DISS. ETH NO. 29160

ARITHMETIC STATISTICS OF FAMILIES OF GALOIS EXTENSIONS AND APPLICATIONS

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES

(Dr. sc. ETH Zurich)

presented by

Ilaria Viglino

Laurea Magistrale in Matematica, Università degli studi di Genova

born on 15.01.1993

accepted on the recommendation of

Prof. Dr. Emmanuel Kowalski, examiner

Prof. Dr. Lillian Pierce, co-examiner

2023

SUMMARY

This thesis investigates the arithmetic of certain families of number fields, obtained as splitting fields of families of polynomials. The first and main example is the family $\mathscr{P}_{n,N}$ of polynomials $f \in \mathbb{Z}[X]$ monic of degree n with height less or equal than N, and then let N go to infinity. It is known that "almost all" polynomials $f \in \mathbb{Z}[X]$ have splitting field K_f over $\mathbb{Q}$ with Galois group G_f isomorphic to the symmetric group S_n. On the other hand, all S_n-extensions of $\mathbb{Q}$ arise in this way for some f. We denote this subset of S_n-polynomials by $\mathscr{P}^0_{n,N}$.

We prove an average version of the Chebotarev Density Theorem for this family. In particular, this gives a Central Limit Theorem for the number of primes with given splitting type in some ranges. As an application, we deduce some estimates for the ℓ-torsion in the class groups.

Moreover, we also consider the analogue over number fields, and prove a result generalizing the work of Bhargava, towards the van der Waerden's conjecture.

ZUSAMMENFASSUNG

In dieser Arbeit wird die Arithmetik bestimmter Familien von Zahlenfeldern untersucht, die als Teilungsfelder von Familien von Polynomen erhalten werden. Das erste und wichtigste Beispiel ist die Familie $\mathscr{P}_{n,N}$ der Polynome $f \in \mathbb{Z}[X]$, die monisch vom Grad n sind und eine Höhe kleiner oder gleich N haben, und dann lässt man N ins Unendliche gehen. Es ist bekannt, dass "fast alle" Polynome $f \in \mathbb{Z}[X]$ ein Spaltfeld K_f über $\mathbb{Q}$ mit der Galoisgruppe G_f, die zur symmetrischen Gruppe S_n isomorph ist. Andererseits entstehen alle S_n-Erweiterungen von $\mathbb{Q}$ auf diese Weise für einige f. Wir bezeichnen diese Teilmenge von Polynomen ohne Affekt mit $\mathscr{P}^0_{n,N}$.

Wir beweisen eine durchschnittliche Version des Dichtesatz von Chebotarev für diese Familie. Insbesondere ergibt sich daraus ein zentraler Grenzwertsatz für die Anzahl der Primzahlen mit gegebenem Aufspaltungstyp in einigen Bereichen. Als Anwendung leiten wir einige Schätzungen für die ℓ-Torsion in den Klassengruppen ab.

Darüber hinaus betrachten wir auch die Analogie über Zahlenfeldern und beweisen ein Ergebnis, das die Arbeit von Bhargava verallgemeinert, und zwar in Richtung der van der Waerden-Vermutung.

ACKNOWLEDGEMENTS

I want to express my sincere gratitude to my advisor, Emmanuel Kowalski, for his guidance, support and human qualities throughout these years. Your assistance and advice, both on mathematical research and other matters have been truly helpful to me.

I would like to thank my co-advisor, Lillian Pierce, for giving me crucial suggestings, so I was able to improve my results.

I also want to use this opportunity to thank my academic brothers, Dante and Maxim, and my academic sister, Seraina, with which I spent many a great time attending and traveling to conferences. I am indebted to Stefano Vigni, Sandro Bettin and Alberto Perelli from the department of mathematics of Genova, where I received my Master's degree, for providing my mathematical foundations over the course of so many years and always trying to challenge my abilities.

I want to thank my family, especially my parents, Fernanda and Gianni, for having paved the way to where I am today. In pleasant and hard times, your love and support are a pillar in my life. I will always be grateful for it, and I am going to do my best to spread your life lessons in every place and context I will be.

My boyfriend Luca, outside the department, has been my personal cheerleader. I appreciate your patience when listening to me attempting to explain to you the Prime Number Theorem. Furthermore, I would like to thank you for always trying indirectly to remind me that there is a world outside of research. Supporting each other with love and protection is crucial and never ceases to amaze me.

Contents

Introduction

Counting S_n-polynomials

We fix a field extension $K/\mathbb{Q}$ of degree d. Let $n \geq 2$ and let N be positive integers. We consider monic polynomials with coefficients in $\mathcal{O}_K$:

$$f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0.$$

Choose an ordered integral basis $(\omega_1, \ldots, \omega_d)$ of $\mathcal{O}_K$ over $\mathbb{Z}$. We have, for all $k = 0, \ldots, n-1$,

$$\alpha_k = \sum_{i=1}^{d} a_i^{(k)} \omega_i$$

for unique $a_i^{(k)} \in \mathbb{Z}$. We view the coefficients $a_i^{(k)}$ as independent, identically distribuited random variables taking values uniformely in $\{-N, \ldots, N\}$. Define the *height* of α_k as $\mathrm{ht}(\alpha_k) = \max_i |a_i^{(k)}|$ and the **height** of the polynomial f to be

$$\mathrm{ht}(f) = \max_k \mathrm{ht}(\alpha_k).$$

For $n \geq 2$, $N > 0$ define

$$\mathscr{P}^0_{n,N}(K) = \{f \in \mathcal{O}_K[X] : \mathrm{ht}(f) \leq N,\ G_{K_f/K} \cong S_n\},$$

where K_f is the splitting field of f over K inside a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We call these polynomials **S_n-polynomials over** K, or simply S_n-polynomials when there is no need to specify the base field.

It has been proven that almost all polynomials are S_n-polynomials in the following sense:

$$\frac{|\mathscr{P}^0_{n,N}(K)|}{|\mathscr{P}_{n,N}(K)|} \underset{N \to +\infty}{\longrightarrow} 1.$$

For instance, in the case $K = \mathbb{Q}$, Van der Waerden gave in [Wa] an explicit error term $O(N^{-1/6})$. It has improved in [Gal] using large sieve to $O(N^{-1/2}\log N)$, and more recently by Dietmann [Di] using resolvent polynomials to $O(N^{-2+\sqrt{2}+\varepsilon})$ for every $\varepsilon > 0$. The best estimate can be found in [Bh1], who proved the following result, conjectured by van der Waerden.

Theorem (Bhargava)**.** *If either $n \geq 5$, one has,*

$$|\mathscr{P}^0_{n,N}(\mathbb{Q})| = (2N)^n + O(N^{n-1}),$$

as $N \to \infty$.

The case of cubic and quartic fields has been proven by Chow and Dietmann in [CD]. In Chapter 1 we generalize this result for polynomials in $\mathscr{P}^0_{n,N}(K)$ for many values of n and d. A simplified version of our result is the following.

Theorem 1. *Let $d \geq 1$ and $n \geq 2$. There exist constants $\theta > 0$ and $\theta_n \geq 0$ such that the number of non S_n-polynomials is*

$$|\mathscr{P}_{n,N}(K) \setminus \mathscr{P}^0_{n,N}(K)| \ll_{n,K} N^{d(n-\theta)}(\log N)^{\theta_n},$$

as $N \to +\infty$. In particular, if n and d lie in some inetervals, we can take $\theta = 1$ and $\theta_n = 0$;

See Theorem 1.1 for the precise statement.

The number of splitting primes

We will be interested, for the family of number fields as above, in understanding statistical arithmetic properties. In particular, we consider the Chebotarev Density Theorem on average. This means, we want to compute the density on average of the number of primes $\wp$ unramified in K_f/K for which f has a given splitting type modulo $\wp$.

Let $r = (r_1, \ldots, r_n)$ be a square-free "splitting type" (see the notations for the precise definition) and $x \geq 1$. Define

$$\pi_{f,r}(x) = \sum_{\substack{\wp \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}\wp \leq x \\ f \text{ of splitting type } r \bmod \wp}} 1 = \sum_{\substack{\wp \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}\wp \leq x}} \mathbb{1}_{f,r}(\wp),$$

where $\wp$ runs over the non-zero prime ideals of K, and

$$\mathbb{1}_{f,r}(\wp) = \begin{cases} 1 & \text{if } f \text{ has splitting type } r \bmod \wp \\ 0 & \text{otherwise.} \end{cases}$$

We may view $\pi_{f,r}(x)$ as a sum of random variables

$$\mathbb{1}_{\cdot,r}(\wp) : \mathscr{P}^0_{n,N} \longrightarrow \{0,1\}.$$

on $\mathscr{P}^0_{n,N}$, seen as a subset of $[-N,N]^{nd}$.

For every N, let $\mathbb{P}_N$ be the uniform probability measure on $[-N,N]^{nd}$. We'll denote by $\mathbb{E}_N$ and σ^2_N the expectation and the variance, respectively.

For a prime $\wp \subseteq \mathcal{O}_K$, let $N_{K/\mathbb{Q}}\wp = p_\wp^{f_\wp} =: q_\wp$, where $p_\wp$ is the characteristic of the residue field of $\wp$, and $f_\wp$ its inertia degree.

Now we state the main theorem about this part, which will be proved in Section 2.2. Here $\pi_K(x)$ is the function counting the number of prime ideals of $\mathcal{O}_K$ of norm less or equal than x, asymptotic to $\mathrm{Li}(x)$ by the prime ideal theorem. We underline here that in the following x is very small compared to N.

Theorem 2. *For $x = N^{1/\log\log N}$ and for any $a < b \in \mathbb{R}$,*

$$\mathbb{P}_N\left(a \leq \frac{\pi_{f,r}(x) - \delta(r)\pi_K(x)}{(\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2}} \leq b\right) \longrightarrow \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt$$

as $N \to +\infty$, where $\delta(r)$ is the order of the conjugacy class $\mathscr{C}_r$ in S_n of elements of cycle-pattern r, over $n!$.

This is a "Central Limit Theorem". It shows how $\pi_{f,r}(x)$ fluctuates about the mean value $\delta(r)\pi_K(x)$, which is the one expected by the Chebotarev Density Theorem.

Example. Let $\mathscr{C}_r$ be the trivial conjugacy class and let $K = \mathbb{Q}$. For $a = -0.9$ and $b = 0.9$ the above integral is about 0.6. If $n = 3$ and N is near 10^2 (so x near 20), the ratio is approximately $\pi_f(x) - 1.11$, which lies in the interval $[-0.9, 0.9]$ if and only if $\pi_{f,r}(x)$ is in $[0.21, 2.01] \sim [0, 3]$. This means that the proportion of cubic S_3-polynomials with coefficients in a box $[-100, 100]$ having less than 3 primes below 20 splitting completely in their splitting field, is about 60 percent.

Application 1

Let f be an S_n-polynomial and let $d_f \in \mathcal{O}_K$ be its discriminant. The relation between d_f and the discriminant $\mathfrak{D}_{K_f/K}$ of its splitting field is still an open problem in many cases, and leads to difficulties when counting ramified primes.

Call an irreducible monic integral polynomial f *essential* if the equality between the two discriminant holds. It is well known that this implies that the ring of integers of the splitting field of f is monogenic.

Our results can be applied to study this relation, and to bound on average the number of primes dividing the discriminant.

Corollary 1. *For almost all $f \in \mathscr{P}^0_{n,N}(K)$, the number of ramified primes is*

$$\ll_{n,K} \log\log N,$$

as $N \to +\infty$.

See Section 3.1 for this discussion.

Application 2

The following theorem is crucial to achieve results on the ℓ-torsion part of the class number $h_f[\ell]$ of K_f for every positive integer ℓ.

Theorem (Ellenberg, Venkatesh)**.** *Let $K/\mathbb{Q}$ be a field extension of degree s and discriminat D_K. Set $\delta < \frac{1}{2\ell(s-1)}$ and suppose that*

$$|\{p \leq D_K^{\delta} : p \text{ splits completely in } K/\mathbb{Q}\}| \geq M.$$

Then, for any $\varepsilon > 0$

$$h_K[\ell] \ll_{s,\ell,\varepsilon} D_K^{1/2+\varepsilon} M^{-1}.$$

Let D_f be the discriminant of $K_f/\mathbb{Q}$ and let d_f be the discriminant of the polynomial f.

Corollary 2. *For every positive integer ℓ, $\varepsilon > 0$ and for all $f \in \mathscr{P}^0_{n,N}$ outside of a set of size $o(N^{dn})$, we have*

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon} D_f^{\frac{1}{2} - \frac{1}{d(2n-2)(n-1)! \log\log |N_{K/\mathbb{Q}} d_f|} + \varepsilon},$$

as $N \to +\infty$.

Application 3

If $\lambda_1, \ldots, \lambda_s$ are elements of $\mathcal{O}_K$, we can factorize the ideals they generate in the Dedekind domain $\mathcal{O}_K$ as

$$\lambda_i \mathcal{O}_K = \prod_{\wp \subseteq \mathcal{O}_K} \wp^{\beta^i_\wp}$$

for all i, where $\beta^i_\wp = 0$ for all but finitely many $\wp$. The *leatest common multiple* of $\lambda_1, \ldots, \lambda_s$ is the ideal of $\mathcal{O}_K$ defined as the leatest common multiple of the ideals $\lambda_1\mathcal{O}_K, \ldots, \lambda_s\mathcal{O}_K$ in the Dedekind domain $\mathcal{O}_K$, that is

$$\operatorname{lcm}(\lambda_1, \ldots, \lambda_s) = \bigcap_{\wp \subseteq \mathcal{O}_K} \wp^{\max\{\beta^1_\wp, \ldots, \beta^s_\wp\}} = \prod_{\wp \subseteq \mathcal{O}_K} \wp^{\max\{\beta^1_\wp, \ldots, \beta^s_\wp\}}.$$

Proposition 1. *One has on average*

$$\mathbb{E}_N(\log |N_{K/\mathbb{Q}}(\operatorname{lcm}(f(\lambda) : \lambda \in \mathcal{O}_K,\ N_{K/\mathbb{Q}}\lambda \leq M))| \sim_{n,K} (n-1) M \log M$$

as $M, N \to +\infty$, with

$$M(\log M)^{\ell} \ll N = o\left(M \frac{\log M}{\log\log M}\right)$$

for some $0 < \ell < 1$.

The precise result is stated in Proposition 3.1.

Further results and problems

- Regarding the range of x, N for the average Chebotarev Theorem, in our proof of Theorem 2, the restriction $x \leq N^{1/\log\log N}$ or something similar is essential. It would be interesting to know in what range of x and N these results actually hold.

- If we consider the Artin L-function $L(s, \chi, K_f/K)$ associated to a fixed character χ of S_n, we have an estimate on average for the partial sum of the coefficients of $\log L(s, \chi, K_f/K)$ and $-\frac{L'}{L}(s, \chi, K_f/K)$ (Corollary 4.1). Moreover, in Lemma 4.4, we prove the following upper bound on average for the conductor $\mathfrak{f}_f(\chi)$ of $L(s, \chi, K_f/K)$:

$$\mathbb{E}_N(\log |N_{K/\mathbb{Q}}(\mathfrak{f}_f(\chi))|) \ll_{n,K,\chi} \log N.$$

- Another goal, is to provide similar results for polynomials in $\mathcal{O}_K[X]$ having as Galois group over K, either S_n or a transitive proper subgroup of S_n. It would be interesting to exploit the Hilbert Irreducibility Theorem to get results for some group $G \subseteq S_n$.

  In Section 2.3, we consider subfamilies $\mathscr{A}$ of $\mathscr{P}^0_{n,N}$ of a specific form. See 3.3.1 for explicit examples. We'd like to work with more families as in 2.3 or with slightly different features, maybe more "favorable" average properties, to study invariants like class numbers attached to them. We expect, for instance, to improve the exponent of D_f of Corollary 2 above.

Notations

- Given a normal extension L over K of degree s, the Galois group $G_{L/K}$ of L over K is defined to be the group of automorphisms of L that fix K pointwise. There is a natural embedding

$$G_{L/K} \hookrightarrow S_s$$

given by the action of the Galois group on the s homomorphisms of L onto $\overline{\mathbb{Q}}$. In the following we'll identify $G_{L/K}$ with its image via the above morphism. If $\wp$ is an unramified prime in L/K, i.e. the inertia group for every prime $\mathfrak{p}$ over $\wp$ of L is trivial, there is a canonical isomorphism between the Galois group of the residue field extension $(\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\wp)$ and the decomposition group $D_{\mathfrak{p}|\wp}$ at $\mathfrak{p}$. Now, $G_{(\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\wp)}$ is cyclic with canonical generator the Frobenius at $\wp$. The corresponding to $\mathfrak{p}$ is $\mathrm{Frob}_{L/K,\mathfrak{p}|\wp} \in D_{\mathfrak{p}|\wp}$. It is the unique element of $G_{L/K}$ such that for all $\alpha \in \mathcal{O}_L$ we have

$$\mathrm{Frob}_{L/K,\mathfrak{p}|\wp}(\alpha) \equiv \alpha^{N_{K/\mathbb{Q}}\wp} \mod \mathfrak{p}.$$

If we consider another prime over $\wp$, that is a conjugated one through an element of the Galois group, the new Frobenius is conjugated to the previous one via the same automorphism. Hence we denote by $\mathrm{Frob}_{L/K,\wp}$ the *Frobenius element* at $\wp$, namely the conjugacy class of Frobenius automorphisms in $G_{L/K}$.
Since the base field K is fixed, we sometimes avoid to indicate it in the notations, unless we need to underline a specific field choice.

- Let $f \in \mathscr{P}^0_{n,N}$. We say that $r = (r_1, r_2, \ldots, r_n)$ is the **splitting type** of f mod a prime $\wp$ if $f \mod \wp$ splits into distinct monic irreducible factors (so a square-free factorization), with r_1 linear factors, r_2 quadratic factors and so on. For the primes $\wp$ that not divide the discriminant D_f of the extension K_f/K, r corresponds to the cycle structure of the Frobenius element $\mathrm{Frob}_{K_f/\mathbb{Q},\wp} =: \mathrm{Frob}_{f,\wp}$ acting on the roots of f. For each r we have

$$\sum_{i=1}^{n} i r_i = n.$$

Let $\mathscr{C}_r$ be the conjugacy class in S_n of elements of cycle type r; the order of $\mathscr{C}_r$ is $n!\delta(r)$, where $\delta(r) = \prod_{i=1}^{n} \frac{1}{i^{r_i} r_i!}$.

- Throughout this thesis, we will make frequent use of various symbols to compare the asymptotic sizes of quantities. We write $f(x) \ll_a g(x)$ or $f(x) = O_a(g(x))$ to state that there exists a constant $C = C(a) > 0$ depending on a, such that $|f(x)| \leq C|g(x)|$ for all x suffciently large.

Similarly, we write $f(x) \gg g(x)$ if there exists a constant $C > 0$ such that $|f(x)| \leq C|g(x)|$ for all x suffciently large. We write $f(x) \asymp g(x)$ if both $f(x) \ll g(x)$ and $f(x) \gg g(x)$. Moreover, we state that $f(x) \sim g(x)$ if $f(x)/g(x) \to 1$ as $x \to +\infty$, and $f(x) = o(g(x))$ if $f(x)/g(x) \to 0$ as $x \to +\infty$.

1 Number of S_n-polynomials over K

Theorem 1.1. *Let $d \geq 1$ and $n \geq 2$. There exist constants $\theta > 0$ and $\theta_n \geq 0$ such that the number of non S_n-polynomials is*

$$|\mathscr{P}_{n,N}(K) \setminus \mathscr{P}^0_{n,N}(K)| \ll_{n,K} N^{d(n-\theta)}(\log N)^{\theta_n},$$

as $N \to +\infty$. In particular,

(1) *if $n = 2$, we can choose $\theta = 1$, $\theta_2 = 1$;*

(2) *for all $d \geq 1$ and $n \geq 3$ the above estimate holds with $\theta = 1/2$ and $\theta_n = 1 - \gamma_n$, where $\gamma_n \sim (2\pi n)^{-1/2}$;*

(3) *if one of the following conditions is satisfied, we can take $\theta = 1$ and $\theta_n = 0$:*

- $d = 1$, $n = 3, 4$;
- $\left[\frac{2d+\sqrt{4d^2-2d}}{d}\right] + 1 \leq n \leq 5$;
- $d \leq 23$, $2(2d+1) \leq n \leq 94$;
- $n \geq \max(95, 2(2d+1))$.

Let G be a subgroup of S_n; define

$$\mathscr{N}_n(N, G; K) = \mathscr{N}_n(N, G) = \{f \in \mathscr{P}_{n,N}(K) : G_f \cong G\},$$

and $N_n(N, G; K) = N_n(N, G) = |\mathscr{N}_n(G, N)|$. Theorem 1.1 states that

$$N_n(N, G) \ll_{n,K} N^{d(n-\theta)}(\log N)^{\theta_n} \tag{1}$$

as $N \to +\infty$ for all $G \subset S_n$.

Recently Bhargava [Bh1] proved the conjecture for all $n \geq 6$ and $K = \mathbb{Q}$. Part (3) of Theorem 1.1 is a generalization of this result for polynomials with integral coefficients in a number field K, for some values of d and n. Finally, for part (2) we apply large sieve to the set $\mathscr{P}_{n,N}$ (see [Gal] for the analogous result for $d = 1$).

1.1 Counting reducible polynomials over K

Firstly, we prove (1) in the case G intransitive subgroup of S_n. The polynomials having such G as Galois group are exactly those that factor over K. Let $1 \leq k \leq n/2$ and let

$$\rho_k(n, N; K) = \rho_k(n, N) = \{f \in \mathscr{P}_{n,N}(K) : f \text{ has a factor of degree } k \text{ over } K\}$$

and

$$\rho(n, N; K) = \rho(n, N) = \{f \in \mathscr{P}_{n,N}(K) : f \text{ reducible over } K\}.$$

Proposition 1.1. *One has*

$$\rho_k(n,N) \ll_{n,K} \begin{cases} N^{d(n-k)} & \text{if } k < n/2 \\ N^{d(n-k)} \log N & \text{if } k = n/2. \end{cases}$$

In particular, if $n \geq 3$,

$$\rho(n,N) \ll_{n,K} N^{d(n-1)},$$

as $N \to +\infty$.

Note that $\rho(n,N) \ll_{n,K} N^{d(n-1)} \log N$ if $n = 2$, which proves Theorem 1.1, part (1).

Lemma 1.1. *Let $\beta \in K$ be a root of $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0 \in \mathcal{O}_K[X]$ of height N. Then*

$$|N_{K/\mathbb{Q}}(\beta)| \ll_{n,K} N^d.$$

Proof. This follows from the analogous results for polynomials with coefficients over $\mathbb{C}$ (see [Di2], Lemma 1). For all $i = 1, \ldots, d$, $\sigma_i(\beta)$ is a complex root of $\sigma_i \circ f \in \mathbb{C}[X]$, hence

$$|\sigma_i(\beta)| \leq \frac{1}{\sqrt[n]{2} - 1} \max_{1 \leq k \leq n} \left| \frac{\sigma_i(\alpha_{n-k})}{\binom{n}{k}} \right|^{1/k}.$$

Then

$$|N_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{1}{\sqrt[n]{2} - 1} \right)^d \prod_{i=1}^{d} \max_{1 \leq k \leq n} |\sigma_i(\alpha_{n-k})|^{1/k} \ll_{n,d} N^d.$$

□

By Proposition 1.1, it follows that

$$\sum_{\substack{G \subset S_n \\ \text{intransitive}}} N_n(N,G) = \rho(n,N) \ll_{n,K} N^{d(n-1)}$$

for all $n \geq 3$, as $N \to +\infty$.

Proof. (Proposition 1.1) Assume that $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ of height $\leq N$ factors over K as $f(X) = g(X)h(X)$, where

$$g(X) = X^q + a_{q-1}X^{q-1} + \cdots + a_0;$$
$$h(X) = X^r + b_{r-1}X^{r-1} + \cdots + b_0,$$

where $n = q+r$. We call this set of f's $\rho_{q,r}(n,N)$. We therefore have to find an upper bound for the number of coefficients of g and h so that $f = gh$ and $\mathrm{ht}(\alpha_i) \leq N$ for all $i = 0, \ldots, n-1$.
By Knonecker's theorem, every product $\zeta = a_i b_j$ is a root of an equation of the form

$$\zeta^m + d_1\zeta^{m-1} + \cdots + d_m = 0,$$

where $d_j = d_j(\alpha_0, \ldots, \alpha_{n-1})$ is homogeneous of degree j in the coefficients of f.
Let $\sigma_i : K \hookrightarrow \mathbb{C}$, $i = 1, \ldots, d$ be the $\mathbb{Q}$-embeddings of K into $\mathbb{C}$. In particular, if $\alpha \in \mathcal{O}_K$, $\alpha = \sum_{k=1}^d a_k\omega_k$ has height $\leq N$, then for all $k = 0, \ldots, n-1$,

$$|\sigma_i(\alpha)| \leq C_{K,i}N$$

for all $i = 1, \ldots, d$, where $C_{K,i} = \sum_{j=1}^d |\sigma_i(\omega_j)|$. Hence

$$\begin{aligned}|N_{K/\mathbb{Q}}(\alpha)| &= \Big|\prod_{i=1}^d \sigma_i(\alpha)\Big| \\ &= \prod_{i=1}^d \Big|\sum_{i=1}^d \sigma_i(\omega_j)a_j\Big| \\ &\leq C_K N^d,\end{aligned}$$

where $C_K = \sum_{i=1}^d C_{K,i}$. It follows that since $\mathrm{ht}(d_j) \ll_{n,K} N^j$,

$$N_{K/\mathbb{Q}}(d_j) \ll_{n,K} N^{dj}$$

for all j. Now,

$$\Big(\frac{\zeta}{N}\Big)^m + \frac{d_1}{N}\Big(\frac{\zeta}{N}\Big)^{m-1} + \cdots + \frac{d_m}{N^m} = 0,$$

hence $\frac{\zeta}{N}$ is a root of an equation with coefficients of norm

$$N_{K/\mathbb{Q}}\Big(\frac{d_j}{N^j}\Big) \ll_{n,K} 1.$$

As in Lemma 1.1, one has $N_{K/\mathbb{Q}}\Big(\frac{\zeta}{N}\Big) \ll_{n,K,q,r} 1$, so

$$N_{K/\mathbb{Q}}(\zeta) = N_{K/\mathbb{Q}}(a_ib_j) \ll_{n,K,q,r} N^d$$

for all i, j. Let

$$\begin{aligned}A &= \max_i |N_{K/\mathbb{Q}}(a_i)|;\\ B &= \max_j |N_{K/\mathbb{Q}}(b_j)|.\end{aligned}$$

By the above

$$AB \ll_{n,K,q,r} N^d.$$

According to the Wiener-Ikehara Tauberian theorem, the number of principal ideals of norm $\leq x$ is $\ll x$. Given A, B sufficiently large, there are at most $\ll_{n,K} AqA^{q-2} = qA^{q-1}$ polynomials g and $\ll_{n,K} rB^{r-1}$ polynomials h, since at least one coefficient of g has norm A (q-possibilities), the remaining $q-1$ have norm $\leq A$, and the same for h. It total, for A, B large enough the number of products gh is at most

$$\ll_{n,K} qrA^{q-1}B^{r-1}.$$

It turns out that

$$\begin{aligned}
\rho_{q,r}(n,N) &\ll_{n,K,q,r} qr \sum_{AB \ll N^d} A^{q-1}B^{r-1} \\
&\ll_{n,K,q,r} \sum_{A \ll N^d} A^{q-1} \sum_{B \ll N^d/A} B^{r-1} \\
&\ll \sum_{A \ll N^d} A^{q-1} \Big(\frac{N^d}{A}\Big)^r \\
&= N^{dr} \sum_{A \ll N^d} A^{q-r-1}.
\end{aligned}$$

We can assume $q \leq r$.

- If $q < r$, the last sum is convergent, so

  $$\rho_{q,r}(n,N) \ll_{n,K,q,r} N^{dr}$$

  as $N \to +\infty$.

- If $q = r$,

  $$\begin{aligned}
  \rho_{q,r}(n,N) &\ll_{n,K,q,r} N^{dr} \sum_{A \ll N^d} \frac{1}{A} \\
  &\ll_{n,K,q,r} N^{dr} \log N
  \end{aligned}$$

  as $N \to +\infty$.

□

In fact, we go further by extending a result of Chela [Ch] and proving an asymptotic for $\rho(n, N; K)$.

Theorem 1.2. *Let $n \geq 3$. Then*

$$\lim_{N\to+\infty} \frac{\rho(n,N;K)}{N^{d(n-1)}} = 2^{d(n-1)} \left(D_{n,K} \cdot \left(\frac{C_K C'_K}{h_K} \right)^{n-1} + 1 + \frac{A_{n,K} k_{n,d}}{2^{d(n-1)}} \right),$$

where $A_{n,K}$ is an explicit constant, C_K is the residue at 1 of ζ_K, h_K is the class number of K,

$$D_{n,K} = \sum_{\substack{\nu\in\mathcal{O}_K \\ 1<|N_{K/\mathbb{Q}}\nu|<C'_K N^d}} \frac{1}{|N_{K/\mathbb{Q}}\nu)|^{n-1}},$$

$$C'_K = \prod_{j=1}^{d} \Big| \sum_{k=1}^{d} \sigma_j(\omega_k) \Big|,$$

$$k_{n,d} = vol(R) = \int_R \cdots \int dy_1^{(0)} \ldots dy_1^{(n-2)} \ldots dy_d^{(0)} \ldots dy_d^{(n-2)},$$

where R is the region of the $d(n-1)$-dimensional Euclidean space defined by

$$|y_k^{(j)}| \leq 1 \quad \forall j,k, \qquad\qquad \Big| \sum_{j=0}^{n-2} y_k^{(j)} \Big| \leq 1 \quad \forall j,k.$$

We assume from now on that $n \geq 3$. By Proposition 1.1 and by definition of ρ, ρ_k if follows that

$$\lim_N \frac{\rho(n,N)}{N^{d(n-1)}} = \lim_N \frac{\rho_1(n,N)}{N^{d(n-1)}}.$$

So we reduce to prove the asymptotic for

$$\frac{\rho_1(n,N)}{N^{d(n-1)}}$$

as $N \to +\infty$.

Let $\nu \in \mathcal{O}_K$ and let

$$T_{n,N}(\nu;K) = T_{n,N}(\nu) := \{f \in\in \mathscr{P}_{n,N}(K) : f \text{ has a linear factor } X+\nu\}.$$

Lemma 1.2. *One has*

$$\rho_1(n,N) - \sum_{\substack{\nu\in\mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu| \ll_{n,K} N^d}} T_{n,N}(\nu) = o(N^{d(n-1)})$$

as $N \to +\infty$.

Proof. Note that $\sum_\nu T_{n,N}(\nu) \geq \rho_1(n,N)$, since in the first sum a polynomial may be counted repeatedly. Let R_i be the number of $f \in \mathscr{P}_{n,N}(K)$ with exactly i distinct linear factors, and let $\rho'_1(n,N)$ be the number of $f \in \mathscr{P}_{n,N}(K)$ with two linear factors (not necessarily distinct).
Each of the R_i is counted in $\sum_\nu T_{n,N}(\nu)$ exactly i times. Moreover for $i > 1$,

$$R_i \leq \rho'_1(n,N) < \rho_2(n,N).$$

By Proposition 1.1, $\rho_2(n,N) = o(N^{d(n-1)})$, therefore $\rho_1(n,N)$ and $\sum_\nu T_{n,N}(\nu)$ differ in a $o(N^{d(n-1)})$ term. □

Lemma 1.3. *One has*

$$\lim_{N\to+\infty} \sum_{\substack{\nu\in\mathcal{O}_K \\ 1<|N_{K/\mathbb{Q}}\nu|\leq C'_K N^d}} \frac{T_{n,N}(\nu)}{N^{d(n-1)}} = 2^{d(n-1)} D_{n,K} \cdot \left(\frac{C_K C'_K}{h_K}\right)^{n-1},$$

where $D_{n,K} \leq \zeta_K(n-1)$.

Proof. Since $T_{n,N}(\nu) = T_{n,N}(\nu')$ if $N_{K/\mathbb{Q}}\nu = N_{K/\mathbb{Q}}\nu'$, we can assume that $2 \leq N_{K/\mathbb{Q}}\nu \leq C'_K N^d$. A polynomial $f \in \mathscr{P}_{n,N}$ with a linear factor $X+\nu$ is of the form

$$f(X) = (X+\nu)(X^{n-1} + \beta_{n-2}X^{n-2} + \cdots + \beta_0) \tag{2}$$

for some $\beta_j \in \mathcal{O}_K$ for all j. Thus $T_{n,N}(\nu)$ is equal to the number of $(n-1)$-tuples $(\beta_{n-2},\dots,\beta_0) \in \mathcal{O}_K^{n-1}$ satisfying (2) for f of height $\leq N$. We get

$$\begin{cases} \beta_0 = \frac{\alpha_0}{\nu} \\ \beta_i = \frac{\alpha_i - \beta_{i-1}}{\nu} & i = 1,\dots,n-2 \\ \alpha_{n-1} = \beta_{n-2} + \nu. \end{cases} \tag{3}$$

Write $\alpha_i = \sum_{k=1}^d a_k^{(i)}\omega_k$ and $\beta_i = \sum_{k=1}^d b_k^{(i)}\omega_k$ for all i, where $a_k^{(i)}, b_k^{(i)} \in \mathbb{Z}$ for all i,k. Now fix β_{i-1} and let α_i varies with $\mathrm{ht}(\alpha_i) \leq N$. One gets from (3),

$$\begin{aligned} N_{K/\mathbb{Q}}\beta_i &= \prod_{j=1}^d \sigma_j(\beta_i) \\ &= \prod_{j=1}^d \sum_{k=1}^d (a_k^{(i)} - b_k^{(i-1)})\sigma_j(\omega_k) \cdot \frac{1}{N_{K/\mathbb{Q}}\nu}. \end{aligned}$$

Once fixed β_{i-1} (i.e. b_k^{i-1} for all k), the norm of β_i lies in an interval of amplitude

$$C'_K \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu},$$

where $C'_K = \prod_{j=1}^d \left| \sum_{k=1}^d \sigma_j(\omega_k) \right|$. By definition of the ideal class group of K, the set of principal ideals of $\mathcal{O}_K$ is the identity element. Let L denote the average over m of the number of principal ideals of norm m. The uniform distribuition of the ideals among the h_K ideal classes of $\mathcal{O}_K$ and the Wiener-Ikehara Tauberian theorem imply that

$$\frac{1}{h_K} \sum_{m \leq x} |\{I \subseteq \mathcal{O}_K : N(I) = m\}| \sim \frac{1}{h_K} C_K x \sim Lx;$$

hence

$$L = \frac{C_K}{h_K},$$

where C_K is the residue at 1 of ζ_K. Therefore there are

$$\left[\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} \right] \text{ or } \left[\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} \right] + 1$$

integral elements β_i. The total number of solutions of the second equation of (3) is of the form

$$\prod_{i=1}^n \left(\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} + r_{\nu,i} \right),$$

where $r_{\nu,i} = 0$ or 1. By induction

$$\beta_{n-2} = \frac{\alpha_{n-2}}{\nu} - \frac{\alpha_{n-1}}{\nu^2} + \cdots + (-1)^{n-2} \frac{\alpha_0}{\nu^{n-1}},$$

from which

$$|N_{K/\mathbb{Q}}\beta_{n-2}| \leq C'_K N^d \left(\frac{1}{N_{K/\mathbb{Q}}\nu} + \frac{1}{(N_{K/\mathbb{Q}}\nu)^2} + \cdots + \frac{1}{(N_{K/\mathbb{Q}}\nu)^{n-1}} \right).$$

So for $\nu \in \mathcal{O}_K$ with $2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d$, the values of β_{n-2} also satisfy the third equation in (3) provided N is large enough. We have therefore

$$\begin{aligned} \sum_{\substack{\nu \in \mathcal{O}_K \\ 1 < |N_{K/\mathbb{Q}}\nu| \leq C'_K N^d}} T_{n,N}(\nu) &= \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d}} H_K(\nu) \cdot T_{n,N}(\nu) \\ &\quad + \sum_{\substack{\nu \in \mathcal{O}_K \\ N_{K/\mathbb{Q}}\nu = C'_K N^d}} H_K(\nu) \cdot T_{n,N}(\nu) \\ &= \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d}} H_K(\nu) \cdot \prod_{i=1}^{n-1} \left(\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} + r_{\nu,i} \right) \\ &\quad + \sum_{\substack{\nu \in \mathcal{O}_K \\ N_{K/\mathbb{Q}}\nu = C'_K N^d}} H_K(\nu) \cdot T_{n,N}(\nu). \end{aligned}$$

If $N_{K/\mathbb{Q}}(\nu) = C'_K N^d$, by arguing as before we get that $T_{n,N}(\nu) \ll_{n,K} 1$. Then the last sum is

$$\ll_{n,K} \sum_{\substack{\nu \in \mathcal{O}_K \\ N_{K/\mathbb{Q}}\nu = C'_K N^d}} 1 \sim \frac{C_K C'_K}{h_K} N^d = o(N^{d(n-1)})$$

for $n \geq 3$. Finally,

$$\begin{aligned}
\sum_{\substack{\nu \in \mathcal{O}_K \\ 1 < |N_{K/\mathbb{Q}}\nu| \leq C'_K N^d}} T_{n,N}(\nu) &= \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d}} H_K(\nu) \cdot \prod_{i=1}^{n-1} \left(\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} + r_{\nu,i} \right) \\
&\quad + o(N^{d(n-1)}) \\
&= \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d}} H_K(\nu) \cdot \left(\left(\frac{C_K C'_K}{h_K} \frac{(2N)^d}{N_{K/\mathbb{Q}}\nu} \right)^{n-1} + O_{n,K}(N^{d(n-3)}) \right) \\
&\quad + o(N^{d(n-1)}) \\
&= N^{d(n-1)} \left(\frac{2^d C_K C'_K}{h_K} \right)^{n-1} \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq N_{K/\mathbb{Q}}\nu < C'_K N^d}} H_K(\nu) \cdot \frac{1}{(N_{K/\mathbb{Q}}\nu)^{n-1}} \\
&\quad + o(N^{d(n-1)}) \\
&= N^{d(n-1)} \left(\frac{2^d C_K C'_K}{h_K} \right)^{n-1} \cdot \sum_{\substack{\nu \in \mathcal{O}_K \\ 2 \leq |N_{K/\mathbb{Q}}\nu| < C'_K N^d}} \frac{1}{|N_{K/\mathbb{Q}}\nu|^{n-1}} + o(N^{d(n-1)}) \\
&= N^{d(n-1)} \left(\frac{2^d C_K C'_K}{h_K} \right)^{n-1} \cdot D_{n,K} + o(N^{d(n-1)}).
\end{aligned}$$

$\square$

Recall that $\alpha_j = \sum_{k=1}^d a_k^{(j)} \omega_k$ for all $j = 0, \dots, n-1$. Let

$$h(f) = (h_1(f), \dots, h_d(f)) \in \mathbb{Z}^d,$$

where $h_k(f) = a_k^{(0)} + \cdots + a_k^{(n-1)}$ for all $k = 1, \dots, d$. Define

$$\mathscr{L}_n(N, h) = \{ f \in \mathscr{P}_{n,N}(K) : h(f) = h \}$$

and $L_n(N, h) = |\mathscr{L}_n(N, h)|$. We have

$$L_n(N, h) = L_n(N, h') \tag{4}$$

if $h'_k = \pm h_k$ for all k; moreover, by a counting argument as in Lemma 1.1, it holds

$$\sum_{\substack{\nu \in \mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu| = 1}} T_{n,N}(\nu) \asymp A_{n,K} L_n(N, (1, \ldots, 1)) \tag{5}$$

for some positive constant $A_{n,K}$. Note that in the left hand side, $T_{n,N}(\nu) = 0$ for almost all $\nu \in \mathcal{O}_K^\times$, since $\mathrm{ht}(\nu)$ is arbitrary large by Dirichlet's unit theorem.

Lemma 1.4. *For all $h \in \mathbb{Z}^d$,*

$$\lim_{N \to +\infty} \frac{L_n(N, h)}{N^{d(n-1)}} = k_{n,d}.$$

Proof. By (4) we may assume that $h_k \geq 0$ for all k. Let $f \in \mathscr{L}_n(N, 0)$ and let

$$f'(X) = X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_0 + \sum_{k=1}^{d} h_k \omega_k.$$

Then $f' \in \mathscr{L}_n(N + \max_k h_k, h)$. This implies

$$L_n(N, 0) \leq L_n(N + \max_k h_k, h).$$

Let now $f \in \mathscr{L}_n(N, h)$ and let

$$f'(X) = X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_0 - \sum_{k=1}^{d} h_k \omega_k.$$

We have

$$L_n(N, h) \leq L_n(N + \max_k h_k, 0).$$

It follows that

$$\frac{L_n(N - \max_k h_k, 0)}{L_n(N, 0)} \leq \frac{L_n(N, h)}{L_n(N, 0)} \leq \frac{L_n(N + \max_k h_k, 0)}{L_n(N, 0)}.$$

In particular

$$L_n(N, h) \sim L_n(N, 0)$$

for all h, as $N \to +\infty$.
Our claim is therefore

$$\lim_{N \to +\infty} \frac{L_n(N, 0)}{N^{d(n-1)}} = k_{n,d}.$$

Let E_{nd} be the nd-dimensional Euclidean space with coordinates $x_1^{(0)}, \ldots, x_1^{(n-1)}, \ldots, x_d^{(0)}, \ldots, x_d^{(n-1)}$. Let Λ_{nd} be the lattice of integral points in E_{nd}. Then $L_n(N,0)$ corresponds to the number of integral points of Λ_{nd} which lie inside the cube

$$C_N:\ |x_k(j)| \le N \quad \forall j = 0,\dots,n-1, \quad \forall k = 1,\dots,d$$

and the hyperplanes

$$H_k:\ x_k^{(0)} + \dots, x_k^{(n-1)} = 0 \quad \forall k = 1,\dots,d.$$

That is,

$$L_n(N,0) = |\Lambda_{nd} \cap C_N \cap H|,$$

where $H = H_1 \cap \dots \cap H_d$. H is a $d(n-1)$-dimensional space; we indentify it with $E_{d(n-1)}$ with coordinates $x_k^{(0)},\dots,x_k^{(n-2)}$ for all $k = 1,\dots,d$. Also,

$$C_N \cap H:\ |x_k^{(j)}| \le N, \qquad \Big|\sum_{j=0}^{n-2} y_k^{(j)}\Big| \le N$$

for all $j = 0,\dots,n-2$ and $k = 1,\dots,d$.
But

$$\lim_{N\to+\infty} \frac{|\Lambda_{nd} \cap C_N \cap H|}{N^{d(n-1)}} = vol(R),$$

where R is the region obtained transforming $C_N \cap H$ by the substituition $x_k^{(j)} = N y_k^{(j)}$ for all j,k. We conclude that

$$\lim_{N\to+\infty} \frac{L_n(N,0)}{N^{d(n-1)}} = vol(R) = \int_R \cdots \int dy_1^{(0)} \dots dy_1^{(n-2)} \dots dy_d^{(0)} \dots dy_d^{(n-2)}$$
$$= k_{n,d}.$$

□

Lemma 1.4 and (5) yield the following.

Corollary 1.1.

$$\lim_{N\to+\infty} \sum_{\substack{\nu\in\mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu|=1}} \frac{T_{n,N}(\nu)}{N^{d(n-1)}} = A_{n,K} k_{n,d}.$$

Proof. (Theorem 1.2) Let $n \ge 3$; write

$$\sum_{\substack{\nu\in\mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu|\le C'_K N^d}} T_{n,N}(\nu) = \sum_{\substack{\nu\in\mathcal{O}_K \\ 1<|N_{K/\mathbb{Q}}\nu|\le C'_K N^d}} T_{n,N}(\nu) + \sum_{\substack{\nu\in\mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu|=1}} T_{n,N}(\nu) + T_{n,N}(0).$$

Now, $T_{n,N}(0) \sim (2N)^{d(n-1)}$; by Lemma 1.1 and Corollary 2

$$\lim_{N\to+\infty} \sum_{\substack{\nu\in\mathcal{O}_K \\ |N_{K/\mathbb{Q}}\nu|\le C'_K N^d}} \frac{T_{n,N}(\nu)}{N^{d(n-1)}} = 2^{d(n-1)} D_{n,K} \cdot \left(\frac{C_K C'_K}{h_K}\right)^{n-1} + A_{n,K} k_{n,d} + 2^{d(n-1)}.$$

The theorem follows by Lemma 1.2. □

1.2 Proof of Theorem 1.1, part 2

1.2.1 Large sieve inequality for number fields

Let $\alpha \in \mathbb{Q}^n/\mathbb{Z}^n$ and let $c(a) \in \mathbb{C}$ for all a lattice vector in $\mathbb{Z}^n$. Define

$$S(\alpha) = \sum_{H(a)\leq N} c(a)e(a\cdot\alpha),$$

where the sum runs over $a \in \mathbb{Z}^n$ of *height* $H(a) \leq N$, where $H(a)$ is the maximum of the absolute values of the components of a. We use the standard notation $e(x) = e^{2\pi i x}$. Let $\operatorname{ord}(\alpha) = \min\{m \in \mathbb{N} : m\alpha \in \mathbb{Z}^n\}$. The following is the multidimensional analogue of the Bombieri-Davenport inequality:

$$\sum_{\operatorname{ord}(\alpha)\leq x} |S(\alpha)|^2 \ll_n (N^s + x^{2s}) \sum_{H(a)\leq N} |c(a)|^2.$$

We want a similar estimate for algebraic number fields. Specifically, let $\mathfrak{a}$ be an integral ideal of K, and let σ be an additive character of $\mathcal{O}_K^n \bmod \mathfrak{a}$. We call σ *proper* if it is not a character mod $\mathfrak{b}$ for any $\mathfrak{b}|\mathfrak{a}$. Let $c(\xi) \in \mathbb{C}$ for all $\xi = (\xi_1, \dots, \xi_n) \in \mathcal{O}_K^n$. As before, define

$$S(\sigma) = \sum_{H(\xi)\leq N} c(\xi)\sigma(\xi),$$

where $H(\xi) = \max_{i=1}^n \operatorname{ht}(\xi_i)$.

Proposition 1.2. *One has*

$$\sum_{N_{K/\mathbb{Q}}\mathfrak{a}\leq x} \sum_{\sigma} |S(\sigma)|^2 \ll_{n,K} (N^{nd} + c_K x^{2n}) \sum_{H(\xi)\leq N} |c(\xi)|^2$$

for some constant c_K, where the second sum is over the proper additive characters $\bmod\, \mathfrak{a}$.

A more precise statement of this result can be found in [Hu], Theorem 2 for the 1-dimensional case. Proposition 1.2 is the multidimensional analogue which can be achieved as for the case $K = \mathbb{Q}$; for further details see [Hu], again.

Let now $\wp$ be a prime ideal of $\mathcal{O}_K$ and let $\Omega(\wp)$ be a subset of $\mathcal{O}_K^n/\wp\mathcal{O}_K^n$, whom order is $\nu(\wp)$, say. For each $\xi \in \mathcal{O}_K^n$, set

$$P(\xi, x) = |\{\wp \in \mathcal{O}_K : N_{K/\mathbb{Q}}\wp \leq x,\ \xi \bmod \wp \in \Omega(\wp)\}|$$

and

$$P(x) = \sum_{N_{K/\mathbb{Q}}\wp\leq x} \frac{\nu(\wp)}{q_\wp^n},$$

where $q_\wp = N_{K/\mathbb{Q}}\wp$.

The next results are classical applications of Proposition 1.2 . We include the proofs for completeness.

Lemma 1.5. *If $N \gg_K x^{2/d}$, then*

$$\sum_{H(\xi)\le N} (P(\xi,x) - P(x)) \ll_{n,K} N^{nd} P(x).$$

Proof. Let $\varphi_\wp$ be the characteristic function of the set $\Omega(\wp)$, that is

$$\varphi_\wp(\xi) = \begin{cases} 1 & \text{if } \xi \bmod \wp \in \Omega(\wp) \\ 0 & \text{otherwise.} \end{cases}$$

It is periodic function mod $\wp$. Its Fourier transform is

$$\widehat{\varphi_\wp}(\sigma) = \frac{1}{q_\wp^n} \sum_{\xi \bmod \wp} \varphi_\wp(\xi)\overline{\sigma(\xi)}.$$

By the inversion formula we get

$$\varphi_\wp(\xi) = \sum_{\sigma \bmod \wp} \widehat{\varphi_\wp}(\sigma)\sigma(\xi),$$

where the sum is over the characters mod $\wp$. In particular

$$\widehat{\varphi_\wp}(1) = \frac{\nu(\wp)}{q_\wp^n} \tag{6}$$

and, by the orthogonality relations,

$$\sum_{\sigma \bmod \wp} |\widehat{\varphi_\wp}(\sigma)|^2 = \frac{\nu(\wp)}{q_\wp^n} \tag{7}$$

From (6), we can write

$$P(\xi,x) = \sum_{N_{K/\mathbb{Q}}\wp \le x} \varphi_\wp(\xi) = P(x) + R(\xi,x),$$

where

$$R(\xi,x) = \sum_{N_{K/\mathbb{Q}} \le x} \sum_{\substack{\sigma \bmod \wp \\ \sigma \ne 1}} \widehat{\varphi_\wp}(\sigma)\sigma(\xi).$$

By the Cauchy-Schwartz inequality one has

$$\begin{aligned} \sum_{H(\xi)\le N} (R(\xi,x))^2 &= \sum_{N_{K/\mathbb{Q}}\wp \le x} \sum_{\substack{\sigma \bmod \wp \\ \sigma \ne 1}} \widehat{\varphi_\wp}(\sigma) \sum_{H(\xi)\le N} R(\xi,x)\sigma(\xi) \\ &\le \left(\sum_{N_{K/\mathbb{Q}}\wp \le x} \sum_{\substack{\sigma \bmod \wp \\ \sigma \ne 1}} |\widehat{\varphi_\wp}(\sigma)|^2 \right)^{1/2} \cdot \left(\sum_{\sigma} |S(\sigma)|^2 \right)^{1/2}, \end{aligned}$$

where the last sum is over $\sigma \neq 1 \bmod \wp$ for some $\wp$ of norm $\leq x$, and

$$S(\sigma) = \sum_{H(\xi)\leq N} R(\xi, x)\sigma(\xi).$$

From (7) and Proposition 1.2 we get

$$\sum_{H(\xi)\leq N} (R(\xi, x))^2 \ll \left(P(x)(N^{nd} + c_K x^{2n}) \sum_{H(\xi)\leq N} |R(\xi, x)|^2 \right)^{1/2},$$

which, for $N \gg x^{2/d}$, implies the lemma. $\square$

Define, for a collection of subsets $\Omega(\wp)$ for each prime $\wp$,

$$E(N) = |\{\xi \in \mathcal{O}_K^n : H(\xi) \leq N,\ \xi \bmod \wp \notin \Omega(\wp)\ \forall \wp\}|.$$

Put

$$\mathcal{S}(x) = \sum_{N_{K/\mathbb{Q}}\mathfrak{a}\leq x} \mu^2(\mathfrak{a}) \prod_{\wp|\mathfrak{a}} \frac{\nu(\wp)}{q_\wp^n - \nu(\wp)},$$

where μ is the Möbius function; in particular

$$\mu^2(\mathfrak{a}) = \begin{cases} 1 & \text{if } \mathfrak{a} \text{ is square-free} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1.6. *If $N \gg_K x^{2/d}$, then*

$$E(N) \ll_{n,K} N^{nd}\mathcal{S}(x)^{-1}.$$

Proof. Let

$$c(\xi) = \begin{cases} 1 & \text{if } \xi \bmod \wp \notin \Omega(\wp)\ \forall \wp \\ 0 & \text{otherwise} \end{cases}$$

for all $\xi \in \mathcal{O}_K^n$. Note that

$$E(N) = \sum_{H(\xi)\leq N} |c(\xi)|^2 = S(1).$$

If we show that

$$\sum_{\sigma \bmod \mathfrak{a}} |S(\sigma)|^2 \geq |S(1)|^2 \prod_{\wp|\mathfrak{a}} \frac{\nu(\wp)}{q_\wp^n - \nu(\wp)} \tag{8}$$

for all square-free $\mathfrak{a}$, then we have, by Proposition 1.2, for $N \gg_K x^{2/d}$,

$$\begin{aligned} E(N)^2\mathcal{S}(x) &\leq \sum_{N_{K/\mathbb{Q}}\mathfrak{a}\leq x} \mu^2(\mathfrak{a}) \sum_{\sigma \bmod \mathfrak{a}} |S(\sigma)|^2 \\ &\ll (N^{nd} + c_K x^{2n}) \sum_{H(\xi)\leq N} |c(\xi)|^2 \\ &\ll N^{nd}E(N), \end{aligned}$$

and the lemma follows.
Proof of (8): for every prime $\wp$, by orthogonality we have

$$\sum_{\sigma \bmod \wp} |S(\sigma)|^2 = q_\wp^n \sum_{\zeta \in \mathcal{O}_K^n/\wp\mathcal{O}_K^n} |S(\zeta,\wp)|^2 - |S(1)|^2 \tag{9}$$

where $S(\zeta,\wp) = \sum_{\substack{\xi \\ \xi \bmod \wp \in \zeta}} c(\xi)$. By the Cauchy-Schwartz inequality,

$$|S(1)|^2 = \Big|\sum_\zeta S(\zeta,\wp)\Big|^2 \leq (q_\wp - \nu(\wp)) \sum_\zeta |S(\zeta,\wp)|^2 \tag{10}$$

since $S(\zeta,\wp) = 0$ for all $\zeta \in \Omega(\wp)$. Equations (9) and (10) imply (8) for the case $\mathfrak{a} = \wp$ prime ideal.

More generally, if σ_1 is a character mod $\wp$, one has

$$\sum_{\sigma \bmod \wp} |S(\sigma \cdot \sigma_1)|^2 \geq |S(\sigma_1)|^2 \frac{\nu(\wp)}{q_\wp^n - \nu(\wp)}$$

by replacing $c(\xi)$ with $c(\xi)\sigma_1(\xi)$.

Let now $\mathfrak{a}$ be square-free. By the unique factorization of ideals we can write $\mathfrak{a} = \wp\mathfrak{b}$ for some prime ideal $\wp$ and for some square-free ideal $\mathfrak{b}$, with $\wp \nmid \mathfrak{b}$. The chinese remainder theorem gives,

$$\begin{aligned}\sum_{\sigma \bmod \mathfrak{a}} |S(\sigma)|^2 &= \sum_{\sigma \bmod \wp} \sum_{\sigma_1 \bmod \mathfrak{b}} |S(\sigma \cdot \sigma_1)|^2 \\ &\geq \frac{\nu(\wp)}{q_\wp^n - \nu(\wp)} \sum_{\sigma_1 \bmod \mathfrak{b}} |S(\sigma_1)|^2.\end{aligned}$$

We conclude by induction on the number of prime factors of $\mathfrak{a}$. □

1.2.2 Sieving polynomials in $\mathscr{P}_{n,N}$

Let $f \in \mathscr{P}_{n,N}$, $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$. We identify f with the lattice vector $\xi = \xi_f = (\alpha_{n-1}, \ldots, \alpha_0)$ formed by its coefficients, so that $H(\xi_f) = \mathrm{ht}(f)$. Similarly, polynomials mod $\wp$ are identified with lattice vectors mod $\wp$.

Proposition 1.3. *Let r be a splitting type. If $N \gg_K x^{2/d}$, then*

$$\sum_{f \in \mathscr{P}_{n,N}} (\pi_{f,r}(x) - \delta(r)\pi_K(x))^2 \ll_{n,K} N^{nd}\pi_K(x).$$

Proof. For every prime $\wp$ of K of norm $q_\wp$, let

$$X_{n,r,\wp} = \Big\{ \Big(\prod_{i=1}^{r_1} g_i^{(1)}\Big) \cdots \Big(\prod_{i=1}^{r_n} g_i^{(n)}\Big) : g_i^{(j)} \in \mathbb{F}_{q_\wp}[X] \text{ irreducile, monic,}$$
$$\deg(g_i^{(j)}) = j,\ g_i^{(j)} \neq g_k^{(j)} \text{ if } i \neq k \Big\}.$$

Namely, $\Omega(\wp) = \Omega_r(\wp) := X_{n,r,\wp}$ is the set of polynomials of (square-free) splitting type r in the finite field $\mathbb{F}_{q_\wp}$. As we'll show later in Chapter 2,

$$\nu_r(\wp) = |X_{n,r,\wp}| = \delta(r) q_\wp^n + O(q_\wp^{n-1}).$$

Therefore

$$P(x) = \sum_{N_{k/\mathbb{Q}}\wp \le x} \frac{\nu_r(\wp)}{q_\wp^n} = \delta(r)\pi_K(x) + O(\log\log x),$$

and $\pi_{f,r}(x) = P(\xi_f, x)$. The proposition thus follows by Lemma 1.5. $\square$

For any $f \in \mathcal{O}_K[X]$, let

$$\pi_f(x) := \sum_{\substack{q_\wp \le x \\ \wp \text{ unramified}}} |\{\alpha \in \mathcal{O}_K : f(\alpha) \equiv 0 \bmod \wp\}|.$$

Observe that if f is irreducible and $f(\alpha) \equiv 0 \bmod \wp$ unramified, then there is a prime $\mathfrak{P}|\wp$ in the field $K(\alpha)$ so that $[\mathcal{O}_{K(\alpha)}/\mathfrak{P} : \mathcal{O}_K/\wp] = 1$, i.e. $N_{K/\mathbb{Q}}\mathfrak{P} = q_\wp$. Therefore $\pi_f(x)$ corresponds to the prime ideal counting function $\pi_{K(\alpha)}(x)$, and the asymptotic

$$\pi_f(x) \sim \pi_K(x),$$

as $x \to +\infty$, holds by the Prime Ideal Theorem.

Corollary 1.2. *If $N \gg_K x^{2/d}$, then*

$$\sum_{f \in \mathscr{P}_{n,N}} (\pi_f(x) - \pi_K(x))^2 \ll_{n,K} N^{nd} \pi_K(x).$$

Proof. Write

$$\begin{aligned}\pi_f(x) &= \sum_r r_1 \pi_{f,r}(x) \\ &= \Big(\sum_r r_1 \delta(r)\Big)\pi_K(x) + \sum_r r_1(\pi_{f,r}(x) - \delta(r)\pi_K(x)).\end{aligned}$$

In order to compute $\sum_r r_1\delta(r)$ we consider the generating function

$$\sum_{n\ge 0}\Big(\sum_{\substack{r_1,\dots,r_n\ge 0 \\ \sum i r_i = n}} r_1\delta(r)\Big) X_1^{r_1} X^{n-r_1} = \sum_{r_1,\dots,r_n\ge 0} \frac{X_1^{r_1}}{r_1!}\prod_{i=2}^n \frac{1}{i^{r_i} r_i!} X^{2r_2} X^{3r_3}\dots.$$

We have that $\sum_r r_1\delta(r)$ corresponds to the coefficients of X^{n-1} of

$$\begin{aligned}\frac{\partial}{\partial X_1}\Big|_{X_1=X} \exp\Big(X_1 + \sum_{n\ge 2}\frac{X^n}{n}\Big) &= \frac{\partial}{\partial X_1}\Big|_{X_1=X} \exp\Big(X_1 + \int_0^X \frac{dt}{1-t} - X\Big) \\ &= \frac{1}{1-X} \\ &= 1 + X + X^2 + \dots\end{aligned}$$

which is 1. It turns out, by the Cauchy-Schwartz inequality, that

$$(\pi_f(x) - \pi_K(x))^2 \ll \sum_r r_1^2(\pi_{f,r}(x) - \delta(r)\pi_K(x))^2,$$

and we apply Proposition 1.3 for each r. $\square$

Fix a splitting type r, and let

$$E_r(N) = |\{f \in \mathscr{P}_{n,N} : f \text{ has splitting type } r \bmod \wp \text{ for no prime } \wp\}|.$$

Corollary 1.3. *One has*

$$E_r(N) \ll_{n,K} N^{d(n-1/2)} \log N.$$

Proof. For $f \in E_r(N)$, $\pi_{f,r}(x) = 0$, so by

$$\begin{aligned}
&\sum_{f\in\mathscr{P}_{n,N}} (\pi_{f,r}(x) - \delta(r)\pi_K(x))^2 \\
&\qquad = \sum_{\substack{f\in\mathscr{P}_{n,N}\\ \pi_{f,r}(x)\neq 0}} (\pi_{f,r}(x) - \delta(r)\pi_K(x))^2 + \sum_{f\in E_r(N)} (\delta(r)\pi_K(x))^2 \\
&\qquad\qquad = \sum_{\substack{f\in\mathscr{P}_{n,N}\\ \pi_{f,r}(x)\neq 0}} (\pi_{f,r}(x) - \delta(r)\pi_K(x))^2 + E_r(N)(\delta(r)\pi_K(x))^2
\end{aligned}$$

we get

$$E_r(N) \asymp \sum_{\substack{f\in\mathscr{P}_{n,N}\\ \pi_{f,r}(x)\neq 0}} (\pi_{f,r}(x) - \delta(r)\pi_K(x))^2(\pi_K(x))^{-2} \ll_{n,K} N^{nd}(\pi_K(x))^{-1}$$

for $N \gg_K x^{2/d}$. Pick $x \asymp N^{d/2}$ and conclude by the prime ideal theorem. $\square$

In order to improve the exponent of $\log N$ we apply Lemma 1.6 to $E_R(N)$, where R is a nonempty set of splitting types and

$$E_R(N) = |\{f \in \mathscr{P}_{n,N} : f \text{ has splitting type in } R \bmod \wp \text{ for no prime } \wp\}|.$$

Put $\delta(R) = \sum_{r\in R} \delta(r)$.

Proposition 1.4. *For any $\delta < \delta(R)$, one has*

$$E_R(N) \ll_{n,K} N^{d(n-1/2)}(\log N)^{1-\frac{\delta}{1-\delta}}.$$

Proof. Let $\Omega_R(\wp) = \bigcup_{r\in R} X_{n,r,\wp}$. Its order is

$$\nu_R(\wp) = \delta(R) q_\wp^n + O(q_\wp^{n-1}).$$

If the norm of $\wp$ is large enough, $q_\wp \geq t$, say, we have

$$\nu_R(\wp) \geq \delta q_\wp^n.$$

If $N \gg_{n,K} x^{2/d}$, Lemma 1.6 gives

$$E_R(N) \ll_{n,K} N^{nd} \mathcal{S}_R(x)^{-1},$$

where

$$\mathcal{S}_R(x) = \sum_{N_{K/\mathbb{Q}}\mathfrak{a}\leq x} \mu^2(\mathfrak{a}) \prod_{\wp|\mathfrak{a}} \frac{\nu_R(\wp)}{q_\wp^n - \nu_R(\wp)}.$$

For $q_\wp \geq t$,

$$\frac{\nu_R(\wp)}{q_\wp^n - \nu_R(\wp)} = \left(\frac{q_\wp^n}{\nu_R(\wp)} - 1\right)^{-1} \geq \frac{\delta}{1-\delta},$$

so

$$\mathcal{S}_R(x) \geq \sum_{\substack{N_{K/\mathbb{Q}}\mathfrak{a}\leq x \\ \wp|\mathfrak{a}\Rightarrow q_\wp\geq t}} \mu^2(\mathfrak{a}) \prod_{\wp|\mathfrak{a}} \frac{\delta}{1-\delta} = \sum_{\substack{N_{K/\mathbb{Q}}\mathfrak{a}\leq x \\ \wp|\mathfrak{a}\Rightarrow q_\wp\geq t}} \mu^2(\mathfrak{a}) \left(\frac{\delta}{1-\delta}\right)^{\omega(\mathfrak{a})}.$$

We hence need a lower bound for the sum

$$\mathcal{S}_{\gamma,t}(x) = \sum_{\substack{N_{K/\mathbb{Q}}\mathfrak{a}\leq x \\ \mathfrak{a}\text{ square-free} \\ \wp|\mathfrak{a}\Rightarrow q_\wp\geq t}} \gamma^{\omega(\mathfrak{a})},$$

where $\gamma := \delta/(1-\delta)$. By a result of Selberg ([Sel], Theorem 2), we get

$$\mathcal{S}_{\gamma,t}(x) \asymp \frac{1}{\Gamma(\gamma)} \prod_{q_\wp<t} \left(1 - \frac{1}{q_\wp}\right)^\gamma \prod_{q_\wp\geq t} \left(1 + \frac{\gamma}{q_\wp}\right) \left(1 - \frac{1}{q_\wp}\right)^\gamma x(\log x)^{\gamma-1}.$$

Putting $x \asymp_{n,K} N^{d/2}$, the claim follows. $\square$

As we said in the introduction, if f mod $\wp$ has splitting type r, for some unramified $\wp$, then the Frobenius at $\wp$ has cycle structure r. If $G \subset S_n$ is a proper subgroup, it's a standard fact that the conjugates of G do not cover S_n; thus f cannot have all the splitting types. It follows that

$$|\mathscr{P}_{n,N} \setminus \mathscr{P}_{n,N}^0| \leq \sum_r E_r(N).$$

We conclude, by Corollary 1.2, that

$$|\mathscr{P}_{n,N} \setminus \mathscr{P}_{n,N}^0| \ll_{n,K} N^{d(n-1/2)} \log N.$$

We are now ready to prove Theorem 1.1, part (2). We use the following lemma to improve the exponent of $\log N$.

Lemma 1.7. *If G is a transitive subgroup of S_n, contains a transposition and contains a p-cycle for some $p > n/2$, then $G = S_n$.*

Proof. See [Gal], page 98. □

Let

$$\begin{aligned} T &= \{r : r_2 = 1,\ r_4 = r_6 = \cdots = 0\}, \\ P &= \{r : r_p = 1 \text{ for some } p > n/2\}. \end{aligned}$$

By using the above correspondence, we can view T as the set of elements of S_n among whose cycles there is just one transposition and no other cycles of even length. Analogously, P is the set of elements of order divisible by some prime $p > n/2$. By Lemma 1.7, we have the inequality

$$|\mathscr{P}_{n,N} \setminus \mathscr{P}^0_{n,N}| \leq \rho(n,N) + E_T(N) + E_P(N) \tag{11}$$

We can estimate $\rho(n,N)$ thanks to Proposition 1.1. For the other summands, we compute $\delta(T)$ and $\delta(P)$ in order to apply Proposition 1.4.

- Write

$$\delta(T) = \frac{1}{2} \sum_{\substack{r_3, r_5, \ldots \\ \sum i r_i = n-2}} \prod_{\substack{i \geq 3 \\ \text{odd}}} \frac{1}{i^{r_i} r_i!}.$$

The generating function is

$$\frac{1}{2} \sum_{r_3, r_5 \ldots} \prod_{\substack{i \geq 3 \\ \text{odd}}} \frac{1}{i^{r_i} r_i!} X^{2 + \sum_{\substack{i \geq 3 \\ \text{odd}}} i r_i} = \frac{X^2}{2} \exp\left(\sum_{n \geq 0} \frac{X^{2n+1}}{2n+1} \right).$$

Therefore $\delta(T)$ is half the coefficient of X^{n-2} of

$$\begin{aligned} \exp\left(\sum_{n \geq 0} \frac{X^{2n+1}}{2n+1} \right) &= \exp\left(\int_0^X \frac{dt}{1-t^2} \right) \\ &= \exp\left(\frac{1}{2} \int_0^X \frac{dt}{1-t} \right) \exp\left(\frac{1}{2} \int_0^X \frac{dt}{1+t} \right) \\ &= \left(\frac{1+X}{1-X} \right)^{1/2} \\ &= (1+X)(1-X^2)^{-1/2} \\ &= (1+X) \frac{\partial}{\partial X} (\arcsin X) \\ &= (1+X) \frac{\partial}{\partial X} \left(\sum_{k \geq 0} \frac{1}{2^{2k}} \binom{2k}{k} X^{2k+1} \right) \\ &= (1+X) \frac{\partial}{\partial X} \left(\sum_{k \geq 0} \frac{(2k)!}{(2^k k!)^2} X^{2k} \right). \end{aligned}$$

It turns out that

$$\delta(T) = \frac{(n-j)!}{2^{n-j+1}\left(\frac{n-j}{2}\right)!^2},$$

where $j=2$ if n is even and $j=3$ if n is odd. By Stirling's approximation $n! \sim \left(\frac{n}{e}\right)^n\sqrt{2\pi n}$ we get, for instance, when n is even,

$$\begin{aligned}\delta(T) &\sim \frac{\left(\frac{n-2}{e}\right)^{n-2}\sqrt{2\pi(n-2)}}{2^{n-2}\left(\left(\frac{n-2}{2}\right)^{\frac{n-2}{2}}\sqrt{\pi(n-2)}\right)^2}\\ &\sim \frac{1}{\sqrt{2\pi n}}.\end{aligned}$$

The case n odd is analogous.

- Write

$$\delta(P) = \sum_{n/2<p\le n}\frac{1}{p}\sum_{\substack{r_i, i\neq p\\ \sum_{i\neq p} ir_i = n-p}}\prod_{i\neq p}\frac{1}{i^{r_i}r_i!}.$$

The generating function of the last sum above for a fixed prime $n/2 < p \le n$ is

$$\sum_{r_i, i\neq p}\prod_{i\neq p}\frac{1}{i^{r_i}r_i!}X^{p+\sum_{i\neq p} ir_i} = X^p\exp\left(\sum_{n\ge 1,\ n\neq p}\frac{X^n}{n}\right).$$

The coefficient of X^{n-p} of $\exp\left(\sum_{n\ge1,\ n\neq p}\frac{X^n}{n}\right)$ is precisely our sum, which is therefore 1, since

$$\begin{aligned}\exp\left(\sum_{n\ge 1,\ n\neq p}\frac{X^n}{n}\right) &= \exp\left(\int_0^X\frac{dt}{1-t}\right)\\ &= \exp(-\log(1-X))\\ &= 1+X+X^2+\dots.\end{aligned}$$

By the classical Martens' estimate, we conclude that

$$\delta(P) = \sum_{n/2<p\le n}\frac{1}{p} \sim \frac{\log 2}{\log n}.$$

By (11), Lemma 1.7 and Proposition 1.1 it follows

$$|\mathscr{P}_{n,N}\setminus\mathscr{P}^0_{n,N}| \ll_{n,K} N^{d(n-1/2)}(\log N)^{1-\gamma_n},$$

where $\gamma_n \sim (2\pi n)^{-1/2}$, that is, part (2) of Theorem 1.1.

1.2.3 Remarks

Let $f \in \mathscr{P}_{n,N}$. By Proposition 1.3, we get in particular that for every $\varepsilon > 0$,

$$\pi_{f,r}(x) - \delta(r)\pi_K(x) = O\left(x^{\frac{1}{2}} \log x\right)$$

as $x \to +\infty$, for all but $O_{n,K}(x^{2n}(\log x)^{-3})$ polynomials f with $\mathrm{ht}(f) \ll x^{2/d}$. Indeed, if

$$E(x) := \{f \in \mathscr{P}_{n,N} : |\pi_{f,r}(x) - \delta(r)\pi_K(x)| > x^{\frac{1}{2}} \log x\}$$

denotes the exceptional set, one has

$$\begin{aligned} x(\log x)^2 |E(x)| &\ll \sum_{f \in \mathscr{P}_{n,N}} |\pi_{f,r}(x) - \delta(r)\pi_K(x)|^2 \\ &\ll N^{nd}\pi_K(x), \end{aligned}$$

if $N \gg x^{2/d}$. Hence

$$|E(x)| \ll \frac{N^{nd}}{x(\log x)^2} \frac{x}{\log x} \ll \frac{x^{2n}}{(\log x)^3}$$

by setting $N \asymp x^{2/d}$ and by letting $x \to +\infty$.

This sharper form

$$\pi_{f,r}(x) - \delta(r)\pi_K(x) = O\left(x^{\frac{1}{2}+\varepsilon}\right)$$

holds for all irreducible f by assuming the Artin's conjecture for the splitting field of f.

The reader can confront this result with the remark after Proposition 2.1, in which, for S_n-polynomials f, we have a significantly improved error term, but a larger set of exceptions.

1.3 Proof of Theorem 1.1, part 3

In order to conclude, it remains to show (1) for G primitive subgroup and for G transitive but imprimitive subgroup.

1.3.1 Case 1: G imprimitive

The irreducible polynomials $f \in \mathscr{P}_{n,N}(K)$ having such G as Galois group are those whose associated field $L_f = K[X]/(f) = K(\alpha)$ (α is any root of

f) has a nontrivial subfield over K.
Note that for any proper divisor e of n,

$$
\begin{aligned}
&|\{f \in \mathscr{P}_{n,N}(K) : f \text{ irreducible, } K(\alpha)/K \text{ has a subfield of degree } e\}| \\
&\leq |\{\beta \in \overline{\mathbb{Q}} : [K(\beta):K] = n,\ K(\beta)/K \text{ has a subfield of degree } e,\ H_K(\beta) \ll N^{1/n}\}| \\
&\leq |\{\theta \in \overline{\mathbb{Q}} : [\mathbb{Q}(\theta):\mathbb{Q}] = nd,\ \mathbb{Q}(\theta)/\mathbb{Q} \text{ has a subfield of degree } ed,\ H(\theta) \ll_K N^{1/n}\}|
\end{aligned}
$$

$$
\begin{tikzcd}
K(\beta) \arrow[d, dash, "n!"'] & = \mathbb{Q}(\theta) \arrow[ddl, dash, "nd"] \\
K \arrow[d, dash, "d"'] & \\
\mathbb{Q} &
\end{tikzcd}
$$

We recall that for a monic polynomial $f \in \mathbb{C}[X]$, the *Mahler measure* of f is

$$M(f) = \sum_{f(\theta)=0} \max\{1, |\theta|\}.$$

For any $x \in \overline{\mathbb{Q}}$ and L/K number field containing x, we define the multiplicative Weil height of x over K as

$$H_K(x) = \prod_{\nu \in M_L} \max\{1, |x|_\nu\}^{[L_\nu:K_\nu]/[L:K]},$$

where ν runs over all the places of L (note that $H_K(x)$ does not depend on the choice of L). For $K = \mathbb{Q}$, $H_{\mathbb{Q}} = H$ is the usual *multiplicative Weil height*. If α is an algebraic number of degree n over K and f is its minimal polynomial over K, then

$$M(f) = H_K(\alpha)^n.$$

Mahler showed that $M(f)$ and $\mathrm{ht}(f)$ are commensurate in the sense that

$$\mathrm{ht}(f) \ll M(f) \ll \mathrm{ht}(f).$$

In particular $H_K(\alpha) \ll N^{1/n}$, which explains the first inequality above.
For the second one, note that $H(\theta) \leq H_K(\theta)$ for all $\theta \in \overline{\mathbb{Q}}$. Moreover, if we fix a primitive element $\gamma \in K$ so that $K = \mathbb{Q}(\gamma)$, we have that $K(\beta) = \mathbb{Q}(\theta)$, where $\theta = \beta + q\gamma$ for all but finitely many $q \in \mathbb{Q}$. Since

$$H_K(\beta + q\gamma) \leq 2H_K(\beta)H_K(q\gamma),$$

it follows that $H(\theta) \ll_K N^{1/n}$.

An upper bound for the set

$$Z(ed, n/e, c_K N^{1/n}) := \{\theta \in \overline{\mathbb{Q}} : [\mathbb{Q}(\theta) : \mathbb{Q}] = nd, \\ \mathbb{Q}(\theta)/\mathbb{Q} \text{ has a subfield of degree } ed,\ H(\theta) \le c_K N^{1/n}\}$$

is given by Widmer ([Wi], Theorem 1.1.), namely

$$Z(ed, n/e, c_K N^{1/n}) \ll_{n,K} N^{d\left(\frac{n}{e}+ed\right)}.$$

Finally

$$|\{f \in \mathscr{P}_{n,N}(K) : f \text{ irreducible, } K(\alpha)/K \text{ has a non trivial subfield}\}| \\ \ll_{n,K} \max_{\substack{1<e<n \\ e|n}} N^{d\left(\frac{n}{e}+ed\right)} \le N^{d\left(\frac{n}{2}+2d\right)},$$

because the function $d\left(\frac{n}{x}+xd\right)$ assumes the maximum in $x = 2$ for $x \in [2, n/2]$. Since it is known, for instance from Kuba [Ku], that

$$\lim_{N\to+\infty} \mathbb{P}(f \text{ irreducible}) = 1$$

with error term $O(N^{-d})$, we get

$$\sum_{\substack{G\subset S_n \\ \text{imprimitive}}} N_n(N, G) \ll_{n,K} N^{d\left(\frac{n}{2}+2d\right)} \ll N^{d(n-1)},$$

as long as $n \ge 2(2d+1)$.

1.3.2 Case 2: G primitive

We need the following result which generalizes a result of Lemke Oliver and Thorne ([LT], Theorem 1.3).

Let G be a transitive subgroup of S_n. Any $f \in \mathscr{N}_n(N, G)$ (which can be assumed to be irreducible) cuts out a field $L_f = K[X]/(f)$ whose normal closure K_f/K has Galois group G with discriminant of norm

$$|N_{K/\mathbb{Q}}\mathfrak{D}_{L_f/K}| \ll_{n,K} N^{d(2n-2)}.$$

Let L/K be an extension of degree n. Define

$$M_L(N; K) = M_L(N) = |\{f \in \mathscr{P}_{n,N} : L_f \simeq L\}|.$$

By a theorem of Schmidt [Sc], the number $F_n(X, K)$ of field extensions L/K of degree n with $|N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}| \le X$ is $O_{n,K}(X^{(n+2)/4})$. For $n \le 5$, precise asymptotic formulas are known (see [DH], [DW], [Bh3], [Bh4], [BSW]).

In particular the above authors proved the Linnik's conjecture for small degrees: $F_n(X,K) \asymp_{n,K} X$. For $n \geq 95$, the best bound is that of Lemke Oliver and Thorne [LT2], namely $F_n(X,\mathbb{Q}) \ll_n X^{c(\log n)^2}$, where $c \leq 1.564$ is an explicitly computable constant. For smaller degrees, $6 \leq n \leq 94$, we use the following improvement to Schmidt bound, by [AGHLLTWZ]: $F_n(X,K) \ll_{n,K} X^{\frac{n+2}{4}-\frac{1}{4n-4}+\varepsilon}$ for all $\varepsilon > 0$.

Denote by

$$\mathscr{F}_n(X,G;K) = \mathscr{F}_n(X,G) = \{L/K : [L:K] = n,\ G_{\widetilde{L}/K} \cong G,\ |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}| \leq X\},$$

where $\widetilde{L}$ is the Galois closure of L over K.

Theorem 1.3. *For any $G \subseteq S_n$ transitive subgroup, one has*

$$N_n(N,G) \ll_{n,K} \begin{cases} N^{d(2n-1)} \cdot (\log N)^{nd-1} & \text{if } n \leq 5; \\ N^{d\left(1+\frac{(2n-2)(n+2)}{4}-\frac{1}{2n-2}\right)+\varepsilon} & \text{if } 6 \leq n \leq 94; \\ N^{d(1+c(2n-1)((\log(nd))^2)} \cdot (\log N)^{nd-1} & \text{if } n \geq 95, \end{cases}$$

as $N \to +\infty$, for all $\varepsilon > 0$. If moreover G is primitive,

$$N_n(N,G) \ll_{n,K} \begin{cases} N^{d(2n-1)-\frac{2}{n}} \cdot (\log N)^{nd-1} & \text{if } n \leq 5; \\ N^{d\left(1+\frac{(2n-2)(n+2)}{4}-\frac{1}{2n-2}\right)-\frac{2}{n}+\varepsilon} & \text{if } 6 \leq n \leq 94; \\ N^{d(1+c(2n-1)((\log(nd))^2)-\frac{2}{n}} \cdot (\log N)^{nd-1} & \text{if } n \geq 95, \end{cases}$$

as $N \to +\infty$, for all $\varepsilon > 0$.

Proof. Since the discriminant of $f \in \mathscr{P}_{n,N}$ satisfies $N_{K/\mathbb{Q}}d_f \ll_{n,K} N^{d(2n-2)}$ (see 3.1), we can write

$$N_n(N,G) \ll_{n,K} \sum_{L \in \mathscr{F}_n(N^{d(n-2)},G)} M_L(N) \tag{12}$$

Now, for any L/K as above with signature (r_1,r_2),

$$\begin{aligned} M_L(N) &\leq |\{\alpha \in \mathcal{O}_L : K(\alpha) \cong L,\ H_K(\alpha) \ll_{n,K} N^{1/n}\}| \\ &\ll_{n,K} |\Omega_{N^{1/n}} \cap (\mathcal{O}_L \setminus K)|, \end{aligned}$$

where for $Y \geq 1$, Ω_Y is the subset of the Minkowski space $L_\infty = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of elements whom Weil height over K is at most Y.
By applying Davenport's lemma and by computing the volume of Ω_Y we achieve

$$|\Omega_Y \cap \mathbb{Z}^n| \ll_{n,d} Y^{nd}(\log Y)^{r_1+r_2-1}.$$

By Proposition 2.2 of [LT],

$$|\Omega_Y \cap \mathcal{O}_L| \ll_{n,d} Y^{nd}(\log Y)^{r_1+r_2-1}$$

as well. In particular

$$M_L(N) \ll_{n,K} N^d(\log N)^{r_1+r_2-1}.$$

As in the last part of the proof of Theorem 2.1 of [LT], one gets the improvement

$$M_L(N) \ll_{n,K} \frac{N^d(\log N)^{r_1+r_2-1}}{\lambda},$$

where $\lambda = \{\|\alpha\| : \alpha \in \mathcal{O}_L \setminus K\}$, $\|\alpha\|$ is the largest archimedean valuation of α.

By (12) and the result of Schmidt follows the first part of the theorem.

Let now G be primitive; in particular L/K has no proper subextensions. Therefore essentially as in [EV], Lemma 3.1, since if $\alpha \in \mathcal{O}_L \setminus K$ then $L = K(\alpha)$, and $\mathcal{O}_K[\alpha]$ is a subring of $\mathcal{O}_L$ which generates $\mathcal{O}_L$ as a K-vector space, one deduces

$$\|\alpha\| \gg |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^{\frac{1}{nd(n-1)}}.$$

Finally, by partial summation we conclude

$$N_n(N,G) \ll_{n,K} \sum_{L\in\mathscr{F}_n(N^{d(2n-2)},G)} \frac{N^d(\log N)^{nd-1}}{|N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^{\frac{1}{nd(n-1)}}},$$

by using the bounds for $F_n(X,K)$ according to n, observing that $F_n(X,K) \leq F_{nd}(C_{n,K}X,\mathbb{Q})$ for some constant $C_{n,K}$. $\square$

Assume now G to be primitive; for $g \in G$, $g = c_1 \dots c_t$ where c_j are disjoint cycles, the index of g is

$$\operatorname{ind}(g) = n - t.$$

The *index* of the group G is

$$\operatorname{ind}(G) = \min_{\substack{g\in G\\ g\neq 1}} \operatorname{ind}(g).$$

Proposition 1.5. *Let $f \in \mathcal{O}_K[X]$ be a monic, irreducible polynomial of degree n with associated field $L_f = K[X]/(f)$. If $\operatorname{ind}(G_f) = k$, then the discriminant $\mathfrak{D}_{L_f/K}$ has the property* P_k*: if $\wp \subseteq \mathcal{O}_K$, $\wp|\mathfrak{D}_{L_f/K}$, then $\wp^k|\mathfrak{D}_{L_f/K}$.*

Proof. The Galois group G_f acts on the n embeddings of L_f into K_f, its Galois closure. Let $\wp \subseteq \mathcal{O}_K$,

$$\wp\mathcal{O}_{L_f} = \prod_i \mathfrak{P}_i^{e_i},$$

where for each i, $\mathfrak{P}_i$ has inertia degree f_i over K. Now, the primes dividing the discriminant of L_f/K are either tamely ramified or wildly ramified.

- If $\wp$ is tamely ramified, the inertia group $I_\wp$ is cyclic, and any generator $g \in G_f$ is the product of disjoint cycles consisting of f_1 clycles of length e_1, f_2 cycles of length e_2 and so on. Hence the exponent of $\wp$ dividing $\mathfrak{D}_{L_f/K}$ is

$$v_\wp(\mathfrak{D}_{L_f/K}) = \sum_i (e_i - 1) f_i = \mathrm{ind}(g) \geq \mathrm{ind}(G_f) = k.$$

- If $\wp$ is wildly ramified, we have the strict inequalities

$$v_\wp(\mathfrak{D}_{L_f/K}) > \sum_i (e_i - 1) f_i > k.$$

In both cases we see that $\wp^k | \mathfrak{D}_{L_f/K}$. □

For a primitive group G, the followings are standard facts.

a. If G contains a transposition, then $G = S_n$. In particular $\mathrm{ind}(G) \geq 2$.

b. If G contains a 3-cycle or a double transposition and $n \geq 9$, then $G = A_n$ or S_n. In particular $\mathrm{ind}(G) \geq 3$.

It follows from Proposition 1.5, a and b that:

Corollary 1.4. *Let $f \in \mathcal{O}_K[X]$ be a monic, irreducible polynomial of degree n with $G_f \subset S_n$ primitive. Then $\mathfrak{D}_{L_f/K}$ has the property* P_2.
If moreover $G_f \neq A_n$ and $n \geq 9$, then $\mathfrak{D}_{L_f/K}$ has the property P_3.

We now follow and generalize the argument of Bhargava [Bh1] by dividing the set $\mathscr{N}_n(N, G)$ into three sets.
For an irreducible $f \in \mathscr{N}_n(N, G)$ with G primitive, let

$$\mathfrak{C}_f := \prod_{\wp | \mathfrak{D}_{L_f/K}} \wp$$

and denote by $\mathfrak{D}_f$ the discriminant $\mathfrak{D}_{L_f/K}$.
Let

$$\mathscr{N}_n(N) := \bigcup_{\substack{G \subset S_n \\ \text{primitive}}} \mathscr{N}_n(N, G).$$

As observed before, we can assume that all polynomials are irreducible.
For $\delta > 0$, the sets $\mathscr{N}_1(N, \delta), \mathscr{N}_2(N, \delta)$ and $\mathscr{N}_3(N, \delta)$ are defined as

$$\begin{aligned}
\mathscr{N}_1(N, \delta) &:= \{ f \in \mathscr{N}_n(N) : |N_{K/\mathbb{Q}} \mathfrak{C}_f| \leq N^{d(1+\delta)},\ |N_{K/\mathbb{Q}} \mathfrak{D}_f| > N^{d(2+2\delta)} \}, \\
\mathscr{N}_2(N, \delta) &:= \{ f \in \mathscr{N}_n(N) : |N_{K/\mathbb{Q}} \mathfrak{D}_f| < N^{d(2+2\delta)} \}, \\
\mathscr{N}_3(N, \delta) &:= \{ f \in \mathscr{N}_n(N) : |N_{K/\mathbb{Q}} \mathfrak{C}_f| > N^{d(1+\delta)} \}.
\end{aligned}$$

We use the following result, in which we identify the space of binary n-ic forms over $\mathcal{O}_K$ having leading coefficient 1 with the space of monic polynomials of degree n over $\mathcal{O}_K$. The proof uses Fourier analysis over finite fields. The index of a binary n-ic forms f over $\mathcal{O}_K$ modulo $\wp|p$ is defined to be

$$\sum_{i=1}^{r}(e_i-1)f_i,$$

where $f \mod \wp = \prod_{i=1}^{r} P_i^{e_i}$, P_i irreducible of degree f_i over $\in \mathbb{F}_{p^{[\mathcal{O}_K/\wp:\mathbb{F}_p]}}$ for all i.

The proofs of the next results which are not included here, can be found in [Bh1].

Proposition 1.6. *Let* $0<\delta \ll_{n,d} 1$ *be small enough and let* $\mathfrak{C}=\wp_1\dots\wp_m$, $\wp_i \neq \wp_j$ $(i\neq j)$ *be a product of primes in* $\mathcal{O}_K$ *of norm* $|N_{K/\mathbb{Q}}\mathfrak{C}|<N^{d(1+\delta)}$. *For each* $i=1,\dots,m$ *pick an integer* k_i. *Then the number of* K*-integral binary* n*-ic forms in a box* $[-N,N]^{d(n+1)}$ *with coefficients of height* $\leq N$, *such that, modulo* $\wp$, *have index at least* k_i, *is at most*

$$\ll_{K,\varepsilon} \frac{N^{nd+\varepsilon}}{\prod_{i=1}^{m}|N_{K/\mathbb{Q}}\wp_i|^{k_i}}$$

for every $\varepsilon>0$.

Theorem 1.1, (3) follows by the three lemmas below together with Section 1.1.

Lemma 1.8. *For* $\delta>0$ *sufficiently small,*

$$|\mathscr{N}_1(N,\delta)| \ll_{n,K} N^{d(n-1)}$$

as $N\to+\infty$.

Proof. Given a number field L/K, let $\mathfrak{C}$ be the product of the ramified primes and let $\mathfrak{D}$ be its discriminant. The polynomials f so that $L_f\cong L$ (so $\mathfrak{C}_f=\mathfrak{C}$ and $\mathfrak{D}_f=\mathfrak{D}$) must have at least a triple root or at least two double roots modulo $\wp$ for every $\wp|\mathfrak{C}_f$. This follows easily by Proposition 1.6. Now, the density of the degree n polynomials over a finite field $\mathbb{F}_q$ having a triple root is $1/q^2$, whereas the density of the ones having two double roots is $2/q^3$. Therefore the density of the above polynomials is

$$\ll \prod_{\wp|\mathfrak{C}_f}\frac{2}{|N_{K/\mathbb{Q}}\wp|^2} \ll \frac{2^{\omega(\mathfrak{D})}}{|N_{K/\mathbb{Q}}\mathfrak{D}|},$$

where $\omega(\mathfrak{D})$ is the number of prime divisors of $\mathfrak{D}$.
By Proposition 1.6 the number of $f\in\mathscr{P}_{n,N}$ with $|N_{K/Q}\mathfrak{C}|\leq N^{d(1+\delta)}$ and $\mathfrak{D}_f=\mathfrak{D}$ is

$$\ll_{K,\varepsilon}\frac{N^{nd+\varepsilon}}{|N_{K/\mathbb{Q}}\mathfrak{D}|}.$$

Summing over all $\mathfrak{D}$ of norm $|N_{K/\mathbb{Q}}\mathfrak{D}| > N^{d(2+2\delta)}$ gives

$$\sum_{\mathfrak{D}} O_{K,\varepsilon}(N^{nd+\varepsilon}2^{\omega(\mathfrak{C})}/|N_{K/\mathbb{Q}}\mathfrak{D}|)$$
$$= O_{K,\varepsilon}(N^{nd+\varepsilon} \cdot 2^{d(1+\delta)} \cdot N^{-2d-2d\delta})$$
$$\ll_{n,K} N^{d(n-1)}.$$

□

Lemma 1.9. *If either*

(1) $\left[\frac{2d+\sqrt{4d^2-2d}}{d}\right] + 1 \leq n \leq 5$, *or*

(2) $dn^3 + 8n^2d - (7d+2)n + 2 > 0$, *or*

(3) $n \geq \left[\frac{d(1+c(\log(nd))^2)+\sqrt{d^2(1+c(\log(nd))^2)^2-2d}}{d}\right] + 1$,

then for $\delta > 0$ sufficiently small

$$|\mathscr{N}_2(N,\delta)| \ll_{n,K} N^{d(n-1)},$$

as $N \to +\infty$.

Proof. Note that one can prove Theorem 1.3 by using a different bound, if holds, for the discriminat insted of $\ll N^{d(2n-2)}$ and improve the result itself. For the polynomials in our set we thus have

$$|\mathscr{N}_2(N,\delta)| \ll_{n,K} \begin{cases} N^{d(2\delta+3)-\frac{2}{n}} + \varepsilon & \text{if } n \leq 5; \\ N^{d\left(1+\frac{(2\delta+2)(n+2)}{4}-\frac{1}{2n-2}\right)-\frac{2}{n}+\varepsilon} & \text{if } 6 \leq n \leq 94; \\ N^{d(1+c(2\delta+2)((\log(nd))^2)-\frac{2}{n}} + \varepsilon & \text{if } n \geq 95, \end{cases}$$

as $N \to +\infty$, for all $\varepsilon > 0$. If n satisfies either (1) or (2) or (3), one has the desired upper bound $O_{n,K}(N^{d(n-1)})$. □

Proposition 1.7. *Let $\wp \in \mathcal{O}_K$ be a prime ideal over p and let $q = p^{[\mathcal{O}_k/\wp:\mathbb{F}_p]}$. If $h(X_1,\ldots,X_n) \in \mathcal{O}_K[X_1,\ldots,X_n]$ is such that*

$$h(c_1,\ldots,c_n) \equiv 0 \mod q^2,$$
$$h(c_1+qd_1,\ldots,c_n+qd_n) \equiv 0 \mod q^2$$

for all $(d_1,\ldots,d_n) \in \mathcal{O}_K^n$, then

$$\frac{\partial}{\partial x_n} h(c_1,\ldots,c_n) \equiv 0 \mod q.$$

Proof. Write

$$h(c_1,\ldots,c_{n-1},X_n) = h(c_1,\ldots,c_n) + \frac{\partial}{\partial x_n} h(c_1,\ldots,c_n)(X_n - c_n) \\ + (X_n - c_n)^2 r(X)$$

where $r(X) \in \mathcal{O}_K[X]$. If we set X_n to be in $\mathcal{O}_K$, $d_n \equiv c_n \mod \wp$, then the first and last terms are multiples of $\wp^2$, hence the middle term must be as well. Therefore $\frac{\partial}{\partial x_n} h(c_1,\ldots,c_n)$ must be zero modulo $\wp$. □

Lemma 1.10. *For $\delta > 0$ sufficiently small,*

$$|\mathscr{N}_3(N,\delta)| \ll_{n,K} N^{d(n-1)}$$

as $N \to +\infty$.

Proof. As in Lemma 1.8, for every $\wp|\mathfrak{C}_f = \mathfrak{C}$, f has either at least a triple root or at least a pair of double roots modulo $\wp$. Let q so that $f \mod \wp \in \mathbb{F}_q[X]$. Apply Proposition 1.7 to $d_f \mod \wp$ for every $\wp|\mathfrak{C}$ as a polynomial in the coefficients $\alpha_{n-1},\ldots,\alpha_0$ of f. It follows that

$$\frac{\partial}{\partial \alpha_0} d_f \equiv 0 \mod \mathfrak{C};$$

hence so is the Sylvester resultant

$$\mathrm{Res}_{\alpha_0}(d_f, \frac{\partial}{\partial \alpha_0} d_f) = \pm d_{d_f(\alpha_0)}.$$

Let $D(\alpha_{n-1},\ldots,\alpha_1) := d_{d_f(\alpha_0)}$. Note that D is not identically zero, thanks to the formulae for iterated discriminants of [LMc]. Moreover, by Lemma 3.1 of [Bh2], the number of $\alpha_{n-1},\ldots,\alpha_1$ in $\mathcal{O}_K$ of height $\le N$ so that $D(\alpha_{n-1},\ldots,\alpha_1) = 0$ is $O(N^{d(n-2)})$; the number of f with such $\alpha_{n-1},\ldots,\alpha_1$ is thus $O(N^{d(n-1)})$.

Fix now $\alpha_{n-1},\ldots,\alpha_1$ so that $D(\alpha_{n-1},\ldots,\alpha_1) \neq 0$. Then $D(\alpha_{n-1},\ldots,\alpha_1) \equiv 0 \mod \mathfrak{C}$ for at most $O_{K,\varepsilon}(N^\varepsilon)$ ideal factors $\mathfrak{C}$ of norm $N_{K/\mathbb{Q}}\mathfrak{C} > N^d$. Once $\mathfrak{C}$ is determined by $\alpha_{n-1},\ldots,\alpha_1$ up to $O(N^\varepsilon)$ possibilities, the number of solutions for $\alpha_0 \mod \mathfrak{C}$ to $d_f \equiv 0 \mod \mathfrak{C}$ is $(\deg_{\alpha_0}(d_f))^{\omega(\mathfrak{C})} \ll_{K,\varepsilon} N^\varepsilon$. This is due to the fact that the number of solutions of $\alpha_0 \mod \wp$ so that $d_f \equiv 0 \mod \wp$ for all $\wp|\mathfrak{C}$ is $\deg_{\alpha_0}(d_f)$.

Since $N_{K/\mathbb{Q}}\mathfrak{C} > N^d$ the possibilities for α_0 of height $\le N$ are also $O_{K,\varepsilon}(N^\varepsilon)$. So the total number of f is $O_{K,\varepsilon}(N^{d(n-1)+\varepsilon})$.

We are going to remove the factor N^ε. To do this, consider

$$\mathfrak{A} := \prod_{\substack{\wp|\mathfrak{C} \\ N_{K/\mathbb{Q}}\wp > N^{d\delta/2}}} \wp.$$

- If $N_{K/\mathbb{Q}}\mathfrak{A} \leq N^d$, then $\mathfrak{C}$ has a factor $\mathfrak{B}$ of norm

  $$N^{d\left(1+\frac{\delta}{2}\right)} \leq N_{K/\mathbb{Q}}\mathfrak{B} \leq N^{d(1+\delta)},$$

  with $\mathfrak{A}|\mathfrak{B}|\mathfrak{C}$. Let $\mathfrak{B}$ be such a factor of largest norm. Define

  $$\mathfrak{D}' := \prod_{\wp|\mathfrak{B}} \wp^{v_\wp(\mathfrak{D})}.$$

  Then $N_{K/\mathbb{Q}}\mathfrak{D}' > N^{d(2+\delta)}$. The same argument of Lemma 1.8 with $\mathfrak{B}$ in place of $\mathfrak{C}$ and $\mathfrak{D}'$ in place of $\mathfrak{D}$ gives the estimate

  $$\sum_{N_{K/\mathbb{Q}}\mathfrak{D}' > N^{d(2+\delta)}} O_{K,\varepsilon}(N^{nd+\varepsilon} \cdot N^{-2d-d\delta}) \ll_{n,K} N^{d(n-1)}.$$

- If $N_{K/\mathbb{Q}}\mathfrak{A} > N^d$, we use the original argument at the beginning of the proof with $\mathfrak{A}$ in place of $\mathfrak{C}$. We have that $\mathfrak{A}$ is a divisor of $D(\alpha_{n-1}, \ldots, \alpha_1)$. Let $\alpha_{n-1}, \ldots, \alpha_1$ so that $D(\alpha_{n-1}, \ldots, \alpha_1) \neq 0$.

  Now, $d_f(\alpha_0)$ is a polynomial in α_0 of degree $\leq 2n-2$; its coefficients are monomials in $\alpha_{n-1}, \ldots, \alpha_1$ of degree $\leq 2n-2$. Therefore D, whose degree is $\leq 4n-6$, has bounded norm

  $$N_{K/\mathbb{Q}}D \ll N^{d(2n-2)(4n-6)}.$$

  The reader can see some details in 3.1. The number of primes $\wp$ with $N_{K/\mathbb{Q}}\wp > N^{d\delta/2}$ dividing D is then at most

  $$\ll \frac{\log(N^{d(2n-2)(4n-6)})}{N^{d\delta/2}} \ll_{n,d} 1.$$

  Once $\mathfrak{A}$ is determined by $\alpha_{n-1}, \ldots, \alpha_1$, the number of solutions for α_0 mod $\mathfrak{A}$ to $d_f \equiv 0 \mod \mathfrak{A}$ is $O_{n,K}(1)$. Since $N_{K/\mathbb{Q}}\mathfrak{A} > N^d$, the total number of f is then $O_{n,K}(N^{d(n-1)})$.

$\square$

We now put it all together. Note that S_3, S_4 and S_5 are primitive groups, hence the upper bound of 1.3.1 is not interesting for $n \leq 5$. For the second case of Lemma 1.9, if $n \leq 2(2d+1)$, the condition (2) becomes

$$32d^4 + 112d^3 + 10d^2 + 57d + 16 > 0,$$

which is true for all $d \geq 1$. Similarly, the condition $n \leq 2(2d+1)$ is stronger than (3) of Lemma 1.9, and we obtain Theorem 1.1.

2 An average version of the Chebotarev Density theorem

From now on, according to Theorem 1.1, we set $\xi > 0$ so that the number of non S_n-polynomials in $\mathscr{P}_{n,N}(K)$ is $\ll_{n,K} N^{d(n-\xi)}$. Specifically, for all $n \geq 3,\ d \geq 1$ we can take $\xi = \frac{1}{2} - \varepsilon$ for an $\varepsilon > 0$ arbitrary small. If moreover n is as in (3) of Theorem 1.1, put $\xi = 1$. 3 All the implied constants in the following may depend on ε, too.

For every splitting type r, and for every prime $\wp$ of norm $q_\wp$, recall that we denoted by $X_{n,r,\wp}$ the set of polynomials in $\mathbb{F}_{q_\wp}$ with square-free factorization of type r. The following key fact is what we'll use to estimate the error term in the asymptotic of the expectation $\mathbb{E}_N(\pi_{f,r}(x))$ of $\pi_{f,r}(x)$ and its powers.

Lemma 2.1. *Let $k \geq 1$, $\wp_1, \dots, \wp_k$ primes and $g_i \in X_{n,r,\wp_i}$ for all $i = 1, \dots, k$. Then if $q_{\wp_i} < N^{d\xi/kn}$ for all $i = 1, \dots, k$*

$$\mathbb{P}_N(f \in \mathscr{P}^0_{n,N} : f \equiv g_i \mod \wp_i \ \forall i = 1, \dots, k) = \frac{1}{(q_{\wp_1} \cdots q_{\wp_k})^n} + O_{n,K}(N^{-d\xi})$$

as $N \to +\infty$.

Proof. We prove the case $k = 1$. An application of the chinese remainder theorem leads to the result for $k > 1$.
Let $g = \sum_{i=1}^n g_i X^i$ and $f = \sum_{i=1}^n f_i X^i$. Now $(\omega_1, \dots, \omega_d)$ is an integral bases of $\mathcal{O}_K$ over $\mathbb{Z}$; by applying linear transformations we can assume that the reduction modulo $\wp$ of $(\omega_1, \dots, \omega_{f_\wp})$ is a basis for the $\mathbb{F}_p$-vector space $\mathcal{O}_K/\wp$. Then write for every $i = 0, \dots, n-1$

$$g_i = \sum_{j=1}^{f_\wp} b_j^{(i)} \omega_j \mod \mathbb{F}_{q_\wp},$$

$$f_i = \sum_{j=1}^{f_\wp} a_j^{(i)} \omega_j \mod \mathbb{F}_{q_\wp},$$

where $a_j^{(i)}, b_j^{(i)} \in \mathbb{Z}$ for all i and j.

One has $f \equiv g \mod \wp$ if and only if $f_i = g_i$ in $\mathbb{F}_{q_\wp}$ for $i = 0, \dots, n-1$. This means $a_j^{(i)} \equiv b_j^{(i)} \mod p$, that is $a_j^{(i)} = b_j^{(i)} + pk_j^{(i)}$ for some $k_j^{(i)} \in \mathbb{Z}$. Since the height of f is less or equal than N, for $j = 1, \dots, f_\wp$ and for all $i = 0, \dots, n-1$ we have

$$\frac{-N - b_j^{(i)}}{p} \leq k_j^{(i)} \leq \frac{N - b_j^{(i)}}{p};$$

so for each of the coefficients $a_1^{(i)}, \dots, a_{f_\wp}^{(i)}$ we have

$$\left\lceil \frac{N - b_j^{(i)}}{p} \right\rceil - \left\lceil \frac{-N - b_j^{(i)}}{p} \right\rceil = \frac{2N}{p} + O(1)$$

choices. Whereas for each coefficient $a_{f_\wp+1}^{(i)}, \dots, a_d^{(i)}$ there are $2N$ choices. Therefore for each coefficient f_i of f one has

$$\Big(\frac{2N}{p} + O(1)\Big)^{f_\wp} \cdot (2N)^{d-f_\wp} = \frac{(2N)^d}{q_\wp} + O(N^{d-1})$$

possibilities. It turns out that

$$|\{f \in \mathscr{P}_{n,N} : f \equiv g \mod \wp\}| = \frac{(2N)^{nd}}{q_\wp^n} + O(N^{dn-1}),$$

so by Theorem 1.1

$$\begin{aligned} |\{f \in \mathscr{P}^0_{n,N} : f \equiv g \mod \wp\}| &= \sum_{\substack{f \in \mathscr{P}_{n,N} \\ f \equiv g \bmod \wp}} 1 + O\Big(\sum_{f \notin \mathscr{P}^0_{n,N}} 1\Big) \\ &= \frac{(2N)^{nd}}{q_\wp^n} + O(N^{d(n-\xi)}). \end{aligned}$$

As long as $q_\wp^n < N^{d\xi}$, we get

$$\begin{aligned} \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \equiv g \bmod \wp}} 1 &= \frac{1}{(2N)^{nd}}(1 + O(N^{d(n-\xi)}))\Big(\frac{(2N)^{nd}}{q_\wp^n} + O(N^{d(n-\xi)})\Big) \\ &= (1 + O(N^{-d\xi}))\Big(\frac{1}{q_\wp^n} + O(N^{-d\xi})\Big) \\ &= \frac{1}{q_\wp^n} + O(N^{-d\xi}). \end{aligned}$$

□

Proposition 2.1. *One has, for all primes $\wp$ with $q_\wp < N^{d\xi/(n+1)}$,*

(1) $\mathbb{P}_N(\mathbb{1}_{f,r}(\wp) = 1) = \mathbb{E}_N(\mathbb{1}_{f,r}(\wp)) = \delta(r) + \frac{C_r}{q_\wp} + O\Big(\frac{1}{q_\wp^2} + q_\wp^n N^{-d\xi}\Big)$, *for some explicit constant C_r;*

(2) $\sigma_N^2(\mathbb{1}_{f,r}(\wp)) = (\delta(r) - \delta(r)^2) + \frac{C_r(1-2\delta(r))}{q_\wp} + O\Big(\frac{1}{q_\wp^2} + q_\wp^n N^{-d\xi}\Big)$.

It follows that, for $x < N^{d\xi/(n+1)}$,

(3) $\mathbb{E}_N(\pi_{f,r}(x)) = \delta(r)\pi_K(x) + C_r \log\log x + O_{n,K}(1)$,

as $x, N \to +\infty$.

Hence, the *normal order* of $\pi_{f,r}(x)$ is $\delta(r)\pi_K(x)$, which means that $\pi_{f,r}(x) \sim \delta(r)\pi_K(x)$ for almost all f, as $x \to +\infty$ and N large enough.

Proof. Once fixed a prime $\wp$,

$$\begin{aligned}
\mathbb{E}_N(\mathbb{1}_{f,r}(\wp)) &= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \mathbb{1}_{f,r}(\wp) \\
&= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \text{ of splitting type } r \bmod \wp}} 1 \\
&= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{g \in X_{n,r,\wp}} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \equiv g \bmod \wp}} 1.
\end{aligned}$$

On the other hand,

$$|X_{n,r,\wp}| = \prod_{k=1}^{n} \binom{A_{q_\wp,k}}{r_k},$$

where $A_{q_\wp,k}$ is the number of degree-k irreducible polynomials in $\mathbb{F}_{q_\wp}[X]$, which, by the Möbius inversion formula, equals

$$\frac{1}{k}\sum_{d|k} \mu(d) q_\wp^{k/d} = \frac{q_\wp^k}{k} + O(q_\wp^{\alpha_k}),$$

where $\alpha_k = 1$ if $k = 2$, and $\alpha_k < k-1$ if $k > 2$. One has, for all $k \geq 2$

$$\begin{aligned}
\binom{A_{q_\wp,k}}{r_k} &= \frac{A_{q_\wp,k}(A_{q_\wp,k}-1)\dots(A_{q_\wp,k}-r_k+1)}{r_k!} \\
&= \frac{1}{r_k!}\Big(\frac{q_\wp^k}{k} + O(q_\wp^{\alpha_k})\Big)\dots\Big(\frac{q_\wp^k}{k} - r_k + 1 + O(q_\wp^{\alpha_k})\Big).
\end{aligned}$$

It turns out that

$$\binom{A_{q_\wp,k}}{r_k} = \begin{cases} \frac{1}{r_1!} q_\wp(q_\wp - 1)\dots(q_\wp - r_1 + 1) & \text{if } k = 1 \\ \frac{1}{r_2! 2^{r_2}} q_\wp^{2r_2} + C(r_2) q_\wp^{2r_2 - 1} + O(q_\wp^{2r_2-2}) & \text{if } k = 2 \\ \frac{1}{r_k! k^{r_k}} q_\wp^{kr_k} + O(q_\wp^{k(r_k-1)+\alpha_k}) & \text{if } k > 1. \end{cases}$$

Hence

$$|X_{n,r,\wp}| = \frac{1}{r_1!}q_\wp(q_\wp{-}1)\dots(q_\wp{-}r_1{+}1)\frac{1}{r_2!2^{r_2}}(q_\wp^{2r_2}{+}C(r_2)q_\wp^{2r_2-1}{+}O(q_\wp^{2r_2-2}))$$
$$\prod_{k=3}^{n}(\frac{1}{r_k!k^{r_k}}q_\wp^{kr_k} + O(q_\wp^{k(r_k-1)+\alpha_k}))$$
$$= \delta(r)q_\wp^n + C_r q_\wp^{n-1} + O(q_\wp^{n-2}),$$

where $C_r = -\delta(r)C(r_2)\frac{(r_1+1)(r_1+2)}{2r_1!}$.

By Lemma 2.1, for $q_\wp^{n+1} < N^{d\xi}$,

$$\mathbb{E}_N(\mathbb{1}_{f,r}(\wp)) = (\delta(r)q_\wp^n + C_r q_\wp^{n-1} + O(q_\wp^{n-2}))\Big(\frac{1}{q_\wp^n} + O(N^{-d\xi})\Big)$$
$$= \delta(r) + \frac{C_r}{q_\wp} + O\Big(\frac{1}{q_\wp^2} + q_\wp^n N^{-d\xi}\Big),$$

which proves (1) and (2) follows by definition.

For (3), by linearity, we simply have to sum over all primes $\wp$ with $N_{K/\mathbb{Q}}\wp \leq x$ and use the estimate

$$\sum_{N_{K/\mathbb{Q}}\wp\leq x} \frac{1}{N_{K/\mathbb{Q}}\wp} = \log\log x + O(1)$$

to get

$$\mathbb{E}_N(\pi_{f,r}(x)) = \delta(r)\pi_K(x) + C_r \log\log x + O(1 + \pi_K(x)^{n+1}N^{-d\xi})$$

as long as

$$\pi_K(x)^{n+1}N^{-d\xi} = o(\log\log x).$$

If moreover $x < N^{d\xi/(n+1)}$, then the term $\pi_K(x)^{n+1}N^{-d\xi}$ is negligible. $\square$

Remark. From (3) of Proposition 2.1, we have that for every $m \geq 2$,

$$\pi_{f,r}(x) - \delta(r)\pi_K(x) = O((\log\log x)^m)$$

as $x \to +\infty$, for all but $O_{n,K}\Big(x^{\frac{(n+1)(n-\xi)}{\xi}}(\log\log x)^{1-m}\Big)$ S_n-polynomials f of height $\ll x^{\frac{(n+1)}{d\xi}}$.

Confront this with the similar result pointed out in Remark 1.2.3, obtained by sieving polynomials.

For $f \in \mathscr{P}^0_{n,N}$, let $\varphi : G_f \to \mathbb{C}$ be a central function, i.e. constant on the conjugacy classes. Define

$$\pi_{f,\varphi}(x) = \sum_{\substack{N_{K/\mathbb{Q}}\wp\leq x \\ \wp\nmid D_f}} \varphi(\mathrm{Frob}_{f,\wp}).$$

Then, if we sum over the conjugacy classes, i.e. over the splitting types $r = (r_1, \ldots, r_n)$, we get

$$\pi_{f,\varphi}(x) = \sum_r \varphi(g_r)\pi_{f,r}(x),$$

where g_r is any element of the conjugacy class $\mathscr{C}_r$ for every r.

Corollary 2.1. *If $x < N^{d\xi/(n+1)}$,*

$$\mathbb{E}_N(\pi_{f,\varphi}(x)) = \sum_r \delta(r)\varphi(g_r)\pi_K(x) + \sum_r \delta(r)\varphi(g_r)\log\log x + O_{n,K}(||\varphi||),$$

where $||\varphi|| = \sup_{g\in G_f} |\varphi(g)|$.

2.1 Higher moments

The following approach is based by the one used in [GS] to compute the moments

$$\sum_{n\le x}(\omega(n) - \log\log x)^k$$

of the prime divisor function, uniformely in a wide range of k. Our aim is to prove Theorem 2 by using the method of moments. This can also be done, as in the classical proof of the Erdős-Kac theorem, by applying the Central Limit Theorem (see Appendix A). However here we get better estimates allowing us to prove Theorem 2 in a significantly faster way.

Fix a splitting type r and a prime $\wp$. Consider the independent discrete random variables $X_\wp$ defined by

$$\mathbb{P}(X_\wp = 1) = \frac{|X_{n,r,\wp}|}{q_\wp^n}.$$

So

$$\mathbb{P}(X_\wp = 1) = \frac{|X_{n,r,\wp}|}{q_\wp^n} = \delta(r) + \frac{C_r}{p} + O\Big(\frac{1}{q_\wp^2}\Big) \tag{13}$$

For all primes $\wp$ we define the function

$$Y_\wp(f) = \begin{cases} 1 - \frac{|X_{n,r,\wp}|}{q_\wp^n} & \text{if } \mathbb{1}_{f,r}(\wp) = 1 \\ -\frac{|X_{n,r,\wp}|}{q_\wp^n} & \text{otherwise .} \end{cases}$$

Now, we consider a generalization $Y_\mathfrak{a}$ of the function $Y_\wp$ for any integral non-zero ideal $\mathfrak{a}$ of K, whose k-moments are "small" unless $\mathfrak{a}$ satisfies the following property $(*)$: $\wp^\alpha || \mathfrak{a} \Rightarrow \alpha \ge 2$ (see the next lemma).

Let $\mathfrak{a} = \prod_{i=1}^s \wp_i^{\alpha_i}$ in K, where the $\wp_i$ are distinct primes of $\mathcal{O}_K$ and $\alpha_i \ge 1$. Let $\mathfrak{A} := \prod_{i=1}^s \wp_i$ be the square-free part of $\mathfrak{a}$. Set

$$Y_\mathfrak{a}(f) = \prod_{i=1}^s Y_{\wp_i}(f)^{\alpha_i}.$$

Lemma 2.2. *Uniformly for* ***even*** *natural numbers k with $k \ll_r \frac{d\xi}{n+1/2}\frac{\log N}{\log z}$, one has*

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right)^k = C_{k,r}\pi_K(z)^{k/2}\left(1+O\left(\frac{k^3}{(1-\delta(r))^{k/2}}\frac{\log\log z}{\pi_K(z)}\right)\right) + O(\pi_K(z)^{k(n+1)}N^{-d\xi}),$$

as $z, N \to +\infty$. While uniformly for ***odd*** *natural numbers k with $k \ll_r \frac{d\xi}{n+1/2}\frac{\log N}{\log z}$, one has*

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right)^k \ll C_{k,r}\pi_K(z)^{k/2}k\frac{\log\log z}{\pi_K(z)^{1/2}}+\pi_K(z)^{k(n+1)}N^{-d\xi},$$

as $z, N \to +\infty$.

Here

$$C_k = \begin{cases}\frac{k!}{2^{k/2}(k/2)!} & \text{for } k \text{ even}\\ \frac{k!}{2^{\frac{k-1}{2}}(\frac{k-1}{2})!} & \text{for } k \text{ odd,}\end{cases}$$

and

$$C_{k,r} = \begin{cases}C_k(\delta(r)-\delta(r)^2)^{k/2} & \text{for } k \text{ even}\\ C_k\delta(r)^{\frac{k-1}{2}} & \text{for } k \text{ odd.}\end{cases}$$

Observe that, for any real number $z < x$, we can write

$$\pi_{f,r}(x) - \delta(r)\pi_K(x) = \sum_{p\le z}Y_\wp(f) + \sum_{z<N_{K/\mathbb{Q}}\wp\le x}\mathbb{1}_{f,r}(\wp) + \Big(\sum_{p\le z}\frac{|X_{n,r,\wp}|}{q_\wp^n} - \delta(r)\pi_K(x)\Big).$$

Pick $z = x - k$. Since

$$\pi_K(z) \sim \frac{x-k}{\log x\left(1+\frac{\log\left(1-\frac{k}{x}\right)}{\log x}\right)} = \frac{x}{\log x} + O\left(\frac{k}{\log x}\right),$$

by the above one has

$$\pi_{f,r}(x) - \delta(r)\pi_K(x) = \sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f) + O_r\left(\frac{k}{\log x}\right).$$

Proof. We may write

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right)^k=\sum_{N_{K/\mathbb{Q}}\wp_1,\dots,N_{K/\mathbb{Q}}\wp_k\le z}\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}Y_{\wp_1\dots\wp_k}(f).$$

Let us then consider more generally $\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}Y_{\mathfrak{a}}(f)$. By definition, for any prime $\wp$, $Y_\wp(f)=Y_\wp(g)$ if $f\equiv g \bmod \wp$; therefore

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}Y_{\mathfrak{a}}(f)=\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{\substack{g_i \bmod \wp_i\\ i=1,\dots,s}}\sum_{\substack{f\in\mathscr{P}^0_{n,N}\\ f\equiv g_i \bmod \wp_i\ \forall i}}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s},$$

where the first sum in the right-hand side is over $g_i\in\mathbb{F}_{q_{\wp_i}}[X]$ monic. As long as $(q_{\wp_1}\dots q_{\wp_s})^n<N^{d\xi}$ the sum is, by Lemma 2.1,

$$\begin{aligned}&\sum_{g_1,\dots,g_s}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{\substack{f\in\mathscr{P}^0_{n,N}\\ f\equiv g_i \bmod \wp_i\ \forall i}}1\\
&\quad=\sum_{g_1,\dots,g_s}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\left(\frac{1}{(q_{\wp_1}\dots q_{\wp_s})^n}+O(N^{-d\xi})\right)\\
&\quad=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^n}\sum_{g_1,\dots,g_s}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}+O\left(N^{-d\xi}\sum_{g_1,\dots,g_s}1\right)\\
&\quad=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^n}\sum_{g_1,\dots,g_s}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}+O((N_{K/\mathbb{Q}}\mathfrak{A})^nN^{-d\xi}),\end{aligned}$$

since $|Y_{\wp_i}(g_i)^{\alpha_i}|\ll 1$. Denoting the main term by $Y(\mathfrak{a})$, we have

$$\begin{aligned}Y(\mathfrak{a})&=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^n}\sum_{g_1}Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\\
&=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^n}\prod_{i=1}^s\left(\sum_{g_i\in X_{n,r,\wp_i}}\left(1-\frac{|X_{n,r,\wp_i}|}{q^n_{\wp_i}}\right)^{\alpha_i}+\sum_{g_i\notin X_{n,r,\wp_i}}\left(-\frac{|X_{n,r,\wp_i}|}{q^n_{\wp_i}}\right)^{\alpha_i}\right)\\
&=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^n}\prod_{i=1}^s\left(|X_{n,r,\wp_i}|\left(1-\frac{|X_{n,r,\wp_i}|}{q^n_{\wp_i}}\right)^{\alpha_i}+(q^n_{\wp_i}-|X_{n,r,\wp_i}|)\left(-\frac{|X_{n,r,\wp_i}|}{q^n_{\wp_i}}\right)^{\alpha_i}\right)\\
&=\prod_{\wp^\alpha||\mathfrak{a}}\left(\frac{|X_{n,r,\wp}|}{q^n_\wp}\left(1-\frac{|X_{n,r,\wp}|}{q^n_\wp}\right)^{\alpha}+\left(1-\frac{|X_{n,r,\wp}|}{q^n_\wp}\right)\left(-\frac{|X_{n,r,\wp}|}{q^n_\wp}\right)^{\alpha}\right),\end{aligned}$$

by using the inductive formula

$$\prod_{i=1}^{\ell}(a_i+b_i)=\sum_{\substack{1\le i_1<\dots<i_k\le\ell\\ j_1<\dots<j_h\le\in\{1,\dots,\ell\}\setminus\{i_1,\dots,i_k\}\\ k+h=\ell}}a_{i_1}\dots a_{i_k}b_{j_1}\dots b_{j_h}.$$

Thus

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}} Y_{\mathfrak{a}}(f) = Y(\mathfrak{a}) + O((N_{K/\mathbb{Q}}\mathfrak{A})^n N^{-d\xi});$$

Observe now that $Y(\mathfrak{a}) = 0$ unless $\alpha_i \geq 2$ for all $i = 1, \ldots, s$. It turns out that

$$\begin{aligned}\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\leq z} Y_{\wp}(f)\right)^k &= \sum_{\substack{N_{K/\mathbb{Q}}\wp_1,\ldots,N_{K/\mathbb{Q}}\wp_k\leq z\\ \wp_1\cdots\wp_k\ (*)}} Y(\wp_1\ldots\wp_k)\\ &\quad + O\left(\sum_{N_{K/\mathbb{Q}}\wp_1,\ldots,N_{K/\mathbb{Q}}\wp_k\leq z}(q_{\wp_1}\ldots q_{\wp_k})^n N^{-d\xi}\right)\\ &= \sum_{\substack{N_{K/\mathbb{Q}}\wp_1,\ldots,N_{K/\mathbb{Q}}\wp_k\leq z\\ \wp_1\cdots\wp_k\ (*)}} Y(\wp_1\ldots\wp_k) + O(\pi_K(z)^{k(n+1)}N^{-d\xi}).\end{aligned}$$

Let $\mathcal{P}_1, \ldots, \mathcal{P}_s$ be the distinct primes in $\wp_1\ldots\wp_k$ with $N_{K/\mathbb{Q}}\mathcal{P}_1 < \cdots < N_{K/\mathbb{Q}}\mathcal{P}_s$. Since $\wp_1\ldots\wp_k$ satisfies $(*)$, we have $s \leq k/2$. The main term above is

$$\sum_{s\leq k/2}\ \sum_{N_{K/\mathbb{Q}}\mathcal{P}_1<\cdots<N_{K/\mathbb{Q}}\mathcal{P}_s\leq z}\ \sum_{\substack{\alpha_1,\ldots,\alpha_s\geq 2\\ \alpha_1+\cdots+\alpha_s=k}}\binom{k}{\alpha_1,\ldots,\alpha_s} Y(\mathcal{P}_1^{\alpha_1}\ldots\mathcal{P}_1^{\alpha_s}) \tag{14}$$

At this point, we divide into two cases, since if k is even there is a term $s = k/2$ with all $\alpha_i = 2$. This main term contributes

$$\begin{aligned}&\frac{k!}{2^{k/2}(k/2)!}\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\ldots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\leq z\\ \mathcal{P}_j\ \text{distinct}}} Y(\mathcal{P}_1^2\ldots\mathcal{P}_{k/2}^2)\\ &\qquad = \frac{k!}{2^{k/2}(k/2)!}\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\ldots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\leq z\\ \mathcal{P}_j\ \text{distinct}}}\prod_{i=1}^{k/2}\frac{|X_{n,r,\mathcal{P}_i}|}{q^n_{\mathcal{P}_i}}\left(1-\frac{|X_{n,r,\mathcal{P}_i}|}{q^n_{\mathcal{P}_i}}\right).\end{aligned}$$

Now, clearly

$$\begin{aligned}&\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\ldots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\leq z\\ \mathcal{P}_j\text{distinct}}}\prod_{i=1}^{k/2}\frac{|X_{n,r,\mathcal{P}_i}|}{q^n_{\mathcal{P}_i}}\left(1-\frac{|X_{n,r,\mathcal{P}_i}|}{q^n_{\mathcal{P}_i}}\right)\\ &\qquad\leq\left(\sum_{N_{K/\mathbb{Q}}\mathcal{P}\leq z}\frac{|X_{n,r,\mathcal{P}}|}{q^n_{\mathcal{P}}}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q^n_{\mathcal{P}}}\right)\right)^{k/2}.\end{aligned}$$

On the other hand, by induction

$$\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\dots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\le z\\ \mathcal{P}_j \text{ distinct}}} \prod_{i=1}^{k/2} \frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\left(1-\frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\right)$$

$$= \sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\dots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2-1}\le z\\ \mathcal{P}_j \text{ distinct}}} \prod_{i=1}^{k/2-1} \frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\left(1-\frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\right) \sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\le z\\ \mathcal{P}_{k/2}\neq\mathcal{P}_j\ \forall j}} \frac{|X_{n,r,\mathcal{P}_{k/2}}|}{q_{\mathcal{P}_{k/2}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}_{k/2}}|}{q_{\mathcal{P}_{k/2}}^n}\right)$$

$$\ge \sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\dots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2-1}\le z\\ \mathcal{P}_j \text{ distinct}}} \prod_{i=1}^{k/2-1} \frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\left(1-\frac{|X_{n,r,\mathcal{P}_i}|}{q_{\mathcal{P}_i}^n}\right) \sum_{N_{K/\mathbb{Q}}\Pi_{k/2}\le N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right)$$

$$\ge \dots \ge \sum_{N_{K/\mathbb{Q}}\Pi_2\le N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right)\cdots \sum_{N_{K/\mathbb{Q}}\Pi_{k/2}\le N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right)$$

$$\ge \left(\sum_{N_{K/\mathbb{Q}}\Pi_{k/2}\le N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right)\right)^{k/2},$$

where Π_n is the n-th prime of smallest norm. By (13)

$$\sum_{N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right) = (\delta(r)-\delta(r)^2)\pi_K(z)+O(\log\log z),$$

$$\sum_{N_{K/\mathbb{Q}}\Pi_{k/2}\le N_{K/\mathbb{Q}}\mathcal{P}\le z} \frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\left(1-\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^n}\right) = (\delta(r)-\delta(r)^2)\pi_K(z)+O(\log\log z+k).$$

The main term in (14) is then

$$\begin{aligned}&\frac{k!}{2^{k/2}(k/2)!}((\delta(r)-\delta(r)^2)\pi_K(z)+O(\log\log z+k))^{k/2}\\ &\quad=\frac{k!}{2^{k/2}(k/2)!}(\delta(r)-\delta(r)^2)^{k/2}(\pi_K(z)^{k/2}+O(k^2\pi_K(z)^{k/2-1}\log\log z)).\end{aligned}$$

We have now to estimate the error term in (14), for $s = k/2-1$. Since

$Y(\mathcal{P}_1^{\alpha_1}\dots\mathcal{P}_s^{\alpha_s}) \le \frac{|X_{n,r,\mathcal{P}_1}|\dots|X_{n,r,\mathcal{P}_s}|}{(q_{\mathcal{P}_1}\cdots q_{\mathcal{P}_s})^n}$ one has

$$\begin{aligned}
&\sum_{N_{K/\mathbb{Q}}\mathcal{P}_1<\dots<N_{K/\mathbb{Q}}\mathcal{P}_s\le z}\ \sum_{\substack{\alpha_1,\dots,\alpha_s\ge 2\\ \alpha_1+\dots+\alpha_s=k}}\binom{k}{\alpha_1,\dots,\alpha_s}Y(\mathcal{P}_1^{\alpha_1}\dots\mathcal{P}_s^{\alpha_s})\\
&\quad\le \frac{k!}{(k/2-1)!}\Big(\sum_{N_{K/\mathbb{Q}}\mathcal{P}\le z}\frac{|X_{n,r,\mathcal{P}}|}{q_{\mathcal{P}^n}}\Big)^{k/2-1}\sum_{\substack{\alpha_1,\dots,\alpha_{k/2-1}\ge 2\\ \alpha_1+\dots+\alpha_{k/2-1}=k}}\frac{1}{\alpha_1!\dots\alpha_{k/2-1}!}\\
&\quad\le \frac{k!}{2^{k/2-1}(k/2-1)!}\binom{k/2}{k/2-2}(\delta(r)\pi_K(z)+O(\log\log z))^{k/2-1}\\
&\quad\ll \frac{k!}{2^{k/2}(k/2)!}k^3\left(\delta(r)^{k/2-1}\pi_K(z)^{k/2-1}+k\pi_K(z)^{k/2-2}\log\log z\right)\\
&\qquad\qquad\ll \frac{k!}{2^{k/2}(k/2)!}k^3\delta(r)^{k/2-1}\pi_K(z)^{k/2-1}.
\end{aligned}$$

We used the fact that the number of sequences of integers $(\alpha_1,\dots,\alpha_{k/2-1})$, $\alpha_i\ge 2$ such that $\sum\alpha_i = k$ is the number of sequences $(\alpha'_1,\dots,\alpha'_{k/2-1})$, $\alpha'_i\ge 1$ such that $\sum\alpha_i = k/2+1$, that is the number of strong compositions of $k/2+1$ into $k/2-1$ parts, which is $\binom{k/2}{k/2-2}$. Thus, for k even,

$$\begin{aligned}
&\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right)^k\\
&\qquad= \frac{k!}{2^{k/2}(k/2)!}(\delta(r)-\delta(r)^2)^{k/2}(\pi_K(z)^{k/2}\\
&\qquad\quad+O\left(k^2\pi_K(z)^{k/2-1}\log\log z+\frac{k^3}{(1-\delta(r))^{k/2}}\pi_K(z)^{k/2-1})\right)\\
&\qquad\quad+O(\pi_K(z)^{k(n+1)}N^{-d\xi})\\
&= \frac{k!}{2^{k/2}(k/2)!}(\delta(r)-\delta(r)^2)^{k/2}\pi_K(z)^{k/2}\left(1+O\left(\frac{k^3}{(1-\delta(r))^{k/2}}\frac{\log\log z}{\pi_K(z)}\right)\right)\\
&\qquad\quad+O(\pi_K(z)^{k(n+1)}N^{-d\xi}).
\end{aligned}$$

Finally, for k odd, we have the estimate for the term with $s=k/2-1/2$ as for the previous case, obtaining

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\sum_{N_{K/\mathbb{Q}}\wp\le z} Y_\wp(f)\right)^k$$
$$\ll \frac{k!}{2^{\frac{k-1}{2}}(\frac{k-1}{2})!}k\left(\delta(r)^{\frac{k-1}{2}}\pi_K(z)^{\frac{k-1}{2}}+O(k\pi_K(z)^{\frac{k-3}{2}}\log\log z)\right)$$
$$+\pi_K(z)^{k(n+1)}N^{-d\xi}$$
$$\ll C_{k,r}\pi_K(z)^{k/2}k\frac{\log\log z}{\pi_K(z)^{1/2}}+\pi_K(z)^{k(n+1)}N^{-d\xi}.$$

□

Proposition 2.2. *Uniformly for* ***even*** *natural numbers k with $k\ll_r \frac{d\xi}{n+1/2}\frac{\log N}{\log x}$, one has*

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}(\pi_{f,r}(x)-\delta(r)\pi_K(x))^k$$
$$=C_{k,r}\pi_K(x)^{k/2}\left(1+O\left(\frac{k^{3/2}}{(1-\delta(r))^{k/2}}\frac{\log\log x}{\pi_K(x)^{1/2}}\right)\right)+O(\pi_K(x)^{k(n+1)}N^{-d\xi}),$$

as $x,N\to+\infty$. While uniformly for ***odd*** *natural numbers k with $k\ll_r \frac{d\xi}{n+1/2}\frac{\log N}{\log x}$,*

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}(\pi_{f,r}(x)-\delta(r)\pi_K(x))^k$$
$$\ll C_{k,r}\pi_K(x)^{k/2}k\frac{\log\log x}{\pi_K(x)^{1/2}}+\pi_K(x)^{k(n+1)}N^{-d\xi},$$

as $x,N\to+\infty$.

Proof. For $z=x-k$ we obtained

$$\pi_{f,r}(x)-\delta(r)\pi_K(x)=\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)+O_r\left(\frac{k}{\log x}\right).$$

In particular,

$$(\pi_{f,r}(x)-\delta(r)\pi_K(x))^k=\left(\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right)^k$$
$$+O\left(\sum_{j=0}^{k-1}\left(\frac{k}{\log x}\right)^{k-j}\binom{k}{j}\left|\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\right|^j\right) \tag{15}$$

The dominant term in the error is obtained for $j = k-1$. If k is even, we apply Lemma 2.2 to (15) and we get

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}(\pi_{f,r}(x)-\delta(r)\pi_K(x))^k$$

$$= C_{k,r}\pi_K(x-k)^{k/2}\left(1+O\left(\frac{k^3}{(1-\delta(r))^{k/2}}\frac{\log\log(x-k)}{\pi_K(x-k)}+k^3\frac{C_{k-1,r}}{C_{k,r}}\frac{\log\log(x-k)}{\pi_K(x-k)\log(x-k)}\right)\right)$$
$$+O(\pi_K(x-k)^{k(n+1)}N^{-d\xi})$$
$$= C_{k,r}\pi_K(x)^{k/2}\left(1+O\left(\frac{k^{3/2}}{(1-\delta(r))^{k/2}}\frac{\log\log x}{\pi_K(x)^{1/2}}\right)\right)$$
$$+O(\pi_K(x)^{k(n+1)}N^{-d\xi}),$$

since

$$\pi_K(x-k)^{k/2} = \pi_K(x)^{k/2} + O\left(\pi_K(x)^{k/2-1}\frac{k^2}{\log x}\right)$$

and

$$\frac{C_{k-1,r}}{C_{k,r}} \ll_r 1.$$

If k is odd, we can handle it using the Cauchy-Schwartz inequality:

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\Big|\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\Big|^{k-1}$$
$$\le\left(\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\Big|\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\Big|^{k-2}\right)^{1/2}\left(\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\Big|\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\Big|^{k}\right)^{1/2}.$$

Lemma 2.2 leads to

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\Big|\sum_{N_{K/\mathbb{Q}}\wp\le z}Y_\wp(f)\Big|^{k-1}\ll(C_{k-2,r}C_{k,r})^{1/2}k\pi_K(z)^{\frac{k}{2}-1}\log\log z.$$

Since

$$\frac{(C_{k-2,r}C_{k,r})^{1/2}}{C_{k,r}}\binom{k}{k-1}\asymp k^{1/2},$$

we obtain from (15)

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}(\pi_{f,r}(x)-\delta(r)\pi_K(x))^k\ll C_{k,r}\pi_K(x)^{\frac{k}{2}}\log\log x\left(\frac{k}{\pi_K(x)^{1/2}}+\frac{k^{3/2}}{\pi_K(x)\log x}\right)$$
$$+\pi_K(x)^{k(n+1)}N^{-d\xi}$$
$$\ll C_{k,r}\pi_K(x)^{k/2}k\frac{\log\log x}{\pi_K(x)^{1/2}}+\pi_K(x)^{k(n+1)}N^{-d\xi}.$$

□

In particular, if $x = o\left(N^{\frac{d\xi}{k(n+1/2)}}\right)$, then the last summand in the error term is negligible, in both cases.

2.2 Proof of the main theorem

Once proved that the normal order of $\pi_{f,r}(x)$ is $\delta(r)\pi_K(x)$, we want to study the distribution of

$$\frac{\pi_{f,r}(x) - \delta(r)\pi_K(x)}{(\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2}}$$

for $x = N^{1/\log\log N}$. As we already stated, this quantity is distributed like a normal distribution with mean 0 and variance 1. Let

$$\Phi(b) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{b} e^{-t^2/2}dt.$$

Firstly, note that the claim is equivalent to say that

$$\mathbb{P}_N\left(\frac{\pi_{f,r}(x) - \delta(r)\pi_K(x)}{(\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2}} \leq b\right) \longrightarrow \Phi(b)$$

as $N \to +\infty$. We use the method of moments here and the asymptotics of 2.1.

By the method of moments, the theorem will follow if we prove that for $k \geq 1$,

$$\mathbb{E}_N\left(\frac{(\pi_{f,r}(x) - \delta(r)\pi_K(x))^k}{((\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2})^k}\right)$$

converges to μ_k as $N \to +\infty$. See Appendix A for more details.

It's well known that

$$\mu_k = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} x^k e^{-x^2/2}dx = \begin{cases} \frac{k!}{2^{k/2}(k/2)!} & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

From Proposition 2.2, if we fix $k \geq 1$, we see exactly that

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\frac{(\pi_{f,r}(x) - \delta(r)\pi_K(x))^k}{((\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2})^k}\right) \underset{x\to+\infty}{\longrightarrow} C_k = \mu_k$$

if k is even, and

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\left(\frac{(\pi_{f,r}(x) - \delta(r)\pi_K(x))^k}{((\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2})^k}\right) \ll_{k,r} \frac{\log\log x}{\pi_K(x)^{1/2}} \underset{x\to+\infty}{\longrightarrow} 0 = \mu_k$$

if k is odd.

2.3 Estimates for subfamilies

Consider a subfamily $\mathscr{A} = \mathscr{A}_{\beta,M}(N)$ of $\mathscr{P}^0_{n,N}$, depending on parameters β, M satisfying the following conditions, for a positive real number x, and for a fixed splitting type r:

1. $1 < \beta \leq n$, $M > 0$.

2. For each prime $\wp$, let
$$\mathscr{A}^{\wp} := \{f \bmod \wp : f \in \mathscr{A}\} \subseteq \mathbb{F}_{q_\wp}[X].$$
For $s \geq 1$, if $g_i \in \mathscr{A}^{\wp_i}$ for every $1 \leq i \leq s$ and $N_{K/\mathbb{Q}}\wp_i \leq x$, then uniformely on $\wp_1, \dots, \wp_s$ with $N_{K/\mathbb{Q}}\wp_1, \dots, N_{K/\mathbb{Q}}\wp_s \leq x$,
$$\sum_{\substack{f \in \mathscr{A} \\ f \equiv g_i \bmod \wp_i\ \forall i}} 1 = \frac{MN^{d\beta}}{(q_{\wp_1} \dots q_{\wp_s})^\beta} + E_{n,K}(N)$$
where $E_{n,K}(N) \ll N^{d(\beta-\xi)}$, as $x, N \to +\infty$ and x sufficiently small with respect to N.

3. Denote by $X^{\mathscr{A}}_{n,r,\wp}$ the intersection $X_{n,r,\wp} \cap \mathscr{A}^{\wp}$. Assume that
$$\begin{aligned} |X^{\mathscr{A}}_{n,r,\wp}| &= \sum_{\substack{f \in \mathscr{A} \\ f \text{ of splitting type } r \bmod \wp}} 1 \\ &= \delta(r) q_\wp^\beta + O(E_\wp), \end{aligned}$$
In many examples we can apply the RH over finite fields, hence we get that the above sum is of size $\delta(r)|\mathscr{A}^{\wp}|$ with error term of size $O(|\mathscr{A}^{\wp}|/\sqrt{q_\wp})$. In particular, in those cases, $E_\wp \ll q_\wp^{\beta-\frac{1}{2}}$.

We proceed in a similar way as in 2.1. Define
$$Y_\wp(f) = \begin{cases} 1 - \frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta} & \text{if } \mathbb{1}_{f,r}(\wp) = 1 \\ -\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta} & \text{otherwise .} \end{cases}$$
and
$$\mu(x) = \sum_{N_{K/\mathbb{Q}}\wp \leq x} \frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta} = \delta(r)\pi_K(x) + O\left(\frac{\sqrt{x}}{\log x}\right).$$
Observe that for every $f \in \mathscr{A}$ one has
$$\pi_{f,r}(x) - \mu(x) = \sum_{N_{K/\mathbb{Q}}\wp \leq x} Y_\wp(f),$$

and so for any positive integer k,

$$\sum_{f\in\mathscr{A}}(\pi_{f,r}(x)-\mu(x))^k=\sum_{N_{K/\mathbb{Q}}\wp_1,\dots,N_{K/\mathbb{Q}}\wp_k\le x}\left(\sum_{f\in\mathscr{A}}Y^L_{\wp_1\dots\wp_k}(f)\right),$$

where as before, if $\mathfrak{a}$ is a non zero integral ideal of K and has prime factorization $\mathfrak{a}=\prod_{i=1}^s\wp_i^{\alpha_i}$, then put $Y_{\mathfrak{a}}(f)=\prod_{i=1}^s Y_{\wp_i}(f)^{\alpha_i}$.

Proposition 2.3. *Let $\mathscr{A}\subseteq\mathscr{P}^0_{n,N}$ with conditions 1, 2 and 3.*

(1) *Uniformly for even k, with $k\ll_{r,n}\frac{\log(MN^{d\beta})}{\log x}$ one has*

$$\begin{aligned}\sum_{f\in\mathscr{A}}&(\pi_{f,r}(x)-\mu(x))^k\\&=C_{k,r}MN^{d\beta}\pi_K(x)^{k/2}\left(1+O\left(\frac{k^3}{(1-\delta(r))^{k/2}}\frac{\sqrt{x}}{\pi_K(x)\log x}\right)\right)\\&\qquad+O\left(\pi_K(x)^{k(n+1)}E_{n,K}(N)\right),\end{aligned}$$

as $x,N\to+\infty$.

(2) *Uniformly for odd k, with $k\ll_{r,n}\min\left((\log x)^{1/2},\frac{\log(MN^{d\beta})}{\log x}\right)$, one has*

$$\begin{aligned}\sum_{f\in\mathscr{A}}&(\pi_{f,r}(x)-\mu(x))^k\\&\ll C_{k,r}MN^{d\beta}\pi_K(x)^{k/2}k\frac{\sqrt{x}}{\pi_K(x)^{1/2}\log x}+\pi_K(x)^{k(n+1)}E_{n,K}(N),\end{aligned}$$

as $x,N\to+\infty$.

(3) *Fix k even. If $x=o\left((MN^{d\xi})^{\frac{1}{k\left(n+\frac{1}{2}\right)}}\right)$, then*

$$\begin{aligned}\sum_{f\in\mathscr{A}}&(\pi_{f,r}(x)-\mu(x))^k\\&=C_{k,r}MN^{d\beta}\pi_K(x)^{k/2}\left(1+O_k\left(\frac{\sqrt{x}}{\pi_K(x)\log x}\right)\right)\\&\qquad+O\left(\pi_K(x)^{k(n+1)}E_{n,K}(N)\right),\end{aligned}$$

as $x,N\to+\infty$.

Proof. As before, we compute more generally $\sum_{f\in\mathscr{A}} Y_{\mathfrak{a}}(f)$ with $q_{\wp_i}\le x$:

$$\begin{aligned}
\sum_{f\in\mathscr{A}} Y_{\mathfrak{a}}(f) &= \sum_{g_i\in\mathscr{A}^{\wp_i}\ \forall i}\ \sum_{\substack{f\in\mathscr{A}\\ f\equiv g_i \bmod \wp_i\ \forall i}} Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\\
&= \sum_{g_i\in\mathscr{A}^{\wp_i}\ \forall i} Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\left(\frac{MN^{d\beta}}{(N_{K/\mathbb{Q}}\mathfrak{A})^\beta}+E_{n,K}(N)\right)\\
&= \frac{MN^{d\beta}}{(N_{K/\mathbb{Q}}\mathfrak{A})^\beta}\sum_{g_i\in\mathscr{A}^{\wp_i}\ \forall i} Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}\\
&\quad + O_r((q_{\wp_1}\dots q_{\wp_s})^\beta E_{n,K}(N))\\
&= MN^{d\beta}Y(\mathfrak{a})+O_r((N_{K/\mathbb{Q}}\mathfrak{A})^\beta E_{n,K}(N)),
\end{aligned}$$

where

$$Y(\mathfrak{a})=\frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^\beta}\sum_{g_i\in\mathscr{A}^{\wp_i}\ \forall i} Y_{\wp_1}(g_1)^{\alpha_1}\dots Y_{\wp_s}(g_s)^{\alpha_s}.$$

One has

$$\begin{aligned}
Y(\mathfrak{a}) &= \frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^\beta}\sum_{g_1\in\mathscr{A}^{\wp_1}} Y_{\wp_1}(g_1)^{\alpha_1}\cdots\sum_{g_s\in\mathscr{A}^{\wp_s}} Y_{\wp_s}(g_s)^{\alpha_s}\\
&= \frac{1}{(N_{K/\mathbb{Q}}\mathfrak{A})^\beta}\prod_{i=1}^{s}\left(\frac{|X^{\mathscr{A}}_{n,r,\wp_i}|}{q^\beta_{\wp_i}}\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp_i}|}{q^\beta_{\wp_i}}\right)^{\alpha_i}+\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp_i}|}{q^\beta_{\wp_i}}\right)\left(-\frac{|X^{\mathscr{A}}_{n,r,\wp_i}|}{q^\beta_{\wp_i}}\right)^{\alpha_i}\right)\\
&= \prod_{\wp^\alpha||\mathfrak{a}}\left(\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q^\beta_{\wp}}\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q^\beta_{\wp}}\right)^{\alpha}+\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q^\beta_{\wp}}\right)\left(-\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q^\beta_{\wp}}\right)^{\alpha}\right).
\end{aligned}$$

As before, $Y(\mathfrak{a})$ is 0 unless $\mathfrak{a}$ satisfies $(*)$. Therefore

$$\begin{aligned}
\sum_{N_{K/\mathbb{Q}}\wp_1,\dots,N_{K/\mathbb{Q}}\wp_k\le x}\ \sum_{f\in\mathscr{A}} Y_{\wp_1\dots\wp_k}(f) = MN^{d\beta}&\sum_{\substack{N_{K/\mathbb{Q}}\wp_1,\dots,N_{K/\mathbb{Q}}\wp_k\le x\\ \wp_1\dots\wp_k\ (*)}} Y(\wp_1\dots\wp_k)\\
&+O(\pi_K(x)^{k(n+1)}E_{n,K}(N)).
\end{aligned}$$

As in Lemma 2.2, if k is even, the main term of the above is

$$\begin{aligned}
&\frac{k!}{2^{k/2}(k/2)!}\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\dots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\le x\\ \mathcal{P}_j \text{ distinct}}} Y(\mathcal{P}_1^2\dots\mathcal{P}_{k/2}^2)\\
&\qquad = C_k\sum_{\substack{N_{K/\mathbb{Q}}\mathcal{P}_1,\dots,N_{K/\mathbb{Q}}\mathcal{P}_{k/2}\le x\\ \mathcal{P}_j \text{ distinct}}}\ \prod_{i=1}^{k/2}\frac{|X^{\mathscr{A}}_{n,r,\mathcal{P}_i}|}{q^\beta_{\mathcal{P}_i}}\left(1-\frac{|X^{\mathscr{A}}_{n,r,\mathcal{P}_i}|}{q^\beta_{\mathcal{P}_i}}\right),
\end{aligned}$$

with the analogous upper and lower bounds. Observe that

$$\sum_{N_{K/\mathbb{Q}}\wp\le x}\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta}\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta}\right)=(\delta(r)-\delta(r)^2)\pi_K(x)+O\left(\frac{\sqrt{x}}{\log x}\right),$$

$$\sum_{N_{K/\mathbb{Q}}\Pi_{k/2}\le N_{K/\mathbb{Q}}\wp\le x}\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta}\left(1-\frac{|X^{\mathscr{A}}_{n,r,\wp}|}{q_\wp^\beta}\right)=(\delta(r)-\delta(r)^2)\pi_K(x)+O\left(\frac{\sqrt{x}}{\log x}+k\right).$$

So the main term contributes

$$C_kMN^{d\beta}(\delta(r)-\delta(r)^2)^{k/2}(\pi_K(x)^{k/2}+O\left(k^2\pi_K(x)^{k/2-1}\frac{\sqrt{x}}{\log x}\right).$$

We now estimate the error term for $s=k/2-1$; since $Y(\mathcal{P}_1^{\alpha_1}\dots\mathcal{P}_s^{\alpha_s})\le\frac{|X^{\mathscr{A}}_{n,r,\mathcal{P}_1}|\dots|X^{\mathscr{A}}_{n,r,\mathcal{P}_s}|}{(q_{\mathcal{P}_1}\cdots q_{\mathcal{P}_s})^\beta}$ one has

$$\begin{aligned}&\sum_{N_{K/\mathbb{Q}}\mathcal{P}_1<\cdots<N_{K/\mathbb{Q}}\mathcal{P}_s\le x}\ \sum_{\substack{\alpha_1,\dots,\alpha_s\ge 2\\ \alpha_1+\cdots+\alpha_s=k}}\binom{k}{\alpha_1,\dots,\alpha_s}Y(\mathcal{P}_1^{\alpha_1}\dots\mathcal{P}_s^{\alpha_s})\\ &\le\frac{k!}{(k/2-1)!}\left(\sum_{N_{K/\mathbb{Q}}\mathcal{P}\le x}\frac{|X^{\mathscr{A}}_{n,r,\mathcal{P}}|}{q_{\mathcal{P}}^\beta}\right)^{k/2-1}\sum_{\substack{\alpha_1,\dots,\alpha_{k/2-1}\ge 2\\ \alpha_1+\cdots+\alpha_{k/2-1}=k}}\frac{1}{\alpha_1!\dots\alpha_{k/2-1}!}\\ &\qquad\ll C_kk^3\delta(r)^{k/2-1}\pi_K(x)^{k/2-1}.\end{aligned}$$

If k is odd, the estimate for $s=k/2-1/2$ gives

$$\begin{aligned}&\sum_{N_{K/\mathbb{Q}}\mathcal{P}_1<\cdots<N_{K/\mathbb{Q}}\mathcal{P}_s\le x}\ \sum_{\substack{\alpha_1,\dots,\alpha_s\ge 2\\ \alpha_1+\cdots+\alpha_s=k}}\binom{k}{\alpha_1,\dots,\alpha_s}Y(\mathcal{P}_1^{\alpha_1}\dots\mathcal{P}_s^{\alpha_s})\\ &\qquad\ll C_{k,r}\pi_K(x)^{k/2}k\frac{\sqrt{x}}{\pi_K(x)^{1/2}\log x}.\end{aligned}$$

By combining all, we have, for even k,

$$\begin{aligned}\sum_{f\in\mathscr{A}}(\pi_{f,r}(x)-\mu(x))^k&=C_{k,r}MN^{d\beta}\pi_K(x)^{k/2}\\ &\quad+O\left(C_{k,r}MN^{d\beta}k^2\pi_K(x)^{k/2-1}\frac{\sqrt{x}}{\log x}+C_kMN^{d\beta}k^3\pi_K(x)^{k/2-1}\right)\\ &\quad+O\left(\pi_K(x)^{k(n+1)}E_{n,K}(N)\right)\\ &=C_{k,r}MN^{d\beta}\pi_K(x)^{k/2}\left(1+O\left(\frac{k^3}{(1-\delta(r))^{k/2}}\frac{\sqrt{x}}{\pi_K(x)\log x}\right)\right)\\ &\quad+O(\pi_K(x)^{k(n+1)}E_{n,K}(N)).\end{aligned}$$

If $x = o(N^{\varepsilon})$, the last summand in the error term is negligible. $\square$

Note. If one applies the same exact method of Section 2.1, that is, applying the previous result to $z < x$ and then to $z = x - k$, one can achieve the following better estimate for the even k-moments related to the family $\mathscr{A}$.

Corollary 2.2. *Let $\mathscr{A} \subseteq \mathscr{P}^0_{n,N}$ with conditions 1, 2 and 3. Then uniformly for even k, with $k \ll_{r,n} \min\left((\log x)^{1/2}, \frac{\log(MN^{d\beta})}{\log x}\right)$, one has*

$$\sum_{f\in\mathscr{A}} (\pi_{f,r}(x) - \mu(x))^k$$
$$= C_{k,r} MN^{d\beta} \pi_K(x)^{k/2} \left(1 + O\left(\frac{k^{3/2}}{(1-\delta(r))^{k/2}} \frac{\sqrt{x}}{\pi_K(x)^{1/2}\log x}\right)\right)$$
$$+ O(\pi_K(x)^{k(n+1)} E_{n,K}(N)),$$

as $x, N \to +\infty$.

3 Applications

3.1 Discriminant and average of ramified primes

Let f be an S_n-polynomial and let $d_f \in \mathcal{O}_K$ be its discriminant. We are going to discuss the relation between the number of primes $\wp \in \mathcal{O}_K$ dividing d_f and the discriminant of its splitting field field K_f/K (i.e. the ramified primes in the extension K_f/K).

For a polynomial $f \in \mathscr{P}_{n,N}$, the bound

$$N_{K/\mathbb{Q}} d_f \ll N^{d(2n-2)}$$

holds, since d_f is given by the $(2n-1)$-dimensional determinant

$$d_f = (-1)^{n(n-1)/2} \det \begin{pmatrix} 1 & \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_0 & 0 & \cdots \\ 0 & \alpha_n & \alpha_{n-1} & \cdots & \alpha_1 & \alpha_1 & \cdots \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & \alpha_n & \cdots & \alpha_1 & \alpha_0 \\ n & (n-1)\alpha_{n-1} & (n-2)\alpha_{n-2} & \cdots & 0 & 0 & \cdots \\ \vdots & & & & & & \vdots \\ 0 & \cdots & \cdots & 0 & n\alpha_n & \cdots & \alpha_1 \end{pmatrix}$$

with $\alpha_n = 1$ in our case. However, it turns out (see [GZ], Corollary 2.2) that

$$N_{K/\mathbb{Q}} d_f \asymp N^{d(2n-2)}$$

for almost all f. Indeed, for all $\varepsilon > 0$ there exists $\delta = \delta(n)$ s.t. for N large enough

$$\mathbb{P}_N(|N_{K/\mathbb{Q}} d_f| > \delta N^{d(2n-2)}) > 1 - \varepsilon.$$

By the primitive element theorem, we know there is an integral element $\theta \in \mathcal{O}_{K_f}$ so that $K_f = K(\theta)$. Let $f_\theta \in K[X]$ be the minimal polynomial of θ. Then it holds the following relation between the discriminant of f_θ and the discriminant $\mathfrak{D}_{K_f/K}$ of the number field extension K_f/K:

$$d_{f_\theta} \mathcal{O}_K = \alpha_{f_\theta}^2 \cdot \mathfrak{D}_{K_f/K},$$

where $\alpha_{f_\theta} \in \mathcal{O}_K$ (see [La], Chapter III).
Now, let α be a root of $f \in \mathscr{P}^0_{n,N}$ and consider the extension generated by α over K.

$$\begin{array}{c} K_f \\ \big|\, {\scriptstyle (n-1)!} \\ K(\alpha) \\ \big|\, {\scriptstyle n} \\ K \\ \big|\, {\scriptstyle d} \\ \mathbb{Q} \end{array}$$

By the transitivity of the discriminant in towers of extensions, one has

$$\mathfrak{D}_{K_f/K} = \mathfrak{D}_{K(\alpha)/K}^{(n-1)!} N_{K(\alpha)/K}(\mathfrak{D}_{K_f/K(\alpha)}).$$

As above, $d_f \mathcal{O}_K = \alpha_f^2 \cdot \mathfrak{D}_{K(\alpha)/K}$ with $\alpha_f \in \mathcal{O}_K$. It turns out that

$$N_{K/\mathbb{Q}} d_f = a_f^2 (N_{K/\mathbb{Q}} \mathfrak{D}_{K_f/K})^{1/(n-1)!} (N_{K/\mathbb{Q}}(N_{K(\alpha)/K} \mathfrak{D}_{K_f/K(\alpha)}))^{1/(n-1)!} \tag{16}$$

where $a_f = N_{K/\mathbb{Q}} \alpha_f \in \mathbb{Z}$

As in Proposition 6.4 of [ABZ], we see that the probability that a monic, irreducible, degree n polynomial with height $\leq N$ has discriminant coprime with $\wp \in \mathcal{O}_K$ is $1 - \frac{1}{q_\wp}$, hence

$$\frac{|\{f \in \mathscr{P}_{n,N}^{\text{irr}} : \wp | d_f \mathcal{O}_K\}|}{|\mathscr{P}_{n,N}^{\text{irr}}|} \underset{N \to +\infty}{\longrightarrow} \frac{1}{q_\wp}.$$

Corollary 3.1. *The average of the number of ramified primes in K_f/K is*

$$\mathbb{E}_N(\wp \in \mathcal{O}_K : \wp | \mathfrak{D}_{K_f/K}) \ll_{n,K} \log\log N,$$

as $N \to +\infty$.

Proof. Since almost all polynomials in $\mathscr{P}_{n,N}$ are irreducible, with error term $O(N^{-d})$, and since $|\mathscr{P}_{n,N}^0| = (2N)^{nd} + O(N^{d(n-\xi)})$, we also have that

$$\frac{|\{f \in \mathscr{P}_{n,N}^0 : \wp | d_f \mathcal{O}_K\}|}{|\mathscr{P}_{n,N}^0|} = \frac{1}{q_\wp} + o(1)$$

as $N \to +\infty$. In particular, for the primes of norm $q_\wp < N^{d\xi/n}$, we can also write down explicitely the error term by applying Lemma 2.1:

$$\begin{aligned} \mathbb{P}_N(f \in \mathscr{P}_{n,N}^0 : \wp | d_f \mathcal{O}_K) &= \frac{1}{|\mathscr{P}_{n,N}^0|} \sum_{\substack{g \in \mathbb{F}_{q_\wp}[X] \\ \text{monic, } \deg g = n \\ g \text{ double root}}} \sum_{\substack{f \in \mathscr{P}_{n,N}^0 \\ f \equiv g \bmod \wp}} 1 \\ &= q_\wp^{n-1} \Big(\frac{1}{q_\wp^n} + O(N^{-d\xi}) \Big) \\ &= \frac{1}{q_\wp} + O(q_\wp^{n-1} N^{-d\xi}) \end{aligned}$$

as $N \to +\infty$, as long as $q_\wp < N^{d\xi/n}$. It follows that

$$\begin{aligned} \mathbb{E}_N(\wp \in \mathcal{O}_K : \wp | d_f \mathcal{O}_K) &= \sum_{q_\wp < N^{d\xi/n}} \frac{1}{|\mathscr{P}_{n,N}^0|} \sum_{\substack{f \in \mathscr{P}_{n,N}^0 \\ \wp | d_f \mathcal{O}_K}} 1 + O\Big(\frac{1}{|\mathscr{P}_{n,N}^0|} \sum_{f \in \mathscr{P}_{n,N}^0} \sum_{\substack{q_\wp \geq N^{d\xi/n} \\ \wp | d_f \mathcal{O}_K}} 1 \Big) \\ &= \log\log N + O_{n,K}(1), \end{aligned}$$

as $N \to +\infty$.

Recall that in $\mathcal{O}_K$, an ideal $\mathfrak{a}$ is divisible by a prime factor of $p\mathcal{O}_K$ if and only if $N_{K/\mathbb{Q}}\mathfrak{a}$ is divisible by p. From the transitive relation (16), one has the claim. $\square$

Let $\theta = \theta_1$ be a root of f, and let $K_1 = K(\theta)$.
For a prime $\wp \in \mathcal{O}_{K_1}$, the ring $\mathcal{O}_{K_1}[\theta]$ is called **$\wp$-maximal** if $\wp$ is not a divisor of α_{f_θ}. In particular $\mathcal{O}_{K_1}[\theta]$ is not $\wp$-maximal if and only if $\wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}$.
There is an equivalent condition for $\mathcal{O}_{K_1}[\theta]$ to be $\wp$-maximal.

Theorem 3.1 ([ABZ], Corollary 3.2). *The ring $\mathcal{O}_{K_1}[\theta]$ is not $\wp$-maximal if and only if there exists $u \in \mathcal{O}_{K_1}[X]$, with $u \mod \wp$ irreducible, such that $f \in \wp^2 + u\wp + u^2\mathcal{O}_{K_1}$ in $\mathcal{O}_{K_1}[X]$.*

In particular, the $\wp$-maximality depends just on $f \mod \wp^2$. The probability that such a polynomial modulo $\wp^2$ is in the above ideal (for a fixed u) is given by the following.

Theorem 3.2 ([ABZ], Proposition 3.4). *Let $g \in \mathbb{F}_{q_\wp}[X]$ monic, of degree m; then*

$$\frac{1}{q_\wp^{2n}} \sum_{\substack{f \in (\mathcal{O}_{K_1}/\wp^2)[X] \\ monic,\ \deg f = n \\ f \in g\wp + g^2\mathcal{O}_{K_1}}} 1 = \begin{cases} 0 & if\ 2m > n \\ \frac{1}{q_\wp^{3m}} & if\ 2m \le n. \end{cases}$$

Corollary 3.2. *In the above notations, the average of the number of primes dividing α_f is*

$$\mathbb{E}_N(\wp \in \mathcal{O}_K : \wp | \alpha_f) \ll_{n,K} 1,$$

as $N \to +\infty$.

Proof. From Theorems 3.1 and 3.2, we deduce that if $g \in \mathbb{F}_{q_\wp}[X]$ is monic, of degree $m \le n/2$, then

$$\begin{aligned}
\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \in \wp^2 + g\wp + g^2\mathcal{O}_{K_1}}} 1 &= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{h \bmod \wp^2 \\ \text{monic},\ \deg h = n \\ h \in g\wp + g^2\mathcal{O}_{K_1}}} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \equiv h \bmod \wp}} 1 \\
&= \sum_{\substack{h \bmod \wp^2 \\ \text{monic},\ \deg h = n \\ h \in g\wp + g^2\mathcal{O}_{K_1}}} \left(\frac{1}{q_\wp^{2n}} + O(N^{-d\xi}) \right) \\
&= \frac{1}{q_\wp^{3m}} + O(q_\wp^{2n-3m} N^{-d\xi}),
\end{aligned}$$

for all primes of norm $q_\wp < N^{d\xi/2n}$.

The next step is to compute the probability $\mathbb{P}_N(f \in \mathscr{P}^0_{n,N} : \wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1})$, which is, by the above

$$\begin{aligned}
&\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{m \le n/2} \sum_{\substack{g \in \mathbb{F}_{q_\wp}[X] \\ \text{monic, irreducible} \\ \deg g = m}} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \in \wp^2 + g\wp + g^2 \mathcal{O}_{K_1}}} 1 \\
&= \sum_{m \le n/2} \sum_{\substack{g \in \mathbb{F}_{q_\wp}[X] \\ \text{monic, irreducible} \\ \deg g = m}} \Big(\frac{1}{q_\wp^{3m}} + O(q_\wp^{2n-3m} N^{-d\xi}) \Big) \\
&= \sum_{m \le n/2} \Big(\frac{q_\wp^m}{m} + O\Big(\frac{q_\wp^{m-1}}{m}\Big)\Big)\Big(\frac{1}{q_\wp^{3m}} + O(q_\wp^{2n-3m} N^{-d\xi})\Big) \\
&= \sum_{m \le n/2} \Big(\frac{1}{m q_\wp^{2m}} + O\Big(\frac{q_\wp^{2n}}{m q_\wp^{2m}} N^{-d\xi} + \frac{1}{m q_\wp^{2m+1}} \Big)\Big) \\
&= \frac{1}{q_\wp^2} + O\Big(q_\wp^{2n-2} N^{-d\xi} + \frac{1}{q_\wp^3} \Big),
\end{aligned}$$

as $N \to +\infty$, for $q_\wp < N^{d\xi/2n}$. Then, the number of primes (on average) diving $d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}$ is

$$\begin{aligned}
&\mathbb{E}_N(|\{\wp : \wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}\}|) \\
&= \sum_{q_\wp < N^{d\xi/2n}} \mathbb{P}_N(f : \wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}) + \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \ge N^{d\xi/2n} \\ \wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}}} 1 \\
&= \sum_{q_\wp < N^{d\xi/2n}} \frac{1}{q_\wp^2} + O(1 + \pi_K(N^{d\xi/2n})^{2n-1} N^{d\xi}) \\
&\ll_{n,K} 1,
\end{aligned}$$

since

$$\sum_{\substack{q_\wp \ge N^{d\xi/2n} \\ \wp | d_f \mathcal{O}_K(\mathfrak{D}_{K_1/K})^{-1}}} 1 \ll_{n,K} \frac{\log N}{\log(N^{d\xi})} \ll_{n,K} 1.$$

□

3.2 Upper bounds for the torsion part of the class number

All these bounds represent evidence towards the so-called ε-conjecture.

Conjecture 3.1. *Let $K/\mathbb{Q}$ be a number field of degree s with discriminant D_K. Then for every integer $\ell \ge 1$ and every $\varepsilon > 0$,*

$$h_K[\ell] \ll_{s,\ell,\varepsilon} D_K^\varepsilon,$$

where $h_K[\ell]$ is the order of the ℓ-torsion subgroup of the class group.

Using the well-known Minkowski bound

$$h_K \leq \frac{s!}{s^s}\frac{4^{r_2}}{\pi^{r_2}} D_K^{1/2} (\log D_K)^{s-1},$$

where r_2 is the number of real $\mathbb{Q}$-embeddings of K, one has

$$h_K \ll_{s,\varepsilon} D_K^{1/2+\varepsilon}$$

for any $\varepsilon > 0$. We can of course use the above to bound the ℓ-part $h_K[\ell]$ of h_K. But we'd like to improve the above estimate, and the main point we're going to use is the existence of "many" splitting completely primes, which contributes significantly to the quotient of the class group by its ℓ-torsion. We state this precisely in Theorem 3.3 below. The GRH guarantees the existence of such primes, but here, we'd like to proceed unconditionally.

Let $K/\mathbb{Q}$ be a number field. Again, the presence of "small" primes that split completely in K, give a means to improve the Minkowski upper bound, using the following theorem ([EV], Lemma 2.3).

Theorem 3.3 (Ellenberg, Venkatesh)**.** *Let $K/\mathbb{Q}$ be a field extension of degree s. Set $\delta < \frac{1}{2\ell(s-1)}$ and suppose that*

$$|\{p \leq D_K^{\delta} : p \text{ splits completely in } K/\mathbb{Q}\}| \geq M.$$

Then, for any $\varepsilon > 0$

$$h_K[\ell] \ll_{s,\ell,\varepsilon} D_K^{1/2+\varepsilon} M^{-1}.$$

Let L/K be a number field extension of degree s, where $K/\mathbb{Q}$ is the degree d field fixed at the beginning of our discussion.

$$\begin{tikzcd} L \arrow[d, dash, "s"] & \\ K \arrow[d, dash, "d"] & \wp \arrow[d, dash] \\ \mathbb{Q} & p \end{tikzcd}$$

Thanks to Theorem 2, we are able to count

$$|\{\wp \in \mathcal{O}_K : |N_{K/\mathbb{Q}}\wp| \leq |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^{\delta},\ \wp \text{ splits completely in } L/K\}|.$$

Some of those primes correspond to the primes p splitting completely in $L/\mathbb{Q}$, such that $\wp|p$. There are exactly d primes $\wp$ for any p and $N_{K/\mathbb{Q}}\wp = p$. By the transitive relation

$$D_L = D_K^s N_{K/\mathbb{Q}}\mathfrak{D}_{L/K},$$

if $\wp | p$ as above, then $p \ll D_L^\delta$.
But in general,

$$\begin{aligned}|\{\wp \in \mathcal{O}_K : |N_{K/\mathbb{Q}}\wp| \leq |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^\delta,\ \wp \text{ splits completely in } L/K\}| \\ \geq d|\{p \ll D_L^\delta : p \text{ splits completely in } L/\mathbb{Q}\}|,\end{aligned}$$

since there are primes $\wp \in \mathcal{O}_K$ splitting completely in L/K, such that the primes p under those ramify in $L/\mathbb{Q}$. We can then write

$$\begin{aligned}|\{\wp \in \mathcal{O}_K : |N_{K/\mathbb{Q}}\wp| \leq |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^\delta,\ \wp \text{ splits completely in } L/K\}| \\ \leq d|\{p \ll D_L^\delta : p \text{ splits completely in } L/\mathbb{Q}\}| \\ + d|\{p : p \text{ ramifies in } K/\mathbb{Q} \text{ and } p\mathcal{O}_K \text{ splits completely in } L/K\}|,\end{aligned}$$

which is

$$\ll_K |\{p \ll D_L^\delta : p \text{ splits completely in } L/\mathbb{Q}\}| + |\{p : p \text{ ramifies in } L/\mathbb{Q}\}|.$$

In Corollary 3.1, we computed an upper bound on the average of the ramified primes in the case $L = K_f$. It turns out that if

$$|\{\wp \in \mathcal{O}_K : |N_{K/\mathbb{Q}}\wp| \leq |N_{K/\mathbb{Q}}\mathfrak{D}_{L/K}|^\delta,\ \wp \text{ splits completely in } L/K\}| \geq M,$$

then on average

$$|\{p \ll D_L^\delta : p \text{ splits completely in } L/\mathbb{Q}\}| \gg_{n,K} M - \log\log N.$$

Corollary 3.3. *For every positive integer ℓ, $\varepsilon > 0$ and for almost all $f \in \mathscr{P}^0_{n,N}$, outside of a set of size $o(N^{dn})$, we have*

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon} D_f^{\frac{1}{2} - \frac{1}{d(2n-2)(n-1)!\log\log|N_{K/\mathbb{Q}}d_f|} + \varepsilon},$$

as $N \to +\infty$.

In order to prove Corollary 3.3, we need the following lemma.

Lemma 3.1. *The density of the set of $f \in \mathscr{P}^0_{n,N}$ so that $N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K} \ll N^{1/\log\log N}$ is zero, as $N \to +\infty$.*

Proof. By using the notations of Theorem 1.3, we have that

$$\sum_{\substack{f\in\mathscr{P}^0_{n,N}\\ N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}\ll N^{1/\log\log N}}} 1$$

$$\ll \sum_{L\in\mathscr{F}_n(N^{1/\log\log N},S_n)}\ \sum_{\substack{f\in\mathscr{P}^0_{n,N}\\ K_f\cong L}} 1$$

$$\ll \sum_{L\in\mathscr{F}_n(N^{1/\log\log N},S_n)}\ \sum_{\substack{\alpha\in\mathcal{O}_L\\ K(\alpha)\cong L\\ H_K(\alpha)\ll N^{1/n}}} 1$$

$$\ll N^{d\left(1+\frac{n+2}{4d\log\log N}\right)+\varepsilon},$$

for every $\varepsilon>0$, by using Schmidt bound [Sc] for the number of field extensions with bounded discriminant. □

Proof. (Corollary 3.3) By Theorem 2, for $x=N^{1/\log\log N}$, r a (square free) splitting type, and $\alpha=\alpha(N)>0$ for large N,

$$\mathbb{P}_N\left(-N^{1/\alpha}\leq\frac{\pi_{f,r}(x)-\delta(r)\pi_K(x)}{(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}}1\leq N^{1/\alpha}\right)\underset{N\to+\infty}{\longrightarrow}1.$$

In particular,

$$\pi_{f,r}(x)\geq\delta(r)\pi_K(x)-N^{1/\alpha}(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}$$

for all but $o(N^{dn})$ f's in $\mathscr{P}^0_{n,N}$. Pick $\alpha=3\log\log N$; then $N^{1/\alpha}\pi_K(x)^{1/2}\ll_r\pi_K(x)$. By enlarging N, we can assume that

$$N^{1/\alpha}(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}\ll_r\frac{1}{2}\delta(r)\pi_K(x).$$

Then we get

$$\pi_{f,r}(x)\gg\delta(r)\pi_K(x).$$

For $\mathscr{C}_r=\{\mathrm{id}\}$, since $N_{K/\mathbb{Q}}d_f\asymp N^{d(2n-2)}$ for almost all f, and by the relation $N_{K/\mathbb{Q}}d_f=(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{1/(n-1)!}a_f^2(N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}))^{1/(n-1)!}$, we are bounding below the primes of norm

$$\begin{aligned}
q_\wp &\ll N^{1/\log\log N}\ll_{n,K}(N_{K/\mathbb{Q}}d_f^{1/d(2n-2)})^{1/\log\log|N_{K/\mathbb{Q}}d_f|}\\
&=\left((N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{1/d(2n-2)(n-1)!}a_f^{1/d(n-1)}(N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}))^{1/d(2n-2)(n-1)!}\right)^{1/\log\log|N_{K/\mathbb{Q}}d_f|}\\
&=\left((N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{d(2n-2)(n-1)!}+\frac{\log a_f}{d(n-1)\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}+\frac{\log|N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})|}{d(2n-2)(n-1)!\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}}\right)^{1/\log\log|N_{K/\mathbb{Q}}d_f|}
\end{aligned}$$

splitting completely in K_f/K. Now, for almost all f, the discriminant satisfies $\log\log|N_{K/\mathbb{Q}}d_f| \gg_K \frac{\ell}{d}\frac{n!-1}{(n-1)(n-1)!}$; moreover by (16), we have that

$$a_f \ll \frac{N^{d(n-1)}}{(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{2(n-1)!}}}$$

and

$$N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}) \ll \frac{N^{\frac{2d}{(n-2)!}}}{N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}}.$$

By Lemma 3.1, we have that for almost all f, the exponent

$$\left(\frac{1}{d(2n-2)(n-1)!} + \frac{\log a_f}{d(n-1)\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|} + \frac{\log|N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})|}{d(2n-2)(n-1)!\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}\right)$$
$$\cdot\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|} \underset{N\to+\infty}{\longrightarrow} 0.$$

In particular, we can take $\delta > 0$ so that

$$\left(\frac{1}{d(2n-2)(n-1)!} + \frac{\log a_f}{d(n-1)\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|} + \frac{\log|N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})|}{d(2n-2)(n-1)!\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}\right)$$
$$\cdot\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|} < \delta < \frac{1}{2\ell(n!-1)}.$$

It turns out that the primes $p \ll D_f^{\delta}$ splitting completely in $K_f/\mathbb{Q}$ are at least

$$\gg_{n,K,\ell} \frac{(N_{K/\mathbb{Q}}d_f)^{\frac{1}{d(2n-2)\log\log|N_{K/\mathbb{Q}}d_f|}}\log\log|N_{K/\mathbb{Q}}d_f|}{\log|N_{K/\mathbb{Q}}d_f|} - \log\log N.$$

By Theorem 3.3,

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon}$$
$$D_f^{\frac{1}{2}+\varepsilon}\log|N_{K/\mathbb{Q}}d_f|\cdot\Big(((N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})\cdot(N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})))^{\frac{1}{d(2n-2)(n-1)!\log\log|N_{K/\mathbb{Q}}d_f|}}$$
$$\cdot a_f^{\frac{1}{d(n-1)\log\log|N_{K/\mathbb{Q}}d_f|}}\log\log|N_{K/\mathbb{Q}}d_f| - \log|N_{K/\mathbb{Q}}d_f|\log\log N\Big)^{-1}.$$

Since by transitivity $D_f = D_K^{n!}N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}$, one has the claim.

□

Note. For example, in the case $K = \mathbb{Q}$, one obtains more precisely the upper bound

$$h_f[\ell] \ll_{n,\ell,\varepsilon} D_f^{\frac{1}{2}-\frac{1}{(2n-2)(n-1)!\log\log d_f}+\varepsilon} \cdot \frac{\log N}{\log\log N}$$

for any $\varepsilon > 0$, for almost all f as $N \to +\infty$.

We can improve this last bound by adding an additional hypothesis.

Theorem 3.4. *Let K be a number field of degree s. There exists $\theta \in \mathcal{O}_K - \mathbb{Z}$ whose minimal polynomial f_θ has height*

$$\mathrm{ht}(f_\theta) \leq 3^s \Big(\frac{D_K}{s}\Big)^{\frac{s}{2s-2}}.$$

Proof. See [GJ], Appendix A. $\square$

Corollary 3.4. *Assume that K_f is generated over K by an element θ of small height of Theorem 3.4. Then for every positive integer ℓ, $\varepsilon > 0$ and for almost all $f \in \mathscr{P}^0_{n,N}$ outside of a set of size $o(N^{dn})$ we have*

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon} D_f^{\frac{1}{2}-\frac{n!+d}{n!(2n-2)(n-1)!}\cdot\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|}+\varepsilon},$$

as $N \to +\infty$.

Proof. In particular we have $\mathrm{ht}(f_\theta) \ll_n D_f^{\frac{n!}{2n!-2}}$ and so

$$N_{K/\mathbb{Q}}d_{f_\theta} = a'^2_{f_\theta} N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K} \asymp D_f^{n!d} = D_K^{n!^2 d}(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{n!d}$$

with high probability. Since $N_{K/\mathbb{Q}}d_f \asymp N^{d(2n-2)}$ for almost all f and

$$N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K} = \frac{(N_{K/\mathbb{Q}}d_f)^{(n-1)!}}{c_f^2 N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})} \asymp \frac{N^{d(2n-2)(n-1)!}}{c_f^2 N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})}$$

for almost all f (here $c_f = a_f^{(n-1)!}$), we obtain

$$N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K} \asymp \frac{N^{n!(2n-2)(n-1)!}D_K^{n!^2 d}}{a'^2_{f_\theta}(c_f^2 N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}))^{n!d}}.$$

It turns out that

$$N \asymp C_n(f,\theta,K)\cdot(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{n!(2n-2)(n-1)!}}$$

for almost all $f \in \mathscr{P}^0_{n,N}$. We denoted by

$$C_n(f,\theta,K) = \frac{(a'^2_{f_\theta}(c_f^2 N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)})^{n!d}))^{\frac{1}{n!(2n-2)(n-1)!}}}{D_K^{\frac{n!d}{(2n-2)(n-1)!}}}.$$

As in Corollary 3.3 we want to count the primes of norm

$$\begin{aligned} q_\wp &\ll_n N^{1/\log\log N} \\ &\ll \left(C_n(f,\theta,K)\cdot(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{n!(2n-2)(n-1)!}}\right)^{1/\log\log|N_{K/\mathbb{Q}}d_f|} \\ &= \left((N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{n!(2n-2)(n-1)!}+\frac{\log C_n(f,\theta,K)}{\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}}\right)^{1/\log\log|N_{K/\mathbb{Q}}d_f|} \end{aligned}$$

splitting completely in K_f/K.
By the above we get

$$\frac{\log C_n(f,\theta,K)}{\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}\cdot\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|}\asymp_{n,K}\frac{\log N}{\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}\cdot\frac{1}{\log\log N},$$

which tends to zero as $N\to+\infty$ for almost all f, by Lemma 3.1.

We can then fix a $\delta>0$ so that

$$\left(\frac{1}{n!(2n-2)(n-1)!}+\frac{\log C_n(f,\theta,K)}{\log|N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K}|}\right)\cdot\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|}<\delta<\frac{1}{2\ell(n!-1)}$$

(by enlarging the norm of d_f if necessary). Therefore the number of primes $p\ll D_f^\delta$ splitting completely in $K_f/\mathbb{Q}$ is bounded below by

$$\gg_{n,K,\ell}\frac{\left(C_n(f,\theta,K)\cdot(N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\frac{1}{n!(2n-2)(n-1)!}}\right)^{1/\log\log|N_{K/\mathbb{Q}}d_f|}\log\log N}{\log N}-\log\log N$$

Note that

$$C_n(f,\theta,K)\gg\frac{(N_{K/\mathbb{Q}}(N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}))^{\frac{1}{d(2n-2)(n-1)!}}}{D_K^{\frac{nd}{2n-2}}}.$$

By the transitive relation

$$\mathfrak{D}_{K_f/K}=\mathfrak{D}_{K(\alpha)/K}^{(n-1)!}N_{K(\alpha)/K}\mathfrak{D}_{K_f/K(\alpha)}$$

and

$$N_{K/\mathbb{Q}}\mathfrak{D}_{K(\alpha)/K}=\frac{N_{K/\mathbb{Q}}d_f}{a_f^2},$$

one has that the number of primes $p\ll D_f^\delta$ splitting completely in $K_f/\mathbb{Q}$ is

$$\begin{aligned} &\gg\Big((N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K})^{\left(\frac{1}{n!(2n-2)(n-1)!}+\frac{1}{d(2n-2)(n-1)!}\right)\frac{1}{\log\log|N_{K/\mathbb{Q}}d_f|}}a_f^{\frac{1}{d(n-1)\log\log|N_{K/\mathbb{Q}}d_f|}}\log\log N \\ &\quad-(N_{K/\mathbb{Q}}d_f)^{\frac{1}{d(2n-2)\log\log|N_{K/\mathbb{Q}}d_f|}}D_K^{\frac{nd}{2n-2\log\log|N_{K/\mathbb{Q}}d_f|}}\log N\log\log N\Big) \\ &\qquad\cdot\left((N_{K/\mathbb{Q}}d_f)^{\frac{1}{d(2n-2)\log\log|N_{K/\mathbb{Q}}d_f|}}D_K^{\frac{nd}{2n-2\log\log|N_{K/\mathbb{Q}}d_f|}}\log N\right)^{-1} \end{aligned}$$

By Theorem 3.3 and the transitivity of the discriminant

$$N_{K/\mathbb{Q}}\mathfrak{D}_{K_f/K} = \frac{D_f}{D_K^{n!}}$$

one gets the desired upper bound for $h_f[\ell]$ for almost all f. $\square$

3.3 Results for subfamilies

Consider a family $\mathscr{A} \subseteq \mathscr{A}_{\beta,M}(N) \subseteq \mathscr{P}^0_{n,N}$ satisfying conditions 1, 2, 3 of Section 2.3 with $\mathscr{C}_r = \{\mathrm{id}\}$.
By using the method of moments, and from Proposition 2.3, the same proof of Theorem 2 leads to

$$\frac{1}{|\mathscr{A}|}\left|\left\{f \in \mathscr{A} : a \leq \frac{\pi_{f,r}(x) - \mu(x)}{(\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2}} \leq b\right\}\right| \underset{N\to+\infty}{\longrightarrow} \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt,$$

where $x = N^{1/\log\log N}$ and $a, b \in \mathbb{R}$.
In particular, as in Corollary 3.3, we have that

$$\pi_{f,r}(x) \geq \mu(x) - N^{1/3\log\log N}(\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2}$$

for all $f \in \mathscr{A}$ outside of a set of size $o(N^{d\beta})$. For N large enough, one gets

$$\pi_{f,r}(x) \gg_{n,K} \delta(r)\pi_K(x),$$

for almost all $f \in \mathscr{A}$.
In many examples, one has that for $f \in \mathscr{A}$, the discriminant satisfies $N_{K/\mathbb{Q}}d_f \asymp N^{d\alpha(n)}$ with $0 < \alpha(n) < 2n-2$.
Let $0 < \delta < \frac{1}{2\ell(n!-1)}$. The same computation as in the proof of Corollary 3.3, togheter with Theorem 3.3, yields to

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon} D_f^{\frac{1}{2} - \frac{1}{d\alpha(n)(n-1)!\log\log|N_{K/\mathbb{Q}}d_f|} + \varepsilon},$$

for every $\varepsilon > 0$, as $N \to +\infty$, for almost all $f \in \mathscr{A}$.

3.3.1 Explicit examples

3.3.2 Families of trinomials

Let $n \geq 2$, $0 \leq t < n$ and let $\mathscr{B}$ be the following family of polynomials over $\mathcal{O}_K$:

$$\mathscr{B} = \{f(X) = X^n + aX^t + b : \mathrm{ht}(a), \mathrm{ht}(b) \leq N\}.$$

Now, the polynomial $F(X,Y,Z) = X^n + YX^t + Z$ in three variables is irreducible over $K[X,Y,Z]$. We can then apply Hilbert's Irreduciblity Theorem.

One of the latest effective versions can be found in [PS], Theorem 1.3. It leads to

$$|\{a, b \in \mathcal{O}_K : \mathrm{ht}(a), \mathrm{ht}(b) \leq N,\ G_{F(X,a,b)} \ncong S_n\}| \ll_{n,K} N^{1/2}.$$

Hence the subfamily $\mathscr{A} = \mathscr{B} \cap \mathscr{P}^0_{n,N}$ satisfies

$$|\mathscr{A}| = 4N^2 + O(N^{1/2}),$$

as $N \to +\infty$. By elementary computations, we can see that if $\wp$ is a prime ideal of $\mathcal{O}_K$ of norm $q_\wp \leq x$, where $x < N^{1/2}$, and $g \in \mathscr{A}^\wp$, then

$$\sum_{\substack{f \in \mathscr{A} \\ f \equiv g \bmod \wp}} 1 = \frac{4N^2}{q_\wp^2} + O(N).$$

The family $\mathscr{A}$ therefore satisfies conditions 1, 2 and 3 of 2.3, with $\beta = 2$, $M = 4$, $E_{n,K}(N) = N$. For a splitting type r, we can apply the RH over finite fields to get

$$|X^{\mathscr{A}}_{n,r,p}| = \delta(r)p^2 + O(p^{3/2}).$$

The discriminant of a trinomial f as in $\mathscr{A}$ is given by

$$d_f = (-1)^{\frac{n(n-1)}{2}} b^{t-1}(n^{n/d'} b^{\frac{n-t}{d'}} - (-1)^{n/d'}(n-t)^{\frac{n-t}{d'}} t^{t/d'} a^{n/d'})^{d'} \asymp_{n,K} N^{d(n+t-1)},$$

where $d' = (n,t)$. We can then upper bound the ℓ-torsion of the class number as follows:

$$h_f[\ell] \ll_{n,K,\ell,\varepsilon} D_f^{\frac{1}{2} - \frac{1}{d(n+t-1)(n-1)! \log\log N} + \varepsilon},$$

for every $\varepsilon > 0$, as $N \to +\infty$, for almost all $f \in \mathscr{A}$.

Subcase

A more explicit example is given by the family of irreducible polynomials over $\mathbb{Q}$:

$$\mathscr{A} = \{f(X) = X^n + aX + b : f \text{ irreducible}, |a|, |b| \leq N,\ ((n-1)a, nb) = 1\}.$$

Osada in [Os] proved that these polynomials are indeed S_n-polynomials. We start by counting them. As above, by an Hilbert's Irreducibility Theorem argument, almost all polynomials of the form $X^n + aX + b$ are irreducible over $\mathbb{Q}$, with an exceptional set of size $\ll_n N^{1/2}$. In other words,

$$|\mathscr{A}| = \sum_{\substack{|a|,|b| \leq N \\ ((n-1)a, nb) = 1}} 1 + O(N^{1/2}).$$

To treat the sum, we use the Möbius function to handle the coprimality condition. In general, let $r \le s$ with $(r,s)=1$; one has

$$\begin{aligned}\sum_{\substack{|a|,|b|\le N\\(ra,sb)=1}} 1 &= \sum_{|a|,|b|\le N}\sum_{\substack{d|sb\\d|ra}}\mu(d)\\ &= \sum_{d\le rN}\mu(d)\sum_{\substack{|a|\le N\\d|ra}}\sum_{\substack{|b|\le N\\d|sb}}1.\end{aligned}$$

Now, if $d|s$, the last sum on the RHS is $2N+O(1)$. Denote by

$$[d|s] = \begin{cases}1 & \text{if } d|s\\ 0 & \text{otherwise;}\end{cases}$$

Analogously, $[d\nmid s] = 1-[d|s]$. It turns out that the above sum is

$$\begin{aligned}&\sum_{d\le rN}\mu(d)\sum_{\substack{|a|\le N\\d|ra}}\Big([d|s](2N+O(1))+[d\nmid s]\sum_{\substack{\ell|d\\\ell|s}}\sum_{\substack{|b|\le N\\\frac{d}{\ell}|b}}1\Big)\\ &=\sum_{d\le rN}\mu(d)\sum_{\substack{|a|\le N\\d|ra}}\left([d|s](2N+O(1))+[d\nmid s]\left(\frac{2N}{d}\sigma((s,d))+O(\tau((s,d)))\right)\right),\end{aligned}$$

where $\sigma(c)=\sum_{\ell|c}\ell$, and τ is the counting-divisors function. The above is

$$\begin{aligned}&4N^2\sum_{d\le rN}\mu(d)\left([d|s]+[d\nmid s]\frac{\sigma((s,d))}{d}\right)\left([d|r]+[d\nmid r]\frac{\sigma((r,d))}{d}\right)+O(N)\\ &=4N^2\Big(\sum_{\substack{d\le rN\\d|(s,r)}}\mu(d)+\sum_{\substack{d\le rN\\d|s,d\nmid r}}\frac{\mu(d)}{d}\sigma((r,d))+\sum_{\substack{d\le rN\\d|r,d\nmid s}}\frac{\mu(d)}{d}\sigma((s,d))+\sum_{\substack{d\le rN\\d\nmid s,d\nmid r}}\frac{\mu(d)}{d^2}\sigma((r,d))\sigma((s,d))\Big)\\ &\qquad+O(N)\\ &\qquad\qquad=4C_nN^2+O(N),\end{aligned}$$

where

$$C_n=\prod_{p|s}\left(1-\frac{1}{p}\right)+\prod_{p|r}\left(1-\frac{1}{p}\right)+\sum_{d\ge1}\frac{\mu(d)}{d^2}\sum_{\ell|s,\ell|d}\ell\sum_{k|r,k|d}k-\sum_{d|r}\frac{\mu(d)}{d^2}\sum_{\ell|d}\ell-\sum_{d|s}\frac{\mu(d)}{d^2}\sum_{\ell|d}\ell.$$

The analogous computations yield, for a prime $p<N^{1/2}$, $g\in\mathscr{A}^p$,

$$\sum_{\substack{f\in\mathscr{A}\\f\equiv g \bmod p}}1=\frac{4C_nN^2}{p^2}+O(N).$$

Hence $\mathscr{A} = \mathscr{A}_{2,4N^2}(N)$ satisfies

$$h_f[\ell] \ll_{n,\ell,\varepsilon} D_f^{\frac{1}{2}-\frac{1}{n(n-1)!\log\log N}+\varepsilon},$$

for every $\varepsilon > 0$, as $N \to +\infty$, for almost all $f \in \mathscr{A}$.

3.4 The Cilleruelo's conjecture on average

For $f \in \mathbb{Z}[X]$ an irreducible polynomial of degree n, the Cilleruelo's conjecture states

$$\log(\operatorname{lcm}(f(1), \ldots, f(M))) \sim (n-1)M \log M$$

as $M \to +\infty$, where $\operatorname{lcm}(f(1), \ldots, f(M))$ is the least common multiple of $f(1), \ldots, f(M)$. It's well-know for $n = 1$ as a consequence of the Dirichlet's theorem for primes in arithmetic progression, and it was proved by Cilleruelo in [Cil] for degree-2 polynomials. Recently the conjecture was shown for a large family of polynomials of any degree (see [RZ]). We want to investigate the case of polynomials in $\mathscr{P}^0_{n,N}(K)$ by considering the leatest common multiple of ideals of $\mathcal{O}_K$.

Proposition 3.1. *Let $N, M > 0$ such that*

$$M(\log M)^\ell \ll N = o\left(M \frac{\log M}{\log\log M}\right)$$

for some $0 < \ell < 1$. Then

$$\mathbb{E}_N(\log |N_{K/\mathbb{Q}}(\operatorname{lcm}(f(\lambda) : \lambda \in \mathcal{O}_K,\ N_{K/\mathbb{Q}}\lambda \le M)|) = (n-1)M \log M + O\left(M \frac{\log M}{\log\log M} + N \log\log M\right),$$

as $N, M \to +\infty$.

Proof. Following [Cil], we compare the behaviour of

$$\operatorname{lcm}(f(\lambda) : N_{K/\mathbb{Q}}\lambda \le M) = \prod_{\wp \in \mathcal{P}_f} \wp^{\beta_\wp(M)}$$

and

$$P_f(M) := \prod_{N_{K/\mathbb{Q}}\lambda \le M} |N_{K/\mathbb{Q}} f(\lambda)| = \prod_{\wp} |N_{K/\mathbb{Q}}\wp|^{\alpha_\wp(M)},$$

where P_f is the set of primes such that the equation $f \equiv 0 \mod \wp$ has some solutions, which is the set of $\wp$ so that $\mathrm{Frob}_{f,\wp} \in G_f$ has fixed points. We start by writing

$$\begin{aligned}
\log(\mathrm{lcm}(f(\lambda) : N_{K/\mathbb{Q}}\lambda \leq M)) = \log P_f(M) + &\sum_{N_{K/\mathbb{Q}}\wp \leq M} \beta_\wp(M) \log N_{K/\mathbb{Q}}\wp \\
&- \sum_{\substack{N_{K/\mathbb{Q}}\wp \leq M \\ \wp \text{ unramified}}} \alpha_\wp(M) \log N_{K/\mathbb{Q}}\wp \\
&- \sum_{\substack{N_{K/\mathbb{Q}}\wp \leq M \\ \wp \text{ ramified}}} \alpha_\wp(M) \log N_{K/\mathbb{Q}}\wp \\
&- \sum_{N_{K/\mathbb{Q}}\wp > M} (\alpha_\wp(M) - \beta_\wp(M)) \log N_{K/\mathbb{Q}}\wp
\end{aligned}$$

and we're going to study all these five terms.

- $\log P_f(M) = \sum_{N_{K/\mathbb{Q}}\lambda \leq M} \log |N_{K/\mathbb{Q}} f(\lambda)|$; Pick $A = A(M, N)$ such that $A = o(M)$ and $A \gg \frac{N}{\log M}$. Then for $A \ll N_{K/\mathbb{Q}}\lambda \leq M$ and $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ one has

$$\begin{aligned}
\log |N_{K/\mathbb{Q}} f(\lambda)| &= n \log |N_{K/\mathbb{Q}}\lambda| + \log \left| N_{K/\mathbb{Q}} \left(1 + \frac{\alpha_{n-1}}{\lambda} + \cdots + \frac{\alpha_0}{\lambda^n} \right) \right| \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + \log \left| \prod_{i=1}^{d} \sigma_i \left(1 + \frac{\alpha_{n-1}}{\lambda} + \ldots \right) \right| \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + \log \prod_{i=1}^{d} \left| 1 + \sigma_i \left(\frac{\alpha_{n-1}}{\lambda} + \ldots \right) \right| \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + \sum_{i=1}^{d} \log \left(\left| 1 + \sigma_i \left(\frac{\alpha_{n-1}}{\lambda} + \ldots \right) \right| \right) \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + \sum_{i=1}^{d} O \left(\sigma_i \left(\frac{\alpha_{n-1}}{\lambda} \right) + \cdots + \sigma_i \left(\frac{\alpha_0}{\lambda^n} \right) \right) \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + \sum_{i=1}^{d} O \left(\frac{N}{N_{K/\mathbb{Q}}\lambda} + \cdots + \frac{N}{N_{K/\mathbb{Q}}\lambda^n} \right) \\
&= n \log |N_{K/\mathbb{Q}}\lambda| + O_{n,K} \left(\frac{N}{A} \right),
\end{aligned}$$

where $\sigma_1, \ldots, \sigma_d$ are the $\mathbb{Q}$-embeddings of K into $\mathbb{C}$.

If $1 \leq N_{K/\mathbb{Q}}\lambda \ll A$, we simply use that $|N_{K/\mathbb{Q}} f(\lambda)| \ll N^d M^n$, so $\log |N_{K/\mathbb{Q}} f(\lambda)| \ll_{n,d} \log N + \log M$. Therefore, since the elements in $\mathcal{O}_K$

of norm at most M are at most M,

$$\begin{aligned}\log P_f(M) &= \sum_{A\ll N_{K/\mathbb{Q}}\lambda\le M}\log|N_{K/\mathbb{Q}}f(\lambda)| + \sum_{N_{K/\mathbb{Q}}\lambda\ll A}\log|N_{K/\mathbb{Q}}f(\lambda)|\\
&= \sum_{A\ll N_{K/\mathbb{Q}}\lambda\le M}\left(n\log N_{K/\mathbb{Q}}\lambda + O\left(\frac{N}{A}\right)\right) + \sum_{N_{K/\mathbb{Q}}\lambda\ll A}\log|N_{K/\mathbb{Q}}f(\lambda)|\\
&= nM\log M + O\left(M + \frac{NM}{A} + A(\log N+\log M)\right)\\
&= nM\log M + O\left(M\frac{\log M}{\log\log M} + N\log\log M\right),\end{aligned}$$

as $M\to+\infty$, by choosing $A=\frac{N}{\log M}\log\log M$ and $N = o\left(M\frac{\log M}{\log\log M}\right)$.

- $\beta_\wp(N) = \max_{N_{K/\mathbb{Q}}\lambda\le M}\max\{k\ge 0 : \wp^k|f(\lambda)\}$; if $\wp^k|f(\lambda)$, then in particular $k\le\frac{\log|N_{K/\mathbb{Q}}f(\lambda)|}{\log q_\wp}\ll\frac{\log N+\log M}{\log q_\wp}$. Thus

$$\begin{aligned}\sum_{q_\wp\le M}\beta_\wp(M)\log q_\wp &\ll \sum_{q_\wp\le M}(\log N+\log M)\\
&\ll M\Big(1+\frac{\log N}{\log M}\Big)\ll M\end{aligned}$$

under the conditions above.

- If $\wp$ is a prime which doesn't divide $\mathfrak{D}_{K_f/K}$, then the number of solutions $s_{\wp^k}(f)$ of $f \mod \wp^k$ is equal to the number $s_\wp(f)$ of solutions mod $\wp$ (see Theorem 1 of [Na]). On the other hand, by dividing the interval $[1,M]$ into consecutive intervals of length $q_\wp^k$, one has

$$s_{\wp^k}(f)\Big[\frac{M}{q_\wp^k}\Big]\le\sum_{\substack{N_{K/\mathbb{Q}}\lambda\le M\\ f(\lambda)\equiv 0\ (\wp^k)}}1\le s_{\wp^k}(f)\Big(\Big[\frac{M}{q_\wp^k}\Big]+1\Big),$$

so

$$\sum_{\substack{N_{K/\mathbb{Q}}\lambda\le M\\ f(\lambda)\equiv 0\ (\wp^k)}}1 = M\frac{s_{\wp^k}(f)}{q_\wp^k}+O(s_{\wp^k}(f)).$$

For those $\wp$, one has

$$\begin{aligned}\alpha_\wp(M) &= \sum_{N_{K/\mathbb{Q}}\lambda\le M}\sum_{\substack{k\ge1\\ \wp^k|f(\lambda)}}1 = \sum_{k\ge1}\sum_{\substack{N_{K/\mathbb{Q}}\lambda\le M\\ f(\lambda)\equiv 0\ (\wp^k)}}1\\
&= \sum_{k\ge1}M\frac{s_{\wp^k}(f)}{q_\wp^k}+O\Big(\sum_{1\le k\le\frac{\log N+\log M}{\log q_\wp}}1\Big)\\
&= M\frac{s_\wp(f)}{q_\wp-1}+O\Big(\frac{\log N}{\log q_\wp}+\frac{\log M}{\log q_\wp}\Big).\end{aligned}$$

Therefore

$$\sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \alpha_\wp(M) \log q_\wp = M \sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp - 1} s_\wp(f) + O(M).$$

Using Proposition 2.1 we can estimate on average $\sum_{\substack{q_\wp \le x \\ \wp \text{ unramified}}} s_\wp(f)$ for $x > 0$, $x < N^{d\xi/(n+1)}$:

$$\begin{aligned}
\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \le x \\ \wp \text{ unramified}}} s_\wp(f) &= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \le x \\ \wp \text{ unram.}}} \sum_{\substack{\alpha \bmod \wp \\ f(\alpha) \equiv 0\ (\wp)}} 1 \\
&= \sum_{\alpha \in \mathcal{O}_K} \sum_{\substack{\sigma \in G_f \\ \sigma\alpha = \alpha}} \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \le x,\ \wp \text{ unram.} \\ \mathrm{Frob}_{f,\wp} = \sigma}} 1 \\
&= \sum_{\alpha \in \mathcal{O}_K} \sum_{\substack{\sigma \in G_f \\ \sigma\alpha = \alpha}} \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \pi_{\mathscr{C}(\sigma), K_f/K}(x) \\
&= \sum_{\alpha \in \mathcal{O}_K} \sum_{\substack{\sigma \in G_f \\ \sigma\alpha = \alpha}} \mathbb{E}_N(\pi_{\mathscr{C}(\sigma), K_f/K}(x)) \\
&= \sum_{\alpha \in \mathcal{O}_K} \sum_{\substack{\sigma \in G_f \\ \sigma\alpha = \alpha}} \Big(\frac{|\mathscr{C}(\sigma)|}{n!} \pi_K(x) + O(\log\log x) \Big) \\
&= \pi_K(x) + O(\log\log x),
\end{aligned}$$

where $\pi_{\mathscr{C}(\sigma), K_f/K}$ is the Chebotarev density theorem function on the conjugacy class $\mathscr{C}(\sigma)$ of σ. Note that

$$\pi_{\mathscr{C}(\sigma), K_f/K} - \pi_{f,r}(x) \ll_{n,K} \log\log x$$

on average, if $\mathscr{C}(\sigma) = \mathscr{C}_r$ for some r. Write

$$s_\wp(f) = 1 + \sigma_\wp(f),$$

where $-1 \le \sigma_\wp(f) \le n - 1$ and

$$\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \le x \\ \wp \text{ unramified}}} \sigma_\wp(f) \ll_{n,K} \log\log x$$

if $x < N^{d\xi/(n+1)}$.

Now,

$$\sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp - 1} s_\wp(f) = \sum_{q_\wp \le M} \frac{\log q_\wp}{q_\wp} - \sum_{\substack{q_\wp \le M \\ \wp \text{ ramified}}} \frac{\log q_\wp}{q_\wp} + \sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f) + O(1).$$

Since

$$\sum_{q_\wp \le M} \frac{\log q_\wp}{q_\wp} = \log M + O(1),$$

and

$$\sum_{\substack{q_\wp \le M \\ \wp \text{ ramified}}} \frac{\log q_\wp}{q_\wp} \ll \log\log |N_{K/\mathbb{Q}} \mathfrak{D}_{K_f/K}| \ll \log\log N$$

(see [RZ], Lemma 3.2), one gets

$$\sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp - 1} s_\wp(f) = \log M + \sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f) + O(\log\log N).$$

Let $0 < \delta < \frac{1}{2(n+1)}$ and $N > M(\log M)^{2\delta(n+1)}$, so that

$$M' := \frac{M^{1/2(n+1)}(\log M)^\delta}{(\log N)^{1/(n+1)}} < N^{d\xi/(n+1)}.$$

Write

$$\sum_{\substack{q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f) = \sum_{\substack{q_\wp \le M' \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f) + \sum_{\substack{M' < q_\wp \le M \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f).$$

For the first term, by partial integration we obtain

$$\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \le M' \\ \wp \text{ unramified}}} \frac{\log q_\wp}{q_\wp} \sigma_\wp(f) \ll \frac{\log M'}{M'} \log\log M' + \int_2^{M'} \log\log t \frac{(1 - \log t)}{t^2} dt \ll 1,$$

since $\int_2^{M'} \log\log t \frac{(1-\log t)}{t^2} dt \ll \int_2^{M'} \frac{t^{1/2}}{t^2} dt \ll 1$.

To treat the second term, note that it is

$$\le (n-1) \sum_{M' < q_\wp \le M} \frac{\log q_\wp}{q_\wp} \le (n-1) \sum_{M-y < q_\wp \le M} \frac{\log q_\wp}{q_\wp},$$

for $y \geq M - M'$. If moreover we pick $M \sim 2y$, then

$$\sum_{M-y<q_\wp \leq M} \frac{\log q_\wp}{q_\wp} \ll \log M - \log(M-y) = o(\log M)$$

as $M \to +\infty$.

Hence we have the following estimate on average:

$$\begin{aligned}\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \leq M \\ \wp \text{ unramified}}} \alpha_\wp(M) \log q_\wp &= M \log M + O\Big(M \log\log N + \frac{M}{y}\Big) \\ &= M \log M + O(M \log\log N),\end{aligned}$$

for $N > M(\log M)^{2\delta(n+1)}$, $0 < \delta < \frac{1}{2(n+1)}$.

• We divide the sum into two terms:

$$\begin{aligned}\sum_{\substack{q_\wp \leq M \\ \wp \text{ ramified}}} \alpha_\wp(M) \log q_\wp = & \sum_{\substack{q_\wp \leq M \\ \wp \text{ ramified}}} \log q_\wp |\{\lambda \in \mathcal{O}_K : N_{K/\mathbb{Q}}\lambda \leq M,\ f(\lambda) \equiv 0 \bmod \wp\}| \\ & + \sum_{\substack{q_\wp \leq M \\ \wp \text{ ramified}}} \log q_\wp \sum_{N_{K/\mathbb{Q}}\lambda \leq M} \sum_{\substack{k \geq 2 \\ f(\lambda) \equiv 0\ (\wp^k)}} 1 \\ & = \mathrm{I} + \mathrm{II}.\end{aligned}$$

To estimate I, note that

$$|\{\lambda \in \mathcal{O}_K : N_{K/\mathbb{Q}}\lambda \leq M,\ f(\lambda) \equiv 0 \bmod \wp\}| = \Big[\frac{M}{q_\wp}\Big] s_\wp(f) \ll \frac{M}{q_\wp} s_\wp(f),$$

so

$$\mathrm{I} \ll \sum_{\substack{q_\wp \leq M \\ \wp \text{ ramified}}} \frac{\log q_\wp}{q_\wp} s_\wp(f) \ll_n M \sum_{\substack{q_\wp \leq M \\ \wp \text{ ramified}}} \frac{\log q_\wp}{q_\wp} \ll M \log\log N.$$

The mean value of II is

$$\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \mathrm{II} \ll \frac{1}{N^{nd}} \sum_{q_\wp \leq M} \log q_\wp \sum_{N_{K/\mathbb{Q}}\lambda \leq M} \sum_{2 \leq k \ll \frac{\log N + \log M}{\log q_\wp}} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f(\lambda) \equiv 0\ (\wp^k)}} 1.$$

Similarly as we computed in Chapter 2, note that for any $\lambda \in \mathcal{O}_K$,

$$\sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f(\lambda) \equiv 0\ (\wp^k)}} 1 = \sum_{\substack{g \in \mathbb{F}_{q_\wp^k}[X] \\ g(\lambda) = 0}} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ f \equiv g \bmod \wp^k}} 1.$$

Since there are $q_\wp^{k(n-2)}$ possibilities for g as in the above sum, one has

$$\sum_{\substack{f\in\mathscr{P}^0_{n,N}\\ f(\lambda)\equiv 0\ (\wp^k)}} 1 = \frac{(2N)^{nd}}{q_\wp^{2k}} + O(N^{d(n-\xi)})$$

as long as $k \ll \frac{\log N}{\log q_\wp}$. Hence

$$\begin{aligned}\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}} \mathrm{II} &\ll M\sum_{q_\wp\le M}\log q_\wp \sum_{k\ge 2}\Big(\frac{1}{q_\wp^2}\Big)^k + \frac{M}{N^{d\xi}}\sum_{q_\wp\le M}\log q_\wp \sum_{k\ll\frac{\log N+\log M}{\log q_\wp}} 1\\ &\ll M + \frac{M^2}{N^{d\xi}}\Big(\frac{\log N}{\log M}+1\Big).\end{aligned}$$

To conclude

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\sum_{\substack{q_\wp\le M\\ \wp \text{ ramified}}} \alpha_\wp(M)\log q_\wp \ll M\log\log N + \frac{M^2}{N^{d\xi}}\Big(\frac{\log N}{\log M}+1\Big).$$

- For $\lambda,\mu\in\mathcal{O}_K$ such that $N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu$ let

$$G(\mu,\lambda) = \frac{f(\mu)-f(\lambda)}{\mu-\lambda}.$$

Once fixed μ, $G(\mu,\lambda)$ is a polynomial in λ of degree $n-1$.

We are now dealing with the primes $\wp$ of norm $q_\wp > M$, for which

$$\begin{aligned}\alpha_\wp(M) &= \sum_{N_{K/\mathbb{Q}}\lambda\le M}\sum_{k\ge1}\mathbb{1}(f(\lambda)\equiv 0 \bmod \wp^k)\\ &= \sum_{k\ge1}\sum_{\substack{N_{K/\mathbb{Q}}\lambda\le M\\ f(\lambda)\equiv 0\ (\wp^k)}} 1 \ll \sum_{1\le k\ll\frac{\log N+\log M}{\log q_\wp}} \ll_{n,K} 1.\end{aligned}$$

For $\wp$ of norm $q_\wp > M$ we then have

$$\alpha_\wp(M) - \beta_\wp(M) \ll_{n,K} 1.$$

Note also that if $\wp|f(\lambda)$, then $|q_\wp| \le |N_{K/\mathbb{Q}}f(\lambda)| \ll N^dM^n$, so $\alpha_\wp(M)=0$ for $q_\wp \gg N^dM^n$. Also, $\alpha_\wp(M)\ne\beta_\wp(M)$ if and only if there exist $\mu,\lambda\in\mathcal{O}_K$, $N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M$ such that $\wp|f(\mu)$ and $\wp|f(\lambda)$, equivalently $\wp|f(\lambda)$ and $\wp|(\mu-\lambda)G(\mu,\lambda)$; but $\wp\nmid(\mu-\lambda)$, since $|N_{K/\mathbb{Q}}(\mu-\lambda)|\le M-1 < q_\wp$, so $\wp|G(\mu,\lambda)$.

Thefore

$$\sum_{q_\wp > M} (\alpha_\wp(M) - \beta_\wp(M)) \log q_\wp \ll \sum_{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\ell) \\ \wp | G(\mu,\lambda)}} \log q_\wp$$

$$= \sum_{\substack{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M \\ G(\mu,\lambda)=0}} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda)}} \log q_\wp + \sum_{\substack{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M \\ G(\mu,\lambda)\neq 0}} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda) \\ \wp | G(\mu,\lambda)}} \log q_\wp$$

$$\ll \sum_{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda)}} \log q_\wp + \sum_{\substack{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M \\ G(\mu,\lambda)\neq 0}} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda) \\ \wp | G(\mu,\lambda)}} \log q_\wp$$

$$\ll (\log N + \log M) \max_{N_{K/\mathbb{Q}}\mu \le M} \{\wp : q_\wp > M,\ \wp | f(\mu)\}$$

$$+ \sum_{\substack{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M \\ G(\mu,\lambda)\neq 0}} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda) \\ \wp | G(\mu,\lambda)}} \log q_\wp.$$

For $N_{K/\mathbb{Q}}\mu \le M$, $|N_{K/\mathbb{Q}} f(\mu)| \ll N^d M^n$, so the primes $\wp$ with $q_\wp > M$ dividing $f(\mu)$ are at most $\ll \frac{\log(N^d M^n)}{\log M} \ll_{n,K} 1$. Thus

$$\sum_{q_\wp > M} (\alpha_\wp(M) - \beta_\wp(M)) \log q_\wp \ll \sum_{\substack{1 \le N_{K/\mathbb{Q}}\lambda < N_{K/\mathbb{Q}}\mu \le M \\ G(\mu,\lambda)\neq 0}} \sum_{\substack{M < q_\wp \ll N^d M^n \\ \wp | f(\lambda) \\ \wp | G(\mu,\lambda)}} \log q_\wp + \log M,$$

or on average

$$
\begin{aligned}
&\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{q_\wp>M}(\alpha_\wp(M)-\beta_\wp(M))\log q_\wp\\
&\ll \sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}}\ \sum_{\substack{M<q_\wp\ll N^dM^n\\ \wp|G(\mu,\lambda)}}\log q_\wp|\{f:f(\lambda)\equiv 0 \bmod \wp\}|+\log M\\
&\quad= \sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}}\ \sum_{\substack{M<q_\wp\ll N^dM^n\\ \wp|G(\mu,\lambda)}}\log q_\wp\Big(\frac{1}{q_\wp^2}+O\Big(\frac{1}{N^{d\xi}}\Big)\Big)+\log M\\
&\qquad\qquad\ll \sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}}\ \sum_{\substack{M<q_\wp\ll N^dM^n\\ \wp|G(\mu,\lambda)}}\frac{\log q_\wp}{q_\wp^2}\\
&\qquad\qquad+\frac{1}{N^{d\xi}}\sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}}\ \sum_{\substack{M<q_\wp\ll N^dM^n\\ \wp|G(\mu,\lambda)}}\log q_\wp+\log M\\
&\qquad\qquad\qquad\qquad\qquad\qquad=\mathrm{I}+\mathrm{II}+\log M.
\end{aligned}
$$

For II, observe that since $|G(\mu,\lambda)|\ll N^dM^{n-1}$, the number of primes $\wp$ of norm $q_\wp>M$ dividing $G(\mu,\lambda)$ is at most $\ll\frac{\log(N^dM^{n-1})}{\log M}\ll 1$, so

$$
\mathrm{II}\ll\frac{M^2}{N^{d\xi}}\log M.
$$

For I, we separate the contribution of small and large prime. Pick $M<B_{M,N}\ll N^dM^n$; for small primes we have

$$
\begin{aligned}
\sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}}\ \sum_{\substack{M<q_\wp\le B_{M,N}\\ \wp|G(\mu,\lambda)}}\frac{\log p}{q_\wp^2}&=\sum_{M<q_\wp\le B_{M,N}}\frac{\log q_\wp}{q_\wp^2}\sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\equiv 0\ (\wp)}}1\\
&\ll M\sum_{M<q_\wp\le B_{M,N}}\frac{\log q_\wp}{q_\wp^2}\ll M,
\end{aligned}
$$

since $\sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\equiv 0\ (\wp)}} 1 \le (n-1)M$. For large primes,

$$\begin{aligned}
&\sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}} \sum_{\substack{B_{M,N}<q_\wp\ll N^d M^n\\ \wp|G(\mu,\lambda)}} \frac{\log q_\wp}{q_\wp^2}\\
&\quad\ll \frac{(\log N+\log M)}{B_{M,N}^2} \sum_{\substack{1\le N_{K/\mathbb{Q}}\lambda<N_{K/\mathbb{Q}}\mu\le M\\ G(\mu,\lambda)\neq 0}} |\{\wp : q_\wp > B_{M,N},\ \wp|G(\mu,\lambda)\}|\\
&\qquad\qquad\ll \frac{M^2}{B_{M,N}^2}\log M \frac{\log M}{\log B_{M,N}},
\end{aligned}$$

by observing that $|\{\wp : q_\wp > B_{M,N},\ \wp|G(\mu,\lambda)\}| \ll \frac{\log(N^d M^{n-1})}{\log B_{M,N}} \ll \frac{\log M}{\log B_{M,N}}$ since $|G(\mu,\lambda)| \ll N^d M^{n-1}$. We obtained

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\sum_{q_\wp>M}(\alpha_\wp(M)-\beta_\wp(M))\log q_\wp \ll M + \frac{M^2}{N^{d\xi}}\log M + \log M$$

by choosing for instance $B_{M,N} = M\log M$.

Finally,

$$\begin{aligned}
\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}} &\log|N_{K/\mathbb{Q}}(\mathrm{lcm}(f(\lambda) : N_{K/\mathbb{Q}}\lambda \le M)) = (n-1)M\log M\\
&+ O\left(M\frac{\log M}{\log\log M} + N\log\log M + M\log\log M + \frac{M^2}{N^{d\xi}}\log M\right)\\
&\qquad = (n-1)M\log M + O\left(M\frac{\log M}{\log\log M} + N\log\log M\right),
\end{aligned}$$

when $M(\log M)^\ell \ll N = o\left(M\frac{\log M}{\log\log M}\right)$, $0<\ell<1$ small enough.

$\square$

In particular

$$\log|N_{K/\mathbb{Q}}(\mathrm{lcm}(f(\lambda) : N_{K/\mathbb{Q}}\lambda \le M))| \sim (n-1)M\log M$$

for all but $o(N^{nd})$ set of f in $\mathscr{P}^0_{n,N}$.

4 Further results and problems

4.1 Other Galois groups

In general, for a subgroup $G \subseteq S_n$, the elements in a conjugacy class in G necessarily have the same cycle type, but the converse need not to be true. That is, the cycle type of a conjugacy class in G need not determine it uniquely. This uniqueness property does hold for cycle types for the full symmetric group, which implies that the cycle type of an S_n-polynomial having a square-free factorization mod p uniquely determines the Frobenius element for an S_n-number field obtained by adjoining one root of it.
Let's consider the case of the alternating group $A_n \subseteq S_n$. A single conjugacy class in S_n that is contained in A_n may split into two distinct classes. Also, note that the fact that conjugacy in S_n is determined by cycle type, means that if $\sigma \in A_n$, then all of its conjugates in S_n also lie in A_n. There is a full characterization of the behaviour of conjugacy classes in A_n.

Lemma. *A conjugacy class in S_n splits into two distinct conjugacy classes under the action of A_n if and only if its cycle type consists of distinct odd integers. Otherwise, it remains a single conjugacy class in A_n.*

Proof. Note that the conjugacy class in S_n of an element $\sigma \in A_n$ splits, if and only if there is no element $\tau \in S_n \setminus A_n$ commuting with σ. For if there is one, for each $\tau' \in S_n \setminus A_n$ we have

$$\tau'\sigma\tau'^{-1} = \tau'\sigma\tau\tau^{-1}\tau'^{-1} = (\tau'\tau)\sigma(\tau'\tau)^{-1},$$

and $\tau\tau' \in A_n$. On the other hand, if $\tau\sigma\tau^{-1}$ and σ, with $\tau \in S_n \setminus A_n$, are conjugated in A_n, then for some $\tau' \in A_n$, we have $\tau\sigma\tau^{-1} = \tau'\sigma\tau'^{-1}$, giving

$$\tau'^{-1}\tau\sigma = \sigma\tau'^{-1}\tau,$$

and hence $\tau'^{-1}\tau \in S_n \setminus A_n$ commutes with σ.

Now suppose, σ has a cycle c_i of even length. A cycle of even length is an element of $S_n \setminus A_n$, and as σ commutes with its cycles, we are done by the above. If σ has two cycles $(a_1 \dots a_k)$ and $(b_1 \dots b_k)$ of the same odd length k, then $(a_1b_1)\dots(a_kb_k)$ is a product of k permutations (hence odd, so an element of $S_n \setminus A_n$) commuting with σ.

Suppose $\sigma = c_1 \dots c_s$ is a product of odd cycles c_i of distinct lengths d_i. Let $\tau \in S_n$ be a permutation commuting with σ. Then τ must fix each of the c_i, that is, τ must be of the form $\tau = c_1^{a_1} \dots c_s^{a_s}$ for some $a_i \in \mathbb{Z}$. But as the c_i are even permutations (as cycles of odd length), we have $\tau \in A_n$. So no $\tau \in S_n \setminus A_n$ commutes with σ and we have the claim. $\square$

As in the case of S_n polynomials, we are going to count the number of G-polynomials, where G is a subgroup of the symmetric group S_n.

By generalizing some results of [Di], [Di2], [HB] and [BHB] we will prove the following.

Theorem 4.1. *For every $\varepsilon > 0$ and positive integer n,*

$$|\{(\alpha_0, \ldots, \alpha_{n-1}) \in \mathcal{O}_K^n : \mathrm{ht}(\alpha_j) \le N \ \forall j,$$
$$f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0 \text{ has } G_{K_f/K} = G\}|$$
$$\ll_{n,d,\varepsilon} N^{d(n-1+1/[S_n:G])+\varepsilon},$$

where $[S_n : G]$ is the index of G in S_n.

4.1.1 Proof of Theorem 4.1

Lemma 4.1. *Let $n > r$, $(n, r) = 1$, $\alpha_1, \ldots, \alpha_{r-1}, \alpha_{r+1}, \ldots, \alpha_{n-1} \in \mathcal{O}_K$ be fixed. Then*

$$X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + t \in (\mathcal{O}_K[t])[X]$$

has for all but at most $O_{n,d}(1)$ α_{n-r} in $\mathcal{O}_K$ the full S_n has Galois group of $K(t)$.

Proof. This follows from Satz 1 of [He]. □

Lemma 4.2. *Let $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0 \in \mathcal{O}_K[X]$ with roots $\beta_1, \ldots, \beta_n \in K_f$ and $G_{K_f/K} = G \subseteq S_n$. Let*

$$\Phi(z; \alpha_0, \ldots, \alpha_{n-1}) = \prod_{\sigma \in S_n/G} \Big(z - \sum_{\tau \in G} \beta_{\sigma\tau(1)} \beta_{\sigma\tau(2)}^2 \cdots \beta_{\sigma\tau(n)}^n \Big)$$

be the Galois resolvent with respect to $\sum_{\tau \in G} X_{\tau(1)} X_{\tau(2)}^2 \cdots X_{\tau(n)}^n$. Then Φ has integral coefficients and the roots are integral over K.

Proof. The polynomial Φ is fixed by any permutation of the roots. Then the coefficients are symmetric polynomials in the roots of f, hence they can be written as integral polynomials in the elementary symmetric polynomials of the roots of f, that is in the coefficients of f.
The root $\sum_{\tau \in G} \beta_{\sigma\tau(1)} \beta_{\sigma\tau(2)}^2 \cdots \beta_{\sigma\tau(n)}^n$ of Φ is fixed by any element of G, so it is in K. It also satisfy a monic polynomial with coefficients in $\mathcal{O}_K$. Then it is integral over K. □

Lemma 4.3. *Let $F \in \mathcal{O}_K[X_1, X_2]$ of degree n be irreducible over K. For $P_i \in \mathbb{R}_{\ge 1}$, $i = 1, 2$, let*

$$N(F; P_1, P_2) = |\{(x_1, x_2) \in \mathcal{O}_K^2 : F(x_1, x_2) = 0,\ \mathrm{ht}(x_i) \le N\ i = 1, 2\}|.$$

Denote by

$$T = \max_{(e_1, e_2)} \{P_1^{de_1}, P_2^{de_2}\},$$

where the maximum takes over all integer 2-uples (e_1, e_2) *for which the corresponding monomial* $X_1^{e_1} X_2^{e_2}$ *occurs in* $F(X_1, X_2)$ *with nonzero coefficient. Then for every* $\varepsilon > 0$

$$N(F; P_1, P_2) \ll_{n,d,\varepsilon} \max\{P_1, P_2\}^{\varepsilon} \cdot \exp\left(\frac{d^2 \log P_1 \log P_2}{\log T}\right).$$

Proof. It is a straightforward generalization of the special case $P_1 = 1$ of Theorem 1 in [BHB]. See also [HB], Theorem 15. As noticed in [Di2], if F is irreducible over K, by Bézout's Theorem $N(F; P_1, P_2) \ll_{n,d} 1$, so we may assume that F is absolutely irreducible, as in [BHB]. □

We can now prove Theorem 4.1. Let G be a subgroup of S_n of index $[S_n : G] = m$. By Lemma 4.2, there exist $b_1, \ldots, b_m \in \mathbb{Z}[\alpha_0, \ldots, \alpha_{n-1}]$ so that

$$\Phi(z; \alpha_0, \ldots, \alpha_{n-1}) = z^m + b_1(\alpha_0, \ldots, \alpha_{n-1}) z^{m-1} + \cdots + b_m(\alpha_0, \ldots, \alpha_{n-1}).$$

By Lemma 1.1, a root $z \in \mathcal{O}_K$ of Φ has norm bounded by

$$|N_{K/\mathbb{Q}}| \ll_{n,d} N^{d\alpha}$$

for some $\alpha \geq 1$.

Now fix $\alpha_{n-1}, \ldots, \alpha_2$ of height N. Our goal is to bound the number of $\alpha_1, \alpha_0 \in \mathcal{O}_K$ of height N so that $G_{K_f/K} = G$. It suffices to show that there are at most $O(N^{d(1+1/m)+\varepsilon})$ such α_1, α_0.

By Lemma 4.1, $X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_1 X + t$ has for all but at most $O_{n,d}(1)$ values of α_1 the full symmetric group as Galois group over $K(t)$. Hence it's enough to fix any such α_1 of height N for which $X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_1 X + t$ has Galois group S_n over $K(t)$ and then show that for those fixed $\alpha_{n-1}, \ldots, \alpha_1$ there are at most $O(N^{d/m+\varepsilon})$ possibilities for α_0, $\mathrm{ht}(\alpha_0) \leq N$, for which f has Galois group G.

Consider $\Phi(z; \alpha_0, \ldots, \alpha_{n-1}) = \Phi(z, \alpha_0)$ as a polynomial in z, α_0. Since $X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_1 X + t$ has Galois group S_n, the resolvent $\Phi(z, \alpha_0)$ must be irreducible over $K[z]$. We can now bound above the number of zeros of $\Phi(z, \alpha_0)$ with $|N_{K/\mathbb{Q}}(z)| \ll N^{d\alpha}$ and $\mathrm{ht}(\alpha_0) \leq N$ by applying Lemma 4.3 with $P_1 \asymp N^{\alpha}$ and $P_2 = N$. In this case $T \gg N^{dm\alpha}$, so

$$\begin{aligned} &|\{(z, \alpha_0) \in \mathcal{O}_K^2 : |N_{K/\mathbb{Q}}(z)| \ll N^{d\alpha},\ \mathrm{ht}(\alpha_0) \leq N,\ \Phi(z, \alpha_0) = 0\}| \\ &\qquad \ll_{n,d,\varepsilon} N^{\varepsilon} \cdot \exp\left(\frac{d^2 \log N^{\alpha} \log N}{dm\alpha \log N}\right) \\ &\qquad\qquad \ll_{n,d,\varepsilon} N^{\frac{d}{m}+\varepsilon}. \end{aligned}$$

This completes the proof of Theorem 4.1.

Consider the set

$$\mathscr{P}^1_{n,N}(K) = \{f \in \mathscr{P}_{n,N}(K) : G_f = S_n \text{ or } A_n\}.$$

Now, if $G \subseteq S_n$, $G \neq S_n, A_n$ then its index in S_n is greater or equal then n. From Theorem 4.1 we thus have that

$$|\mathscr{P}^1_{n,N}(K)| = (2N)^{nd} + O\left(N^{d\left(n-1+\frac{1}{n}\right)+\varepsilon}\right).$$

Let $\mathscr{C}_r \in A_n$ be a conjugacy class, with $r = (r_1, \ldots, r_n)$ a square-free splitting type such that either r_i is even for some i, or all the r_i's are odd but $r_i = r_j$ for some $i \neq j$.

By following the same argument as in Lemma 2.1 and Proposition 2.1, we get the Chebotarev Theorem on average:

$$\frac{1}{|\mathscr{P}^1_{n,N}(K)|} \sum_{f \in \mathscr{P}^1_{n,N}} \Big(\sum_{\substack{N_{K/\mathbb{Q}}\wp \leq x \\ \mathrm{Frob}_{f,\wp} \in \mathscr{C}_r}} 1 \Big) = \delta(r)\pi_K(x) + C_r \log\log x + O_{n,K}(1),$$

as $x, N \to +\infty$, if $x < N^{\frac{d(1-(1/n))-\varepsilon}{n+1}}$.

Remark. Note that even if one doesn't fully control the conjugacy classes of a subgroup $G \subseteq S_n$ in terms of the cycle type, there is still interesting information to extract from it. Especially, about the number of totally splitting primes (corresponding to the trivial conjugacy class), which was the main tool in the application to class group torsion upper bounds of Section 3.2.

4.2 Other subfamilies

It is reasonable to consider subfamilies of S_n-polynomials as in Section 2.3. However, there are some interesting examples that don't fit those criteria. The following is subset of $\mathscr{P}^0_{n,N}(\mathbb{Q})$, since it fullfills the conditions of Corollary 1 in [Os]. Namely, $\mathscr{A}$ is the family of polynomials of the form

$$f(X) = f_{\ell,q,r}(X) = X^n + qrX^{n-1} + \ell r X^{n-2} + \ell qr X^{n-3} + \cdots + \ell qr X^3$$
$$+\ell r X^2 + \ell qr X + \ell qr,$$

where ℓ, q, r are distinct primes, and $\ell qr \leq N$.
Let p be a prime. We have that

$$\mathscr{A}^p = \{f \bmod p : f \in \mathscr{A}\}$$

consists of all polynomials $g \in \mathbb{F}_p[X]$ of the form

$$g(X) = X^n + AX^{n-1} + BX^{n-2} + CX^{n-3} + \cdots + CX^3 + BX^2 + CX + C,$$

where $A, B, C \in \mathbb{F}_p$. In particular, $|\mathscr{A}^p| = p^3$. Let $g \in \mathscr{A}^p$ as above. We are going to count the number of $f \in \mathscr{A}$ congruent to g mod p. We need to distinguish the case when p possibly equals one of the primes ℓ, q, r. We avoid to indicate $\ell \neq q \neq r$ in the notations. It turns out that

$$\sum_{\substack{f \in \mathscr{A} \\ f \equiv g \bmod p}} 1 = |\{(\ell, q, r) : \ell q r \leq N,\ qr \equiv A,\ \ell r \equiv B,\ \ell q r \equiv C \bmod p\}|$$

$$= |\{(q, r) : qr \leq N/p,\ qr \equiv A \bmod p\}| + |\{(\ell, r) : \ell r \leq N/p,\ \ell r \equiv B \bmod p\}| + |\{(\ell, q) : \ell q \leq N/p\}|$$

$$+ |\{(\ell, q, r) : \ell, q, r \neq p,\ \ell q r \leq N,\ qr \equiv A,\ \ell r \equiv B,\ \ell q r \equiv C \bmod p\}|.$$

With a little work, one can show that

$$\sum_{\substack{f \in \mathscr{A} \\ f \equiv g \bmod p}} 1 = \frac{N \log\log N}{p \log N} + E_p(N),$$

where the error term $E_p(N)$ depends on g and on p. Indeed:

$$E_p(N) \ll_n \begin{cases} \frac{\log p}{p} \frac{N \log\log N}{(\log N)^2} + \frac{N}{p \log N} & \text{if } A \equiv B \equiv 0; \\ \frac{\log p}{p} \frac{N \log\log N}{(\log N)^2} + \frac{N}{p \log N} + \frac{N \log\log N}{p^2 \log N} + \frac{N (\log\log N)^2}{p^3 \log N} & \text{if } A, B, C \not\equiv 0; \\ \frac{\log p}{p} \frac{N \log\log N}{(\log N)^2} + \frac{N}{p \log N} + \frac{N \log\log N}{p^2 \log N} & \text{otherwise,} \end{cases}$$

as long as $p < N$, and $(\log\log N)^{1/2} < p < N$ for the middle case.
Fix a splitting type r. To count the polynomials in $\mathscr{A}^p$ of splitting type r, we make again use of the RH over finite fields. Consider the morphism

$$\{(x, \ell, q, r) \in \mathbb{A}^4 : f_{\ell,q,r}(x) = 0\} \xrightarrow{F} \mathbb{A}^3$$
$$(x, \ell, q, r) \longmapsto (\ell, q, r).$$

For a prime p, let G be the Galois group the Galois closure of the extension $\mathbb{F}_p(A, B, C)[x]/\mathbb{F}_p(A, B, C)$, where $x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \cdots + Cx^3 + Bx^2 + Cx + C = 0$. On can show that "almost always" $G = S_n$, so the Chebotarev Density Theorem over $\mathbb{F}_p$ implies that

$$\{(A, B, C) \in \mathbb{F}_p^3 : \mathrm{Frob}_p \text{ acts as a permutation of cycle type } r \text{ on } F^{-1}(\ell, r, q)\}$$
$$= \delta(r) p^3 + O(p^{5/2}).$$

In the notation of Section 2.3, we get

$$|X^{\mathscr{A}}_{n,r,p}| = \delta(r) p^3 + O(p^{5/2}).$$

We can view the above example as one a family as in 2.3, with M not a constant, but $M = \frac{\log\log N}{\log N}$. However, the relation between p and N is more delicate here.

The aim is to work with families $\mathscr{A}$ like the last one, and even extended, to improve the main term in the higher moments for the Chebotarev Theorem, and have results for the class group bounds, holding for all $f \in \mathscr{A}$.

4.3 Artin L-functions

Let $f \in \mathscr{P}^0_{n,N}$ and fix an irreducible representation ρ of the symmetric group S_n. Let χ be the associated character $\chi = \mathrm{Tr} \circ \rho$. For a prime $\wp$ of $\mathcal{O}_K$, we denote by $\overline{\rho}$ the subrepresentation of ρ on $V_\rho^{I_{\mathfrak{p}|\wp}}$, that is, invariant under the action of the inertia group $I_{\mathfrak{p}|\wp}$ for a prime $\mathfrak{p}$ over $\wp$. If $\wp$ is unramified on K_f, clearly $\rho = \overline{\rho}$. For $\Re s > 1$ the Artin L-function associated to χ is

$$L(s,\chi) = L_f(s,\chi) = \prod_{\wp} \prod_{i=1}^{\chi(1)} (1 - \alpha_{\wp,i,\chi} q_\wp^{-s})^{-1},$$

where $\alpha_{\wp,i,\chi}$ are the eigenvalues of $\overline{\rho}(\mathrm{Frob}_{f,\wp})$.

By taking the logarithm we see that

$$\begin{aligned}
\log L(s,\chi) &= \sum_{\wp, m\geq 1} \sum_{i=1}^{\chi(1)} \frac{\alpha_{\wp,i,\chi}^m}{m q_\wp^{ms}} \\
&= \sum_{\wp, m\geq 1} \frac{1}{m} \chi(\mathrm{Frob}_{f,\wp}^m) q_\wp^{-ms} \\
&= \sum_{n\geq 1} \sum_{\substack{\wp, m\geq 1 \\ q_\wp^m = n}} \frac{1}{m} \chi(\mathrm{Frob}_{f,\wp}^m) n^{-s} \\
&= \sum_{n\geq 1} a_{n,\chi,f} n^{-s},
\end{aligned}$$

where we define

$$a_{n,\chi,f} = \sum_{\substack{\wp, m\geq 1 \\ q_\wp^m = n}} \frac{1}{m} \chi(\mathrm{Frob}_{f,\wp}^m).$$

Let

$$\widetilde{\pi}_{f,\chi}(x) = \sum_{\substack{\wp, m\geq 1 \\ q_\wp^m \leq x}} \frac{1}{m} \chi(\mathrm{Frob}_{f,\wp}^m) = \sum_{n \leq x} a_{n,\chi,f},$$

where $\mathrm{Frob}_{f,\wp}$ denotes the canonical generator of $D_\wp / I_\wp$ for the ramified primes, whereas in general set

$$\chi(\mathrm{Frob}_{f,\wp}^m) = \frac{1}{|I_\wp|} \sum_{\substack{\tau \in D_\wp \\ \tau \equiv \mathrm{Frob}_{f,\wp}^m \bmod I_\wp}} \chi(\tau).$$

Similarily, for the logarithmic derivative:

$$\mathbb{E}_N\Big(-\frac{L'}{L}(s,\chi)\Big) = \sum_{n\geq 1} \Lambda(n) \mathbb{E}_N(a'_{n,\chi,f}) n^{-s},$$

where $a'_{n,\chi,f} = \sum_{\substack{\wp,m\geq 1\\ q_\wp^m=n}} \chi(\mathrm{Frob}^m_{f,\wp})$. Let

$$\pi'_{f,\chi}(x) = \sum_{n\leq x} a'_{n,\chi,f}.$$

Corollary 4.1. *One has*

(1) $\mathbb{E}_N(\widetilde{\pi}_{f,\chi}(x)) = \sum_r \delta(r)\chi(g_r)\pi_K(x) + O_{n,K,\chi}(\log N + \sqrt{x})$;

(2) $\mathbb{E}_N(\pi'_{f,r}(x)) = \sum_r \delta(r)\chi(g_r)\log x\ \pi_K(x) + O_{n,K,\chi}\left(\left(\frac{x}{\log x} + \log N \log x\right)\right)$,

as $x, N \to +\infty$, *if* $x < N^{d\xi/(n+1)}$.

In particular,

$$\sum_{n\leq x} \mathbb{E}_N(a_{n,\chi,f}) \sim \sum_r \delta(r)\chi(g_r)\frac{x}{\log x}$$

and

$$\sum_{n\leq x} \Lambda(n)\mathbb{E}_N(a'_{n,\chi,f}) \sim \sum_r \delta(r)\chi(g_r)x,$$

if $x < N^{d\xi/(n+1)}$, as $x, N \to +\infty$.

Proof. As in [Se] Proposition 7 of section 2.6, we get

$$\widetilde{\pi}_{f,\chi}(x) - \pi_{f,\chi}(x) \ll \|\chi\|(\log N + \sqrt{x})$$

as $x \to +\infty$, where $\|\chi\| = \sup_{\sigma\in G_f} |\chi(\sigma)|$.
We thus have (1) by Corollary 2.1.

Again, using an analogous argument as in [Se],

$$\pi'_{f,\chi}(x) - \pi_{f,\chi}(x) \ll \|\chi\|(\log N + \sqrt{x})$$

as $x, N \to +\infty$. Hence by partial integration

$$\sum_{n\leq x} \Lambda(n)\mathbb{E}_N(a'_{n,\chi,f}) = \mathbb{E}_N\Big(\sum_{1\leq q_\wp \ll \log x}\ \sum_{q_\wp\leq x} \log q_\wp \cdot \chi(\mathrm{Frob}^m_{f,\wp})\Big)$$

$$= \mathbb{E}_N\Big(\sum_{1\leq q_\wp\ll \log x} \log x \sum_{q_\wp\leq x}\chi(\mathrm{Frob}^m_{f,\wp}) - \sum_{1\leq q_\wp\ll\log x}\int_2^x \sum_{q_\wp\leq t}\chi(\mathrm{Frob}^m_{f,\wp})\frac{dt}{t}\Big)$$

$$\log x\ \mathbb{E}_N(\pi'_{f,\chi}(x)) + O\Big(\int_2^x \mathbb{E}_N(\pi'_{f,\chi}(x))\frac{dt}{t}\Big)$$

$$= \sum_r \delta(r)\chi(g_r)\log x\ \pi_K(x) + O\Big(\|\chi\|(\log N\log x + \sqrt{x}\log x) + \|\chi\|\int_2^x \frac{\pi_K(t)}{t}dt\Big)$$

$$= \sum_r \delta(r)\chi(g_r)\log x\ \pi_K(x) + O\Big(\|\chi\|\Big(\frac{x}{\log x} + \log N\log x\Big)\Big),$$

which shows (2). □

Let $N_f(t,\chi)$ be the function counting the net number of zeros of $L_f(s,\chi)$ with imaginary part in $(0,t]$. A consequence of Corollary 3.1 is the following upper bound on average for the logarithm $\mathfrak{f}(\chi) = \mathfrak{f}_f(\chi)$ of the global Artin conductor.

Lemma 4.4. *For almost all $f \in \mathscr{P}^0_{n,N}$, it holds*

$$\log |N_{K/\mathbb{Q}}\mathfrak{f}(\chi)| \ll_{n,K,\chi} \log N,$$

as $N \to +\infty$.

Proof. Recall that the global conductor $\mathfrak{f}(\chi)$ is the product over primes $\wp \subseteq \mathcal{O}_K$ of $\wp$ to the local conductor $\mathfrak{f}_\wp(\chi)$, where the local factor at $\wp$ is given in terms of the the ramification groups $G_{i,\wp}$ of G_f at $\wp$ as

$$\begin{aligned}
\mathfrak{f}_\wp(\chi) &= \sum_{i\geq 0} \frac{|G_{i,\wp}|}{|G_{0,\wp}|}\mathrm{codim} V^{G_{i,\wp}} \\
&= \sum_{i\geq 0} \frac{|G_{i,\wp}|}{|G_{0,\wp}|}\Big(\chi(1) - \frac{1}{|G_{i,\wp}|}\sum_{\sigma\in G_{i,\wp}} \chi(\sigma)\Big) \\
&= \Big(\chi(1) - \frac{1}{e_{\wp,f}}\sum_{\sigma\in G_{0,\wp}} \chi(\sigma)\Big) + \sum_{i\geq 1} \frac{|G_{i,\wp}|}{|G_{0,\wp}|}\Big(\chi(1) - \frac{1}{|G_{i,\wp}|}\sum_{\sigma\in G_{i,\wp}} \chi_f(\sigma)\Big) \\
&= \mathfrak{f}_\wp^{\mathrm{tame}}(\chi) + \mathfrak{f}_\wp^{\mathrm{wild}}(\chi),
\end{aligned}$$

where $e_{\wp,f} = |G_{0,\wp}| = |I_\wp|$ is the ramification index at $\wp$. Moreover one has

$$\mathfrak{f}_\wp^{\mathrm{tame}}(\chi) \ll \Big(1 - \frac{1}{e_{\wp,f}}\Big)\|\chi\|$$

and

$$\mathfrak{f}_\wp^{\mathrm{wild}}(\chi) \ll \Big(1 - \frac{1}{q_\wp}\Big)\|\chi\|.$$

In the following, we say that a polynomial $f \in \mathscr{P}^0_{n,N}$ is tamely or wildly ramified at a prime $\wp$ if $\wp$ is tamely or wildly ramified in the extension K_f/K. The logarithm of the norm of the conductor is then

$$\begin{aligned}
\log |N_{K/\mathbb{Q}}\mathfrak{f}(\chi)| &= \sum_{\wp} \mathfrak{f}_\wp(\chi)\log q_\wp \\
&= \sum_{\substack{\wp \\ \wp \text{ ramifies}}} \mathfrak{f}_\wp(\chi)\log q_\wp \\
&= \sum_{\substack{\wp \\ \wp \text{ tamely} \\ \text{ramified}}} \mathfrak{f}_\wp^{\mathrm{tame}}(\chi)\log q_\wp + \sum_{\substack{\wp \\ \wp \text{ wildly} \\ \text{ramified}}} (\mathfrak{f}_\wp^{\mathrm{tame}}(\chi) + \mathfrak{f}_\wp^{\mathrm{wild}}(\chi))\log q_\wp.
\end{aligned}$$

Note that the primes that are wildly ramified have norm dividing their exponent in the discriminant, hence dividing the order of $G_f = S_n$. So their norm is $\ll_{n,K} 1$. By Corollary 3.1,

$$\begin{aligned}
\mathbb{E}_N(\log|N_{K/\mathbb{Q}}\mathfrak{f}(\chi)|) \ll \|\chi\| \Big(&\sum_{q_\wp < N^{d\xi/(n+1)}} \log q_\wp \cdot \mathbb{P}_N(f \in \mathscr{P}^0_{n,N} : \wp \text{ tamely ramified}) \\
&+ \sum_{q_\wp \geq N^{d\xi/(n+1)}} \log q_\wp \, \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{f \in \mathscr{P}^0_{n,N} \\ \wp \text{ tamely} \\ \text{ramified}}} 1 + \sum_{q_\wp \ll 1} \Big(1 - \frac{1}{q_\wp}\Big) \log q_\wp \Big) \\
&\ll \|\chi\| \Big(\sum_{q_\wp < N^{d\xi/(n+1)}} \log q_\wp \cdot \mathbb{P}_N(f \in \mathscr{P}^0_{n,N} : \wp \text{ tamely ramified}) \\
&\qquad + \log N \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{\substack{q_\wp \geq N^{d\xi/(n+1)} \\ \wp \text{ ramified}}} 1 \Big) \\
&\ll \|\chi\| \Big(\sum_{q_\wp < N^{d\xi/(n+1)}} \log q_\wp \cdot \mathbb{P}_N(f \in \mathscr{P}^0_{n,N} : \wp \text{ ramified}) + \log N \Big) \\
&\qquad \ll_{n,K,\chi} \sum_{q_\wp < N^{d\xi/(n+1)}} \frac{\log q_\wp}{q_\wp} + \log N \\
&\qquad\qquad \ll_{n,K,\chi} \log N.
\end{aligned}$$

$\square$

Classically, one deduces Chebotarev Theorems from the information about the zeros of the Artin L-functions, by using the explicit formulas. We aim to do the opposite, that is, to compare the explicit formulas with Corollary 4.1, and get results about the distribution on average of zeros of $L_f(s, \chi)$.

Appendix A

Higher moments

We prove a bound for the k-moments $\mathbb{E}_N(\pi_{f,r}(x)^k)$ for every $k \geq 2$ by using a standard application of the multimonomial theorem. Then we prove Theorem 2 by applying the Central Limit Theorem, as in the classical proof of the Erdős-Kac theorem for the prime divisors counting function.

Proposition 4.1. *Let $x = o(N^\varepsilon)$ for all $\varepsilon > 0$. Then uniformly for natural numbers $k \geq 2$ with $(k-1)! \ll_{n,r,K} \log\log x$, there exists a constant $C(n,r,K)$ such that*

$$\mathbb{E}_N(\pi_{f,r}(x)^k) - \delta(r)^k \pi_K(x)^k - k\delta(r)^{k-1} C_r \pi_K(x)^{k-1} \log\log x \leq C(n,r,K) k! \pi_K(x)^{k-1},$$

for x, N large enough.

Moreover, for a fixed $k \geq 2$, $x < N^{d\xi/(kn+1)}$,

$$\mathbb{E}_N(\pi_{f,r}(x)^k) = \delta(r)^k \pi_K(x)^k + k\delta(r)^{k-1} C_r \pi_K(x)^{k-1} \log\log x + O(\pi_K(x)^{k-1})$$

and

$$\mathbb{E}_N((\pi_{f,r}(x) - \delta(r)\pi_K(x))^k) \ll_{n,K} k! \binom{k}{[k/2]} \pi_K(x)^{k-1}$$

as $n, N \to +\infty$.

Proof.

$$\begin{aligned}
&\mathbb{E}_N(\pi_{f,r}(x)^k) \\
&= \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{f \in \mathscr{P}^0_{n,N}} \sum_{u=1}^{k} \frac{1}{u!} \sum_{\substack{k_1,\dots,k_u \geq 2 \\ k_1+\dots+k_u = k}} \binom{k}{k_1,\dots,k_u} \sum_{\substack{\wp_1 \neq \dots \neq \wp_u \\ N_{K/\mathbb{Q}}\wp_i \leq x}} \mathbb{1}_{f,r}(\wp_1)\dots\mathbb{1}_{f,r}(\wp_u).
\end{aligned}$$

The average sum $\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{\wp_1 \neq \dots \neq \wp_u \\ N_{K/\mathbb{Q}}\wp_i \leq x}} \mathbb{1}_{f,r}(\wp_1)\dots\mathbb{1}_{f,r}(\wp_u)$ (which is the dominant term in the above, for $u = k$) is the probability of f of splitting type r mod $\wp_1, \dots, \wp_k$, i.e.

$$\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{\wp_1 \neq \dots \neq \wp_k \\ N_{K/\mathbb{Q}}\wp_i \leq x}} \mathbb{1}_{f,r}(\wp_1)\dots\mathbb{1}_{f,r}(\wp_k) = \frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{g_i \in X_{n,r,\wp_i} \\ i=1,\dots,k}} \sum_{\substack{f_i \equiv g_i \bmod \wp_i \\ i=1,\dots,k}} 1.$$

By Lemma 2.1 we get

$$\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{f_i \equiv g_i \bmod \wp_i \\ i=1,\dots,k}} 1 = \frac{1}{(q_{\wp_1}\dots q_{\wp_k})^n} + O(N^{-d\xi}).$$

Hence

$$\frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{\substack{\wp_1\neq\dots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_i\leq x}}\mathbb{1}_{f,r}(\wp_1)\dots\mathbb{1}_{f,r}(\wp_k)=|X_{n,r,\wp_1}|\dots|X_{n,r,\wp_k}|\Big(\frac{1}{(q_{\wp_1}\dots q_{\wp_k})^n}+O(N^{-d\xi})\Big)$$

$$=(\delta(r)q_{\wp_1}^n+C_rq_{\wp_1}^{n-1}+O(q_{\wp_1}^{n-2}))\dots(\delta(r)q_{\wp_k}^n+C_rq_{\wp_k}^{n-1}+O(q_{\wp_k}^{n-2}))\Big(\frac{1}{(q_{\wp_1}\dots q_{\wp_k})^n}+O(N^{-d\xi})\Big)$$

$$=(\delta(r)^k(q_{\wp_1}\dots q_{\wp_k})^n$$

$$+\delta(r)^{k-1}C_r((q_{\wp_1}\dots q_{\wp_{k-1}})^nq_{\wp_k}^{n-1}+(q_{\wp_1}\dots q_{\wp_{k-2}})^nq_{\wp_{k-1}}^{n-1}q_{\wp_k}^n+\dots+q_{\wp_1}^{n-1}(q_{\wp_2}\dots q_{\wp_k})^n)$$

$$+\delta(r)^{k-2}C_r^2((q_{\wp_1}\dots q_{\wp_{k-2}})^nq_{\wp_{k-1}}^{n-1}q_{\wp_k}^{n-1}+\dots)$$

$$+O((q_{\wp_1}\dots q_{\wp_{k-1}})^nq_{\wp_k}^{n-2}+\dots+q_{\wp_1}^{n-2}(q_{\wp_2}\dots q_{\wp_k})^n))\Big(\frac{1}{(q_{\wp_1}\dots q_{\wp_k})^n}+O(N^{-d\xi})\Big)$$

$$=\delta(r)^k+\delta(r)^{k-1}C_r\Big(\frac{1}{q_{\wp_1}}+\dots+\frac{1}{q_{\wp_k}}\Big)+\delta(r)^{k-2}C_r^2\Big(\sum_{1\leq i<j\leq k}\frac{1}{q_{\wp_i}q_{\wp_j}}\Big)$$

$$+\dots+\delta(r)C_r\Big(\sum_{1\leq j_1<\dots<j_{k-1}\leq k}\frac{1}{q_{\wp_{j_1}}\dots q_{\wp_{j_{k-1}}}}\Big)$$

$$+O\Big(\frac{1}{q_{\wp_1}\dots q_{\wp_k}}+\frac{1}{q_{\wp_1}^2}+\dots+\frac{1}{q_{\wp_k}^2}+(q_{\wp_1}\dots q_{\wp_k})^nN^{-d\xi}\Big)$$

$$=\delta(r)^k+\delta(r)^{k-1}C_r\Big(\frac{1}{q_{\wp_1}}+\dots+\frac{1}{q_{\wp_k}}\Big)$$

$$+O\Big(\sum_{1\leq i<j\leq k}\frac{1}{q_{\wp_i}q_{\wp_j}}+\frac{1}{q_{\wp_1}^2}+\dots+\frac{1}{q_{\wp_k}^2}+(q_{\wp_1}\dots q_{\wp_k})^nN^{-d\xi}\Big).$$

as long as $(q_{\wp_1}\dots q_{\wp_k})^nN^{-d\xi}<\frac{1}{q_{\wp_1}}+\dots+\frac{1}{q_{\wp_k}}$, e.g. when $q_{\wp_i}<N^{d\xi/(kn+1)}$ for all $i=1,\dots,k$. By induction over k, one has the following estimates:

$$\sum_{\substack{\wp_1\neq\dots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_i\leq x}}\frac{1}{q_{\wp_1}}=\sum_{q_{\wp_1}\leq x}\frac{1}{q_{\wp_1}}\sum_{\substack{\wp_1\neq\wp_2\neq\dots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_2,\dots,N_{K/\mathbb{Q}}\wp_k\leq x}}1$$

$$=\sum_{q_{\wp_1}\leq x}\frac{1}{q_{\wp_1}}(\pi_K(x)^{k-1}+O((k-1)!\pi_K(x)^{k-2}))$$

$$=\pi_K(x)^{k-1}\log\log x+O((k-1)!\pi_K(x)^{k-1});$$

$$\sum_{\substack{\wp_1\neq\dots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_i\leq x}}\frac{1}{q_{\wp_1}q_{\wp_2}}=\sum_{q_{\wp_1}\leq x}\frac{1}{q_{\wp_1}}\sum_{\substack{\wp_1\neq\wp_2\\ N_{K/\mathbb{Q}}\wp_2\leq x}}\frac{1}{q_{\wp_2}}\sum_{\substack{\wp_1\neq\wp_2\neq\wp_3\neq\dots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_3,\dots,N_{K/\mathbb{Q}}\wp_k\leq x}}1$$

$$=\pi_K(x)^{k-2}(\log\log x)^2$$

$$+O(\pi_K(x)^{k-2}\log\log x+(k-2)!\pi_K(x)^{k-3}(\log\log x)^2);$$

$$\sum_{\substack{\wp_1\neq\ldots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_i\leq x}}(q_{\wp_1}\cdots q_{\wp_k})^n=\sum_{q_{\wp_1}\leq x}q_{\wp_1}^n\sum_{\substack{\wp_1\neq\wp_2\\ N_{K/\mathbb{Q}}\wp_2\leq x}}q_{\wp_2}^n\cdots\sum_{\substack{\wp_1\neq\ldots\neq\wp_k\\ N_{K/\mathbb{Q}}\wp_k\leq x}}q_{\wp_k}^n$$
$$\ll\pi_K(x)^{k(n+1)}.$$

In the last one we used the asymptotic

$$\sum_{N_{K/\mathbb{Q}}\wp\leq x}q_\wp^n\sim\pi_K(x)^{n+1}.$$

Finally,

$$\begin{aligned}\mathbb{E}_N(\pi_{f,r}(x)^k)&=\delta(r)^k\pi_K(x)^k+k\delta(r)^{k-1}C_r\pi_K(x)^{k-1}\log\log x\\&\quad+O\Big(\pi_K(x)^{k-1}+\pi_K(x)^{k(n+1)}N^{-d\xi}\Big)\end{aligned}$$

as $x,N\to+\infty$.

The term $\pi_K(x)^{k(n+1)}N^{-d\xi}$ is negligible for $x<N^{d\xi/(kn+1)}$. Since, by induction

$$\sum_{i=0}^k\binom{k}{i}i(-1)^{k-i}=0,$$

the second estimate is straightforward:

$$\begin{aligned}\mathbb{E}_N((\pi_{f,r}(x)-\delta(r)\pi_K(x))^k)&=\sum_{i=0}^k\binom{k}{i}\mathbb{E}_N(\pi_{f,r}(x)^i)(-\delta(r)\pi_K(x))^{k-i}\\
&=\sum_{i=0}^k\binom{k}{i}(\delta(r)^i\pi_K(x)^i+i\delta(r)^{i-1}C_r\pi_K(x)^{i-1}\log\log x\\
&\quad+O(i!\pi_K(x)^{i-1}))(-\delta(r)\pi_K(x))^{k-i}\\
&=\sum_{i=0}^k\binom{k}{i}(\delta(r)^i\pi_K(x)^i)(-\delta(r)\pi_K(x))^{k-i}\\
&\quad+\sum_{i=0}^k\binom{k}{i}(i\delta(r)^{i-1}C_r\pi_K(x)^{i-1}\log\log x)(-\delta(r)\pi_K(x))^{k-i}\\
&\quad+O(\sum_{i=0}^k\binom{k}{i}(i!\pi_K(x)^{i-1})(\delta(r)\pi_K(x))^{k-i})\\
&=0+C_r\delta(r)^{k-1}\pi_K(x)^{k-1}\log\log x\sum_{i=0}^k\binom{k}{i}i(-1)^{k-i}\\
&\quad+O(\sum_{i=0}^k\binom{k}{i}\delta(r)^{k-i}i!\pi_K(x)^{k-1})\\
&=O(k!\binom{k}{[k/2]}\pi_K(x)^{k-1}),\end{aligned}$$

□

By enlarging the error term, one has

$$\mathbb{E}_N(\pi_{f,r}(x)^k) = \delta(r)^k \pi_K(x)^k + O(\pi_K(x)^{k-1} \log\log x) \tag{17}$$

for $x = o(N^{d\xi/(kn+1)})$. In particular, if we choose

$$x = N^{1/\log\log N},$$

then (17) holds for all $k \geq 1$.

Alternative proof of the main theorem

Fix a splitting type r and a prime $\wp$. We are going to compare the behaviour of $\mathbb{1}_{f,r}(\wp)$ with that of the independent discrete random variables $X_\wp$ defined in 2.1. Let

$$S(x) := \sum_{N_{k/\mathbb{Q}}\wp \leq x} X_\wp.$$

By (3) of Proposition 2.1,

$$\mathbb{E}_N(\pi_{f,r}(x)) = \mathbb{E}(S(x)) + O(\pi_K(x)^{n+1} N^{-d\xi}).$$

Moreover, for $k \geq 2$, the k-moment can be written as

$$\mathbb{E}_N(\pi_{f,r}(x)^k) = \mathbb{E}(S(x)^k) + O(\pi_K(x)^{k(n+1)} N^{-d\xi}). \tag{18}$$

In fact, looking at the beginning of the proof of Proposition 4.1, one has, for all $t = 1, \ldots, k$

$$\begin{aligned}
\frac{1}{|\mathscr{P}^0_{n,N}|} \sum_{\substack{\wp_1 \neq \ldots \neq \wp_k \\ N_{K/\mathbb{Q}}\wp_i \leq x}} & \mathbb{1}_{f,r}(\wp_1) \ldots \mathbb{1}_{f,r}(\wp_t) \\
&= |X_{n,r,\wp_1}| \ldots |X_{n,r,\wp_t}| \Big(\frac{1}{(q_{\wp_1} \ldots q_{\wp_k})^n} + O(N^{-d\xi}) \Big) \\
&\qquad = \sum_{\substack{\wp_1 \neq \ldots \neq \wp_t \\ N_{K/\mathbb{Q}}\wp_i \leq x}} \mathbb{E}(X_{\wp_1} \ldots X_{\wp_t}) + O(\pi_K(x)^{t(n+1)} N^{-d\xi}).
\end{aligned}$$

Therefore

$$
\begin{aligned}
&\mathbb{E}_N(\pi_{f,r}(x)^k)\\
&= \frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\sum_{u=1}^{k}\frac{1}{u!}\sum_{\substack{k_1,\dots,k_u\geq 2\\ k_1+\dots+k_u=k}}\binom{k}{k_1,\dots,k_u}\sum_{\substack{\wp_1\neq\dots\neq\wp_u\\ N_{K/\mathbb{Q}}\wp_i\leq x}}\mathbb{E}(X_{\wp_1}\dots X_{\wp_u})\\
&= \frac{1}{|\mathscr{P}^0_{n,N}|}\sum_{f\in\mathscr{P}^0_{n,N}}\sum_{u=1}^{k}\frac{1}{u!}\sum_{\substack{k_1,\dots,k_u\geq 2\\ k_1+\dots+k_u=k}}\binom{k}{k_1,\dots,k_u}\sum_{\substack{\wp_1\neq\dots\neq\wp_t\\ N_{K/\mathbb{Q}}\wp_i\leq x}}\mathbb{E}(X_{\wp_1}\dots X_{\wp_u})\\
&\qquad\qquad + O(\pi_K(x)^{t(n+1)}N^{-d\xi})\\
&\qquad\qquad\qquad = \mathbb{E}(S(x)^k) + O(\pi_K(x)^{t(n+1)}N^{-d\xi}).
\end{aligned}
$$

Since the variables $(X_\wp)_\wp$ are independent, by the central limit theorem

$$
\mathbb{P}\left(\frac{S(x)-\mathbb{E}(S(x))}{\sigma(S(x))}\leq b\right)\underset{N\to+\infty}{\longrightarrow}\Phi(b) \tag{19}
$$

Now,

$$
\mathbb{E}(S(x)) = \delta(r)\pi_K(x) + O(\log\log x)
$$

and

$$
\begin{aligned}
\sigma^2(S(x)) &= \sum_{N_{K/\mathbb{Q}}\wp\leq x}\sigma^2(X_\wp)\\
&= \sum_{N_{K/\mathbb{Q}}\wp\leq x}(\mathbb{E}(X_\wp^2)-\mathbb{E}(X_\wp)^2)\\
&= \sum_{N_{K/\mathbb{Q}}\wp\leq x}\Big(\delta(r)-\delta(r)^2+O\Big(\frac{1}{q_\wp}\Big)\Big)\\
&= (\delta(r)-\delta(r)^2)\pi_K(x) + O(\log\log x);
\end{aligned}
$$

thus

$$
\begin{aligned}
\frac{S(x)-\mathbb{E}(S(x))}{\sigma(S(x))} &= \frac{S(x)-\delta(r)\pi_K(x)+O(\log\log x)}{((\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2})\Big(1+O\Big(\frac{\log\log x}{\pi_K(x)}\Big)\Big)}\\
&= \frac{S(x)-\delta(r)\pi_K(x)+O(\log\log x)}{(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}}(1+o(1))\\
&= \frac{S(x)-\delta(r)\pi_K(x)}{(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}}+o(1).
\end{aligned}
$$

Therefore, by (19)

$$
\begin{aligned}
\mathbb{P}\left(\frac{S(x)-\delta(r)\pi_K(x)}{(\delta(r)-\delta(r)^2)^{1/2}\pi_K(x)^{1/2}}\leq b\right) &\sim \Phi(b)+\frac{1}{\sqrt{2\pi}}\int_b^{b+o(1)}e^{-t^2/2}dt\\
&= \Phi(b)+o(1)\longrightarrow\Phi(b).
\end{aligned}
$$

Since the function Φ is determined by its moments

$$\mu_k = \int_{-\infty}^{+\infty} x^k d\Phi(x),$$

if a family of distribution functions F_n satisfies $\int_{-\infty}^{+\infty} x^k dF_n(x) \to \mu_k$ for all $k \geq 1$, then $F_n(x) \to \Phi(x)$ pointwise (see [Fel], p. 262). On the other hand, if $F_n(x) \to \Phi(x)$ for each x and if $\int_{-\infty}^{+\infty} |x|^{k+\varepsilon} dF_n(x)$ is bounded in n for some $\varepsilon > 0$, then $\int_{-\infty}^{+\infty} x^k dF_n(x) \to \mu_k$ ([Fel], p. 245).

So the theorem will follow by the method of moments if we prove that for $k \geq 1$,

$$\mathbb{E}_N\left(\frac{(\pi_{f,r}(x) - \delta(r)\pi_K(x))^k}{((\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2})^k}\right)$$

converges to μ_k as $N \to +\infty$. We shall first show that its difference with

$$\mathbb{E}\left(\frac{(S(x) - \delta(r)\pi_K(x))^k}{((\delta(r) - \delta(r)^2)^{1/2}\pi_K(x)^{1/2})^k}\right)$$

converges to 0, and then show that the above itself converges to μ_k.

By (18),

$$\mathbb{E}(S(x)^k) - \mathbb{E}_N(\pi_{f,r}(x)^k) \ll \pi_K(x)^{k(n+1)} N^{-d\xi}$$

then

$$\begin{aligned}
&\mathbb{E}((S(x) - \delta(r)\pi_K(x))^k) - \mathbb{E}_N((\pi_{f,r}(x) - \delta(r)\pi_K(x))^k) \\
&\ll \sum_{i=0}^{k} \binom{k}{i} \pi_K(x)^{i(n+1)} N^{-d\xi} (\delta(r)\pi_K(x))^{k-i} \\
&\ll \pi_K(x)^{k(n+1)} N^{-d\xi},
\end{aligned}$$

which converges to 0 by the choice of x. The last step is to show that the moments

$$\mathbb{E}\left(\frac{(S(x) - \delta(r)\pi_K(x))^k}{\sigma^k(S(x))}\right)$$

are bounded. Let

$$Y_\wp = X_\wp - \frac{|X_{n,r,\wp}|}{q_\wp^n} = X_\wp - \mathbb{E}(X_\wp).$$

It holds, by the multimonomial theorem,

$$\begin{aligned}
&\mathbb{E}((\sum_{N_{K/\mathbb{Q}}\wp \leq x} Y_\wp)^k) = \mathbb{E}((S(x) - \mathbb{E}(S(x)))^k) \\
&= \sum_{u=1}^{k} \sum_{k_1+\cdots+k_u=k} \binom{k}{k_1, \ldots, k_u} \sum_{N_{K/\mathbb{Q}}\wp_1 < \cdots < N_{K/\mathbb{Q}}\wp_u \leq x} \mathbb{E}(Y_{\wp_1}^{k_1}) \ldots \mathbb{E}(Y_{\wp_u}^{k_u}).
\end{aligned}$$

Since $\mathbb{E}(Y_\wp) = 0$, the last sum equals

$$\sum_{u=1}^{k} \sum_{\substack{k_1+\cdots+k_u=k \\ k_i>1}} \binom{k}{k_1,\ldots,k_u} \sum_{N_{K/\mathbb{Q}}\wp_1<\cdots<N_{K/\mathbb{Q}}\wp_u\le x} \mathbb{E}(Y_{\wp_1}^{k_1})\ldots\mathbb{E}(Y_{\wp_u}^{k_u}).$$

Then $|\mathbb{E}(Y_{\wp_i}^{k_i})| \le |\mathbb{E}(Y_{\wp_i}^{2})|$, so

$$\begin{aligned}\sum_{N_{K/\mathbb{Q}}\wp_1<\cdots<N_{K/\mathbb{Q}}\wp_u\le x} \mathbb{E}(Y_{\wp_1}^{k_1})\ldots\mathbb{E}(Y_{\wp_u}^{k_u}) &\le (\sum_{N_{K/\mathbb{Q}}\wp\le x} \sigma^2(Y_\wp))^u \\ &=\le (\sum_{N_{K/\mathbb{Q}}\wp\le x} \sigma^2(X_\wp))^u \\ &= (\sigma^2(S(x)))^u.\end{aligned}$$

Since $k_1+\cdots+k_u = k$ and $k_i \ge 2$, one has $2u \le k$. Consider N large enough such that $\sigma^2(S(x)) \ge 1$. It turns out that

$$\begin{aligned}\mathbb{E}((S(x)-\mathbb{E}(S(x)))^k) \le \sigma^k(S(x)) &\sum_{u=1}^{k} \sum_{\substack{k_1+\cdots+k_u=k \\ k_i>1}} \binom{k}{k_1,\ldots,k_u} \\ &\ll \sigma^k(S(x));\end{aligned}$$

in other words

$$\sup_x \left| \mathbb{E}\left(\frac{(S(x)-\delta(r)\pi_K(x))^k}{\sigma^k(S(x))} \right) \right| < \infty,$$

which completes the proof.

References

[AGHLLTWZ] Anderson, T., Gafni, A., Hughes, K., Lemke Oliver, R., Lowry-Duda, D., Thorne, F., Wang, J., Zhang, R., Improved bounds on number fields of small degree, arXiv:2204.01651v2 [math.NT] 7 Sep 2022.

[ABZ] Avner A., Brakenhoff J., Zarrabi T., Equality of Polynomial and Field Discriminants. Experiment. Math. 16 (2007), no. 3, 367–374.

[Bh1] Bhargava, M. Galois groups of random integer polynomials and van der Waerden's Conjecture, arXiv:2111.06507v1 [math.NT] 12 Nov 2021.

[Bh2] Bhargava, M. The geometric sieve and the density of squarefree values of invariant polynomials (2014), arXiv:1402.0031v1.

[Bh3] Bhargava, M., The density of discriminants of quartic rings and fields, Annals of Mathematics (2005) 1031-1063.

[Bh4] Bhargava, M., The density of discriminants of quintic rings and fields, Annals of Mathematics (2010) 1559-1591.

[BSW] Bhargava, M., Shankar, A., Wang, X., Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces, arXiv preprint arXiv:1512.03035 (2015)

[Bo] Booker, A. R. Artin's conjecture, Turing's method and the Riemann hypothesis, Experimental Mathematics 15 (2006), no. 4, 385-407.

[Br] Browning, T.D. Power-free values of polynomials, Arch. Math. (Basel) 96 (2011), 139-150.

[BHB] Browning, T.D., Heath-Brown, D.R. Plane curves in boxes and equal sums of two powers, Math. Z. 251 (2005), 233-247.

[Ch] Chela, R. Reducible polynomials, J. Lond. Math. Soc. 38 (1963), 183-188.

[CD] Chow, S., Dietmann, R. Enumerative Galois theory for cubics and quartics, Adv. Math. 372 (2020): 107282.

[Cil] Cilleruelo, J. The least common multiple of a quadratic sequence, Compositio Math. 147 (2011), 1129-1150.

[DW] Datskovsky, B., Wright, D. J., Density of discriminants of cubic extensions, J. reine angew. Math 386 (1988) 116-138.

[DH] Davenport, H., Heilbronn, H., On the density of discriminants of cubic fields. II, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1971) 405-420.

[Di] Dietmann, R. Probabilistic Galois theory. Bull. London Math. Soc. 45(3), 453-462 (2013).

[Di2] Dietmann, R. On the distribution of Galois groups, accepted in Mathematika, see also arXiv:1010.5341.

[EV] Ellenberg, J. S., Venkatesh, A. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric Methods in Algebra and Number Theory,* volume 235 of Progr. Math., pages 151-168. Birkhäuser Boston, Boston, MA, 2005.

[Fel] Feller, W. An introduction to Probability Theory and Its Applications, vol. II, Wiley, New York, 1966.

[Gal] Gallagher, P. X. The large sieve and probabilistic Galois theory. In Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pages 91-101. Amer. Math. Soc., Providence, R.I., 1973.

[GJ] Gélin, A., Joux, A. Reducing number field defining polynomials: an application to class group computations. Algorithmic Number Theory Symposium XII, Aug 2016, Kaiserslautern, Germany. pp.315-331.

[GZ] Götze F., Zaporozhets D., Discriminant and root separation of integral polynomials. Reprinted in J. Math. Sci. (N.Y.) 219 (2016), no. 5, 700-706.

[GS] Granville A., Soundararajan, K. (2007) Sieving and the Erdős-Kac Theorem. In: Granville A., Rudnick Z. (eds) Equidistribution in Number Theory, An Introduction. NATO Science Series, vol 237. Springer, Dordrecht.

[HB] Heath-Brown, D.R. Counting rational points on algebraic varieties, Springer Lecture Notes 1891 (2006), 51-95.

[He] Hering, H. Seltenheit der Gleichungen mit Affekt bei linearem Parameter, Math. Ann. 186, 263-270 (1970).

[Hu] Huxley, M. N. The large sieve inequality for algebraic number fields, Mathematika 15 (1968), 178-187.

[Ku] Kuba, G. On the distribution of reducible polynomials. Mathematica Slovaca, 59:3 (2009), 349-356. Available at: degruyter.com/0131-6.

[LO] Lagarias, J.C., Odlyzdo, A.M. Effective versions of the chebotarev density theorem. In A. Frohlich, editor, Algebraic Number Fields, L-Functions and Galois Properties, pages 409-464. Academic Press, New York, London, 1977.

[LW] Lagarias, J. C., Weiss, B. L. Splitting behavior of S_n polynomials, arXiv:1408.6251.

[La] Lang, S. Algebraic number theory, Graduate Texts in Mathematics 110 2 ed. (1994) New York: Springer-Verlag.

[LMc] Lazard, D., McCallum, S. Iterated discriminants, J. Symb. Comp. 44 (2009), no. 9, 1176-1193.

[LT] Lemke Oliver, R. J., Thorne, F., Upper bounds on number fields of given degree and bounded discriminant (2020), arXiv:2005.14110v1.

[LT2] Lemke Oliver, R. J., Thorne, F., Upper bounds on number fields of given degree and bounded discriminant. Duke Math Journal, 2020.

[MS] Montgomery, H. and Soundararajan, K. (2004) Primes in short intervals, *Comm. Math. Phys.* 252, 589-617.

[MV] Montgomery, H, Vaughan, R., Multiplicative Number Theory I: Classical Theory, Cambridge University Press, 2007.

[MM] Ram M. Murty, Kumar V. Murty, Non-vanishing of L-Functions and Applications, Progress in Mathematics, 157, 1997th Edition.

[Na] Nagel, T. Généralisation d'un théorème de Tchebycheff Journal de mathématiques pures et appliquées 8e série, tome 4 (1921), p. 343-356.

[No] Noether, E. Ein algebraisches Kriterium für absolute Irreduzibilität, Math Ann. 85 (1922), 26-33.

[Os] Osada, H., The Galois group of the polynomial $x^n + ax^l + b$, Tôhoku Math. Journ., 39 (1987), 437-445.

[PS] Parades, M., Sasyk, R., Effective Hilbert's Irreducibility Theorem for global fields, arXiv:2202.10420v2 [math.NT], 2022.

[PTW] Pierce, L.B., Turnage-Butterbaugh, C.L. and Wood, M.M., An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups, 2017.

[RZ] Rudnick, Z., Zehavi, S. On Cilleruelo's conjecture for the least common multiple of polynomial sequences, arXiv:1902.01102v2 [math.NT] 15 Apr 2019.

[Sc] Schmidt, W. M. , Number fields of given degree and bounded discriminant, Astérisque 228 (1995), No. 4, 189-195.

[Sel] Selberg, A. Note on a paper by L.G. Sathe, J. Indian Math. Soc. 18 (1954), 83-87, MR 16, 676.

[Se] Serre, J-P. Quelques applications du théorème de densité de Chebotarev. Publ. Math. I.H.E.S. 54 (1981), 123-201; Oeuvres III, 563-641. Springer, Berlin, 1986.

[Tu] Turing, A., Some calculations of the Riemann zeta-function, Proc. London Math. Soc. (3), 3:99-117, 1953.

[Uc] Uchida, K. Unramified extensions of quadratic number fields, II, Tôhoku Math. Journ. 22 (1970), 220-224.

[Wa] van der Waerden, R. J. Die Seltenheit der reduziblen Gleichungen und der Gleichungenmit Affekt, Monatsh. Math. Phys., 43 (1936), No. 1, 133-147.

[Wi] Widmer, M. On number fields with nontrivial subfields, International Journal of NumberTheory 7 (2011), No. 3, 695-720.

Ilaria Viglino

Curriculum Vitae

Personal information

Address Ilaria Viglino - J 63, ETH Eidgenössische Technische Hochschule Zürich, Rämistrasse 101, 8092 Zürich, Switzerland.

E-mail ilaria.viglino@yahoo.it

Website https://math.ethz.ch/the-department/people.html?u=viglinoi

Phone +41 764 098 003

OrcID https://orcid.org/ 0000-0002-0230-5495

Education

Sept. 16 - Sept. 18 **MSc in Mathematics**, *Università degli studi di Genova*, IT, final grade: 110/110 cum laude
The Master's thesis was written under the supervision of Prof. Stefano Vigni and Prof. Sandro Bettin.

Sept. 13 - July 16 **BSc in Mathematics**, *Università degli studi di Genova*, IT, final grade: 110/110 cum laude
The Bachelor's thesis was written under the supervision of Prof. Stefano Vigni.

Employment history

Oct. 18 - Sep. 23 **PhD in Mathematics**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH, under the supervision of Prof. Emmanuel Kowalski.

Teaching activities

Jan. 23 - Aug. 23 **Teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Algebra II.

Jan. 23 - Aug. 23 **Coordinator**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Linear Algebra II.

Sept. 22 - Dec. 22 **Coordinator**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Linear Algebra I.

Jan. 22 - Aug. 22 **Coordinator**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Lineare Algebra und Statistik.

Jan. 22 - Aug. 22 **Teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Topologie.

Jan. 21 - Aug. 21 **Coordinator and teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Probabilistic Number Theory.

Sept. 21 - Dec. 21 **Coordinator and teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Commutative Algebra

Jan. 20 - Aug. 20 **Coordinator and teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Algebraic Geometry.

Jan. 20 - Aug. 20 **Coordinator**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Complex Analysis.

Sept. 19 - Dec. 19 **Coordinator and teaching assistant**, *ETH Eidgenössische Technische Hochschule*, Zürich, CH
Commutative Algebra.

Sept. 16 - June. 18 **Tutor**, *Università degli studi di Genova*, IT
Analysis I and Algebra I.

Personal skills

Languages Italian (Mothertongue), English (Proficient), German (Beginner), French (Matura), Spanish (Matura).

Computer LaTeX, CoCoA, C++, Matlab.

Contributions to conferences

28th Feb. 2023 **Number Theory Seminar**, *EPFL Lausanne*, CH
Invited speaker.

29th Nov. 2022 **Number Theory Seminar**, *Università degli studi di Genova*, IT
Invited speaker.

28th Mar. 2022 **Workshop: Young Scholars in the Analytic Theory of Numbers and Automorphic Forms**, *University of Bonn*, DE
Contributed talk.

1st June 2021 **Number Theory Online 2021**, *Università di Pisa, Sapienza Università di Roma, Università della Calabria, Università di Parma*
Invited speaker.

8th Nov. 2019 **Number Theory Seminar**, *Università degli studi di Genova*, IT
Contributed talk.