b} + 1$. Now, writing Φ_d for the d-th cyclotomic polynomial, the $\mathbf{Q}$-irreducible factorisation of $T^{2k} + 1$ is given by

$$T^{2k} + 1 = \frac{T^{4k} - 1}{T^{2k} - 1} = \prod_{\substack{d \mid 4k \\ d \nmid 2k}} \Phi_d. \tag{8.1}$$

Recall that two polynomials A and B have a common factor if and only if their resultant $\operatorname{Res}(A, B)$ vanishes. Furthermore, the function Res is multiplicative in both arguments up to

sign. Therefore $T^{2a}+1$ and $T^{2b}+1$ are coprime if and only if $\mathrm{Res}(\Phi_t, \Phi_s) \neq 0$ for all $t \mid 4a$, $t \nmid 2a$ and $s \mid 4b$, $s \nmid 2b$. Now, over $\mathbf{Q}$, we have

$$\mathrm{Res}(\Phi_t, \Phi_s) = \begin{cases} 0 & \text{if } t = s \\ q^{\varphi(\min\{s,t\})} & \text{if } t/s = q^\lambda \text{ for some } \lambda \in \mathbf{Z} \setminus \{0\} \text{ and prime } q \\ 1 & \text{else,} \end{cases}$$

where φ is Euler's totient function (see, for example, [30, §3.3.6]). Over $\mathbf{F}_p$, it follows that $\mathrm{Res}(\Phi_t, \Phi_s) \neq 0$ if $t/s \neq p^\lambda$ for all $\lambda \in \mathbf{Z}$. Combining this with (8.1) and our assumptions proves the first claim in part (a). The second claim immediately follows from this.

(b) By the same reasoning as above, we find that the polynomials C_a/T and C_b/T are coprime if the polynomials $(T^{2a}+1)/(T^2+1)$ and $(T^{2b}+1)/(T^2+1)$ are coprime. Since we work modulo 2 here, it suffices that the polynomials

$$\frac{T^{2a}-1}{T^2-1} = \prod_{\substack{t \mid 2a \\ t \nmid 2}} \Phi_t \qquad \text{and} \qquad \frac{T^{2b}-1}{T^2-1} = \prod_{\substack{s \mid 2b \\ s \nmid 2}} \Phi_s$$

are coprime. Let us write $t = 2^v t_1$ and $s = 2^w s_1$ with t_1, s_1 odd. By the discussion in part (a), we would only have a common factor if $t/s = 2^\lambda$ for some $\lambda \in \mathbf{Z}$. Equivalently, $t_1 = s_1$. Since we have assumed that $\gcd(a, b) = 1$, we must then have that $t_1 = s_1 = 1$, meaning that t and s are both powers of 2. We further know that a or b is odd. If a is odd, then the relation $t = 2^v \mid 2a$ implies that $t \in \{1, 2\}$, which is impossible. Similarly, if b is odd, we find that $s \in \{1, 2\}$, which is again impossible. This completes the proof of the first claim of part (b). The second claim then follows readily. □

Lemma 8.6. *Fix positive integers j, k, and m with $j+2k-1 \leqslant m$. Consider the linear subspace $\mathcal{R}_p(j,k)$ of $\mathcal{R}_p^{\mathsf{sh}}(m)$ consisting of all polynomials of the form*

$$C(T) = T^m \sum_{i=0}^{2k-1} c_i (T^{j+i} + T^{-j-i}) \quad \text{with } c_0, c_1, \dots, c_{2k-1} \in \mathbf{F}_p. \tag{8.2}$$

Fix $D \in \mathcal{R}_p(k)$; in case $p = 2$, assume in addition that $T^2+1 \nmid D$. Then

$$\mathcal{R}_p(j,k) \to \mathcal{R}_p^{\mathsf{sh}}(m), \quad C \mapsto C \bmod D$$

is a linear map that surjects onto $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$.

Proof. Let $i \geqslant 0$ be an integer. The Chebyshev polynomial $C_{j+i} \in \mathbf{F}_p[T]$ is monic of degree $j+i > 0$. Hence the span V of the polynomials $C_j, C_{j+1}, \dots, C_{j+2k-1}$ over $\mathbf{F}_p$ is of dimension $2k$. Since $k \leqslant m$ here, tracing the proof of Lemma 8.1 we find that we may split the map that sends an element $C \in \mathcal{R}_p(j,k)$ to its reciprocal remainder $C \bmod D$ into three pieces:

$$\begin{array}{ccccccc} \mathcal{R}_p(j,k) & \xrightarrow{(-)_{\mathsf{R},m}} & V & \xrightarrow{\bmod D_{\mathsf{R}}} & \mathbf{F}_p[T]_{\leqslant k-1} & \xrightarrow{(-)^{\mathsf{R},m}} & T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1) \\ C & \longmapsto & C_{\mathsf{R},m} & \longmapsto & C_{\mathsf{R},m} \bmod D_{\mathsf{R}} & \longmapsto & C \bmod D. \end{array} \tag{8.3}$$

The third map is a linear isomorphism by Lemma 5.3. The first map is also a linear isomorphism by Lemma 5.3; indeed, domain and codomain are of equal dimension over $\mathbf{F}_p$, and given C as in (8.2), we have

$$C_{\mathsf{R},m}(T) = \sum_{i=0}^{2k-1} c_i C_{j+i}(T) \in V.$$

It remains to show that the linear map in the middle of (8.3) is surjective.

Firstly, using (5.2) and induction on ℓ, we have the formula

$$T^\ell C_a = \sum_{i=0}^{\ell} \binom{\ell}{i} C_{a+\ell-2i} \tag{8.4}$$

for any integers a and $\ell \geqslant 0$. Let $\ell \in \{0, 1, \dots, k-1\}$. In particular, we find that the polynomials $T^\ell C_{j+k-1}(T)$ and $T^\ell C_{j+k}(T)$ lie in V.

Secondly, note that the map $\bmod D_{\mathsf{R}} \colon V \to \mathbf{F}_p[T]_{\leqslant k-1}$ is the same as first sending an element of V to $\mathbf{F}_p[T]/(D_{\mathsf{R}})$ by reduction modulo D_{R}, and then picking the unique representative of its image that is of degree $< k$. Now, if $p \neq 2$ then C_{j+k-1} and C_{j+k} are coprime over $\mathbf{F}_p$ by Lemma 8.5(a). Hence there exist polynomials $F, G \in \mathbf{F}_p[T]$ such that $FC_{j+k-1} + GC_{j+k} = 1$ in $\mathbf{F}_p[T]$, and the same equality also holds in $\mathbf{F}_p[T]/(D_{\mathsf{R}})$. Denote by F_ℓ the unique lift of $T^\ell F \bmod D_{\mathsf{R}} \in \mathbf{F}_p[T]/(D_{\mathsf{R}})$ to $\mathbf{F}_p[T]$ that is of degree $< k$, and let G_ℓ be a similar lift of $T^\ell G$. Then the polynomials $F_\ell C_{j+k-1} + G_\ell C_{j+k} \in \mathbf{F}_p[T]$ with $\ell = 0, 1, \dots, k-1$ all lie in V by the discussion in the preceding paragraph. Therefore the reduction $F_\ell C_{j+k-1} + G_\ell C_{j+k} = T^\ell \bmod D_{\mathsf{R}} \in \mathbf{F}_p[T]_{\leqslant k-1}$ lies in the image of V under the reduction map modulo D_{R}. This finishes the proof for odd p.

Similarly, if $p = 2$, then $(C_{j+k-1}, C_{j+k}) = T$ by Lemma 8.5(b). So there exist polynomials F' and G' such that $F'C_{j+k-1} + G'C_{j+k} = T$ in $\mathbf{F}_p[T]$. Since $T^2 + 1$ does not divide D, the trace polynomial D_{R} is coprime with T, so there exists a polynomial $H \in \mathbf{F}_p[T]$ so that $HF'C_{j+k-1} + HG'C_{j+k} = 1 \in \mathbf{F}_p[T]/(D_{\mathsf{R}})$. We now set $F = HF'$ and $G = HG'$ and repeat the same steps as in the case of $p \neq 2$ above to finish the proof for $p = 2$ as well. □

9. Character theory and special residues

Sections §§9–12 are dedicated to proving Proposition 2.5. The present section consists of preparatory work for the Fourier analysis carried out in §§10–12.

Denote by $\mathcal{P} = \{p_1, \dots, p_r\}$ a set of r (distinct) primes. For reasons explained in §2, we need to control the joint divisor structure distribution of $\boldsymbol{A} = (A_p)_{p\in\mathcal{P}}$ inside $\mathbf{F}_{\mathcal{P}}[T] \coloneqq \prod_{p\in\mathcal{P}} \mathbf{F}_p[T]$. We first introduce the theoretical framework, mostly following [7]. Let $\boldsymbol{k} = (k_p) \in \mathbf{Z}_{\geqslant 0}^r$ be a tuple of nonnegative integers. Denote by $\boldsymbol{D} = (D_p)_{p\in\mathcal{P}}$ a tuple of reciprocal polynomials in $\mathbf{F}_{\mathcal{P}}[T]$, with $D_p \in \mathcal{R}_p(k_p)$; briefly, we will write $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k})$ for this datum. Define $\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D}) \coloneqq \prod_{p\in\mathcal{P}} \mathbf{F}_p[T]/(D_p)$. In similar fashion, denote $\boldsymbol{B} \bmod \boldsymbol{D} \coloneqq (B_p \bmod D_p)_{p\in\mathcal{P}} \in \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$.

As $\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$ is an abelian group for addition, we may apply Fourier inversion to expand the indicator function of $\boldsymbol{A} \equiv \boldsymbol{C} \bmod \boldsymbol{D}$ as a sum of characters. Denote by $\mathbf{F}_p((1/T))$ the field of Laurent series $X(T) = \sum_{-\infty<j\leqslant J} c_j T^j$ where $J \in \mathbf{Z}$ and $c_j \in \mathbf{F}_p$. For $X \in \mathbf{F}_p((1/T))$, set $\operatorname{res}(X) \coloneqq c_{-1}$. Define $\mathbf{F}_{\mathcal{P}}((1/T)) \coloneqq \prod_{p\in\mathcal{P}} \mathbf{F}_p((1/T))$ and $\operatorname{res}(\boldsymbol{X}) \coloneqq (\operatorname{res}(X_p))_{p\in\mathcal{P}}$, and let

$$\psi_{\mathcal{P}} \colon \mathbf{F}_{\mathcal{P}}((1/T)) \to \mathbf{R}/\mathbf{Z}, \quad \psi_{\mathcal{P}}(\boldsymbol{X}) \coloneqq \sum_{p\in\mathcal{P}} \frac{\operatorname{res}(X_p)}{p}.$$

In addition, set

$$\psi_{\mathcal{P}}^{(m,j)}(\boldsymbol{X}) \coloneqq \begin{cases} \psi_{\mathcal{P}}(T^m \boldsymbol{X}) & \text{if } j = 0 \\ \psi_{\mathcal{P}}(T^{m-j}\boldsymbol{X} + T^{m+j}\boldsymbol{X}) & \text{if } j \neq 0, \end{cases}$$

where, for each i, the expression $T^i\boldsymbol{X}$ is shorthand for the tuple $(T^i X_p)_{p\in\mathcal{P}}$. We use the notation $\psi_p \coloneqq \psi_{\{p\}}$ and $\psi_p^{(m,j)} \coloneqq \psi_{\{p\}}^{(m,j)}$. Lastly, recall the notation $e(x) \coloneqq \exp(2\pi i x)$.

Major and minor residues. Fix $m \in \mathbf{Z}_{\geqslant 0}$, $\boldsymbol{k} \in \mathbf{Z}_{\geqslant 0}^r$ and $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k})$. Denote by $R_m(\boldsymbol{D})$ the Cartesian product

$$R_m(\boldsymbol{D}) \coloneqq \prod_{p \in \mathcal{P}} R_m(D_p) \subset \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D}), \tag{9.1}$$

with $R_m(D_p)$ as in Definition 8.4. If $k_p \leqslant m+1$ for all $p \in \mathcal{P}$, Lemma 8.3 ensures that $R_m(\boldsymbol{D})$ is also the image of $\mathcal{R}_{\mathcal{P}}^{\mathsf{sh}}(m)$ inside $\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$. We have $\boldsymbol{A} \bmod \boldsymbol{D} \in R_m(\boldsymbol{D})$ for any $\boldsymbol{D}$, but if $k_p > m+1$ for some p, then $\boldsymbol{A} \bmod \boldsymbol{D}$ will a priori (i.e., without knowing anything about the probability distribution on $\boldsymbol{A}$) already lie in a proper subset of $R_m(\boldsymbol{D})$.

The set $R_m(\boldsymbol{D})$ is a subgroup of the additive abelian group of $\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$. Moreover, the usual multiplication by the ring $\mathbf{F}_{\mathcal{P}}$ endows it with a module structure over $\mathbf{F}_{\mathcal{P}}$.

Let us now consider the maps

$$\widetilde{\chi}_{\boldsymbol{B}} \colon \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D}) \to \mathbf{C}^\times, \quad \boldsymbol{C} \mapsto e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D}))$$

with $\boldsymbol{B}$ varying over a complete set of residue classes modulo $\boldsymbol{D}$. They form a complete set of characters of the group $\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$. We then introduce the following important notions:

Definition 9.1 (Major and minor residues)**.** Let m, $\mathcal{P}$ and $\boldsymbol{D}$ be as above. We write $N_m(\boldsymbol{D})$ for the set of residues $\boldsymbol{B} \in \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$ for which the restriction $\chi_{\boldsymbol{B}} \coloneqq \widetilde{\chi}_{\boldsymbol{B}}\big|_{R_m(\boldsymbol{D})}$ is trivial. We call these the *major residues* modulo $\boldsymbol{D}$.

On the other hand, we shall refer to the residues $\boldsymbol{B}$ mod $\boldsymbol{D}$ that do not lie in $N_m(\boldsymbol{D})$ as the *minor residues*.

The set $N_m(\boldsymbol{D})$ is an abelian group. Moreover, since $R_m(D)$ is an $\mathbf{F}_{\mathcal{P}}$-module, so is $N_m(\boldsymbol{D})$. Hence, the quotient

$$\mathcal{L}_m(\boldsymbol{D}) \coloneqq (\mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D}))/N_m(\boldsymbol{D})$$

is an $\mathbf{F}_{\mathcal{P}}$-module as well.

Lemma 9.2. *Let m, $\mathcal{P}$ and $\boldsymbol{D}$ be as above.*

(a) The maps

$$\chi_{\boldsymbol{B}} \colon R_m(\boldsymbol{D}) \to \mathbf{C}^\times, \quad \boldsymbol{C} \mapsto e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})),$$

with $\boldsymbol{B}$ mod $\boldsymbol{D}$ varying over any complete set of representatives of the cosets of $N_m(\boldsymbol{D})$ in $\mathbf{F}_p[T]/(\boldsymbol{D})$, form a complete set of characters for $R_m(\boldsymbol{D})$.

(b) The set $N_m(\boldsymbol{D})$ has cardinality $\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}$.

Remark. In view of part (b) of Lemma 9.2 above, for each $p \in \mathcal{P}$ the component

$$\mathcal{L}_m(D_p) \coloneqq (\mathbf{F}_p[T]/(D_p))/N_m(D_p)$$

of $\mathcal{L}_m(\boldsymbol{D})$ is a vector space of dimension $\deg(D_p)/2$ over $\mathbf{F}_p$.

Proof. For a group G, denote by $\hat{G}$ its group of characters. If $H \leqslant G$ is a subgroup, set

$$H^\perp \coloneqq \{\chi \in \hat{G} : \chi = 1 \text{ on } H\}.$$

(a) We use a fundamental result from character theory: if G is a finite abelian group and $H \leqslant G$ a subgroup, then each character of H can be extended to a character of G. In other words, the restriction map $\hat{G} \to \hat{H}$ defined by $\chi \mapsto \chi|_H$ is a surjective homomorphism. It has kernel $H^\perp$, so we obtain the isomorphism $\hat{G}/H^\perp \cong \hat{H}$. Applying these results to the group $G = \mathbf{F}_{\mathcal{P}}[T]/(\boldsymbol{D})$ and the subgroup $H = R_m(\boldsymbol{D})$ yields the claim. This is because the paragraph preceding Definition 9.1 implies that we may identify $\hat{G}$ with G, and $H^\perp$ with $N_m(\boldsymbol{D})$.

(b) If G and H are in the end of the proof of part (a), then the above discussion implies that $|N_m(\boldsymbol{D})| = |H^\perp| = |\hat{G}|/|\hat{H}| = |G|/|H|$, where we used that a finite abelian group is isomorphic to its own character group. Since $|G| = \|\boldsymbol{D}\|_{\mathcal{P}} = \prod_{p \in \mathcal{P}} p^{2k_p}$ and $|H| = |R_m(\boldsymbol{D})| = \prod_{p \in \mathcal{P}} p^{k_p}$, the proof of the lemma is complete. □

Next is a basic result regarding the multiplicative relations between the various sets of major residues.

Lemma 9.3. *Let p be a prime, let $D, D' \in \mathcal{R}_p$, and let B be a residue modulo D.*

(a) The projection $\mathbf{F}_p[T]/(DD') \to \mathbf{F}_p[T]/(D)$ given by reduction modulo D restricts to a surjection $R_m(DD') \to R_m(D)$.

(b) We have $B \in N_m(D)$ if, and only if, $BD' \in N_m(DD')$.

Proof. (a) Let $\deg(D) = 2k$ and $\deg(D') = 2k'$. Assume the convention that $\mathcal{R}_p^{\mathsf{sh}}(-1) = \{0\}$. Then, for every $C \in R_m(DD')$, there exists a polynomial $F' \in \mathcal{R}_p^{\mathsf{sh}}(k + k' - 1)$ such that $C \equiv T^{m-k-k'+1}F' \bmod DD'$. So $C \equiv T^{m-k-k'+1}F' \bmod D$. By Lemma 8.3, there is a polynomial $F \in \mathcal{R}_p^{\mathsf{sh}}(k-1)$ such that $F' \equiv T^{(k+k'-1)-(k-1)}F \equiv T^{k'}F \bmod D$. So $C \equiv T^{m-k+1}F \bmod D$.

Lastly, we prove that the map $R_m(DD') \to R_m(D)$ is surjective. If $k = 0$, then the claim is trivial because $R_m(D) = \{0\}$ in this case. Assume now that $k \geqslant 1$ and consider $C \in R_m(D)$. We thus have $C \equiv T^{m-k+1}F \bmod D$ for some $F \in \mathcal{R}_p^{\mathsf{sh}}(k-1)$. The polynomial $F = T^{k'}F$ is $(k' + k - 1)$-shifted reciprocal (see remark (c) following Definition 5.1). Hence, if we let C' be the class of $T^{m-k-k'+1}F'$ modulo DD', then $C' \in R_m(DD')$ and $C' \equiv C \bmod D$. This proves the claim that the map $R_m(DD') \to R_m(D)$ is surjective.

(b) Let $B \in N_m(D)$. For each $C' \in R_m(DD')$, we must show that $\psi_p(C'BD'/(DD')) = 0$. Indeed, we have $\psi_p(C'BD'/(DD')) = \psi_p(C'B/D)$. Moreover, part (a) implies the existence of $C \in R_m(D)$ such that $C' \equiv C \bmod D$. We thus have $\psi_p(C'B/D) = \psi_p(CB/D) = 0$ by our assumption that $B \in N_m(D)$.

Conversely, assume that B is a residue modulo D such that $BD' \in N_m(DD')$. For each $C \in R_m(D)$, we must show that $\psi_p(CB/D) \equiv 0 \bmod 1$. Indeed, by part (a), there exists $C' \in R_m(DD')$ such that $C' \equiv C \bmod D$. Thus $\psi_p(CB/D) \equiv \psi_p(C'B/D) \equiv \psi_p((C'BD')/(DD')) \bmod 1$, with the last equality following from our assumption that $BD' \in N_m(DD')$. □

We will also use the following more amenable characterisation of the major residues:

Lemma 9.4. *Let p be a prime, let $m \in \mathbf{Z}_{\geqslant 0}$, let $k \in \mathbf{Z}_{\geqslant 1}$, and let $D \in \mathcal{R}_p(k)$. A residue $B \bmod D$ lies in $N_m(D)$ if, and only if,*

$$\psi_p^{(m,j)}(B/D) \equiv 0 \bmod 1 \quad \text{for } j = 0, 1, \ldots, k-1.$$

Proof. By definition, $B \in N_m(D)$ if, and only if, $\psi_p(CB/D) \equiv 0 \bmod 1$ for all $C \in R_m(D)$. Since $R_m(D)$ is the image of $T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1) \bmod D$, this is equivalent to having

$$\psi_p\left(\frac{(c_{k-1}T^{m-k+1} + \cdots + c_1T^{m-1} + c_0T^m + c_1T^{m+1} + \cdots + c_{k-1}T^{m+k-1})B}{D}\right) \equiv 0 \bmod 1$$

for all $c_0, \ldots, c_{k-1} \in \mathbf{F}_p$. By $\mathbf{F}_p$-linearity of ψ_p, this is equivalent to having $\psi_p^{(m,j)}(B/D) \equiv 0 \bmod 1$ for all $j \in \{0, 1, \ldots, k-1\}$. □

Good representatives. The goal of this section is to establish the existence of a set of 'good' representatives for the quotient $\mathcal{L}_m(D)$ of $N_m(D)$ inside $\mathbf{F}_p[T]/(D)$. More precisely, we find such representatives for all D at once.

Definition 9.5 (Good representatives)**.** A collection of sets

$$L_m := \{L_m(D) : D \in \mathcal{R}_p\}$$

is a *system of good representatives* if it satisfies the following properties for all $D \in \mathcal{R}_p$:

(1) $L_m(D) \subset \mathbf{F}_p[T]/(D)$ is a complete set of representatives for the cosets of $N_m(D)$ in $\mathcal{L}_m(D)$;

(2) if $B \in L_m(D)$, then $\deg(B, D)_{\boldsymbol{r}}$ is maximal among all $B' \in B + N_m(D)$;

(3) if $B \in L_m(D)$, then $B/(B,D)_{\boldsymbol{r}} \in L_m(D/(B,D)_{\boldsymbol{r}})$.

Lemma 9.6. *A system L_m of good representatives exists.*

Proof. Any coset of $N_m(D)$ can certainly be represented by some $B \in \mathbf{F}_p[T]/(D)$ that satisfies property (2). Thus we can adhere to properties (1) and (2) of Definition 9.5, and it remains to show that we can achieve property (3) simultaneously. To prove the claim, we will construct each layer

$$L_{m,k} \coloneqq \big\{L_m(D) \subset \mathbf{F}_p[T]/(D) : D \in \mathcal{R}_p(k)\big\} \subset L_m$$

separately, by induction on k.

For $k = 0$ we only have $D = 1$ with the residue $B = 0$, and indeed $L_m(1) = \{0\}$ satisfies all properties. Next, suppose we have constructed layers $L_{m,j}$ for all $j < k$. Let $D \in \mathcal{R}_p(k)$ and suppose we have a set $L'_m(D)$ satisfying properties (1) and (2), that is to say, we know that: (1) $L'_m(D)$ is a complete set of representatives for the cosets of $N_m(D)$ in $\mathcal{L}_m(D)$; (2) if $B' \in L'_m(D)$, then $\deg (B',D)_{\boldsymbol{r}}$ is maximal among all $B'' \in B' + N_m(D)$. We now show how to construct $L_m(D)$ that also satisfies property (3).

Let $B' \in L'_m(D)$ and write $K = (B',D)_{\boldsymbol{r}}$. We will find some $B \equiv B' \bmod N_m(D)$ for which properties (2) and (3) are both satisfied, so we will use this B as the choice in $L_m(D)$ of the representative of the class of B'.

- If $K = 1$, property (3) is trivially true, so we simply take $B = B'$.
- If $K \neq 1$, set $B' = GK$ and $D = HK$. Since $\deg H < \deg D$, there exists $N \in N_m(H)$ such that $G+N \in L_m(H)$ by the induction hypothesis and property (1) applied to H. We claim that we may take $B = B' + NK$. Indeed, we have $NK \in N_m(D)$ by Lemma 9.3(b), and thus $B \equiv B' \bmod N_m(H)$ as needed. Moreover, we have $(B' + NK, D)_{\boldsymbol{r}} = K = (B',D)_{\boldsymbol{r}}$, which is maximal within the coset of B', and thus of B, modulo $N_m(H)$. Lastly, we have $B/K = G + N \in L_m(H)$, so B satisfies property (3) as well.

This completes the inductive construction of L_m. □

The proof of Lemma 9.6 does not indicate whether such a system L_m is unique. In fact, it is not: for example, if D is irreducible, $L_m(D)$ can be any complete set of representatives as properties (2) and (3) are trivial. However, the proof does show that our freedom in constructing L_m lies at most in the choice of the *minimal residues*:

Definition 9.7 (Minimal residues)**.** If $G \in L_m(H)$ and $(G,H)_{\boldsymbol{r}} = 1$, then we call G a *minimal residue* modulo H. In this case, we also say that G/H is a *minimal* or *reduced* fraction, that (G,H) is a *minimal pair*, and that the equivalence class of G in $\mathcal{L}_m(H)$ is a *minimal class*.

We will consider L_m, and hence the sets $L_m(D)$, to be fixed from now on, for all p. We then also adopt the notational convention

$$L_m(\boldsymbol{D}) = \prod_{p \in \mathcal{P}} L_m(D_p).$$

for all r-tuples $\boldsymbol{D} = (D_p)_{p\in\mathcal{P}}$ such that $D_p \in \mathcal{R}_p$ for all $p \in \mathcal{P}$.

Crossing residues. This section provides crucial input for the L^1 bounds that will be established in §12.

By Lemma 9.3(b), there are multiplicative relations between the sets $N_m(D)$ as $D \in \mathbf{F}_p[T]$ varies: if $B_0 \in N_m(D_0)$, then $B_0D_1 \in N_m(D_0D_1)$. (The subscripts no longer refer to indices of the tuple $\boldsymbol{D}$.) Swapping the roles of D_0 and D_1, and recalling that $N_m(D_0D_1)$ is an abelian group, we obtain the bilinear map

$$\Psi\colon N_m(D_0) \times N_m(D_1) \to N_m(D_0D_1), \quad (B_0,B_1) \mapsto B_0D_1 - B_1D_0. \tag{9.2}$$

We may ask to what extent $N_m(D_0D_1)$ can be generated from $N_m(D_0)$ and $N_m(D_1)$ alone:

Lemma 9.8. *Let p be a prime, and let $D_0, D_1 \in \mathcal{R}_p$ be coprime. Then the map Ψ defined in (9.2) is a bijection.*

Proof. Since the cardinalities of $N_m(D_0) \times N_m(D_1)$ and $N_m(D_0D_1)$ are finite and equal by Lemma 9.2(b), it suffices to show that the map Ψ is injective. Let $(B_0, B_1), (B_0', B_1') \in N_m(D_0) \times N_m(D_1)$ and suppose $B_0D_1 - B_1D_0 = B_0'D_1 - B_1'D_0$. Then $(B_0 - B_0')D_1 = (B_1 - B_1')D_0$. Since D_0 and D_1 are coprime, we find that D_0 divides $B_0 - B_0'$ and D_1 divides $B_1 - B_1'$. Hence $B_0 = B_0'$ and $B_1 = B_1'$. □

Definition 9.9 (Crossing residues)**.** Let p be a prime, let $H_0, H_1 \in \mathcal{R}_p$, and consider residues $G_0 \bmod H_0$ and $G_1 \bmod H_1$. We then say that the pairs (G_0, H_0) and (G_1, H_1) are (a pair of) *crossing residues* if $G_0H_1 - G_1H_0 \in N_m(H_0H_1)$.

The next statement, a supplement to Lemma 9.8, says that there are no nontrivial minimal crossing residues.

Lemma 9.10. *Let p be a prime, let $H_0, H_1 \in \mathcal{R}_p$, and consider minimal residues $G_0 \in L_m(H_0)$ and $G_1 \in L_m(H_1)$. If $G_0H_1 - G_1H_0 \in N_m(H_0H_1)$, then $H_0 = H_1$ and $G_0 = G_1$.*

Proof. Write $K = (H_0, H_1)_{\boldsymbol{r}} = (H_0, H_1)$ and fix a factorisation $K = K_0K_1$ such that H_0/K_0 and H_1/K_1 are both reciprocal and coprime to each other (cf. Proposition 2.2). Lemma 9.3(b) yields that

$$G_0\frac{H_1}{K} - G_1\frac{H_0}{K} \in N_m\Big(\frac{H_0H_1}{K}\Big) = N_m\Big(\frac{H_0}{K_0}\frac{H_1}{K_1}\Big).$$

Hence by Lemma 9.8, there are $\overline{G}_0 \in N_m(H_0/K_0)$ and $\overline{G}_1 \in N_m(H_1/K_1)$ such that

$$G_0\frac{H_1}{K} - G_1\frac{H_0}{K} = \overline{G}_0\frac{H_1}{K_1} - \overline{G}_1\frac{H_0}{K_0} = \overline{G}_0K_0\frac{H_1}{K} - \overline{G}_1K_1\frac{H_0}{K}.$$

Therefore $(G_0 - \overline{G}_0K_0)H_1/K = (G_1 - \overline{G}_1K_1)H_0/K$. Since H_1/K and H_0/K are also coprime, the polynomial H_0/K divides $G_0 - \overline{G}_0K_0$. On the other hand, we have $\overline{G}_0K_0 \in N_m(H_0)$ by Lemma 9.3(b), so G_0 and $\overline{G}_0K_0$ belong to the same class in $\mathcal{L}_m(H_0)$. Since $G_0 \in L_m(H_0)$ is minimal, G_0 and H_0 are reciprocally coprime. Hence the second property of Definition 9.5 of the system L_m guarantees that $G_0 - \overline{G}_0K_0$ and H_0 are also reciprocally coprime. So H_0/K, itself being reciprocal, can only divide $G_0 - \overline{G}_0K_0$ if $K = H_0$.

By the same argument applied to H_1 instead of H_0, we find that $K = H_1$. In particular, $H_0 = H_1$. Hence $G_0, G_1 \in L_m(H_0)$ and $(G_0 - G_1)H_1 \in N_m(H_0H_1)$. Using Lemma 9.3(b), we conclude that $G_0 - G_1 \in N_m(H_0)$. Thus, G_0 and G_1 represent the same class in $\mathcal{L}_m(H_0)$, implying that $G_0 = G_1$. □

10. Fourier analysis on $\mathcal{R}_{\mathcal{P}}$

In this section, we develop the necessary tools from Fourier analysis for reciprocal polynomials in order to establish Proposition 2.5.

Lemma 10.1 (Fourier inversion)**.** *Let $\mathcal{P}$ be a finite set of primes, let $\boldsymbol{D} = (D_p)_{p\in\mathcal{P}}$ be such that $D_p \in \mathcal{R}_p$ for each p, let $m \in \mathbf{Z}_{\geqslant 0}$, and let $\boldsymbol{C} \in R_m(\boldsymbol{D})$. Then*

$$\frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\boldsymbol{B}\in L_m(\boldsymbol{D})} e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})) = 1_{\boldsymbol{C}\equiv\boldsymbol{0} \bmod \boldsymbol{D}}.$$

Proof. Observe that

$$\sum_{\boldsymbol{B} \bmod \boldsymbol{D}} e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})) = \sum_{\boldsymbol{B}\in L_m(\boldsymbol{D})} \sum_{\boldsymbol{B}'\in N_m(\boldsymbol{D})} e(\psi_{\mathcal{P}}(\boldsymbol{C}(\boldsymbol{B}+\boldsymbol{B}')/\boldsymbol{D})).$$

Since $e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})) = e(\psi_{\mathcal{P}}(\boldsymbol{C}(\boldsymbol{B}+\boldsymbol{B}')/\boldsymbol{D}))$ for any $\boldsymbol{B}' \in N_m(\boldsymbol{D})$, and we know from Lemma 9.2(b) that $N_m(\boldsymbol{D})$ contains $\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}$ elements, we find that

$$\frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}} \sum_{\boldsymbol{B} \bmod \boldsymbol{D}} e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})) = \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\boldsymbol{B} \in L_m(\boldsymbol{D})} e(\psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})).$$

By the orthogonality relations for characters mod p, the former sum is equal to the indicator function $1_{\forall \boldsymbol{B} \bmod \boldsymbol{D} \colon \psi_{\mathcal{P}}(\boldsymbol{CB}/\boldsymbol{D})=0} = 1_{\boldsymbol{C} \equiv \boldsymbol{0} \bmod \boldsymbol{D}}$. □

Let $A \in \mathbf{Z}[T]$ be a random reciprocal polynomial selected according to $\mathbb{P}_{\mathcal{R}(m)}$ and denote by $\boldsymbol{A}$ the induced tuple in $\mathcal{R}_{\mathcal{P}}(m)$. Fixing $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k})$ and $\boldsymbol{C} \in R_m(\boldsymbol{D})$, and replacing $\boldsymbol{C}$ in Lemma 10.1 by $\boldsymbol{A} - \boldsymbol{C}$, we find

$$\begin{aligned}\mathbb{P}_{\mathcal{R}_{\mathcal{P}}(m)}\big(\boldsymbol{A} \equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) &= \mathbb{E}_{\mathcal{R}_{\mathcal{P}}(m)}\left[\frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\boldsymbol{B} \in L_m(\boldsymbol{D})} e(\psi_{\mathcal{P}}((\boldsymbol{A}-\boldsymbol{C})\boldsymbol{B}/\boldsymbol{D}))\right] \\ &= \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\boldsymbol{B} \in L_m(\boldsymbol{D})} e(\psi_{\mathcal{P}}(-\boldsymbol{CB}/\boldsymbol{D}))\mathbb{E}_{\mathcal{R}_{\mathcal{P}}(m)}\big[e(\psi_{\mathcal{P}}(\boldsymbol{AB}/\boldsymbol{D}))\big].\end{aligned} \tag{10.1}$$

The remainder of this section follows [7, §4] to establish a first step in the proof of Proposition 2.5, namely the reduction to (10.10) below.

Lemma 10.2. *Let $m \in \mathbf{Z}_{\geqslant 0}$. For every $\boldsymbol{X} \in \mathbf{F}_{\mathcal{P}}((1/T))$, we have*

$$\mathbb{E}_{\boldsymbol{A} \in \mathcal{R}_{\mathcal{P}}(m)}\big[e(\psi_{\mathcal{P}}(\boldsymbol{AX}))\big] = e(\psi_{\mathcal{P}}(\boldsymbol{X} + T^{2m}\boldsymbol{X})) \prod_{j=0}^{m-1} \hat{\mu}_j\big(\psi_{\mathcal{P}}^{(m,j)}(\boldsymbol{X})\big). \tag{10.2}$$

Proof. We argue similarly to the proof of [7, Lemma 4.1]. Let $A \in \mathcal{R}(m)$ be a polynomial sampled according to the measure $\mathbb{P}_{\mathcal{R}(m)}$, and let A_p be each reduction modulo p. We may thus write $A = a_m + a_{m-1}T + \cdots + a_0T^m + a_1T^{m+1} + \cdots + a_mT^{2m}$, where $a_m = 1$. As a consequence, we have

$$e(\psi_{\mathcal{P}}(\boldsymbol{AX})) = e(a_0\psi_{\mathcal{P}}(T^m\boldsymbol{X})) \prod_{j=1}^{m} e(a_j\psi_{\mathcal{P}}(T^{m-j}\boldsymbol{X} + T^{m+j}\boldsymbol{X})). \tag{10.3}$$

The terms in the product on the right-hand side in (10.3) are independent, and we always have $a_m = 1$. Hence, taking the expectation on both sides yields the claimed (10.2). □

Let $\sigma_{\mathcal{P}}(m; \boldsymbol{X})$ be the absolute value of the right-hand side in (10.2), that is

$$\sigma_{\mathcal{P}}(m; \boldsymbol{X}) := \left|\prod_{j=0}^{m-1} \hat{\mu}_j\big(\psi_{\mathcal{P}}^{(m,j)}(\boldsymbol{X})\big)\right|.$$

Assume the notation of Lemma 10.2. By (10.1) and Lemma 10.2, followed by an application of the triangle inequality, we have

$$\max_{\boldsymbol{C} \in R_m(\boldsymbol{D})} \left|\mathbb{P}_{\boldsymbol{A} \in \mathcal{R}_{\mathcal{P}}(m)}\big(\boldsymbol{A} \equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) - \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}}\right| \leqslant \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\substack{\boldsymbol{B} \in L_m(\boldsymbol{D}) \\ \boldsymbol{B} \neq \boldsymbol{0}}} \sigma_{\mathcal{P}}(m; \boldsymbol{B}/\boldsymbol{D}).$$

Let $k \in \mathbf{Z}_{\geqslant 1}$, recall the definition of $\Delta_{\mathcal{P}}^{\mathsf{R}}(m; k)$ from (2.2), and recall also Lemma 8.1 and Definition 8.4. Using the above inequality, we find that

$$\Delta_{\mathcal{P}}^{\mathsf{R}}(m; k) \leqslant \sum_{\substack{\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}} \\ \deg \boldsymbol{D} \leqslant 2k}} \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\substack{\boldsymbol{B} \in L_m(\boldsymbol{D}) \\ \boldsymbol{B} \neq \boldsymbol{0}}} \sigma_{\mathcal{P}}(m; \boldsymbol{B}/\boldsymbol{D}). \tag{10.4}$$

Write $L_m(\boldsymbol{k})$ for the set of all tuples $(\boldsymbol{B}, \boldsymbol{D})$ with $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k})$ and $\boldsymbol{B} \in L_m(\boldsymbol{D})$. Then

$$\sum_{\substack{\boldsymbol{D}\in\mathcal{R}_{\mathcal{P}}\\ \deg \boldsymbol{D}\leqslant 2k}} \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\substack{\boldsymbol{B}\in L_m(\boldsymbol{D})\\ \boldsymbol{B}\neq\boldsymbol{0}}} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}) = \sum_{\substack{\boldsymbol{k}:k_p\leqslant k\\ \forall p\in\mathcal{P}}} \frac{1}{\prod_{p\in\mathcal{P}} p^{k_p}} \sum_{\substack{(\boldsymbol{B},\boldsymbol{D})\in L_m(\boldsymbol{k})\\ \boldsymbol{B}\neq\boldsymbol{0}}} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}). \quad (10.5)$$

For each $\boldsymbol{\ell} \in \mathbf{Z}^r_{\geqslant 0}$, let $L_m(\boldsymbol{k}, \boldsymbol{\ell})$ be the subset of $L_m(\boldsymbol{k})$ consisting of all $(\boldsymbol{B}, \boldsymbol{D})$ for which the corresponding minimal pair $(\boldsymbol{G}, \boldsymbol{H}) = (\boldsymbol{B}/(\boldsymbol{B}, \boldsymbol{D})_{\boldsymbol{r}}, \boldsymbol{D}/(\boldsymbol{B}, \boldsymbol{D})_{\boldsymbol{r}})$ lies in $L_m(\boldsymbol{\ell})$. Then

$$\sum_{\substack{(\boldsymbol{B},\boldsymbol{D})\in L_m(\boldsymbol{k})\\ \boldsymbol{B}\neq\boldsymbol{0}}} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}) = \sum_{\substack{\boldsymbol{\ell}\neq\boldsymbol{0}\\ \ell_p\leqslant k\ \forall p\in\mathcal{P}}} \sum_{(\boldsymbol{B},\boldsymbol{D})\in L_m(\boldsymbol{k},\boldsymbol{\ell})} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}), \quad (10.6)$$

where we used property (3) of Definition 9.5. The set $L_m(\boldsymbol{k}, \boldsymbol{\ell})$ is nonempty only if $\ell_p \leqslant k_p$ for all $p \in \mathcal{P}$. Conversely, if $\ell_p \leqslant k_p$ for all $p \in \mathcal{P}$, and $\boldsymbol{G}/\boldsymbol{H}$ is a minimal fraction in $L_m(\boldsymbol{\ell})$, then the pair $(\boldsymbol{GK}, \boldsymbol{HK})$ lies in $L_m(\boldsymbol{k}, \boldsymbol{\ell})$ if, and only if, $\boldsymbol{K} \in \mathcal{R}_{\mathcal{P}}(\boldsymbol{k} - \boldsymbol{\ell})$, which is nonempty. Therefore

$$\begin{aligned}\sum_{(\boldsymbol{B},\boldsymbol{D})\in L_m(\boldsymbol{k},\boldsymbol{\ell})} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}) &= \sum_{\boldsymbol{K}\in\mathcal{R}_p(\boldsymbol{k}-\boldsymbol{\ell})} \sum_{\substack{(\boldsymbol{G},\boldsymbol{H})\in L_m(\boldsymbol{\ell})\\ (\boldsymbol{G},\boldsymbol{H}) \text{ minimal}}} \sigma_{\mathcal{P}}(m;\boldsymbol{GK}/\boldsymbol{HK})\\ &= \prod_{p\in\mathcal{P}} p^{k_p-\ell_p} \sum_{(\boldsymbol{G},\boldsymbol{H})\in L_m(\boldsymbol{\ell})}{}^{*} \sigma_{\mathcal{P}}(m;\boldsymbol{G}/\boldsymbol{H}), \quad (10.7)\end{aligned}$$

where $\sum^*$ means that the summation runs over minimal pairs $(\boldsymbol{G}, \boldsymbol{H})$. With the definition

$$\delta^{\mathsf{R}}_{\mathcal{P}}(m;\boldsymbol{\ell}) := \frac{1}{\prod_{p\in\mathcal{P}} p^{\ell_p}} \sum_{(\boldsymbol{G},\boldsymbol{H})\in L_m(\boldsymbol{\ell})}{}^{*} \sigma_{\mathcal{P}}(m;\boldsymbol{G}/\boldsymbol{H}), \quad (10.8)$$

the equalities (10.5), (10.6) and (10.7) imply

$$\sum_{\substack{\boldsymbol{D}\in\mathcal{R}_{\mathcal{P}}\\ \deg \boldsymbol{D}\leqslant 2k}} \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}^{1/2}} \sum_{\substack{\boldsymbol{B}\in L_m(\boldsymbol{D})\\ \boldsymbol{B}\neq\boldsymbol{0}}} \sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}) = \sum_{\substack{\boldsymbol{k}:k_p\leqslant k\\ \forall p\in\mathcal{P}}} \sum_{\substack{\boldsymbol{\ell}\neq\boldsymbol{0}\\ \ell_p\leqslant k_p\ \forall p\in\mathcal{P}}} \delta^{\mathsf{R}}_{\mathcal{P}}(m;\boldsymbol{\ell}). \quad (10.9)$$

From (10.4) and (10.9), we conclude

$$\Delta^{\mathsf{R}}_{\mathcal{P}}(m;k) \leqslant \sum_{\substack{\boldsymbol{k}:k_p\leqslant k\\ \forall p\in\mathcal{P}}} \sum_{\substack{\boldsymbol{\ell}\neq\boldsymbol{0}\\ \ell_p\leqslant k_p\ \forall p\in\mathcal{P}}} \delta^{\mathsf{R}}_{\mathcal{P}}(m;\boldsymbol{\ell}) \leqslant (k+1)^{2r} \max_{\substack{\boldsymbol{\ell}=(\ell_p)_{p\in\mathcal{P}}\neq\boldsymbol{0}\\ 0\leqslant\ell_p\leqslant k\ \forall p\in\mathcal{P}}} \delta^{\mathsf{R}}_{\mathcal{P}}(m;\boldsymbol{\ell}).$$

To prove Proposition 2.5, it thus suffices to show

$$\max_{\substack{\boldsymbol{\ell}=(\ell_p)_{p\in\mathcal{P}}\\ 0\leqslant\ell_p\leqslant\gamma m+m^{0.88}\ \forall p\in\mathcal{P}}} \delta^{\mathsf{R}}_{\mathcal{P}}(m;\boldsymbol{\ell}) \ll_r m^{-2r} e^{-m^{1/10}}. \quad (10.10)$$

11. L^∞ BOUNDS

In this section, we prove a bound on $\sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D})$ that is useful when the tuple $\boldsymbol{D}$ has a component of small degree.

Lemma 11.1. *Let $m \in \mathbf{Z}_{>0}$, let $\mu_0, \mu_1, \dots, \mu_{m-1}$ be probability measures on the integers, let $\mathcal{P}$ be a set of r primes whose product is P, and let $\beta \in [0,1]$ be such that*

$$\left|\hat{\mu}_j(s/P)\right| \leqslant \beta \quad \text{for all } s = 1, 2, \dots, P-1 \text{ and } j = 0, 1, \dots, m-1.$$

Let $\boldsymbol{D} \in \mathcal{R}_{\mathcal{P}}$ be such that $\deg(D_p) \leqslant 2(m+1)$ for all $p \in \mathcal{P}$, let $\boldsymbol{B} \notin N_m(\boldsymbol{D})$ be a minor residue class modulo $\boldsymbol{D}$, and let $p \in \mathcal{P}$ and $k \in [1, m+1] \cap \mathbf{Z}$ be such that $2k = \deg D_p$ and $B_p \notin N_m(D_p)$. If $p = 2$, assume in addition that $T^2 + 1 \nmid D_p$. Then

$$\sigma_{\mathcal{P}}(m;\boldsymbol{B}/\boldsymbol{D}) \leqslant \beta^{\lfloor (m+k)/(2k)\rfloor}.$$

Furthermore, such p and k exist.

Proof. To start with the very last claim, observe that since $\boldsymbol{B} \notin N_m(\boldsymbol{D})$, there exists a $p \in \mathcal{P}$ such that $B_p \notin N_m(D_p)$. Select any such p and set $D := D_p$ and $B := B_p$ and $k := (\deg D)/2$. Then $k > 0$, because for constant D there is no B available with $B \notin N_m(D)$.

Now, by Lemma 9.4, the condition $B \notin N_m(D)$ is equivalent to having

$$\operatorname{res}\left(\frac{T^m B}{D}\right) \not\equiv 0 \bmod p \quad \text{or} \quad \operatorname{res}\left(\frac{(T^{m-i}+T^{m+i})B}{D}\right) \not\equiv 0 \bmod p \text{ for some } i \in \mathbf{Z} \cap [0,k).$$

In particular, we have

$$\prod_{i=0}^{k-1} \hat{\mu}_i\big(\psi_{\mathcal{P}}^{(m,i)}(\boldsymbol{B}/\boldsymbol{D})\big) \leqslant \beta. \tag{11.1}$$

Now, let $j \in \mathbf{Z} \cap [k, m-2k]$ be such that

$$\operatorname{res}\left(\frac{(T^{m-i}+T^{m+i})B}{D}\right) \equiv 0 \bmod p \text{ for all } i \in \{j, j+1, \dots, j+2k-1\}. \tag{11.2}$$

In the notation of Lemma 8.6, by $\mathbf{F}_p$-linearity, it follows that $\operatorname{res}(CB/D) \equiv 0 \bmod p$ for any $C \in \mathcal{R}_p(j,k) \subset \mathcal{R}_p^{\mathsf{sh}}(m)$. Write $R = C \operatorname{rmod} D$ (cf. Definition 8.2). Since R and C differ by a multiple of D modulo p, we have

$$\operatorname{res}\left(\frac{RB}{D}\right) \equiv \operatorname{res}\left(\frac{CB}{D}\right) \equiv 0 \bmod p. \tag{11.3}$$

Lemma 8.6 implies that the map $\mathcal{R}_p(j,k) \to T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$ given by $C \mapsto C \operatorname{rmod} D$ is surjective. Hence (11.3) holds for any $R \in T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$. Using Lemma 9.4, this contradicts the assumption $B \notin N_m(D)$. It follows that there exists a j in any interval of $[k,m] \cap \mathbf{Z}$ of length $2k$ such that (11.2) fails to hold. That is, there is an i in any interval of $[k, m-1] \cap \mathbf{Z}$ of length $2k$ such that

$$\operatorname{res}\left(\frac{(T^{m-i}+T^{m+i})B}{D}\right) \not\equiv 0 \bmod p.$$

Hence there are at least $\lfloor (m-k)/(2k) \rfloor$ values of $i \in [k, m-1] \cap \mathbf{Z}$ such that

$$\hat{\mu}_i\big(\psi_{\mathcal{P}}^{(m,i)}(\boldsymbol{B}/\boldsymbol{D})\big) \leqslant \beta.$$

Together with (11.1), this completes the proof of the lemma. □

Remark 11.2. The condition $T^2 + 1 \nmid D_2$ in Lemma 11.1 is the origin of the same requirement in the definition of $\Delta_{\mathcal{P}}^{\mathsf{R}}$, see (2.2).

12. L^1 BOUNDS

The purpose of this section is to establish bounds of 'L^1 shape' that will allow us to prove (10.10), and thus Proposition 2.5. Before we proceed, recall the notion of minimal residues (cf. Definition 9.7).

Definition 12.1. Let p be a prime and $H \in \mathcal{R}_p$. We denote by $L_m^*(H)$ the set consisting of nonzero minimal residues $G \in L_m(H)$. Furthermore, for every $\ell \geqslant 0$, let $L_m^*(\ell) := \{(G,H) : H \in \mathcal{R}_p(\ell), G \in L_m^*(H)\}$. Similarly, if $\mathcal{P}$ is a finite set of primes and $\boldsymbol{H} \in \mathcal{R}_{\mathcal{P}}$, then we let

$$L_m^*(\boldsymbol{H}) = \big\{(\boldsymbol{G}, \boldsymbol{H}) : (G_p, H_p) \in L_m^*(H_p)\ \forall p \in \mathcal{P}\big\}.$$

Motivated by (10.8), we will develop a general bound for the quantity

$$\sum_{H\in\mathcal{R}_p(\ell)}\sum_{G\in L_m^*(H)} F_\nu(G/H),$$

where p is a prime, $m \geqslant \ell \geqslant 1$ and $\nu \geqslant 1$ are integers, $f_0, f_1, \ldots : \mathbf{R}/\mathbf{Z} \to \mathbf{R}_{\geqslant 0}$ are functions, and

$$F_\nu(X) = \prod_{j=0}^{\nu-1} f_j\big(\psi_p^{(m,j)}(X)\big) \quad \text{for each } X \in \mathbf{F}_p((1/T)). \tag{12.1}$$

We first describe a suitable cover of the 'unit circle' $\mathbf{T}_p := \{\sum_{j<0} c_j T^j \in \mathbf{F}_p((1/T))\}$. For each $X \in \mathbf{F}_p((1/T))$, let

$$\mathcal{B}_w(X) := \Big\{Y \in \mathbf{T}_p : \psi_p^{(m,j)}(Y) = \psi_p^{(m,j)}(X) \text{ for all } j = 0, 1, \ldots, w-1\Big\}.$$

Note that F_ν is constant on $\mathcal{B}_w(X)$ for $w \geqslant \nu$. In addition, these 'balls' have the property

$$Y \in \mathcal{B}_w(X) \implies \mathcal{B}_w(Y) = \mathcal{B}_w(X). \tag{12.2}$$

Lemma 12.2. *Let p be a prime, $w \in \mathbf{Z}_{\geqslant 0}$ and $X \in \mathbf{F}_p((1/T))$. Then $\mathcal{B}_w(X)$ has Haar measure p^{-w}.*

Proof. Denote by $\mathcal{Y}$ the set of all p^w elements of $\mathbf{T}_p$ of the form

$$\sum_{i=0}^{w-1} c_i T^{-m-i-1}. \tag{12.3}$$

It suffices to prove that $\mathcal{S} = \{Y + \mathcal{B}_w(X) : Y \in \mathcal{Y}\}$ is a disjoint cover of $\mathbf{T}_p$. Indeed, note that the elements of $\mathcal{S}$ are p^w translates of $\mathcal{B}_w(X)$, so the translation-invariance of the Haar measure immediately yields that the measure of $\mathcal{B}_w(X)$ is p^{-w}.

To show that $\mathcal{S}$ covers $\mathbf{T}_p$, let $Z \in \mathbf{T}_p$ and, for each $j \in \{0, 1, \ldots, w-1\}$, let $a_j \in \mathbf{F}_p$ be such that $\psi_p^{(m,j)}(Z) = a_j/p + \psi_p^{(m,j)}(X)$. For

$$Y = \sum_{i=0}^{w-1} a_i T^{-m-i-1}$$

we have $\psi_p^{(m,j)}(Y) = a_j/p$ for each j, meaning that $Z \in Y + \mathcal{B}_w(X) \in \mathcal{S}$. This proves that $\mathcal{S}$ is a cover of $\mathbf{T}_p$.

It remains to show that the elements of $\mathcal{S}$ are disjoint. Indeed, assume that $Z \in (Y_1 + \mathcal{B}_w(X)) \cap (Y_2 + \mathcal{B}_w(X))$ with $Y_1, Y_2 \in \mathcal{Y}$. Then, for each $j \in \{0, 1, \ldots, w-1\}$ we have

$$\psi_p^{(m,j)}(Z - Y_1) = \psi_p^{(m,j)}(X) = \psi_p^{(m,j)}(Z - Y_2),$$

whence $\psi_p^{(m,j)}(Y_1) = \psi_p^{(m,j)}(Y_2)$ by $\mathbf{F}_p$-linearity. Expanding the latter equality, and using that Y_1 and Y_2 are both of the form (12.3), we find that the coefficients of the monomial T^{-m-j-1} in the expansions of Y_1 and Y_2 coincide. Another application of (12.3) yields $Y_1 = Y_2$. This completes the proof of the assertion that the elements of $\mathcal{S}$ are disjoint, and thus of the lemma. □

Lemma 12.3. *Let p be a prime, let $\nu \in \mathbf{Z}_{\geqslant 0}$, let $f_0, f_1, \ldots, f_{\nu-1} : \mathbf{R}/\mathbf{Z} \to \mathbf{R}$ be functions, and let F_ν be defined by (12.1). Then*

$$\int_{\mathbf{T}_p} F_\nu(X)\,\mathrm{d}X = p^{-\nu} \prod_{j=0}^{\nu-1} \left(\sum_{\xi=0}^{p-1} f_j(\xi/p)\right).$$

Proof. Let $\mathcal{Y}$ denote the set of residues of the form (12.3) with $w = v$, and observe that F_v is constant on $Y + \mathcal{B}_v(0)$, for each $Y \in \mathcal{Y}$. Hence, the proof of Lemma 12.2 implies that

$$\int_{\mathbf{T}_p} F_v(X)\,\mathrm{d}X = \sum_{Y\in W}\int_{Y+\mathcal{B}_v(0)} F_v(X)\,\mathrm{d}X = p^{-v}\sum_{Y\in\mathcal{Y}} F_v(Y) = p^{-v}\sum_{c_0,\dots,c_{v-1}\in\mathbf{F}_p}\cdots\sum\prod_{j=0}^{v-1} f_j(c_j/p).$$

Interchanging sum and product yields the claim of the lemma statement. □

Lemma 12.4. *Assume the notation of Lemma 12.3, and let $\ell \in \mathbf{Z}_{\geqslant v/2}$. Then*

$$\sum_{H\in\mathcal{R}_p(\ell)}\sum_{G\in L_m^*(H)}\prod_{j=0}^{v-1} f_j(\psi_p^{(m,j)}(G/H)) \leqslant p^{2\ell-v}\prod_{j=0}^{v-1}\left(\sum_{\xi=0}^{p-1} f_j(\xi/p)\right). \tag{12.4}$$

Proof. Set $\mathcal{B}(X) = \mathcal{B}_{2\ell}(X)$ for any $X \in \mathbf{F}_p((1/T))$. Then F_v is constant on $\mathcal{B}(X)$ by the assumption that $\ell \geqslant v/2$. Thus the left-hand side in (12.4) equals

$$\sum_{H\in\mathcal{R}_p(\ell)}\sum_{G\in L_m^*(H)} F_v(G/H) = \sum_{H\in\mathcal{R}_p(\ell)}\sum_{G\in L_m^*(H)} p^{2\ell}\int_{\mathcal{B}(G/H)} F_v(X)\,\mathrm{d}X \tag{12.5}$$

by Lemma 12.2. Next, we show no two balls for varying G and H overlap. Let $H, H' \in \mathcal{R}_p(\ell)$ and take $G \in L_m^*(H)$ and $G' \in L_m^*(H')$. Suppose $\mathcal{B}(G'/H')$ and $\mathcal{B}(G/H)$ intersect nontrivially, in which case they must be equal (cf. (12.2)). Then for each $j \in \{0, 1, \dots, 2\ell - 1\}$ we have $\psi_p^{(m,j)}(G'/H') = \psi_p^{(m,j)}(G/H)$, that is, $\psi_p^{(m,j)}((G'H - GH')/(HH')) = 0$. Lemma 9.4 thus implies that $G'H - GH' \in N_m(HH')$. By Lemma 9.10, we find that $H = H'$ and $G = G'$ as needed.

We have thus shown that no two balls for varying G and H overlap. It follows that

$$\sum_{H\in\mathcal{R}_p(\ell)}\sum_{G\in L_m^*(H)} p^{2\ell}\int_{\mathcal{B}(G/H)} F_v(X)\,\mathrm{d}X \leqslant p^{2\ell}\int_{\mathbf{T}_p} F_v(X)\,\mathrm{d}X = p^{2\ell-v}\prod_{j=0}^{v-1}\left(\sum_{\xi=0}^{p-1} f_j(\xi/p)\right) \tag{12.6}$$

by Lemma 12.3. Combining (12.5) and (12.6) proves the result. □

Lemma 12.5. *Let $\mathcal{P}$ be a finite set of odd primes with $P := \prod_{p\in\mathcal{P}} p$. Suppose $\gamma \geqslant 1/2$ and $\alpha \geqslant 0$ are such that*

$$\sum_{k=0}^{Q-1}\left|\hat{\mu}_j(k/Q + \ell/R)\right| \leqslant \alpha Q^{1-\gamma}$$

for all $j = 0, 1, \dots, m-1$ and all $Q, R, \ell \in \mathbf{Z}$ with $QR = P$ and $Q > 1$. Let $\boldsymbol{\ell} \in \mathbf{Z}_{\geqslant 0}^r$ and $L = \max\{\ell_p : p \in \mathcal{P}\}$. Then

$$\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell}) \leqslant P^{\max\{0,\,L-\gamma m\}}\alpha^{\min\{m,\,2L\}}.$$

Proof. The needed bound follows immediately by translating the corresponding proof [7, Lemma 6.3] to our setting. In that lemma, there is a parameter s; here, we only consider the corresponding case where $s = 1$, which makes the proof here slightly easier. In particular, the proof in [7] starts by expanding their formula (4.7) (which corresponds to our (10.8)), then removing some of the terms using the trivial bound $\left|\hat{\mu}_j\right| \leqslant 1$ and applying Hölder. We do not need this step. More precisely, we need to stick with the case corresponding to $s = 1$ because we cannot carry out the Hölder procedure, see Remark 12.6 below. Note also that the letter m here corresponds to the parameter $(n-1)/s$ in the notation of [7] (which is denoted by m in [7]). □

Remark 12.6. Taking $s > 1$ in [7, Theorem 7], we find that the authors proved results that are, in their strongest form, of type "a standard polynomial B of degree n has no divisors of degree $\leqslant \theta n$" for some absolute $0 < \theta < 1/2$. As commented on in the introduction and in Remark 3.1, we do not prove such results here. Indeed, the case $s > 1$ in [7] requires using Hölder in their Lemma 6.3, which is the analogue of our Lemma 12.5. After applying Hölder, they can simply shift the residues and obtain their inequality (6.2). In contrast, such shifting of residues $\boldsymbol{G}$ mod $\boldsymbol{H}$ would not be possible after applying Hölder to the expression for our $\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell})$ (roughly (10.8)) because such shifts do not always land in $L_m^*(\boldsymbol{H})$. This *can* be circumvented by changing in the definition of our $\Delta_{\mathcal{P}}^{\mathsf{R}}$ (see (2.2)) that the sum only extends over $\boldsymbol{D}$ for which D_p is coprime with $T^{2i}+1$ for all $i = 1, 2, \dots, m$ and all $p \in \mathcal{P}$. Unfortunately, this leads to further problems in the anatomy (§13).

We now come to the proof of Proposition 2.5.

Proof of Proposition 2.5. We follow the proof of [7, Proposition 2.3]. Recall that it suffices to prove (10.10). We denote $L = \max\{\ell_p : p \in \mathcal{P}\}$.

First suppose $L \leqslant (m/\log m)^{1/2}/(2P)$. Using the assumptions with $Q = p \in \mathcal{P}$ and $\ell = 0$, we find that $\sum_{k=0}^{p-1}\left|\hat{\mu}_j(k/p)\right| \leqslant \sqrt{p}$. Combining this with [7, Equation (2.8) and Lemma 3.6], we deduce that $\left|\hat{\mu}_j(k/P)\right| \leqslant e^{-1/P^2}$ for all k not divisible by P and all $j = 0, \dots, m-1$. Thus we may apply apply the the L^∞ bound from Lemma 11.1 with $\beta = e^{-1/P^2}$ to obtain

$$\begin{aligned}\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell}) &\leqslant \prod_{p\in\mathcal{P}} p^{\ell_p} \max_{(\boldsymbol{G},\boldsymbol{H})\in L_m^*(\boldsymbol{\ell})} \sigma_{\mathcal{P}}(m;\boldsymbol{G}/\boldsymbol{H}) \leqslant P^L e^{-\lfloor (m+L)/(2L)\rfloor/P^2} \\ &\ll \exp(L\log P - m/(2LP^2)).\end{aligned}$$

Eliminating L and then P using the assumption $P \leqslant m^{1/4}$ shows

$$L\log P - \frac{m}{2LP^2} \leqslant \frac{m^{1/2}(\log P - 2\log m)}{2P(\log P)^{1/2}} \leqslant -\frac{7}{8}m^{1/4}(\log m)^{1/2},$$

which is $\leqslant -m^{1/5}$ since $m \geqslant P^4 \geqslant 16$. Hence

$$\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell}) \ll e^{-m^{1/5}},$$

proving (10.10) in this regime.

In the range

$$(m/\log m)^{1/2}/(2P) \leqslant L \leqslant \gamma m$$

we apply the L^1 bound from Lemma 12.5, where we may use $\alpha = 1 - m^{-1/10}$ as input by our assumptions. This yields

$$\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell}) \leqslant P^{\max\{0,\,L-\gamma m\}}\alpha^{\min\{m,\,2L\}} \leqslant \alpha^L \leqslant \exp(-Lm^{-1/10}),$$

which, using $P \leqslant m^{1/4}$, is $\leqslant \exp(-m^{3/20}/(4\log m)^{1/2}) \ll \exp(-m^{1/8}) \ll_r m^{-2r}e^{-m^{1/10}}$.

This leaves the range

$$\gamma m \leqslant L \leqslant \gamma m + m^{0.88},$$

for which we employ the L^1 bound from Lemma 12.5 again. In this case we find

$$\delta_{\mathcal{P}}^{\mathsf{R}}(m;\boldsymbol{\ell}) \leqslant P^{\max\{0,\,L-\gamma m\}}\alpha^{\min\{m,\,2L\}} \leqslant P^{m^{0.88}}\alpha^m \leqslant \exp(m^{0.88}\log m - m^{0.9}) \ll \exp(-m^{0.89}),$$

proving (10.10) in this range as well. □

13. Anatomy and large degree factors

In this section, we prove Proposition 2.6, which shows how bounds on $\Delta_{\mathcal{P}}^{\mathsf{R}}$ translate to irreducibility.

Recall Definition 5.8, where we defined a measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$ on the set $\mathcal{M}(m)$ of monic degree m polynomials in $\mathbf{Z}[T]$. This is the measure induced by $\mathbb{P}_{\mathcal{R}(m)}$ after taking the trace polynomial. It induces further probability measures $\mathbb{P}_{\mathsf{R},\mathcal{M}_p(m)}$ and $\mathbb{P}_{\mathsf{R},\mathcal{M}_{\mathcal{P}}(m)}$ in the same manner as the measures $\mathbb{P}_{\mathcal{R}_p(m)}$ and $\mathbb{P}_{\mathcal{R}_{\mathcal{P}}(m)}$ are induced by $\mathbb{P}_{\mathcal{R}(m)}$. Set

$$\Delta_{\mathsf{R},\mathcal{P}}(m;k) := \sum_{\substack{\boldsymbol{D}\in\mathcal{M}_{\mathcal{P}}\\ \deg \boldsymbol{D}\leqslant k\\ T\nmid D_p\ \forall p\in\mathcal{P}}} \max_{\boldsymbol{C} \bmod \boldsymbol{D}} \left|\mathbb{P}_{\mathsf{R},\boldsymbol{A}\in\mathcal{M}_{\mathcal{P}}(m)}\big(\boldsymbol{A}\equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) - \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}}\right|. \tag{13.1}$$

Lemma 13.1. *Let $m \geqslant k \geqslant 1$ be two integers. For any choice of probability measure $\mathbb{P}_{\mathcal{R}(m)}$, we have $\Delta_{\mathsf{R},\mathcal{P}}(m;k) \leqslant \Delta_{\mathcal{P}}^{\mathsf{R}}(m;k)$. In particular, the conditions of Proposition 2.5 imply*

$$\Delta_{\mathsf{R},\mathcal{P}}\big(m; m/2 + m^{0.88}\big) \ll_r \exp\big(-m^{1/10}\big).$$

Proof. For all polynomials $A, C, D \in \mathbf{F}_p[T]$ such that $\deg(A) = m$ and $\deg(C), \deg(D) \leqslant m$, we have $A \equiv C \bmod D$ if, and only if, $A^{\mathsf{R},m} \equiv C^{\mathsf{R},m} \bmod D^{\mathsf{R}}$ by Lemma 5.3. Thus, if we let $\tilde{\boldsymbol{A}} = \boldsymbol{A}^{\mathsf{R},m} = \boldsymbol{A}^{\mathsf{R}}$, $\tilde{\boldsymbol{C}} = \boldsymbol{C}^{\mathsf{R},m}$ and $\tilde{\boldsymbol{D}} = \boldsymbol{D}^{\mathsf{R}}$, then we find

$$\mathbb{P}_{\mathsf{R},\boldsymbol{A}\in\mathcal{M}_{\mathcal{P}}(m)}\big(\boldsymbol{A}\equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) = \mathbb{P}_{\tilde{\boldsymbol{A}}\in\mathcal{R}_{\mathcal{P}}(m)}\Big(\tilde{\boldsymbol{A}}\equiv \tilde{\boldsymbol{C}} \bmod \tilde{\boldsymbol{D}}\Big).$$

Consequently,

$$\begin{aligned}\Delta_{\mathsf{R},\mathcal{P}}(m;k) &= \sum_{\substack{\boldsymbol{D}\in\mathcal{M}_{\mathcal{P}}\\ \deg \boldsymbol{D}\leqslant k\\ T\nmid D_p\ \forall p\in\mathcal{P}}} \max_{\boldsymbol{C} \bmod \boldsymbol{D}} \left|\mathbb{P}_{\tilde{\boldsymbol{A}}\in\mathcal{R}_{\mathcal{P}}(m)}\Big(\tilde{\boldsymbol{A}}\equiv T^m\boldsymbol{C}(T+T^{-1}) \bmod \boldsymbol{D}^{\mathsf{R}}\Big) - \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}}\right| \\ &= \sum_{\substack{\tilde{\boldsymbol{D}}\in\mathcal{R}_{\mathcal{P}}\\ \deg \tilde{\boldsymbol{D}}\leqslant 2k\\ T^2+1\nmid \tilde{D}_p\ \forall p\in\mathcal{P}}} \max_{\boldsymbol{C} \bmod \tilde{\boldsymbol{D}}_{\mathsf{R}}} \left|\mathbb{P}_{\tilde{\boldsymbol{A}}\in\mathcal{R}_{\mathcal{P}}(m)}\Big(\tilde{\boldsymbol{A}}\equiv T^m\boldsymbol{C}(T+T^{-1}) \bmod \tilde{\boldsymbol{D}}\Big) - \frac{1}{\|\tilde{\boldsymbol{D}}\|_{\mathcal{P}}^{1/2}}\right|.\end{aligned}$$

Since the map $\mathbf{F}_{\mathcal{P}}[T]/(\tilde{\boldsymbol{D}}_{\mathsf{R}}) \to R_m(\tilde{\boldsymbol{D}})$ sending $\boldsymbol{C} \mapsto T^m\boldsymbol{C}(T+T^{-1}) \bmod \tilde{\boldsymbol{D}}$ is bijective when $\deg(D_p) \leqslant m$ (cf. Lemma 8.1 and Definition 8.4), we conclude that the only difference between $\Delta_{\mathsf{R},\mathcal{P}}(m;k)$ and $\Delta_{\mathcal{P}}^{\mathsf{R}}(m;k)$ (see (2.2)) is that in the latter we require $T^2+1 \nmid D_2$ whereas in the former we demand $T^2+1 \nmid D_p$ for all $p \in \mathcal{P}$. Hence $\Delta_{\mathsf{R},\mathcal{P}}(m;k) \leqslant \Delta_{\mathcal{P}}^{\mathsf{R}}(m;k)$. □

We will show that this suffices to prove that A_{R} is irreducible with high probability. Indeed, as we will argue below, the main result of [7, §§8–10] is roughly the following. Given a probability measure $\mathbb{P}_{\mathcal{M}(m)}$ on $\mathcal{M}(m)$, a finite set of primes $\mathcal{P}$ and integers $m, k \geqslant 1$, let

$$\Delta_{\mathcal{P}}(m;k) := \sum_{\substack{\boldsymbol{D}\in\mathcal{M}_{\mathcal{P}}\\ \deg \boldsymbol{D}\leqslant k\\ T\nmid D_p\ \forall p\in\mathcal{P}}} \max_{\boldsymbol{C} \bmod \boldsymbol{D}} \left|\mathbb{P}_{\boldsymbol{A}\in\mathcal{M}_{\mathcal{P}}(m)}\big(\boldsymbol{A}\equiv \boldsymbol{C} \bmod \boldsymbol{D}\big) - \frac{1}{\|\boldsymbol{D}\|_{\mathcal{P}}}\right|. \tag{13.2}$$

In [7], the authors used the measure $\mathbb{P}_{\mathcal{M}(m)}$ such that the coefficient a_j of T^j is sampled independently from the rest according to a probability measure μ_j on $\mathbf{Z}[T]$ satisfying various conditions. They showed for this measure that if $\Delta_{\mathcal{P}}(m;k)$ is small for k slightly larger than $m/2$, then A does not have any factors of degree in $[m^{1/10}, m/2]$ (see Lemma 9.4 and §10 in [7]), which is the analogous result to Proposition 2.6. It turns out that this proof uses very little

about the specific structure of the measure $\mathbb{P}_{\mathcal{M}(m)}$ with each coefficient sampled independently. We will thus be able to adapt it easily to the measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$. To stress this point, we will prove a more general result.

Recall that

$$\lambda_0 := \frac{1}{4 - 4\log 2}.$$

We then have the following general lemma.

Lemma 13.2 (Large degree factors in [7, Proposition 2.2])**.** *Let $\varepsilon \in (0, 1/100]$, let $m \in \mathbf{Z}_{\geqslant 1}$, and let $\mathbb{P}_{\mathcal{M}(m)}$ be a probability measure on the set $\mathcal{M}(m)$ of monic polynomials of degree m satisfying the following conditions:*

(1) There is a set $\mathcal{P}$ of four primes such that $\Delta_{\mathcal{P}}(m; m/2 + m^{\lambda_0+\varepsilon}) \leqslant m^{-30}$;

(2) $\mathbb{P}_{A\in\mathcal{M}(m)}\big(T^{1+\lceil 4m^{\varepsilon/200}\log m\rceil} \mid A_p\big) \leqslant m^{-4}$ for all $p \in \mathcal{P}$.

Then there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{A\in\mathcal{M}(m)}\Big(A \text{ has a factor of degree in } \big[m^{1/10}, m/2\big]\Big) \leqslant Cm^{-c}.$$

Proof. We make some observations about the use of independence in [7, §§8–9]. First, everything in their §8 is already formulated in the required generality. In their §9, we encounter the sequence of probability measures $\mu_0, \mu_1, \ldots$ in each of their Lemmas 9.1-9.4. The proofs of their Lemmas 9.1-9.3 do not use that the measure $\mathbb{P}_{\mathcal{M}(m)}$ is induced by these, so the lemmas may as well be stated for a general measure $\mathbb{P}_{\mathcal{M}(m)}$. This leaves only their Lemma 9.4, a statement having as one of its hypotheses the anti-concentration inequality

$$\sup_{1\leqslant j<m} \sum_{a\equiv 0 \bmod p} \mu_j(a) \leqslant 1 - \delta \quad \forall p \in \mathcal{P}. \tag{$\star$}$$

To be precise, this is the right-hand side of their (9.15). However, the assumption ($\star$) only serves the purpose of showing, in their notation,

$$\mathbb{P}_{A\in\mathcal{M}(m)}\Big(T^{1+\lceil r\delta^{-1}\log m\rceil} \mid A_p\Big) \leqslant m^{-r} \quad \forall p \in \mathcal{P}; \tag{13.3}$$

Indeed, this is established in and around their (9.17) and (9.18). Thus we may take (13.3) as an assumption in [7, Lemma 9.4] instead of ($\star$). The remainder of the proof of their Lemma 9.4 does not make use of the independence of the coefficients of A.

Now, observe that condition (1) in Lemma 13.2 is the same as condition (b) in [7, Proposition 2.2] in the case $\theta = 1/2$. Our condition (2) is implied by the latter half of their condition (c), and in particular suffices for our purposes, which are to be able to apply the revised version of [7, Lemma 9.4] where ($\star$) is replaced by (13.3). Their condition (a) as well as the first half of their condition (c) are only used to rule out factors of small degree by means of [7, Proposition 2.1], and thus we do not need them here. Hence the result follows by the proof of [7, Proposition 2.2], given in their §10. □

This brings us to the proof of Proposition 2.6. We first prove the following, more general version.

Proposition 13.3 (Large degree factors alternative)**.** *Let $m \in \mathbf{Z}_{\geqslant 1}$ and $\varepsilon \in (0, 1/100]$. Let $\mathbb{P}_{\mathcal{R}(m)}$ be any probability measure on $\mathcal{R}(m)$ satisfying the following:*

(1) There is a set $\mathcal{P}$ of four primes such that $\Delta^{\mathsf{R}}_{\mathcal{P}}(m; m/2 + m^{\lambda_0+\varepsilon}) \leqslant m^{-30}$.

(2) $\mathbb{P}_{A\in\mathcal{R}(m)}\big((T^2+1)^{1+\lceil 4m^{\varepsilon/200}\log m\rceil} \mid A_p\big) \leqslant m^{-4}$ for all $p \in \mathcal{P}$.

Then there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{A\in\mathcal{R}(m)}\Big(A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k \in \big[m^{1/10}, m/2\big]\Big) \leqslant Cm^{-c}.$$

Proof. In light of Lemma 13.1, the conditions in Proposition 13.3 imply those of Lemma 13.2 for the probability measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$. Thus there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\Big(B \text{ has a factor of degree in } \big[m^{1/10}, m/2\big]\Big) \leqslant Cm^{-c}.$$

Making the change of variables $A = B^{\mathsf{R}}$, and noticing that B has a factor of degree k if and only if A has a reciprocal factor in $\mathcal{R}(k)$, this is equivalent to

$$\mathbb{P}_{A\in\mathcal{R}(m)}\Big(A \text{ has a reciprocal divisor } D \in \mathcal{R}(k) \text{ with } k \in \big[m^{1/10}, m/2\big]\Big) \leqslant Cm^{-c},$$

which was to be shown. □

When the coefficients of the reciprocal polynomial A are induced by a sequence of probability measures μ_j — as we assume everywhere else in the paper — we may replace condition (2) of Proposition 13.3 by a (perhaps more appealing) condition on the μ_j. This is entirely similar to the result that (⋆) implies (13.3). In particular, to prove Proposition 2.6, it suffices to show that its condition (2) implies condition (2) of Proposition 13.3. To prove this, we first give a general lemma.

Lemma 13.4. *Let $\mu_0, \dots, \mu_{m-1}$ be probability measures on $\mathbf{Z}$, and let $\mathbb{P}_{\mathcal{R}(m)}$ be the measure defined by (1.3). Let p be a prime and $\delta > 0$, and suppose that*

$$\sup_{0\leqslant b\leqslant p-1} \sum_{a\equiv b \bmod p} \mu_j(a) \leqslant 1-\delta \quad \text{for all } j \in \{0, 1, \dots, m-1\}. \tag{13.4}$$

Then, for every $D \in \mathcal{R}_p(k)$ with $k \in \mathbf{Z} \cap [1, m]$, we have

$$\mathbb{P}_{A\in\mathcal{R}(m)}\big(D \mid A_p\big) \leqslant e^{-\delta k}.$$

In particular, if we let $v = \lceil c\delta^{-1} \log m\rceil$ with $c > 0$, then

$$\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\big(T^v \mid B_p\big) \leqslant m^{-c}.$$

Proof. This is essentially [11, Lemma 39] or [25, Lemma 4.1], adapted to the reciprocal setting. For each $j \in [k, m-1] \cap \mathbf{Z}$, pick a_j according to the measure on $\mathbf{F}_p$ induced by μ_j and set $A' = \sum_{j=k}^{m} a_j(T^{m-j} + T^{m+j}) \in \mathbf{F}_p[T]$. Write $R \coloneqq A' \bmod D \in T^{m-k+1}\mathcal{R}_p^{\mathsf{sh}}(k-1)$ for the polynomial with $R = A' \bmod D$. Conditionally on the choice of $a_k, \dots, a_{m-1}$, we have that

$$\begin{aligned} D|A_p \quad &\iff \quad a_0T^m + a_1(T^{m+1} + T^{m-1}) + \dots + a_{k-1}(T^{m-k+1} + T^{m+k-1}) \equiv -A' \bmod D \\ &\iff \quad a_0T^m + a_1(T^{m+1} + T^{m-1}) + \dots + a_{k-1}(T^{m-k+1} + T^{m+k-1}) = -R. \end{aligned}$$

We thus see that the coefficients $a_0, \dots, a_{k-1}$ are fixed. Using our assumption (13.4) proves that the probability that $D|A_p$ conditionally on the choice of $a_k, \dots, a_{m-1}$ is $\leqslant (1-\delta)^k \leqslant e^{-\delta k}$. This proves the first claim.

To see the second claim, note that

$$\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\big(T^v \mid B_p\big) = \mathbb{P}_{A\in\mathcal{R}(m)}\big((T^2+1)^v \mid A_p\big) \leqslant m^{-c},$$

where we made the change of variables $A = B^{\mathsf{R}}$. Thus the proof is complete. □

Proposition 2.6 is now a simple corollary of Proposition 13.3:

Proof of Proposition 2.6. It suffices to show that the conditions of Proposition 13.3 are met. To this end, it suffices to show that condition (2) of Proposition 2.6 implies condition (2) of Proposition 13.3 for the measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$. Indeed, applying Lemma 13.4 with $\delta = m^{-\varepsilon/200}$ and $c = 4$ yields, for any $p \in \mathcal{P}$, the inequality $\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}(T^{\lceil 4m^{\varepsilon/200}\log m\rceil} \mid B_p) \leqslant m^{-4}$. This is stronger than condition (2) of Proposition 13.3, thus completing the proof. □

14. The hyperoctahedral group and its subgroups

We have now proven Propositions 2.3–2.6, which together yield that A is irreducible with high probability under a wide range of choices of the probability measures μ_j — essentially (1.6). In the remainder of the paper, we study the Galois group of A.

In this section, we describe the generic Galois group of a reciprocal polynomial $A \in \mathcal{R}(m)$, which is the *hyperoctahedral group* denoted $C_2 \wr \mathcal{S}_m$. Furthermore, we describe the 'large' subgroups of $C_2 \wr \mathcal{S}_m$, in a sense made precise by Lemmas 14.4 and 14.5. The latter is a Łuczak–Pyber theorem for the group $C_2 \wr \mathcal{S}_m$, which is not used in this article but might be of independent interest.

The hyperoctahedral group. The zeros of a squarefree reciprocal polynomial $A \in \mathcal{R}(m)$ are $2m$ distinct algebraic integers that may be labelled as

$$\alpha_1, \alpha_2, \dots, \alpha_m \text{ and } \alpha_{-1} := \alpha_1^{-1}, \alpha_{-2} := \alpha_2^{-1}, \dots, \alpha_{-m} := \alpha_m^{-1}.$$

An element σ of the Galois group $\mathcal{G}_A \leqslant \mathcal{S}_{2m}$ of A is in particular a field automorphism and thus $\sigma(\alpha_{-j}) = \sigma(\alpha_j)^{-1}$ for all j. In other words, the Galois group $\mathcal{G}_A$ preserves the *block system*

$$\mathcal{B}_1 = \{\alpha_1, \alpha_{-1}\}, \dots, \mathcal{B}_m = \{\alpha_m, \alpha_{-m}\}$$

in the sense that for all i and all σ, there exists j such that $\sigma(\mathcal{B}_i) = \mathcal{B}_j$. This shows that the action of the permutation group $\mathcal{G}_A$ on the set of zeros of A is *imprimitive*. (In general, if a permutation group $G \leqslant \mathcal{S}_n$ preserves some partitioning of $\{1, 2, \dots, n\}$ into at least two sets of equal size, then G is called *imprimitive*.)

The group $\mathcal{G}_A$ naturally lies in the *hyperoctahedral group* $C_2 \wr \mathcal{S}_m$, which is an example of a *permutational wreath product*. In general, if G is an abstract group and $K \leqslant \mathcal{S}_m$ is a permutation group, then $G \wr K$ is the semidirect product $G^m \rtimes K$ under the automorphism of G^m induced by K through permutation of the m copies of G. Explicitly, it is the group with elements $G^m \times K$ and product

$$((\varepsilon_i)_i, \sigma) \cdot ((\varepsilon'_i)_i, \sigma') = ((\varepsilon_i \varepsilon'_{\sigma^{-1}(i)})_i, \sigma\sigma').$$

The group $C_2 \wr \mathcal{S}_m$ is also known as the Coxeter group of type B_m or as the signed symmetric group. The last name comes from its action on the set $\{-m, \dots, -1, 1, \dots, m\}$ of $2m$ signed letters (the set of indices of the α_j) given by the explicit formula

$$((\varepsilon_i)_i, \sigma).k = \operatorname{sign}(k) \varepsilon_{\sigma(|k|)} \sigma(|k|). \tag{14.1}$$

This induces the action of $\mathcal{G}_A$ on the zeros of A; it is clear that this action preserves the pairs $\{k, -k\}$. Moreover, the formula (14.1) gives a procedure to determine the cycle decomposition of an element $((\varepsilon_i)_i, \sigma)$, viewed as an element of $\mathcal{S}_{2m}$. For example, we have $C_2 \wr \mathcal{S}_4 \ni ((-1, 1, -1, 1), (12)) = (1\,2\,{-1}\,{-2})(3\,{-3}) \in \mathcal{S}_8$.

We refer to [33] for a proof that a generic reciprocal polynomial of degree $2m$ has Galois group $C_2 \wr \mathcal{S}_m$.

Subgroups of the hyperoctahedral group. Consider the following proper subgroups of $C_2 \wr \mathcal{S}_m$:

(1) The index-2 subgroup

$$G_1 := \{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m \ : \ \prod_i \varepsilon_i = 1\} = (C_2 \wr \mathcal{S}_m) \cap \mathcal{A}_{2m}; \tag{14.2}$$

(2) The index-2 subgroup

$$G_2 := \{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m \ : \ \operatorname{sign}(\sigma) \prod_i \varepsilon_i = 1\} \tag{14.3}$$

which, as a set, is $((C_2^m \times \mathcal{A}_m) \cap \mathcal{A}_{2m}) \cup ((C_2^m \times (\mathcal{S}_m \setminus \mathcal{A}_m)) \cap (\mathcal{S}_{2m} \setminus \mathcal{A}_{2m}))$;

(3) The index-2 subgroup

$$G_3 := \{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m \ : \ \operatorname{sign}(\sigma) = 1\} = C_2 \wr \mathcal{A}_m; \tag{14.4}$$

(4) The index-4 subgroup arising as the intersection of G_1, G_2, and G_3,

$$G_4 := \{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m \ : \ \operatorname{sign}(\sigma) = \prod_i \varepsilon_i = 1\} = (C_2 \wr \mathcal{A}_m) \cap \mathcal{A}_{2m}. \tag{14.5}$$

Remark 14.1. The groups G_2 and G_1 are not permutation isomorphic, but they *are* isomorphic when m is odd: the map is $G_2 \to G_1$, $((\varepsilon_i)_i, \sigma) \mapsto ((\varepsilon_i \operatorname{sign}(\sigma))_i, \sigma)$.

The group $C_2 \wr \mathcal{S}_m$ comes with the projection map

$$\begin{aligned} \operatorname{proj} \colon C_2 \wr \mathcal{S}_m &\to \mathcal{S}_m, \\ ((\varepsilon_i)_i, \sigma) &\mapsto \sigma. \end{aligned}$$

The purpose of this subsection is to show that any proper subgroup $H \leqslant C_2 \wr \mathcal{S}_m$ that projects onto $\mathcal{S}_m$ or $\mathcal{A}_m$ is either one of the 'large' groups G_1, G_2, G_3 and G_4, or is contained in the 'small' group

$$G_5 := \{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m \ : \ \varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m\} \cong C_2 \times \mathcal{S}_m. \tag{14.6}$$

The reason to restrict to subgroups projecting onto $\mathcal{A}_m$ or $\mathcal{S}_m$ is because we prove in §15 that $\operatorname{proj}(\mathcal{G}_A)$ is with high probability either $\mathcal{A}_m$ or $\mathcal{S}_m$.

We start with the following standard result on the subgroups of a semidirect product.

Lemma 14.2. *Let $G \rtimes K$ be a semidirect product, with G an abelian group. For any subgroup $H \leqslant G \rtimes K$ with $\operatorname{proj}(H) = K$, the set $V = G \cap H = \{((\varepsilon_i)_i, \mathrm{id}) \in H\}$ is a K-invariant subgroup of G. Furthermore, given a K-invariant subgroup V of G, the set of subgroups H (up to conjugation) with $G \cap H = V$ is in bijective correspondence with the first cohomology group $\mathcal{H}^1(K, G/V)$, via the map*

$$\mathcal{H}^1(K, G/V) \ni \xi \mapsto H_\xi = \{(g, \sigma) : \sigma \in K,\ g \equiv \xi(\sigma) \bmod V\}. \tag{14.7}$$

Proof. Since H is closed under conjugation by itself and G is abelian, the group V contains the element

$$((\varepsilon_i')_i, \sigma) \cdot ((\varepsilon_i)_i, \mathrm{id}) \cdot ((\varepsilon_i')_i, \sigma)^{-1} = ((\varepsilon_{\sigma^{-1}(i)})_i, \mathrm{id})$$

for any $((\varepsilon_i)_i, \mathrm{id}), ((\varepsilon_i')_i, \sigma) \in H$. Hence V is a K-invariant subgroup of G. This proves the first claim. For the second claim, we refer the reader to [2, Section 17] or [1, Lemma 3.3]. □

To apply Lemma 14.2, we study the invariant subgroups of C_2^m by the permutation actions of $\mathcal{A}_m$ and $\mathcal{S}_m$. The following lemma is probably well-known.

Lemma 14.3. *For $m \in \mathbf{Z}_{\geqslant 3}$, the only invariant subgroups $V \subset C_2^m$ by the permutation action of $\mathcal{A}_m$ are*

- $V_0 = \{(1, \ldots, 1)\}$,
- $V_1 = \{(-1, \ldots, -1), (1, \ldots, 1)\}$,
- $V_{m-1} = \{\varepsilon \in C_2^m : \prod_i \varepsilon_i = 1\}$,
- $V_m = C_2^m$.

The same is true if $\mathcal{A}_m$ is replaced by $\mathcal{S}_m$.

Proof. For $\mathcal{S}_m$, a proof of this result is given in [3, Lemma 4.2]. The proof for $\mathcal{A}_m$ we give here proceeds in similar vein. If an invariant subset $V \subset C_2^m$ is different from V_0 and V_1, then there exists $\varepsilon \in V$ and distinct i, j, and k such that $\varepsilon_i = \varepsilon_j = -\varepsilon_k$. Consider $\sigma = (ijk) \in \mathcal{A}_m$. Then $\varepsilon' := \varepsilon \cdot \sigma(\varepsilon)$ has all entries equal to 1 except for the i-th and the k-th. Permuting ε' by permutations that are products of two transpositions, we can form all tuples in C_2^m with only two entries equal to -1. Such tuples span V_{m-1}. If $V \neq V_{m-1}$, then $V = V_m$ since V_{m-1} is of codimension 1 in V_m. □

Lemma 14.4. *Let $m \geqslant 5$. Let $H \leqslant C_2 \wr \mathcal{S}_m$ be a nontrivial subgroup that projects onto $K \in \{\mathcal{S}_m, \mathcal{A}_m\}$.*

- *If $[C_2 \wr \mathcal{S}_m : H] < 2^{m-1}$ and $K = \mathcal{S}_m$, then $H \in \{G_1, G_2\}$.*
- *If $[C_2 \wr \mathcal{S}_m : H] < 2^{m-1}$ and $K = \mathcal{A}_m$, then $H \in \{G_3, G_4\}$.*
- *If $[C_2 \wr \mathcal{S}_m : H] \geqslant 2^{m-1}$, then $H \leqslant V_1 \times \mathcal{S}_m = G_5$.*

Proof. We apply Lemma 14.2. Let $K \in \{\mathcal{S}_m, \mathcal{A}_m\}$. Suppose $V = V_0$ and $\xi \in H^1(K, C_2^m/V)$. Then each $\sigma \in K$ gives rise to precisely one element in the subgroup H_ξ appearing on the right-hand side of (14.7). Hence H_ξ is of cardinality $|K|$, so its index in $C_2 \wr \mathcal{S}_m$ is 2^m. Similarly, if $V = V_1$, the index of any resulting H_ξ is 2^{m-1}. We may thus disregard the cases $V \in \{V_0, V_1\}$. It remains to compute the cohomology groups and resulting groups H_ξ for $V \in \{V_{m-1}, V_m\}$. We consider the case $K = \mathcal{A}_m$, since the case $K = \mathcal{S}_m$ was already covered in [1, Theorem 3.4 and Remark 3.6]. First,

$$H^1(\mathcal{A}_m, C_2^m/V_{m-1}) = \operatorname{Hom}(\mathcal{A}_m, C_2^m/V_{m-1}) = \operatorname{Hom}(\mathcal{A}_m, C_2),$$

since the action of $\mathcal{A}_m$ on C_2^m/V_{m-1} is trivial and $C_2^m/V_{m-1} \cong C_2$. Hence $H^1(\mathcal{A}_m, C_2^m/V_{m-1})$ is trivial, because $\mathcal{A}_m$ is simple by the assumption $m \geqslant 5$ (so any homomorphism must have kernel $\mathcal{A}_m$ or 1, and only the former is possible in this case). The corresponding map ξ is hence the map sending everything to 1, which gives the group $\{((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{A}_m : \prod \varepsilon_i = 1\} = G_4$. For $V = V_m$, we find

$$H^1(\mathcal{A}_m, C_2^m/V_m) = H^1(\mathcal{A}_m, 1) = 1$$

which gives the full group $C_2 \wr \mathcal{A}_m = G_3$. □

The next result is an immediate consequence of the preceding discussion and the classical Łuczak–Pyber theorem; even if it is not needed anywhere else in the paper, we include it as we could not find it recorded anywhere else.

Lemma 14.5 (Łuczak–Pyber for $C_2 \wr \mathcal{S}_m$)**.** *Let $\mathcal{T}_m$ be the union of all proper subgroups $H \leqslant C_2 \wr \mathcal{S}_m$ with $H \neq G_1, G_2, G_3, G_4$ that are transitive on the set $\{-m, \dots, -1, 1, \dots, m\}$ by the action given in (14.1). Then there is an absolute constant $c > 0$ such that*

$$\#\mathcal{T}_m / \#(C_2 \wr \mathcal{S}_m) \ll m^{-c}.$$

Proof. Let H be a subgroup of $C_2 \wr \mathcal{S}_m$. Then $\operatorname{proj}(H)$ is a subgroup of $\mathcal{S}_m$ and comes with the action on the set of pairs $\mathcal{Y} = \{\{j, -j\} : j \in \mathbf{Z} \cap [1, m]\}$ given by $\sigma\{j, -j\} := \{\sigma(j), -\sigma(j)\}$ for any $\sigma \in \operatorname{proj}(H)$. This coincides with the action of H given by (14.1) on $\mathcal{Y}$. In particular, if the action of H on $\{-m, \dots, -1, 1, \dots, m\}$ given by (14.1) is transitive, then the action of H on $\mathcal{Y}$ is transitive, so the action of $\operatorname{proj}(H)$ on $\mathcal{Y}$ is transitive as well — i.e., $\operatorname{proj}(H)$ is a transitive subgroup of $\mathcal{S}_m$.

Now write

$$\mathcal{T}_m = \mathcal{T}_m' \cup \mathcal{T}_m''$$

where $\mathcal{T}_m'$ is the union of all transitive $H \leqslant C_2 \wr \mathcal{S}_m$ with $\operatorname{proj}(H) \notin \{\mathcal{S}_m, \mathcal{A}_m\}$, and $\mathcal{T}_m''$ is the union of all transitive $H \leqslant C_2 \wr \mathcal{S}_m$ with $\operatorname{proj}(H) \in \{\mathcal{S}_m, \mathcal{A}_m\}$ and $H \neq G_1, G_2, G_3, G_4$. Then the classical Łuczak–Pyber theorem [26] implies the existence of an absolute constant $c > 0$ such that $\operatorname{proj}(\mathcal{T}_m')$ is of size $\ll m!/m^c$. Since the map $\operatorname{proj}\colon C_2 \wr \mathcal{S}_m \to \mathcal{S}_m$ is 2^m-to-one, this implies $\mathcal{T}_m'$ is of size $\ll 2^m m!/m^c$. Lastly, by Lemma 14.4, we find that $\mathcal{T}_m''$ is contained in $C_2 \times \mathcal{S}_m$, which is of size $2m!$. This completes the proof. □

15. The Galois group of A_{R}

The projection $\operatorname{proj}(\mathcal{G}_A)$ conveniently equals the Galois group of A_{R}, as we show in the following lemma.

Lemma 15.1. *We have $\mathcal{G}_{A_{\mathsf{R}}} = \operatorname{proj}(\mathcal{G}_A)$.*

Proof. Let $B = A_{\mathsf{R}}$. The trace polynomial B has zeros $\alpha_1 + \alpha_{-1}, \dots, \alpha_m + \alpha_{-m}$. Denote the splitting fields of B and A by K_B and K_A. These are Galois extensions of $\mathbf{Q}$ with $K_B \subset K_A$. A standard result in Galois theory now says that any automorphism $\sigma \in \mathcal{G}_B$ can be extended to an element of $\mathcal{G}_A$, and conversely that the restriction of an element of $\mathcal{G}_A$ to K_B gives an element of $\mathcal{G}_B$. Suppose $\tau := ((\varepsilon_i)_i, \sigma) \in \mathcal{G}_A$. Then the restriction $\tau|_{K_B} \in \mathcal{G}_B$ maps $\alpha_k + \alpha_{-k}$ to $\alpha_{\sigma(k)} + \alpha_{-\sigma(k)}$. In particular, since the zeros of B are invariant under the maps $\alpha_j \mapsto \alpha_{-j}$, the action of τ on the zeros of B only depends on σ. So we may identify $\tau|_{K_B}$ with $\mathrm{proj}(\tau) = \sigma$. Conversely, if $\sigma \in \mathcal{G}_B$, then any extension of σ to $\mathcal{G}_A$ is of the form $((\varepsilon_i)_i, \sigma)$ for some $(\varepsilon_i)_i \in C_2^m$. □

In the remainder of this section, we show that $\mathcal{G}_{A_{\mathsf{R}}}$ is $\mathcal{A}_m$ or $\mathcal{S}_m$ with high probability. Here we use the results from [7], but since the coefficients of A_{R} are not independent random variables, we have to make a careful analysis of the use of independence there, just as we did in §13. We start with the following lemma. For this, we recall the notation Δ_p defined in (13.2) (with the usual convention that $\Delta_p = \Delta_{\{p\}}$).

Lemma 15.2. *Let $\mathbb{P}_{\mathcal{M}(m)}$ be any probability measure on the set $\mathcal{M}(m)$ of monic polynomials of degree m. Sample B according to $\mathbb{P}_{\mathcal{M}(m)}$ and let $B_p := (B \bmod p) \in \mathbf{F}_p[T]$ be its reduction modulo p. Fix a prime p. Furthermore, fix a real number $\varepsilon > 0$ with the properties*

(1) $\Delta_p\big(m, m/2 + m^{\lambda_0+\varepsilon}\big) \leqslant m^{-10}$,

(2) For $v > (\log m)^3$, we have $\mathbb{P}_{B\in\mathcal{M}(m)}\big(T^v \mid B_p\big) \ll 1/m$.

Then there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{B\in\mathcal{M}(m)}\Big(\mathcal{G}_B \notin \{\mathcal{A}_m, \mathcal{S}_m\} \text{ and } B \text{ is irreducible}\Big) \leqslant Cm^{-c}.$$

Proof. This is an adaptation of [7, Proposition 2.4]. Denote their sequence of probability measures by $\mu'_0, \dots, \mu'_{m-1}$. The difference between that proposition and our lemma is that we replaced the condition

$$\sup_{1\leqslant j<m} \sum_{a\equiv 0 \bmod p} \mu'_j(a) \leqslant 1 - \frac{1}{(\log m)^2} \tag{15.1}$$

by our condition (2) and dropped the condition that $\mathbb{P}_{\mathcal{M}(m)}$ is induced by a sequence of measures $\mu'_0, \dots, \mu'_{m-1}$ — that is, that the coefficients of the polynomial $\mathcal{M}(m)$ are *independent* random variables. To show that the conclusion of the lemma continues to hold under this weakened condition (2), we analyze the use of (15.1) in [7]. Note that this is the right-hand side of their Assumption (11.3), which is used in the following places:

- Proof of Lemma 11.1(b): Here, the assumption is only used to ensure that the conditions of [7, Lemma 9.4] are met with $\varepsilon = 1/100$, $\delta = 1/(\log n)^2$, $\theta = 1/2$, and $\mathcal{P} = \{p\}$. However, in the proof of Lemma 13.2, we showed that the conditions of [7, Lemma 9.4] can be weakened to a condition that holds under our condition (2).
- Proof of Lemma 11.5: The assumption is used only to prove our condition (2).
- Statement of Lemma 11.6: The assumption is also included here. But Lemma 11.6 follows immediately from combining Proposition 12.1, which does not use this assumption, with Lemma 11.1, which we already discussed.

This finishes the proof. □

Now we adapt Lemma 15.2 to the setting of reciprocal polynomials.

Lemma 15.3. *Consider probability measures $\mu_0, \mu_1, \dots, \mu_{m-1}$ on the integers. Fix a prime p and a real number $\varepsilon > 0$ with the properties*

(1) $\Delta_p^{\mathsf{R}}(m, m/2 + m^{\lambda_0+\varepsilon}) \leqslant m^{-10}$,

(2) $\sup_{0\leqslant j<m} \sup_{0\leqslant b<p} \sum_{a\equiv b \bmod p} \mu_j(a) \leqslant 1 - \frac{1}{(\log m)^2}$.

Then there are constants $c, C > 0$ depending at most on ε such that

$$\mathbb{P}_{A\in\mathcal{R}(m)}\Big(\mathcal{G}_{A_{\mathsf{R}}} \notin \{\mathcal{A}_m, \mathcal{S}_m\} \text{ and } A \text{ is irreducible}\Big) \leqslant Cm^{-c}.$$

Proof. Our aim is to show this using Lemma 15.2 for the probability measure $\mathbb{P}_{\mathsf{R},\mathcal{M}(m)}$. In light of Lemma 13.1, the first condition in Lemma 15.2 follows from our condition (1) here. In addition, Lemma 13.4, which we may apply with $\delta = (\log m)^{-2}$ and $c = 1$, yields $\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}(T^{\lceil(\log m)^3\rceil} \text{ divides } B_p) \leqslant 1/m$, which is more than we needed to show. Lastly, if A is irreducible then $B = A_{\mathsf{R}}$ is irreducible, so the conclusion of the lemma follows from Lemma 15.2. □

16. The Galois group of A

This section contains the proof of Proposition 2.7. The only remaining preparatory work to complete that proof, as we will now explain, is to show that with negligible probability $\mathcal{G}_A \leqslant G_5 \cong C_2 \times \mathcal{S}_m$ (recall its definition, (14.6)). Indeed, if A is irreducible, combining the results of §14 and §15 already yields with high probability that

$$\mathcal{G}_A \in \big\{C_2 \wr \mathcal{S}_m, G_1, G_2, G_3, G_4\big\} \quad \text{or} \quad \mathcal{G}_A \leqslant G_5.$$

Observe that $G_4 \leqslant G_1$ for any m. To prove Proposition 2.7, it thus suffices to show that $\mathcal{G}_A \leqslant G_1$ and $\mathcal{G}_A \leqslant G_5$ occur with negligible probability (in fact, $G_5 \leqslant G_1$ for even m, but we shall not use this observation in the proof). Recall that $G_1 \leqslant \mathcal{A}_{2m}$, and that a squarefree polynomial A has $\mathcal{G}_A \leqslant \mathcal{A}_{2m}$ if, and only if, its discriminant $\Delta(A)$ is a nonzero square (Lemma 7.1). We already studied the question how often $\Delta(A)$ is a nonzero square in §7, where we proved Proposition 2.8; this will suffice for our purposes. Thus it remains to treat the group G_5, which we do here.

The group G_5 is very small compared to $C_2 \wr \mathcal{S}_m$ — of index 2^{m-1} in the latter, to be precise; one should thus expect it to be unlikely to be the Galois group of A. The next lemma forms the basis of our proof that this intuition is correct.

Lemma 16.1. *Let $m \in \mathbf{Z}_{\geqslant 1}$ and let $A \in \mathcal{R}(m)$ be squarefree. In addition, let p be a prime, let $d \in \mathbf{Z}_{\geqslant 1}$ and let $I \in \mathcal{R}_p(2d)$ be irreducible over $\mathbf{F}_p$ and such that $I \mid A_p$ but $I^2 \nmid A_p$. Then $\mathcal{G}_A \nleqslant C_2 \times \mathcal{S}_m$.*

Proof. The proof is inspired by [7, Lemma 11.3]. Let F be the splitting field of A over $\mathbf{Q}$ and write O_F for the ring of integers in F. For $x \in O_F$, denote by $\overline{x}$ its reduction mod $\mathfrak{p}$ to the field $O_F/\mathfrak{p}$. Consider a prime ideal $\mathfrak{p}$ of O_F lying over p. Recall that the Frobenius automorphism $\phi_p \colon O_F/\mathfrak{p} \to O_F/\mathfrak{p}$, defined as $\phi_p(\overline{x}) = \overline{x}^p$, lifts to an element $\phi \in \mathcal{G}_A$.

Write $\overline{\alpha}_1, \dots, \overline{\alpha}_{2d}, \overline{\alpha}_{-1} = (\overline{\alpha}_1)^{-1}, \dots, \overline{\alpha}_{-2d} = (\overline{\alpha}_{2d})^{-1} \in O_K/\mathfrak{p}$ for the zeros of I. Since I is irreducible and divides A_p just once, the action of ϕ_p on the $\overline{\alpha}_j$ is transitive and the orbit of each $\overline{\alpha}_j$ is of length $4d$.

Without loss of generality we may label the zeros of I so that

$$\phi(\{\overline{\alpha}_j, \overline{\alpha}_{-j}\}) = \{\overline{\alpha}_{j+1}, \overline{\alpha}_{-(j+1)}\} \quad \text{for } j = 1, 2, \dots, 2d,$$

with the convention that $\overline{\alpha}_{\pm(2d+1)} = \overline{\alpha}_{\pm 1}$. Hence, if we identify $\mathcal{S}_{2m}$ with the group of permutations of the symbols $\pm 1, \pm 2, \dots, \pm m$, with the convention that $\pm j$ corresponds to $\overline{\alpha}_{\pm j}$ for $j = 1, \dots, 2d$, then we find that ϕ contains the cycle $(1\,2\,\dots\,2d\,-1\,-2\,\dots\,-2d)$ in its disjoint cycle decomposition. Writing $\phi = ((\varepsilon_i)_i, \sigma) \in C_2 \wr \mathcal{S}_m$, this implies that σ contains the cycle $\tau = (1\,2\,\dots\,2d)$ in its disjoint cycle decomposition.

Let us now consider $\phi_+ := ((1, \dots, 1), \sigma)$ and $\phi_- := ((-1, \dots, -1), \sigma)$. If $\mathcal{G}_A \leqslant C_2 \times \mathcal{S}_m$, then we must have $\phi \in \{\phi_\pm\}$. But this is not possible. Indeed, by (14.1), viewing $\phi_\pm$ as elements of $\mathcal{S}_{2m}$, we get that ϕ_+ contains

$$\pi_+ := (1\,2\,\dots\,2d)(-1\,-2\,\dots\,-2d)$$

in its disjoint cycle decomposition, and that ϕ_- contains

$$\pi_- := (1\ {-2}\ 3\ {-4}\ \dots\ {-2d})({-1}\ 2\ {-3}\ 4\ \dots\ 2d)$$

in its disjoint cycle decomposition. In particular, $\phi \neq \phi_\pm$. □

Our next result about Galois groups, Lemma 16.3, necessitates the following auxiliary lemma.

Lemma 16.2 (Prime Polynomial Theorem for reciprocal polynomials)**.** *Suppose $m \in \mathbf{Z}_{\geqslant 1}$ is an integer and p is a prime and let $S_p(2m)$ denote the number of monic irreducible reciprocal polynomials of degree $2m$ over $\mathbf{F}_p$. Then, denoting by μ the Möbius function, we have*

$$S_p(2m) = \begin{cases} \frac{1}{2m}(p^m - 1) & \text{if } p > 2 \text{ and } m = 2^s \text{ for some } s, \\ \frac{1}{2m}\sum_{d \mid m,\, 2\nmid d} \mu(d) p^{m/d} & \text{otherwise.} \end{cases} \tag{16.1}$$

In particular,

$$S_p(2m) > \frac{p^m}{2m} - \frac{p^{m/3}}{m}. \tag{16.2}$$

Proof. The expression for $S_p(2m)$ in (16.1) comes from [28, Theorem 3]. Combining that with the trivial lower bound $\mu(d) \geqslant -1$ for $d \geqslant 3$ yields (16.2). □

Lemma 16.3. *Let $m \in \mathbf{Z}_{\geqslant 1}$ and p be a prime. Suppose $\Delta_p^{\mathsf{R}}(m; m/2) \leqslant m^{-9}$. Then, for every fixed $\varepsilon > 0$, we have*

$$\mathbb{P}_{A \in \mathcal{R}(m)}\Big(A \text{ is irreducible and } \mathcal{G}_A \leqslant C_2 \times \mathcal{S}_m\Big) \ll_\varepsilon m^{-1/4+\varepsilon}.$$

Proof. Define the set

$$\mathcal{I} = \bigcup_{1 \leqslant d \leqslant m/(2\log m)} \big\{I \in \mathcal{R}_p(2d) : I \text{ irreducible over } \mathbf{F}_p\big\}.$$

Observe that $\mathcal{I}$ is the set of candidate polynomials I in the statement of Lemma 16.1 in a restricted degree range. Hence it suffices to prove that for any $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ such that

$$\mathbb{P}_{A \in \mathcal{R}(m)}\Big(\exists I \in \mathcal{I} : I \mid A_p,\ I^2 \nmid A_p\Big) \geqslant 1 - C_\varepsilon m^{-1/4+\varepsilon}. \tag{16.3}$$

Since each $I \in \mathcal{I}$ is irreducible and the map $(-)_{\mathsf{R}}$ is injective, the polynomials I_{R} with $I \in \mathcal{I}$ are irreducible and distinct. Now, consider

$$f : \mathbf{F}_p[T] \setminus \{0\} \to \mathbf{Z}_{\geqslant 0}, \qquad f(G) = \sum_{\substack{I \in \mathcal{I} \\ I \mid G^{\mathsf{R}},\, I^2 \nmid G^{\mathsf{R}}}} 1.$$

The function f is *additive*: that is, $f(G_1G_2) = f(G_1) + f(G_2)$ whenever G_1 and G_2 are coprime (because we must then also have that G_1^{R} and G_2^{R} are coprime — see Lemma 5.11). With this notation, (16.3) is equivalent to showing that

$$\mathbb{P}_{\mathsf{R}, B \in \mathcal{M}(m)}\big(f(B_p) = 0\big) \leqslant C_\varepsilon m^{-1/4+\varepsilon}. \tag{16.4}$$

Let

$$\ell = \lfloor m/\log m \rfloor$$

and, for $G \in \mathcal{M}(m)$, write

$$G_p^{S(\ell)} = \prod_{\substack{J^v \| G_p,\ J \text{ irreducible} \\ \deg J \leqslant \ell,\, J \neq T}} J^v$$

for the *ℓ-smooth part* of G_p (see [7, Equation (9.2)]). We have

$$\mathbb{P}_{\mathsf{R}, B \in \mathcal{M}(m)}\big(f(B_p) = 0\big) \leqslant \mathbb{P}_{\mathsf{R}, B \in \mathcal{M}(m)}\Big(f\big(B_p^{S(\ell)}\big) = 0\Big). \tag{16.5}$$

Having set up notation, observe that $f(J^v) \in \{0,1\}$ when $J \in \mathbf{F}_p[T]$ is monic and irreducible and $v \in \mathbf{Z}_{\geqslant 1}$. So we may apply [7, Lemma 9.2(a)] with parameters $\theta = 1/2$, $C_1 = 3$, $t = 0$, and with their m being our ℓ. In addition, note that $\Delta_{\mathsf{R},p}(m; m/2) \leqslant \Delta_p^{\mathsf{R}}(m; m/2) \leqslant m^{-9}$ by Lemma 13.1. In conclusion,

$$\mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\big(f(B_p) = 0\big) \leqslant \mathbb{P}_{\mathsf{R},B\in\mathcal{M}(m)}\Big(f\big(B_p^{S(\ell)}\big) = 0\Big) \leqslant e^{-L} + 1/m,$$

where

$$L := \sum_{\substack{\deg J \leqslant \ell \\ f(J)=1 \\ J \text{ irreducible}}} \frac{1}{\|J\|_p} = \sum_{I\in\mathcal{I}} \frac{1}{\|I\|_p^{1/2}}.$$

By the Prime Polynomial Theorem for reciprocals, Lemma 16.2, we have

$$L = \sum_{1\leqslant d\leqslant \ell/2} \frac{S_p(4d)}{p^{2d}} \geqslant \sum_{1\leqslant d\leqslant \ell/2} \frac{1 - 2p^{-4d/3}}{4d} = \frac{\log \ell}{4} + O(1).$$

Since $\log \ell = \log m + O(\log\log m)$, the result follows. □

We are now ready to prove Proposition 2.7.

Proof of Proposition 2.7. Define the events

$$\begin{aligned}
\mathcal{E}_1 &:= \Big\{\mathcal{G}_A \notin \{C_2 \wr \mathcal{S}_m, G_2, G_3\} \text{ and } A \text{ is irreducible}\Big\},\\
\mathcal{E}_2 &:= \Big\{\operatorname{proj}(\mathcal{G}_A) \notin \{\mathcal{A}_m, \mathcal{S}_m\} \text{ and } A \text{ is irreducible}\Big\},\\
\mathcal{E}_3 &:= \Big\{\Delta(A) \neq 0 \text{ is a square and } A \text{ is irreducible}\Big\},\\
\mathcal{E}_4 &:= \Big\{\mathcal{G}_A \leqslant C_2 \times \mathcal{S}_m \text{ and } A \text{ is irreducible}\Big\}.
\end{aligned}$$

For an event $\mathcal{E}$, denote by $\mathcal{E}^{\mathrm{comp}}$ the complementary event. Then

$$\mathbb{P}(\mathcal{E}_1) \leqslant \mathbb{P}\Big(\mathcal{E}_1 \cap \mathcal{E}_2^{\mathrm{comp}} \cap \mathcal{E}_3^{\mathrm{comp}} \cap \mathcal{E}_4^{\mathrm{comp}}\Big) + \mathbb{P}(\mathcal{E}_2) + \mathbb{P}(\mathcal{E}_3) + \mathbb{P}(\mathcal{E}_4).$$

We will treat the four terms on the right-hand side separately.

We first show that the event $\mathcal{E} := \mathcal{E}_1 \cap \mathcal{E}_2^{\mathrm{comp}} \cap \mathcal{E}_3^{\mathrm{comp}} \cap \mathcal{E}_4^{\mathrm{comp}}$ is empty, so that $\mathbb{P}(\mathcal{E}) = 0$. Indeed, suppose $\mathcal{E}$ holds. Then A is irreducible on account of $\mathcal{E} \subset \mathcal{E}_1$. Furthermore, since $\mathcal{E} \subset \mathcal{E}_3^{\mathrm{comp}}$, we find that $\Delta(A)$ is not a square, so $\mathcal{G}_A \not\leqslant \mathcal{A}_{2m}$ by Lemma 7.1. In particular $\mathcal{G}_A \notin \{G_1, G_4\}$, since the latter groups lie in $\mathcal{A}_{2m}$. Lastly, since $\mathcal{E} \subset \mathcal{E}_2^{\mathrm{comp}} \cap \mathcal{E}_4^{\mathrm{comp}}$, we also have $\mathcal{G}_A \not\leqslant C_2 \times \mathcal{S}_m$ and $\operatorname{proj}(\mathcal{G}_A) \in \{\mathcal{A}_m, \mathcal{S}_m\}$. By Lemma 14.4 we obtain that $\mathcal{G}_A \in \{C_2 \wr \mathcal{S}_m, G_2, G_3\}$, contradicting $\mathcal{E}_1$.

To estimate $\mathbb{P}(\mathcal{E}_2)$, note that conditions (1) and (2) of Lemma 15.3 are met. Combined with Lemma 15.1, this implies the existence of constants $c_0, C_0 > 0$ depending at most on ε such that

$$\mathbb{P}(\mathcal{E}_2) \leqslant C_0 m^{-c_0}.$$

For $\mathbb{P}(\mathcal{E}_3)$, observe that condition (3) implies $\|\mu_j\|_\infty \leqslant 1 - (\log m)^{-2}$ as well. Combining this with condition (1) means we may apply Proposition 2.8 with parameter $\varepsilon_{\text{Proposition 2.8}} = (\log m)^{-2}$. Hence $\Delta(A) \neq 0$ is a square with probability $\mathbb{P}(\mathcal{E}_3) \leqslant C_1 m^{-\alpha/2}$, for some $C_1 > 0$ depending at most on α and B.

Lastly, since the conditions of Lemma 16.3 are met, we immediately establish the bound $\mathbb{P}(\mathcal{E}_4) \ll_\delta m^{-1/4+\delta}$ for every $\delta > 0$. This concludes the proof. □

Remark 16.4. Condition (2) of Lemma 15.3 and condition (3) of Proposition 2.7 may be replaced by something weaker, just as condition (2) of Lemma 15.2 replaced condition (15.1). The adjusted condition would then bound the probability that T^2+1 divides A_p to a large power. In Proposition 2.7, we would still require an anti-concentration condition on all measures μ_j over the integers, so that we may still apply Proposition 2.8.

Remark 16.5. We have $\mathcal{G}_A \leqslant G_2$ if and only if $(-1)^m A(1)A(-1)\Delta(A_{\mathsf{R}})$ is a nonzero square [1, Lemma 3.8(b)] and $\mathcal{G}_A \leqslant G_3$ if and only if $\Delta(A_{\mathsf{R}})$ is a nonzero square.

References

1. T. C. Anderson, A. Bertelli and E. M. O'Dorney, *Galois groups of reciprocal polynomials and the Van der Waerden–Bhargava theorem*, preprint arXiv:2406.18970, 21 pp.
2. M. Aschbacher, *Finite group theory* (second edition), Cambridge Studies in Advanced Mathematics **10**, Cambridge University Press, Cambridge, 2000.
3. E. Bank, L. Bary-Soroker, and A. Fehm, *Sums of two squares in short intervals in polynomial rings over finite fields*, Amer. J. Math. **140** (2018), 1113–1131.
4. L. Bary-Soroker, O. Ben-Porath, and V. Matei, *Probabilistic Galois Theory – The Square Discriminant Case*, Bull. Lond. Math. Soc. **56** (2024), 2162–2177.
5. L. Bary-Soroker and N. Goldgraber, *Full Galois groups of polynomials with slowly growing coefficients*, Bull. Lond. Math. Soc. **57** (2025), 941–955.
6. L. Bary-Soroker, D. Hokken, G. Kozma, and B. Poonen, *Irreducibility of Littlewood polynomials of special degrees*, to appear in Int. Mat. Res. Not., preprint arXiv:2308.04878, 4 pp., 2023.
7. L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), 1041–1120.
8. L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height*, Duke Math. J. **169** (2020), 579–598.
9. P. T. Bateman, *The distribution of values of the Euler function*, Acta Arith. **21** (1972), 329–345.
10. M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's conjecture*, Ann. of Math. (2) **201** (2025), 339–377.
11. E. Breuillard and P. Varjú, *Irreducibility of random polynomials of large degree*, Acta Math. **223** (2019), 195–249.
12. F. Brunault and W. Zudilin, *Many variations of Mahler measures—a lasting symphony*, Australian Mathematical Society Lecture Series **28**, Cambridge University Press, Cambridge, 2020.
13. A. Cafure and E. Cesaratto, *Irreducibility criteria for reciprocal polynomials and applications*, Amer. Math. Monthly **124** (2017), 37–53.
14. S. Chow and R. Dietmann, *Towards van der Waerden's conjecture*, Trans. Amer. Math. Soc. **376** (2023), 2739–2785.
15. S. David, W. Duke, and X. Sun, *Probabilistic Galois theory of reciprocal polynomials*, Exposition. Math. **16** (1998), 263–270.
16. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
17. A. Dubickas, *Salem numbers as Mahler measures of nonreciprocal units*, Acta Arith. **176** (2016), 81–88.
18. S. Eberhard, *The characteristic polynomial of a random matrix*, Combinatorica **42** (2022), 491–527.
19. A. Entin, *Galois groups of random polynomials over the rational function field*, J. Lond. Math. Soc. (2) **111** (2025), Paper No. e70061, 23 pp.
20. A. Ferber, V. Jain, A. Sah, and M. Sawhney, *Random symmetric matrices: rank distribution and irreducibility of the characteristic polynomial*, Math. Proc. Cambridge Philos. Soc. **174** (2023), 233–246.
21. P. X. Gallagher, *The large sieve and probabilistic Galois theory*. In: *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV)*, Amer. Math. Soc., Providence, RI, 1973, 91–101.
22. W. Hoeffding, *Probability inequalities for sums of bounded random variables*, J. Amer. Statist. Assoc. **58** (1963), 13–30.
23. D. Hokken, *Counting (skew-)reciprocal Littlewood polynomials with square discriminant*, to appear in Isr. J. Math., preprint arXiv:2301.05656, 20 pp., 2025.
24. E. Kim, *Characterizing the support of semiclassical measures for higher-dimensional cat maps*, preprint arXiv:2410.13449, 64 pp., with an appendix by T. C. Anderson and R. J. Lemke Oliver.
25. S. V. Konyagin, *On the number of irreducible polynomials with* $0, 1$ *coefficients*, Acta Arith. **88** (1999), 333–350.

26. T. Łuczak and L. Pyber, *On random generation of the symmetric group*, Combin. Probab. Comput. **2** (1993), 505–512.
27. A. Odlyzko and B. Poonen, *Zeros of polynomials with* 0, 1 *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.
28. H. Meyn and W. Götz, *Self-reciprocal polynomials over finite fields*, Séminaire Lotharingien de Combinatoire Oberfranken **21** (1989), Article B21d, 8 pp.
29. H. T. Pham and M. W. Xu, *Irreducibility of random polynomials of bounded degree*, Discrete Anal. (2021), Paper No. 7, 16 pp.
30. V. V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics **11**, Springer-Verlag, Berlin, 2004.
31. B. A. Rogozin, *An estimate of the concentration functions*, Teor. Verojatnost. i Primenen. **6** (1961), 103–105.
32. M. I. Stronina, *Integral points on circular cones*, Izv. Vyss. Učebn. Zaved. Matematika **8** (1969), 112-116.
33. P. Viana and P. M. Veloso, *Galois theory of reciprocal polynomials*, Amer. Math. Monthly **109** (2002), 466-471.
34. B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.
35. B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), 133–147.

DH: Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland
Email address: d.p.t.hokken@uu.nl

DK: Département de mathématiques et de statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal, QC H3C 3J7, Canada
Email address: dimitris.koukoulopoulos@umontreal.ca