# FULL GALOIS GROUPS OF POLYNOMIALS WITH SLOWLY GROWING COEFFICIENTS 

LIOR BARY-SOROKER AND NOAM GOLDGRABER


#### Abstract

Choose a polynomial $f$ uniformly at random from the set of all monic polynomials of degree $n$ with integer coefficients in the box $[-L, L]^{n}$. The main result of the paper asserts that if $L=L(n)$ grows to infinity, then the Galois group of $f$ is the full symmetric group, asymptotically almost surely, as $n \rightarrow \infty$.

When $L$ grows rapidly to infinity, say $L>n^{7}$, this theorem follows from a result of Gallagher. When $L$ is bounded, the analog of the theorem is open, while the state-of-the-art is that the Galois group is large in the sense that it contains the alternating group (if $L<17$, it is conditional on the general Riemann hypothesis). Hence the most interesting case of the theorem is when $L$ grows slowly to infinity.

Our method works for more general independent coefficients.


## 1. Introduction

The study of the Galois group of a random polynomial is going back to the foundational works of Hilbert [16] and van der Waerden [24]. Expressed in terms of probability theory, they proved that if we uniformly choose at random a monic polynomial $f$ of degree $n$ whose coefficients are within the box $([-L, L] \cap \mathbb{Z})^{n}$, then its Galois group $G_{f}$ is the full symmetric group, almost surely as $L \rightarrow \infty$ and $n$ is fixed; i.e. $\lim _{L \rightarrow \infty} \mathbb{P}\left(G_{f}=S_{n}\right)=1$. We call this model the large box model.

Van der Waerden conjectured that the second most probable group in the large box model is $S_{n-1}$ coming from polynomials having a rational root. Chela [10, Theorem 1] computed that $\mathbb{P}\left(G_{f}=S_{n-1}\right) \sim \frac{c_{n}}{L}$, as $L \rightarrow \infty$ and $n>2$, where $c_{n}=\Theta\left(2^{n}\right)$ is an explicit constant. Thus, the van der Waerden conjecture may be stated as $\mathbb{P}\left(G_{f} \neq S_{n}\right) \sim \frac{c_{n}}{L}, L \rightarrow \infty$. A slightly weaker version of the conjecture is that $\mathbb{P}\left(G_{f} \neq S_{n}\right)=O\left(L^{-1}\right)$, as $n$ is fixed and $L \rightarrow \infty$. The weaker version is occasionally also referred to as the van der Waerden conjecture.

After almost of a century of progress [1, 11, 12, 13, 15, 18, 24, the latter bound was established by Bhargava [6]. The main challenge in the above results is to bound $\mathbb{P}\left(G_{f}=A_{n}\right)$ from above, in particular, a key result in [6] is that

$$
\mathbb{P}\left(G_{f}=A_{n}\right)=O\left(L^{-1}\right), \quad L \rightarrow \infty .
$$

This is the state-of-the-art, even though it is believed to be not sharp, see [2, Conjecture 1.1].

In the large box model, the degree $n=\operatorname{deg} f$ is fixed. In particular, the rate of convergence and the implied constants depend on $n$. Indeed, in the majority of the results mentioned above, the implied constant is at least exponential, sometimes super-exponential in $n$, or not given explicitly. A notable exception is the method of Gallagher [15] that is based on the large sieve and gives a polynomial dependence on $n$ :

$$
\begin{equation*}
\mathbb{P}\left(G_{f} \neq S_{n}\right) \ll \frac{n^{3} \log L}{\sqrt{L}}, \tag{1}
\end{equation*}
$$

where the implied constant is absolute, see also [20, Theorem 4.2].
Random polynomials are central in probability theory. One of the most natural and well-studied models are when the coefficients are sampled independently and the degree goes to infinity. This model goes back to the seminal works of BlochPólya [8], Littlewood-Offord [21], Kac [17], and Erdôs-Túran [14]. As an example model, take $f$ as previously defined, but with $L \geq 1$ fixed and with $n \rightarrow \infty$. We call this model the restricted box model.

It is a folklore conjecture that in the restricted box model, $f$ is irreducible and $G_{f}=S_{n}$ asymptotically almost surely, as $n \rightarrow \infty$ (conditioning on $f(0) \neq 0$, of course), cf. [22]. Recently there has been progress on this problem based on the methods developed by Konyagin [19]: Bary-Soroker and Kozma [4] proved that if the length of the interval is divisible by at least 4 distinct primes, then $f$ is irreducible and $A_{n} \leq G_{f}$ asymptotically almost surely, provided $f(0) \neq 0$. Breuillard and Varjú [9] proved the same for any $L \geq 1$ assuming the General Riemann Hypothesis (GRH). In fact, they consider a more general model, where the coefficient are i.i.d. with an arbitrary finite support law of distribution. Bary-Soroker, Koukoulopoulos, and Kozma [3] also deal with general measures. Their results are independent of GRH, and the coefficients are not required to be identical. In particular, in the restricted box model they prove that $\mathbb{P}\left(A_{n} \leq G_{f} \mid f(0) \neq 0\right) \rightarrow 1$, $n \rightarrow \infty$ if the interval is of length $\geq 35$ and $\liminf _{n \rightarrow \infty} \mathbb{P}\left(A_{n} \leq G_{f}\right)>0$ if the length of the interval is between 2 to 34 , see [3, Theorem 6].

As in the large box model, the most challenging case is $G_{f}=A_{n}$. Unlike the large box model, in the restricted box model none of the results give that $\mathbb{P}\left(G_{f}=\right.$ $\left.A_{n}\right) \rightarrow 0$, hence it is open whether $\mathbb{P}\left(G_{f}=S_{n}\right) \rightarrow 1$ as $n \rightarrow \infty$.

The goal of this paper is to get as close as we can to the restricted box model. We get that $G_{f}=S_{n}$ asymptotically almost surely, as $L \rightarrow \infty$, uniformly in $n$. In particular, $L$ may grow arbitrarily slowly with respect to $n$.

Theorem 1.1. Let $L$ and $n$ be positive integers and let

$$
f=X^{n}+\sum_{k=0}^{n-1} \zeta_{k} X^{k}
$$

FULL GALOIS GROUPS OF POLYNOMIALS WITH SLOWLY GROWING COEFFICIENTS 3
be a random polynomial, where $\zeta_{k}$ are chosen independently and identically distributed, taking values uniformly in $[-L, L] \cap \mathbb{Z}$. Then,

$$
\lim _{L \rightarrow \infty} \mathbb{P}\left(G_{f}=S_{n}\right)=1,
$$

uniformly in $n$.
In the regime $L \geq n^{7}$, the theorem immediately follows from (1). The interesting part of the theorem is when $L=L(n)$ tends slowly to infinity as $n$ tends to infinity.

The main difficulty lies in the event $G_{f}=A_{n}$. Since $G_{f} \leq A_{n}$ if and only if disc $f$ is a perfect square, provided $\operatorname{disc}(f) \neq 0$, we get that $\mathbb{P}\left(G_{f}=A_{n}\right) \leq \mathbb{P}(\operatorname{disc}(f)=\square)$. Hence, Theorem 1.1 follows from the following theorem, see $\$ 4.1$.

Theorem 1.2. For every $\frac{1}{2}>\delta>0$ there exists $N>0$ such that the following holds: Let $\frac{1}{8}>\varepsilon>0$, let $a, L, n$ be integers such that $n>8$ and $L \geq N$, let $\zeta_{0}, \zeta_{1}, \ldots$ be independent random variables taking values uniformly in $[a+1, a+L] \cap \mathbb{Z}$, and let

$$
f=X^{n}+\sum_{k=0}^{n-1} \zeta_{k} X^{k}
$$

be the corresponding random polynomial. Then,

$$
\mathbb{P}(\operatorname{disc}(f)=\square) \ll 2^{-\left(\frac{1}{2}-\delta\right) \frac{\log L}{\log \log L}}+\frac{\log L}{\log \log L}\left(\frac{2}{(1-\delta) \log L}\right)^{\left(\frac{1}{4}-\varepsilon\right) n},
$$

where the implied constant is absolute.
The proof of Theorem 1.2 is based on harmonic analysis and on bounds for exponential-Möbius sums over function fields [7, 23]. Our method allows us to prove this theorem for general measures that satisfy several conditions, (see Proposition (2.1). We deduce Theorem 1.2 from Proposition 2.1 in 84.3 .

## Acknowledgments

The authors thank Zeev Rudnick for a beneficial conversation regarding exponential sums.

This research was supported by the Israel Science Foundation (grant no. 702/19).

## 2. Square discriminant for general measures

2.1. Harmonic analysis over finite fields. We introduce the notation and basic results needed to prove the main theorem. We restrict to prime fields for simplicity of notation. For a prime $p$, let $\mathbb{F}_{p}$ be the finite field with $p$ elements and $\mathbb{F}_{p}[T]$ the polynomials ring over $\mathbb{F}_{p}$. We denote by $\mathcal{M}_{p, n} \subseteq \mathcal{M}_{p} \subset \mathbb{F}_{p}[T]$ the subsets of monic polynomials of degree $n$ and of all monic polynomials, respectively. Let $\mathbb{F}_{p}\left(\left(T^{-1}\right)\right)$ be the field of Laurent series of the form $\xi=\sum_{-\infty}^{N} c_{j} T^{j}, N \in \mathbb{Z}, c_{j} \in \mathbb{F}_{p}$ and let

$$
\mathbb{T}_{p}=\mathbb{F}_{p}\left(\left(T^{-1}\right)\right) / \mathbb{F}_{p}[T]
$$

Each element in $\mathbb{T}_{p}$ has a unique representative of the form $\sum_{j<0} c_{j} T^{j}, c_{j} \in \mathbb{F}_{p}$. Let resp: $\mathbb{T}_{p} \rightarrow \mathbb{F}_{p}$ be the additive function defined by $\operatorname{res}_{p}(\xi)=c_{-1}$. In the classical analogy between $\mathbb{Z}$ and $\mathbb{F}_{p}[T], \mathcal{M}_{p}$ plays the role of $\mathbb{Z}_{>0}$, and $\mathcal{M}_{p, n}$ the role of $[x, 2 x] \cap \mathbb{Z}$, with $\log x$ corresponding to $n$. The analog of $\mathbb{R}$ is $\mathbb{F}_{p}\left(\left(T^{-1}\right)\right)$ and of $\mathbb{T}=\mathbb{R} / \mathbb{Z}$ is $\mathbb{T}_{p}$. Let

$$
e(z)=e^{2 \pi i z} \quad \text { and } \quad e_{p}(\xi)=e\left(\operatorname{res}_{p}(\xi) / p\right)
$$

for $z \in \mathbb{C}$ and $\xi \in \mathbb{T}_{p}$. The latter is well defined. We define the Fourier transform of $\eta: \mathcal{M}_{p, n} \rightarrow \mathbb{C}$ to be

$$
\widehat{\eta}(\xi)=\sum_{G \in \mathcal{M}}^{p, n} 1 \eta(G) e_{p}(\xi G), \quad \xi \in \mathbb{T}_{p}
$$

This is the analogue of the discrete Fourier transform in the classical setting.
Our method necessitates considering several primes simultaneously. Let $\mathcal{P}$ be a finite set of primes and $P=\prod_{p \in \mathcal{P}} p$. Let

$$
\mathbb{F}_{\mathcal{P}}=\prod_{p \in \mathcal{P}} \mathbb{F}_{p}, \quad \mathbb{F}_{\mathcal{P}}\left(\left(T^{-1}\right)\right)=\prod_{p \in \mathcal{P}} \mathbb{F}_{p}\left(\left(T^{-1}\right)\right), \quad \text { and } \quad \mathcal{M}_{\mathcal{P}, n}=\prod_{p \in \mathcal{P}} \mathcal{M}_{p, n}
$$

Denote the elements of $\mathcal{M}_{\mathcal{P}, n}$ and of $\mathbb{F}_{\mathcal{P}}\left(T^{-1}\right)$ by $\boldsymbol{F}=\left(F_{p}\right)_{p \in \mathcal{P}}$ and $\boldsymbol{\xi}=\left(\xi_{p}\right)_{p \in \mathcal{P}}$, respectively. Then, we set

$$
\psi_{\mathcal{P}}(\boldsymbol{\xi})=\sum_{p \in \mathcal{P}} \frac{\operatorname{res}\left(\xi_{p}\right)}{p} \bmod 1, \quad \quad e_{\mathcal{P}}(\boldsymbol{\xi})=e\left(\psi_{\mathcal{P}}(\boldsymbol{\xi})\right)=\prod_{p \in \mathcal{P}} e_{p}\left(\xi_{p}\right)
$$

Then, for $\eta: \mathcal{M}_{\mathcal{P}, n} \rightarrow \mathbb{C}$ we define $\widehat{\eta}: \mathbb{F}_{\mathcal{P}}\left(\left(T^{-1}\right)\right) \rightarrow \mathbb{C}$ by

$$
\widehat{\eta}(\boldsymbol{\xi})=\sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \eta(\boldsymbol{G}) e_{\mathcal{P}}(\boldsymbol{\xi} \boldsymbol{G}) .
$$

We have the following three classical formulas. The first one is orthogonality of characters: for $\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}$,

$$
\sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} e_{\mathcal{P}}\left(T^{-n} \boldsymbol{F} \boldsymbol{G}\right)= \begin{cases}P^{n} & F_{p}=T^{n}, \forall p \in \mathcal{P}  \tag{2}\\ 0 & \text { otherwise }\end{cases}
$$

The second is the Fourier inversion formula saying that if $\eta: \mathcal{M}_{\mathcal{P}, n} \rightarrow \mathbb{C}$, then

$$
\begin{equation*}
\eta(\boldsymbol{F})=\frac{1}{P^{n}} \sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \widehat{\eta}\left(T^{-n} \boldsymbol{G}\right) e_{\mathcal{P}}\left(-T^{-n} \boldsymbol{G} \boldsymbol{F}\right) \tag{3}
\end{equation*}
$$

and the last is the Parserval-Plancherel theorem, which for real functions $\eta, \zeta: \mathcal{M}_{\mathcal{P}, n} \rightarrow$ $\mathbb{R}$ gives that

$$
\begin{equation*}
\sum_{\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}} \eta(\boldsymbol{F}) \zeta(\boldsymbol{F})=\frac{1}{P^{n}} \sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \widehat{\eta}\left(T^{-n} \boldsymbol{G}\right) \widehat{\zeta}\left(-T^{-n} \boldsymbol{G}\right) \tag{4}
\end{equation*}
$$

Since these are so classical we omit their proofs.
2.2. Main technical result. Let $f$ be a random monic polynomial of degree $n$ with coefficients in $\mathbb{Z}$. The pushforward defines a probability measure $\mathbb{P}_{\mathcal{P}}$ on $\mathbb{F}_{\mathcal{P}}[X]$, supported on $\mathcal{M}_{\mathcal{P}, n}$, and an expectation function $\mathbb{E}_{\mathcal{P}}$ :
(5) $\mathbb{P}_{\mathcal{P}}(\boldsymbol{F}):=\mathbb{P}\left(\bigcap_{p \in \mathcal{P}}\left\{f_{p}=F_{p}\right\}\right) \quad$ and $\quad \mathbb{E}_{\mathcal{P}}(\eta)=\mathbb{E}_{\mathcal{P}}(\eta(\boldsymbol{F}))=\sum_{\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}} \mathbb{P}_{\mathcal{P}}(\boldsymbol{F}) \eta(\boldsymbol{F})$.

The Möbius function $\mu_{p}$ on $\mathbb{F}_{p}[T]$ is defined by

$$
\mu_{p}\left(F_{p}\right)= \begin{cases}(-1)^{r} & F_{p} \text { is a product of } r \text { distinct irreducible polynomials } \\ 0 & F_{p} \text { is not squarefree } .\end{cases}
$$

Proposition 2.1. Let $0<\alpha, 1 \leq \gamma<4 / 3$, and $0<c<\frac{4-3 \gamma}{4 \gamma}$. Then there exists $C>0$ such that the following holds. Let $\left(\lambda_{k}\right)_{k=0}^{\infty}$ be a sequence of probability measures on $\mathbb{Z}$, let $\left(\zeta_{k}\right)_{k=0}^{\infty}$ be a sequence of independent random variables with $\zeta_{k}$ distributing according to $\lambda_{k}, k=0,1, \ldots$, and let $f=X^{n}+\sum_{k=0}^{n-1} \zeta_{k} X^{k}$ be the corresponding random polynomial. Let $\mathcal{P}$ a finite set of primes and let $\omega: \mathcal{P} \rightarrow \mathbb{R}_{\geq 0}$ be a function. Assume that
(2.1.1) $\min \mathcal{P} \geq C$,
(2.1.2) $\sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}}\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{G}\right)\right|^{\gamma} \leq \alpha^{\gamma n}$, and
(2.1.3) for every subset $\mathcal{Q}=\left\{p_{1}, \ldots, p_{r}\right\} \subseteq \mathcal{P}$, we have

$$
\left|\sum_{1 \leq i_{1}, \ldots, i_{r} \leq \frac{n}{2}} \sum_{\substack{D_{k} \in \mathcal{M}_{k, i_{k}} \\ \forall 1 \leq k \leq r}} \cdots \sum_{1} \mathbb{P}\left(D_{1}^{2}\left|f_{p_{1}}, \ldots, D_{r}^{2}\right| f_{p_{r}}\right) \prod_{1 \leq m \leq r} \mu_{p_{m}}\left(D_{m}\right)\right| \leq \prod_{1 \leq m \leq r} \omega\left(p_{m}\right)^{-1} .
$$

Then,

$$
\begin{equation*}
\mathbb{P}(\operatorname{disc}(f)=\square) \leq \prod_{p \in \mathcal{P}}\left(1+\frac{1}{2 p^{c n}}\right)-1+\frac{1}{2^{\# \mathcal{P}}} \cdot \prod_{p \in \mathcal{P}}\left(1+\omega(p)^{-1}\right) . \tag{6}
\end{equation*}
$$

The proof of Proposition 2.1 is given in \$3.3. It is based on the following two ingredients.

Let $q$ be an odd prime power, let $\mathbb{F}_{q}$ be the finite field with $q$ elements, $\chi_{q}$ the quadratic character of $\mathbb{F}_{q}$, and $\mu$ the Möbius function. The first is the formula of Stickelberger and Swan:

$$
\chi_{q}(\operatorname{disc}(F))=(-1)^{\operatorname{deg} F} \mu(F),
$$

see, for example, Theorem 6.68 in 5 and the discussion after its proof. Thus,

$$
\begin{equation*}
\mathbb{1}_{\operatorname{disc}(F)=\square}=\frac{1+(-1)^{\operatorname{deg} F} \mu(F)+\mathbb{1}_{\mu(F)=0}}{2} \tag{7}
\end{equation*}
$$

where $\mathbb{1}_{\mu(F)=0}=1-\mu^{2}(F)$ is the indicator function of non-squarefree polynomials. The second is a bound on the $L_{\infty}$ norm of $\widehat{\mu}_{q}$ proved independently by Porrit [23] and Bienvenue and Lê [7]:

Theorem 2.2. For every $0<\varepsilon<1 / 4$ there exists $q_{0}>0$ such that for every prime power $q \geq q_{0}$ we have

$$
\max _{\vartheta \in \mathbb{T}}\left|\widehat{\mu}_{q}(\vartheta)\right| \leq q^{\left(\frac{3}{4}+\varepsilon\right) n}
$$

A key step in the proof is to evaluate the probability that the discriminant being a square modulo $p$. In particular, we may prove the following result on finite fields, which we state formally as it may be interesting on its own.
Proposition 2.3. Let $1 \leq \gamma<4 / 3, \alpha>0$ and $0<c<\frac{4-3 \gamma}{4 \gamma}$. Then, there exists $C>0$ such that the following holds. Let $q \geq C$ be a prime power, let $\left(\lambda_{k}\right)_{k=0}^{\infty}$ be a sequence of probability measures on $\mathbb{F}_{q}$, let $\left(\zeta_{k}\right)_{k=0}^{\infty}$ be a sequence of independent random variables with $\zeta_{k}$ distributing according to $\lambda_{k}, k=0,1, \ldots$, and let $F=$ $X^{n}+\sum_{k=0}^{n-1} \zeta_{k} X^{k}$ be the corresponding random polynomial. Assume that
(1) $\left.\sum_{F \in \mathcal{M}_{q, n}} \widehat{\mathbb{P}}\left(T^{-n} F\right)\right|^{\gamma} \leq \alpha^{\gamma n}$, and
(2) $\sum_{i=1}^{\lfloor n / 2\rfloor} \sum_{D \in \mathcal{M}_{q, i}} \mu(D) \cdot \mathbb{P}\left(D^{2} \mid F\right) \leq \omega_{q}^{-1}$ for some $\omega_{q} \in \mathbb{R}_{\geq 0}$. Then,

$$
\left|\mathbb{P}(\operatorname{disc}(F)=\square)-\frac{1}{2}\right| \leq \frac{1}{2 q^{c n}}+\frac{1}{2 \omega_{q}} .
$$

## 3. General measures

3.1. Number theory auxiliary results. For the reader's convenience, we recall some well-known results from number theory that shall be used in subsequent sections. Mertens' second theorem says that

$$
\begin{equation*}
\sum_{p \leq x} \frac{1}{p}=\log \log x+M+O(1 / \log x) \tag{8}
\end{equation*}
$$

where $M=0.261 \ldots$ is the Meissel-Mertens constant. Thus,

$$
\sum_{z<p \leq 2 z} \frac{1}{p}=\log \log 2 z-\log \log z+O(1 / \log z) \ll 1
$$

for all $z>1$. Hence, if $\omega(p) \geq C^{-1} p$ for all $z<p \leq 2 z$, then

$$
\begin{equation*}
\prod_{z<p \leq 2 z}\left(1+\omega(p)^{-1}\right) \leq \exp \left(C \sum_{z<p \leq 2 z} \frac{1}{p}\right) \ll 1 . \tag{9}
\end{equation*}
$$

The prime number theorem has the following two classical formulations

$$
\begin{align*}
& \pi(x):=\sum_{p \leq x} 1 \quad=\frac{x}{\log x}+O\left(x /(\log x)^{2}\right),  \tag{10}\\
& \vartheta(x):=\sum_{p \leq x} \log p=x+O(x / \log x) \tag{11}
\end{align*}
$$

We may deduce the following bound for $\alpha>1$ :

$$
\begin{equation*}
\prod_{z<p \leq 2 z}\left(1+C p^{-\alpha}\right) \leq \exp \left(C^{\prime} \frac{z}{z^{\alpha} \log z}\right)=1+O_{\alpha}\left(\frac{z}{z^{\alpha} \log z}\right) . \tag{12}
\end{equation*}
$$

3.2. The indicator function of non-squarefrees. The goal of this section is to provide a formula for the expectation value of the indicator function of nonsquarefrees modulo several primes.

Let $f$ be a random monic polynomial over $\mathbb{Z}$ with independent coefficients, such as in Proposition 2.1. For a prime $p \in \mathbb{Z}$, let $f_{p} \in \mathbb{F}_{p}[X]$ denote the polynomial one gets by reducing the coefficients of $f$ modulo $p$. Similarly, if $\mathcal{P}$ is a set of primes, then we denote $f_{\mathcal{P}}:=\left(f_{p}\right)_{p \in \mathcal{P}} \in \mathcal{M}_{\mathcal{P}, n}$ and view it as a random variable.

For a subset $\mathcal{Q} \subseteq \mathcal{P}$, we extend multiplicatively the definitions of the Möbius function and the of indicator function of non-squarefrees: For $\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}}$, we define

$$
\begin{align*}
& \mu_{\mathcal{Q}}(\boldsymbol{F}):=\prod_{p \in \mathcal{Q}} \mu_{p}\left(F_{p}\right), \\
& \eta_{\mathcal{Q}}(\boldsymbol{F}):=\prod_{p \in \mathcal{Q}} \mathbb{1}_{\mu_{p}\left(F_{p}\right)=0 .} . \tag{13}
\end{align*}
$$

By the Möbius inversion formula applied to the squareful part of $F \in \mathcal{M}_{p, n}$ one gets

$$
\begin{equation*}
\mu_{p}^{2}(F)=\sum_{D^{2} \mid F} \mu_{p}(D), \tag{14}
\end{equation*}
$$

so since $\mathbb{1}_{\mu_{q}(F)=0}=1-\mu^{2}(F)$, we conclude that

$$
\begin{equation*}
\eta_{\mathcal{Q}}(\boldsymbol{F})=\prod_{p \in \mathcal{Q}}\left(1-\sum_{D_{p}^{2} \mid F_{p}} \mu_{p}\left(D_{p}\right)\right)=(-1)^{\# \mathcal{Q}} \prod_{\substack { p \in \mathcal{Q} \\
\begin{subarray}{c}{D_{D}^{2} \mid F_{p} \\
D_{p} \neq 1{ p \in \mathcal { Q } \\
\begin{subarray} { c } { D _ { D } ^ { 2 } | F _ { p } \\
D _ { p } \neq 1 } }\end{subarray}} \mu_{p}\left(D_{p}\right) . \tag{15}
\end{equation*}
$$

Lemma 3.1. Let $F$ be a random variable taking values in $\mathcal{M}_{p, n}$ and let $E$ be an event. Then,

$$
\mathbb{P}\left(E \cap\left\{\mu_{p}(F)=0\right\}\right)=-\sum_{i=1}^{\lfloor n / 2\rfloor} \sum_{D \in \mathcal{M}_{p, i}} \mu_{p}(D) \cdot \mathbb{P}\left(E, D^{2} \mid F\right) .
$$

Proof. Apply (15) with $\mathcal{Q}=\{p\}$ to get

$$
\mathbb{P}\left(E \cap\left\{\mu_{q}(F)=0\right\}\right)=\mathbb{E}\left(\mathbb{1}_{E} \eta_{p}(F)\right)=-\sum_{D \neq 1} \mu_{q}(D) \mathbb{E}\left(\mathbb{1}_{E, D^{2} \mid F}\right) .
$$

We are done, since $\mathbb{E}\left(\mathbb{1}_{E, D^{2} \mid F}\right)=\mathbb{P}\left(E, D^{2} \mid F\right)$ and $\operatorname{deg} D \leq \frac{n}{2}$ as $D^{2} \mid F$.
Proposition 3.2. Let $f$ be chosen as in Proposition 2.1, and let $\mathcal{Q}=\left\{p_{1}, \ldots, p_{r}\right\} \subseteq$ $\mathcal{P}$ be finite sets of prime numbers. Then,

$$
\mathbb{E}_{\mathcal{P}}\left(\eta_{Q}\right)=(-1)^{r} \sum_{\substack{1 \leq i_{1}, \ldots, i_{r} \leq\lfloor n / 2\rfloor}} \sum_{\substack{D_{k} \in \mathcal{M}_{p_{k}, i i_{k}} \\ \forall \leq \leq \leq \leq r}} \cdots \prod_{1 \leq m \leq r} \mu\left(D_{m}\right) \cdot \mathbb{P}_{\mathcal{P}}\left(D_{1}^{2}\left|F_{p_{1}}, \ldots, D_{r}^{2}\right| F_{p_{r}}\right) .
$$

Proof. Since $\mathbb{E}_{\mathcal{P}}\left(\eta_{Q}\right)=\mathbb{P}_{\mathcal{P}}\left(\mu_{p_{1}}\left(f_{p_{1}}\right)=0, \ldots, \mu_{p_{r}}\left(f_{p_{r}}\right)=0\right)$, we may apply Lemma3.1 inductively, to conclude the proof.
3.3. Proof of Proposition 2.1. We choose $C$ to be sufficiently large depending only on $\alpha, \gamma$, and $c$, with exact value to be determined in the course of the proof. Let $s=\# \mathcal{P}$ and $\nu=\min \mathcal{P}$.

The condition $\operatorname{disc}(f)=\square$ implies that $\operatorname{disc}\left(f_{p}\right)=\square$ for all $p \in \mathcal{P}$, since $\operatorname{disc}\left(f_{p}\right) \equiv$ $\operatorname{disc}(f) \bmod p$. Recalling (5) and writing $\boldsymbol{F}=\left(F_{p}\right)_{p \in \mathcal{P}} \in \mathcal{M}_{\mathcal{P}, n}$, we get that

$$
\begin{align*}
\mathbb{P}(\operatorname{disc}(f)=\square) & \leq \mathbb{P}_{\mathcal{P}}\left(\bigcap_{p \in \mathcal{P}} \operatorname{disc}\left(F_{p}\right)=\square\right)=\mathbb{E}_{\mathcal{P}}\left(\prod_{p \in \mathcal{P}} \mathbb{1}_{\operatorname{disc}\left(F_{p}\right)=\square}\right) \\
& \stackrel{(7)}{=} 2^{-s} \mathbb{E}_{\mathcal{P}}\left(\prod_{p \in \mathcal{P}}\left(1+(-1)^{n} \mu_{p}\left(F_{p}\right)+\mathbb{1}_{\mu_{p}\left(F_{p}\right)=0}\right)\right)  \tag{16}\\
& \stackrel{(13)}{=} 2^{-s}\left(\sum_{\mathcal{Q} \subseteq \mathcal{P}} \mathbb{E}_{\mathcal{P}}\left(\eta_{\mathcal{Q}}\right)+\sum_{\varnothing \neq \mathcal{Q} \subseteq \mathcal{P}}(-1)^{\left.n|\mathcal{Q}|_{\mathbb{E}_{\mathcal{P}}}\left(\mu_{\mathcal{Q}} \sum_{\mathcal{R} \subseteq \mathcal{P} \backslash \mathcal{Q}} \eta_{\mathcal{R}}\right)\right) .}\right.
\end{align*}
$$

We bound the first summand by Proposition 3.2 and (2.1.3):

$$
\begin{equation*}
\left|\sum_{\mathcal{Q} \subseteq \mathcal{P}} \mathbb{E}_{\mathcal{P}}\left(\eta_{\mathcal{Q}}\right)\right|=\sum_{\mathcal{Q} \subseteq \mathcal{P}} \mathbb{E}_{\mathcal{P}}\left(\eta_{\mathcal{Q}}\right) \leq \sum_{\mathcal{Q} \subseteq \mathcal{P}} \prod_{p \in \mathcal{Q}} \omega(p)^{-1}=\prod_{p \in \mathcal{P}}\left(1+\omega(p)^{-1}\right) \tag{17}
\end{equation*}
$$

Let $\mathfrak{S}:=2^{-s}\left|\sum_{\varnothing \neq \mathcal{Q} \subseteq \mathcal{P}}(-1)^{n \mid \mathcal{Q}} \mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}} \sum_{\mathcal{R} \subseteq \mathcal{P} \backslash \mathcal{Q}} \eta_{\mathcal{R}}\right)\right|$. We have

$$
\left|\sum_{\mathcal{R} \subseteq \mathcal{P} \backslash \mathcal{Q}} \eta_{\mathcal{R}}(\boldsymbol{F})\right|=\sum_{\mathcal{R} \subseteq \mathcal{P} \backslash \mathcal{Q}} \eta_{\mathcal{R}}(\boldsymbol{F}) \leq 2^{s-|\mathcal{Q}|} .
$$

Hence,

$$
\begin{equation*}
\mathfrak{S} \leq \sum_{\varnothing \neq \mathcal{Q} \subseteq \mathcal{P}} 2^{-|\mathcal{Q}|}\left|\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)\right| \tag{18}
\end{equation*}
$$

To this end, fix $\varnothing \neq \mathcal{Q} \subseteq \mathcal{P}$. By (4),

$$
\begin{equation*}
\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)=\frac{1}{P^{n}} \sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{G}\right) \widehat{\mu}_{\mathcal{Q}}\left(-T^{-n} \boldsymbol{G}\right) \tag{19}
\end{equation*}
$$

Expanding $\widehat{\mu}_{\mathcal{Q}}$ by definition gives

$$
\begin{aligned}
& \widehat{\mu}_{\mathcal{Q}}\left(-T^{-n} \boldsymbol{G}\right)=\sum_{\boldsymbol{H} \in \mathcal{M}_{\mathcal{P}, n}} \mu_{\mathcal{Q}}(\boldsymbol{H}) e_{\mathcal{P}}\left(-T^{-n} \boldsymbol{G} \boldsymbol{H}\right) \\
& =\prod_{p \in \mathcal{Q}}\left(\sum_{H_{p} \in \mathcal{M}_{p, n}} \mu_{p}\left(H_{p}\right) e\left(\psi_{p}\left(-T^{-n} G_{p} H_{p}\right)\right)\right) \cdot \prod_{p \in \mathcal{P} \backslash \mathcal{Q}}\left(\sum_{H_{p} \in \mathcal{M}_{p, n}} e\left(\psi_{p}\left(-T^{-n} G_{p} H_{p}\right)\right)\right)
\end{aligned}
$$

By (2), the product on the right vanishes unless $G_{p}=T^{n}$ for all $p \in \mathcal{P} \backslash \mathcal{Q}$, in which case it equals $P^{n} / Q^{n}$, where $Q=\prod_{p \in \mathcal{Q}} p$. Plugging this in (19) gives

$$
\begin{equation*}
\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)=\frac{1}{Q^{n}} \sum_{\substack{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n} \\ \forall p \notin \mathcal{Q}: G_{p}=T^{n}}} \widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{G}\right) \prod_{p \in \mathcal{Q}} \widehat{\mu}_{p}\left(-T^{n} G_{p}\right) \tag{20}
\end{equation*}
$$

Let $\delta=\frac{\gamma}{\gamma-1}>4$, with $\delta=\infty$ if $\gamma=1$, so that $\frac{1}{\gamma}+\frac{1}{\delta}=1$. Applying Hölder's inequality to (20) gives that

$$
\begin{equation*}
\left|\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)\right| \leq \frac{1}{Q^{n}}\left(\sum_{\substack{G \in \mathcal{M}_{\mathcal{P}, n} \\ \forall p \notin \mathcal{Q}: G_{p}=T^{n}}}\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{G}\right)\right|^{\gamma}\right)^{\frac{1}{\gamma}}\left(\sum_{\substack{G \in \mathcal{M}_{\mathcal{P}, n} \\ \forall p \notin \mathcal{Q}: G_{p}=T^{n}}} \prod_{p \in \mathcal{Q}}\left|\widehat{\mu}_{p}\left(-T^{n} G_{p}\right)\right|^{\delta}\right)^{\frac{1}{\delta}} . \tag{21}
\end{equation*}
$$

The first term is at most $\alpha^{n}$ by (2.1.2). By the choice of $c$, we have that $\frac{1}{4}-\frac{1}{\delta}-c>0$. Hence we may take $\varepsilon_{0}=\varepsilon_{0}(\gamma, \varepsilon)>0$ so small such that $\frac{1}{4}-\frac{1}{\delta}-\varepsilon_{0}>c$. Applying Theorem 2.2 with $\varepsilon_{0}$ yields $q_{0}=q_{0}(\gamma, c)$ such that if $p>q_{0}$, then $\left\|\widehat{\mu}_{p}\right\|_{\infty} \leq p^{\left(3 / 4+\varepsilon_{0}\right) n}$. So,

$$
\left|\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)\right| \leq \frac{\alpha^{n}}{Q^{n}}\left(Q^{n} \cdot \prod_{p \in \mathcal{Q}} p^{\left(3 / 4+\varepsilon_{0}\right) n \delta}\right)^{\frac{1}{\delta}} \leq Q^{-u n},
$$

where $u=\frac{1}{4}-\frac{1}{\delta}-\varepsilon_{0}-\frac{\log \alpha}{\log Q}$. As $Q \geq p \geq C$, if we take $C \geq q_{0}$ and to be sufficiently large so that $u>c$, then

$$
\left|\mathbb{E}_{\mathcal{P}}\left(\mu_{\mathcal{Q}}\right)\right| \leq Q^{-c n} .
$$

We plug this into (18) to get

$$
\mathfrak{S} \leq \sum_{\varnothing \neq \mathcal{Q} \subseteq \mathcal{P}} 2^{-|\mathcal{Q}|} Q^{-c n}=\prod_{p \in \mathcal{P}}\left(1+\frac{1}{2 p^{c n}}\right)-1 .
$$

Plugging this and (17) into (16) finishes the proof.
3.4. Proof of Proposition 2.3. Similarly to the proof of Proposition 2.1, we calculate the probability by

$$
\begin{align*}
\mathbb{P}(\operatorname{disc}(F)=\square) & =\mathbb{E}_{q}\left(\mathbb{1}_{\operatorname{disc}(F)=\square}\right) \\
& \stackrel{(7 \pi}{=} \frac{1}{2} \mathbb{E}\left(1+(-1)^{n} \mu(F)+\mathbb{1}_{\mu_{q}(F)=0}\right)  \tag{22}\\
& =\frac{1}{2}+\frac{(-1)^{n}}{2} \mathbb{E}(\mu(F))+\frac{1}{2} \mathbb{E}\left(\mathbb{1}_{\operatorname{disc}(F)=\square}\right)
\end{align*}
$$

We bound each of the terms separately. Similarly to (21), by Hölder's inequality we have

$$
\left|\mathbb{E}\left(\mu_{q}\right)\right| \leq \frac{1}{q^{n}}\left(\sum_{G \in \mathcal{M}_{q, n}}\left|\widehat{\mathbb{P}}\left(T^{-n} G\right)\right|^{\gamma}\right)^{\frac{1}{\gamma}}\left(\sum_{G \in \mathcal{M}_{q, n}}\left|\widehat{\mu_{q}}\left(-T^{n} G\right)\right|^{\delta}\right)^{\frac{1}{\delta}} .
$$

The first term is at most $\alpha^{n}$ by Condition 1. In a similar manner as in (21), we get that if we pick $C$ sufficiently large relatively to $\alpha, \gamma$ and $c$, then

$$
\left|\mathbb{E}\left(\mu_{q}\right)\right| \leq q^{-c n} .
$$

For the second term, using Lemma 3.1 and Condition 2, we have

$$
\left|\mathbb{E}_{q}\left(\mathbb{1}_{\operatorname{disc}(F)=\square}\right)\right|=\left|\sum_{i=1}^{\lfloor n / 2\rfloor} \sum_{D \in \mathcal{M}_{i}} \mu_{q}(D) \cdot \mathbb{P}\left(D^{2} \mid F\right)\right| \leq \omega_{q}^{-1},
$$

which completes the proof.

## 4. Proof of the main theorems

4.1. Theorem 1.2 implies Theorem 1.1. We prove that Theorem 1.2 implies a slightly more general version of Theorem 1.1.

Theorem 4.1. Let $L, n$ be positive integers, let $a \in \mathbb{Z}$ and let

$$
f=X^{n}+\sum_{k=0}^{n-1} \zeta_{k} X^{k}
$$

be a random polynomial, where $\zeta_{k}$ are chosen independently and identically distributed, taking values uniformly in $[a+1, a+L] \cap \mathbb{Z}$. Then,

$$
\lim _{L \rightarrow \infty} \mathbb{P}\left(G_{f}=S_{n}\right)=1,
$$

uniformly on all pairs $(n, a)$ with $n \geq 1, a \in \mathbb{Z}$, and such that if $n^{7}>L$, then $|a| \leq \frac{1}{2} e^{n^{1 / 3}}$.

Theorem 1.1 follows from Theorem 4.1 immediately by replacing $L$ by $2 L+1$ and setting $a=-L$.
Proof of Theorem 4.1. Let $f$ be as in Theorem 1.1 and let $p=\mathbb{P}\left(G_{f} \neq S_{n}\right)$. We need to prove that $p \rightarrow 0$ as $L \rightarrow \infty$ uniformly on $(n, a) \in\left\{(n, a): n^{7}>L \Rightarrow|a| \leq \frac{1}{2} e^{n^{1 / 3}}\right\}$. By (1), $p \rightarrow 0$ uniformly as $L \geq n^{7}$.

To this end, assume $n^{7}>L$. Since $|a| \leq \frac{1}{2} e^{n^{1 / 3}}$, we get that $[a+1, a+L] \subseteq$ $\left[-e^{n^{1 / 3}}, e^{n^{1 / 3}}\right]$, for $L$ sufficiently large. Hence Condition (a) of [3, Theorem 8] is satisfied. Condition (b) is satisfied with $P=210$ since we may assume that $L \geq$ 33, 730 (the details appear in the proof of [3, Theorem 1(a)]). Hence, we may apply [3, Theorem 8] to get that $\mathbb{P}\left(A_{n} \nsubseteq G_{f}\right)=O\left(n^{-c}\right)$, with $c>0$ absolute.

Finally, by Theorem [1.2, we get that, in this regime,

$$
\begin{aligned}
p \leq \mathbb{P}\left(A_{n} \nsubseteq G_{f}\right)+\mathbb{P}(\operatorname{disc} f & =\square) \\
& \ll n^{-c}+2^{-\left(\frac{1}{2}-\delta\right) \frac{\log L}{\log \log L}}+\frac{\log L}{\log \log L}\left(\frac{2}{(1-\delta) \log L}\right)^{\left(\frac{1}{4}-\varepsilon\right) n} .
\end{aligned}
$$

Thus, $p \rightarrow 0$ uniformly as $n^{7}>L \rightarrow \infty$, and this concludes the proof.
4.2. Preliminaries for the proof of Theorem $\mathbf{1 . 2}$. We will apply Proposition 2.1] to prove Theorem [1.2. The following two lemmas are needed to establish (2.1.2) and (2.1.3).

We start with a simple bound: Let $\xi$ be a random variable distributed uniformly on an interval $[a+1, a+L] \cap \mathbb{Z}$ of length $L$ and let $u, d \in \mathbb{Z}$ with $d>0$. Write $L=q d+r$ with $0 \leq r<d$, then

$$
\mathbb{P}(\xi \equiv u \bmod d)=\frac{\#\{v \in[a+1, a+L] \cap \mathbb{Z}: v \equiv u \bmod d\}}{L}=\frac{q+\alpha}{L},
$$

FULL GALOIS GROUPS OF POLYNOMIALS WITH SLOWLY GROWING COEFFICIENTS11 where $\alpha=\#\{v \in[a+q d+1, a+L]: v \equiv u \bmod d\} \in\{0,1\}$. Thus

$$
\begin{equation*}
\frac{1}{d}-\frac{1}{L} \leq \mathbb{P}(\zeta \equiv u \quad \bmod d) \leq \frac{1}{d}+\frac{1}{L} \tag{23}
\end{equation*}
$$

Lemma 4.2. Let $f$ be as in Theorem 1.2, let $\mathcal{P}$ be a finite set of primes, and let $P:=\Pi_{\mathcal{P}} p$. Then,

$$
\sum_{\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}}\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{F}\right)\right| \leq\left(1+\frac{P(P-1)}{L}\right)^{n}
$$

Proof. For a polynomial $H \in \mathbb{F}_{p}[T]$, we denote by $H^{i}$ its $i$-th coefficient, i.e. $H=$ $\sum_{i=0}^{\operatorname{deg} H} H^{i} T^{i}$. Since $\left(\zeta_{i}\right)_{i=0}^{n-1}$ are independent,

$$
\begin{aligned}
\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{F}\right)\right| & =\left|\sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \mathbb{P}_{\mathcal{P}}(\boldsymbol{G}) e_{\mathcal{P}}\left(T^{-n} \boldsymbol{F} \boldsymbol{G}\right)\right| \\
& =\left|\sum_{\boldsymbol{G} \in \mathcal{M}_{\mathcal{P}, n}} \prod_{i=0}^{n-1} \mathbb{P}\left(\zeta_{i} \equiv G_{p}^{i} \quad \bmod p, \forall p \in \mathcal{P}\right) \prod_{p \in \mathcal{P}} \prod_{i=0}^{n-1} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right)\right| \\
& =\prod_{i=0}^{n-1}\left|\sum_{\left(G_{p}^{i}\right)_{p \in \mathcal{P}} \in \mathbb{F}_{\mathcal{P}}} \mathbb{P}\left(\zeta_{i} \equiv G_{p}^{i} \quad \bmod p, \forall p \in \mathcal{P}\right) \prod_{p \in \mathcal{P}} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right)\right| .
\end{aligned}
$$

To this end, fix $0 \leq i \leq n-1$. If $F_{p}^{n-1-i}=0$ for all $p$, then
as a sum over all probabilities. Otherwise, there exists a $p$ such that $F_{p}^{n-1-i} \neq 0$. Hence,

$$
\begin{aligned}
& \quad \sum_{\left(G_{p}^{i}\right)_{p \in \mathcal{P} \in \mathbb{F}_{\mathcal{P}}}} \mathbb{P}\left(\zeta_{i} \equiv G_{p}^{i} \quad \bmod p, \forall p \in \mathcal{P}\right) \prod_{p \in \mathcal{P}} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right) \mid \\
& \stackrel{(2)}{=} \mid \sum_{\left(G_{p}^{i}\right)_{p \in \mathcal{P} \in \mathbb{F}_{\mathcal{P}}}} \mathbb{P}\left(\zeta_{i} \equiv G_{p}^{i} \bmod p, \forall p \in \mathcal{P}\right) \prod_{p \in \mathcal{P}} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right) \\
& \left.\quad-\sum_{\left(G_{p}^{i}\right)_{p \in \mathcal{P} \in \mathbb{P}}} \frac{1}{P} \prod_{p \in \mathcal{P}} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right) \right\rvert\, \stackrel{(23)}{\leq} \frac{P}{L}
\end{aligned}
$$

Writing $k(\boldsymbol{F})=\#\left\{0 \leq i \leq n-1: \exists p \in \mathcal{P}, F_{p}^{n-1-i} \neq 0\right\}$, we get that

$$
\prod_{i=0}^{n-1}\left|\sum_{\left(G_{p}^{i}\right)_{p \in \mathcal{P} \in \mathbb{F}_{\mathcal{P}}}} \mathbb{P}\left(\zeta_{i} \equiv G_{p}^{i} \quad \bmod p, \forall p \in \mathcal{P}\right) \prod_{p \in \mathcal{P}} e\left(\psi_{p}\left(G_{p}^{i} F_{p}^{n-1-i}\right)\right)\right| \leq\left(\frac{P}{L}\right)^{k(\boldsymbol{F})} .
$$

Hence,

$$
\sum_{\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}}\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{F}\right)\right| \leq \sum_{k=0}^{n}\binom{n}{k}\left(\frac{P}{L}\right)^{k}(P-1)^{k}=\left(1+\frac{P(P-1)}{L}\right)^{n},
$$

as needed.
Lemma 4.3. Assume the setting of Proposition 2.1. Let $h: \mathcal{P} \rightarrow \mathbb{R}_{\geq 0}$ a function such that $h(p)^{2}>p$, for all $p \in \mathcal{P}$. Assume that for all $d \mid P, \alpha \in \mathbb{Z}$, and $k \geq 0$ we have $\mathbb{P}_{\mathcal{P}}\left(\zeta_{k}=\alpha \bmod d\right) \leq \prod_{p \mid d} h(p)^{-1}$. Then, $\omega(p)=\frac{h(p)^{2}}{p}-1$ satisfies (2.1.3).
Proof. By assumption and the Chinese Remainder Theorem

$$
\begin{aligned}
\sum_{1 \leq i_{1}, \ldots, i_{r} \leq\lfloor n / 2\rfloor} & \sum_{\substack{D_{k} \in \mathcal{M}_{p_{k}, i_{k}} \\
\forall 1 \leq k \leq r}} \cdots \sum_{1} \mathbb{P}\left(D_{1}^{2}\left|f_{p_{1}}, \ldots, D_{r}^{2}\right| f_{p_{r}}\right) \leq \sum_{1 \leq i_{1}, \ldots, i_{r} \leq\lfloor n / 2\rfloor} \prod_{k=1}^{r} \frac{p_{k}^{i_{k}}}{h\left(p_{k}\right)^{2 i_{k}}} \\
= & \prod_{k=1}^{r} \sum_{i=1}^{\lfloor n / 2\rfloor}\left(\frac{p_{k}}{h\left(p_{k}\right)^{2}}\right)^{i} \leq \prod_{k=1}^{r} \sum_{i=1}^{\infty}\left(\frac{p_{k}}{h\left(p_{k}\right)^{2}}\right)^{i} \leq \prod_{k=1}^{r} \frac{\frac{p_{k}}{h\left(p_{k}\right)^{2}}}{1-\frac{p_{k}}{h\left(p_{k}\right)^{2}}}=\prod_{k=1}^{r} \omega\left(p_{k}\right)^{-1}
\end{aligned}
$$

as needed.
4.3. Proof of Theorem 1.2. First we show that if $L$ is sufficiently large with respect to $\delta$ then the conditions of Proposition 2.1 are satisfied with $\lambda_{k}$ uniformly distributed on $[a+1, a+L] \cap \mathbb{Z}, \alpha=2, \gamma=1, c=\frac{1}{4}-\varepsilon$, and $\omega(p)=\frac{p-4}{4}$ : Let $\mathcal{P}$ be the set of all primes $\frac{1-\delta}{2} \log L<p \leq(1-\delta) \log L$ and $P=\prod_{p \in \mathcal{P}} p$. Then, $\min \mathcal{P} \geq \frac{1-\delta}{2} \log L$, and so (2.1.1) holds true for $L$ sufficiently large. By (11), $L \geq P(P-1)$ if $L$ is sufficiently large, so by Lemma 4.2, we have

$$
\sum_{\boldsymbol{F} \in \mathcal{M}_{\mathcal{P}, n}}\left|\widehat{\mathbb{P}}_{\mathcal{P}}\left(T^{-n} \boldsymbol{F}\right)\right| \leq\left(1+\frac{P(P-1)}{L}\right)^{n} \leq 2^{n}
$$

Hence, (2.1.2) is satisfied. Let $h: \mathcal{P} \rightarrow \mathbb{R}_{\geq 0}$ be the function defined by $h(p)=\frac{p}{2}$ so that $\omega(p)=\frac{h(p)^{2}}{p}-1$. For $d \mid P$ and $u \in \mathbb{Z}$, we have $d \leq P \leq L$, hence

$$
\mathbb{P}\left(\zeta_{i}=u \bmod d\right) \stackrel{\sqrt{[23]}}{\leq} \frac{1}{d}+\frac{1}{L} \leq \prod_{p \mid d} h(p)^{-1} .
$$

This implies (2.1.3) by Lemma 4.3,
Now we may apply Proposition 2.1 to get that

$$
\begin{equation*}
\mathbb{P}(\operatorname{disc}(f)=\square) \leq \prod_{p \in \mathcal{P}}\left(1+2^{-1} p^{-\left(\frac{1}{4}-\varepsilon\right) n}\right)-1+\frac{1}{2^{\# \mathcal{P}}} \prod_{p \in \mathcal{P}}\left(1+\omega(p)^{-1}\right) \tag{24}
\end{equation*}
$$

By (9) and (10), we have

$$
\frac{1}{2^{\# \mathcal{P}}} \prod_{p \in \mathcal{P}}\left(1+\omega(p)^{-1}\right) \ll 2^{-\frac{1-\delta}{2} \log L} \log \log L,
$$

where the implied constant is absolute.

By (12), (note that $\left.\left(\frac{1}{4}-\varepsilon\right) n>\frac{n}{8}>1\right)$, we have

$$
\prod_{p \in \mathcal{P}}\left(1+2^{-1} p^{-\varepsilon n}\right)-1 \ll \frac{\log L}{\left(\frac{1-\delta}{2} \log L\right)^{\left(\frac{1}{4}-\varepsilon\right) n} \log \left(\frac{1-\delta / 2}{2} \log L\right)}
$$

where the implied constant is absolute. Since $\log \left(\frac{1-\delta / 2}{2} \log L\right)=\log \log L+O(1)$, plugging the above bounds into (24) completes the proof.

## References

[1] T. C. Anderson, A. Gafni, R. J. Lemke Oliver, D. Lowry-Duda, G. Shakan, and R. Zhang. Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants. Int. Math. Res. Not. IMRN, (3):2188-2214, 2023.
[2] L. Bary-Soroker, O. Ben-Porath, and V. Matei. Probabilistic Galois theory-the square discriminant case. Bull. Lond. Math. Soc., in press, expected 2024.
[3] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma. Irreducibility of random polynomials: general measures. Invent. Math., 233(3):1041-1120, 2023.
[4] L. Bary-Soroker and G. Kozma. Irreducible polynomials of bounded height. Duke Math. J., 169(4):579-598, 2020.
[5] E. R. Berlekamp. Algebraic coding theory (revised edition). World Scientific, 2015.
[6] M. Bhargava. A proof of van der Waerden's conjecture on random Galois groups of polynomials. Pure Appl. Math. Q., 19(1):45-60, 2023.
[7] Pierre-Yves Bienvenu and Thái Hoàng Lê. Linear and quadratic uniformity of the Möbius function over $\mathbb{F}_{q}[t]$. Mathematika, 65(3):505-529, 2019.
[8] A. Bloch and G. Pólya. On the roots of certain algebraic equations. Proc. London Math. Soc. (2), 33(2):102-114, 1931.
[9] E. Breuillard and P. P. Varjú. Irreducibility of random polynomials of large degree. Acta Mathematica, 223(2):195-249, 2019.
[10] R. Chela. Reducible polynomials. J. London Math. Soc., 38:183-188, 1963.
[11] S. Chow and R. Dietmann. Enumerative Galois theory for cubics and quartics. Adv. Math., 372:107282, 37, 2020.
[12] S. Chow and R. Dietmann. Towards van der Waerden's conjecture. Trans. Amer. Math. Soc., 376(4):2739-2785, 2023.
[13] R. Dietmann. On the distribution of Galois groups. Mathematika, 58(1):35-44, 2011.
[14] P. Erdős and P. Turán. On the distribution of roots of polynomials. Ann. of Math. (2), 51:105-119, 1950.
[15] P. X. Gallagher. The large sieve and probabilistic Galois theory. In Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), volume Vol. XXIV of Proc. Sympos. Pure Math., pages 91-101. Amer. Math. Soc., Providence, RI, 1973.
[16] D. Hilbert. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. J. Reine Angew. Math., 110:104-129, 1892.
[17] M. Kac. On the average number of real roots of a random algebraic equation. Bull. Amer. Math. Soc., 49:314-320, 1943.
[18] H.-W. Knobloch. Die Seltenheit der reduziblen Polynome. Jber. Deutsch. Math.-Verein., 59:12-19, 1956.
[19] S. V. Konyagin. On the number of irreducible polynomials with 0,1 coefficients. Acta Arith., 88(4):333-350, 1999.
[20] E. Kowalski. The large sieve and its applications, volume 175 of Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.
[21] J. E. Littlewood and A. C. Offord. On the number of real roots of a random algebraic equation. J. London Math. Soc., 13(4):288-295, 1938.
[22] A. M. Odlyzko and B. Poonen. Zeros of polynomials with 0,1 coefficients. Enseign. Math. (2), 39(3-4):317-348, 1993.
[23] S. Porritt. A note on exponential-möbius sums over $\mathbb{F}_{q}[t]$. Finite Fields and Their Applications, 51:298-305, 2018.
[24] B. L. van der Waerden. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. Monatsh. Math. Phys., 43(1):133-147, 1936.

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel Email address: barylior@tauex.tau.ac.il

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel Email address: noam3goldgraber@gmail.com

