Where are the zeroes of a random p-adic polynomial?

Xavier Caruso

October 9, 2021

Abstract

We study the repartition of the roots of a random p-adic polynomial in an algebraic closure of $\mathbb{Q}_p$. We prove that the mean number of roots generating a fixed finite extension K of $\mathbb{Q}_p$ depends mostly on the discriminant of K, an extension containing less roots when it gets more ramified. We prove further that, for any positive integer r, a random p-adic polynomial of sufficiently large degree has about r roots on average in extensions of degree at most r.

Beyond the mean, we also study higher moments and correlations between the number of roots in two given subsets of $\mathbb{Q}_p$ (or, more generally, of a finite extension of $\mathbb{Q}_p$). In this perspective, we notably establish results highlighting that the roots tend to repel each other and quantify this phenomenon.

Contents

Introduction

The distribution of roots of a random real polynomial is a classical subject of research that has been thoroughly studied since the pioneer work of Bloch and Polya [4], Littlewood and Offord [13, 14, 15] and Kac's famous paper [10], in which an *exact* formula giving the avegare number of roots of a random polynomial with gaussian coefficients appears for the first time.

Investigating similarly the behaviour of roots of p-adic random polynomials is a natural question which have recently received some attention. The story starts in 2006 when Evans published the article [8], in which he managed to adapt Kac's strategy and eventually compute the average number of zeros in $\mathbb{Z}_p$ of a random polynomial of degree n with coefficients uniformly[1] distributed in $\mathbb{Z}_p$. The same year, Buhler, Goldstein, Moews and Rosenberg [5] found formulas for the probability that a random p-adic polynomial has all

[1] By uniform distribution, we mean the distribution coming from the Haar measure on the compact group $(\mathbb{Z}_p, +)$. It turns out that it is the correct p-adic analogue of the normal distribution.

its roots in $\mathbb{Q}_p$. After about ten years without further significant contributions, the subject was revived a couple of years ago by Lerario and his collaborators who started to undertake a systematical study of these phenomena. With Kulkarni [11], they notably extend Crofton's formula to the p-adic setting and derive new estimations on the number of roots of a p-adic polynomial, establishing in particular that a uniformly distributed random polynomial of fixed degree over $\mathbb{Z}_p$ has exactly one root in $\mathbb{Q}_p$ on average, independently from p and from the degree. On a slightly different note, Ait El Mannsour and Lerario [1] obtain formulas counting the average number of lines in random projective p-adic varieties. More recently, the case of nonuniform distributions has also been addressed by Shmueli [20], who came up with sharp estimations on the average number of roots.

Most of the aforementioned works are concerned with the *mean* of the random variable Z_n couting the number of roots of a p-adic polynomial of degree n. Beyond the mean (for which one can rely on Kac's techniques), obtaining more information about the Z_n's is a fundamental question that has been recently addressed and elegently solved by Bhargava, Cremona, Fisher and Gajović [3]. In their paper, they set up a general strategy to compute all probabilities Prob$[Z_n{=}r]$ with n and r running over the integers. In addition, they observed that the formulas they obtained are all rational functions in p which are symmetric under the transformation $p \leftrightarrow p^{-1}$. This beautiful and fascinating property remains nowadays quite mysterious.

Apart from the distinction between archimedean and nonarchimedean, $\mathbb{Q}_p$ differs from $\mathbb{R}$ in that its arithmetic is definitely much richer; while the absolute Galois group of $\mathbb{R}$ is somehow boring, that of $\mathbb{Q}_p$ is large, intricated and encodes much arithmetical subtle information. In other words, the set of finite extensions of $\mathbb{Q}_p$ has a prominent structure which is part of the strength and the complexity of the p-adic world. Therefore, looking at the roots of a random p-adic polynomial not only in $\mathbb{Q}_p$ but in an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ sounds like a very natural and appealing question, which is the one we address in the present paper.

To this end, we fix a finite extension F of $\mathbb{Q}_p$ together with an algebraic closure $\bar{F}$ of F. We endow $\bar{F}$ with the p-adic norm $\|\cdot\|$ normalized by $\|p\| = p^{-[F:\mathbb{Q}_p]}$ and use the letter q to denote the cardinality of the residue field of F. Given a positive integer n, a finite extension K of F and a compact open subset U of K, we introduce the random variable $Z_{U,n}$ counting the number of roots in U of a random polynomial of degree n with coefficients in the ring of integers $\mathcal{O}_F$ of F. Our first theorem gives an integral expression of the expected values of the $Z_{U,n}$'s.

Theorem A. *There exists a family of functions $\rho_{K,n} : K \to \mathbb{R}^+$ (K running over the set of finite extensions of F included in $\bar{F}$ and n running the set of positive integers) satisfying the following property: for any positive integer n, any extension finite extension K of F sitting inside $\bar{F}$ and any open subset U of E, we have:*

$$\mathbb{E}[Z_{U,n}] \;=\; \sum_{K' \subset K} \int_{U \cap K'} \rho_{K',n}(x)\, dx$$

where the sum runs over all extensions K' of F included in K.

The functions $\rho_{K,n}$'s are called the *density functions* as their values at a given point x reflect the number of roots one may expect to find in a small neighborhood of x. Our second theorem provides rather precise information about the density functions.

Theorem B. *Let n be a positive integer, let $K \subset \bar{F}$ be a finite extension of F and let $x \in K$. Write r for the degree of the extension K/F.*

1. (Vanishing) *If $F[x] \neq K$ or $n < r$, then $\rho_{K,n}(x) = 0$.*

2. (Continuity) *The function $\rho_{K,n}$ is continuous on K.*

3. (Invariance under isomorphisms) *Given a second finite extension L of F and an isomophism of F-algebras $\sigma : K \to L$, we have $\rho_{K,n}(x) = \rho_{L,n}\big(\sigma(x)\big)$.*

4. (Transformation under homography) *For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_F)$, we have:*

$$\rho_{K,n}\left(\frac{ax+b}{cx+d}\right) = \|cx+d\|^{2r} \cdot \rho_{K,n}(x).$$

5. (Monotony) *We have $\rho_{K,n}(x) \leq \rho_{K,n+1}(x)$ and the inequality is strict if and only if $F[x] = K$ and $r \leq n < 2r-1$.*

6. (Formulas for extremal degrees) *If $F[x] = K$ and $x \in \mathcal{O}_K$, then*

$$\rho_{K,r}(x) = \|D_K\| \cdot \frac{1}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)} \cdot \frac{q^{r+1}-q^r}{q^{r+1}-1}$$

$$\text{for } n \geq 2r-1, \quad \rho_{K,n}(x) = \|D_K\| \cdot \int_{\mathcal{O}_F[x]} \|t\|^r \, dt$$

where D_K is the discrimant of the extension K/F.

A first remarkable consequence of Theorem B is that the functions $\rho_{K,n}$ are independant of n provided that $n \geq 2r-1$. A similar behaviour was already noticed in [3] for higher moments of the random variables $Z_{F,n}$. Besides, it is in theory feasible to derive from Theorem B closed formulas for $\rho_{K,n}$ and its integral over K, at least when $n = r$ or $n \geq 2r-1$. For example, Theorem C below covers the case of quadratic extensions. Before stating it, it is convenient to introduce the notation:

$$\rho_n(K) = \int_K \rho_{K,n}(x) \, dx. \tag{1}$$

By Theorem A, $\rho_n(K)$ counts the number of roots of a random polynomial of degree n which fall inside K but outside all strict subfields of K containing F.

Theorem C. *Let K be a quadratic extension of F.*

(i) If K/F is unramified, we have:

$$\rho_2(K) = \frac{q^2-q+1}{q^2+q+1},$$

$$\text{for } n \geq 3, \quad \rho_n(K) = \frac{q^4+1}{q^4+q^3+q^2+q+1}.$$

(ii) If K/F is totally ramified, we have:

$$\rho_2(K) = \|D_K\| \cdot \frac{q^2}{q^2+q+1},$$

$$\text{for } n \geq 3, \quad \rho_n(K) = \|D_K\| \cdot \frac{q^2(q^2+1)}{q^4+q^3+q^2+q+1}.$$

When K is the quadratic unramified extension of F, we notice that $\rho_n(K)$ is a rational function in q which is self-reciprocal, *i.e.* invariant under the transformation $q \leftrightarrow q^{-1}$. As recalled previously, this remarkable property also holds for all higher moments of the random variable $Z_{F,n}$. On the contrary, when K/F is totally ramified, the function $\rho_n(K)$ is not self-reciprocal. One can nevertheless recover the expected symmetry by summing up over all totally ramified quadratic extensions of F. Indeed, using Serre's mass formula [18], we end up with:

$$\sum_K \rho_2(K) = \frac{2q}{q^2+q+1},$$
$$\text{for } n \geq 3, \quad \sum_K \rho_n(K) = \frac{2q(q^2+1)}{q^4+q^3+q^2+q+1}.$$

(where both sums run over all totally ramified quadratic extensions of F sitting inside $\bar{F}$) which are indeed self-reciprocal rational functions in q.

Another panel of interesting corollaries of Theorem B concerns the orders of magnitude of the functions $\rho_{K,n}$'s. Roughly speaking, Theorem B tells us that the size of $\rho_{K,n}$ is controlled by the p-adic norm of D_K. It is in fact even more transparent when we integrate over the entire space.

Theorem D. *Let $K \subset \bar{F}$ be a finite extension of F. Write r for the degree of K/F and f for its residuel degree. We have the estimations:*

$$\frac{\rho_r(K)}{\|D_K\|} = \left(1-\frac{1}{q}\right) \cdot \sum_{m|f} \mu\left(\frac{f}{m}\right) q^{m-f} + O\left(\frac{1}{q^f}\right)$$
$$\text{for } n \geq 2r-1, \quad \frac{\rho_n(K)}{\|D_K\|} = \sum_{m|f} \mu\left(\frac{f}{m}\right) q^{m-f} + O\left(\frac{1}{q^f}\right)$$

where μ denotes the Moebius function and the constants hidden in the $O(-)$ are absolute.

The dominant term in the two sums above is the summand corresponding to $m = f$ and is equal to 1. Hence, $\rho_n(K)$ is roughly equal to $\|D_K\|$ for $n = r$ or $n \geq 2r-1$. More precisely, one finds $\rho_n(K) = \|D_K\| \cdot (1 + O(q^{-1}))$ in both cases. It turns out that this conclusion continues to holds for all $n \geq r$ thanks to the monotony property of Theorem B.

One can also sum up the estimations of Theorem D over all extensions of a fixed degree. Doing so, we obtain the following theorem.

Theorem E. *For any positive integers r and n with $n \geq 2r-1$, we have the estimation:*

$$\sum_{K \in \mathbf{Ex}_r} \rho_n(K) = \sum_{m|r} \varphi\left(\frac{r}{m}\right) q^{m-r} + O\left(\frac{r \cdot \log\log r}{q^r}\right)$$

where $\mathbf{Ex}_r$ denotes the set of all extensions of F of degree r inside $\bar{F}$ and φ is the Euler's totient function.

Again, the dominant term in the sum of Theorem E corresponds to $m = r$ and its value is 1. Therefore, we conclude that a random polynomial of degree n has, on average, one root in the ground field F, one more root in the union of extensions of degree 2, one more root in the union of extensions of degree 3, *etc.* until the degree n where all roots have been found. Many variations on this theme are possible; for example, one can prove that

all roots of a random polynomial lie in the maximal unramified extension of F expect $\frac{2}{q} + O\big(\frac{1}{q^2}\big)$ of them. On the other hand, we deduce from Theorem C that the quadratic totally ramified extensions of F contain $\frac{2}{q} + O\big(\frac{1}{q^2}\big)$ roots outside F. We then conclude that there is no more than $O\big(\frac{1}{q^2}\big)$ new roots in ramified extensions of degree at least 3.

On a different note, it is also quite instructive to study the fluctuations of the density functions $\rho_{K,n}$. Theorem B indicates that they are governed by the size of the $\mathcal{O}_F$-algebra generated by x. As a consequence, we deduce that elements which generate a large extension K but are close for the p-adic distance to a strict subfield of K have less chance to show up as a root of a random polynomial. In other words, if a root x of a random polynomial is congruent to an element of a given extension K modulo a large power of p, it is very likely that x actually lies in K. In some sense, subfields attract all roots in a neighborhood.

Beyond the mean, it is important to understand higher moments of the $Z_{U,n}$'s to draw a more precise picture of the behaviour of these random variables. We address this question by enlarging a bit our setting: instead of restricting ourselves to finite extensions of F, we consider more generally products of such extensions, *i.e.* finite étale algebras over F. The nice observation is that Theorem A admits a straightforward generalization to this extended framework. Applying it with $E = K^r$ (for some given finite extension K of F) provides information about the r-th moment of $Z_{K,d}$ and, more generally, sheds some light on the distribution of r-tuples of roots in K^r. For $K = F$ and $r = 2$, this yoga has already interesting consequences as it permits to compute the covariances between the $Z_{U,n}$'s for $U \subset F$.

Theorem F. *Let U and V be two balls in $\mathcal{O}_F$ that do not meet. Pick $u \in U$ and $v \in V$. We have:*

$$\frac{\mathrm{Cov}\big(Z_{U,n}, Z_{V,n}\big)}{\mathbb{E}[Z_{U,n}] \cdot \mathbb{E}[Z_{V,n}]} \;=\; -1 \;+\; \frac{(q+1)^2}{q^2+q+1} \cdot \|u-v\| \;-\; \frac{q}{q^2+q+1} \cdot \|u-v\|^4$$

for all $n \geq 3$.

Although the above formula might look unattractive at first glance, it is quite instructive. Indeed, to begin with, it indicates that $\mathrm{Cov}\big(Z_{U,n}, Z_{V,n}\big)$ vanishes if and only if $\|u-v\| = 1$. In other words, the random variables $Z_{U,n}$ and $Z_{V,n}$ are uncorrelated if and only if U and V are sufficiently far away. Otherwise, $Z_{U,n}$ and $Z_{V,n}$ are correlated and the covariance is always negative (still assuming that $U \cap V = \emptyset$). Moreover, the correlation gets more and more significant when U and V gets closer. This tends to show that roots repel each other. This conclusion can been understood as a consequence of the general principle that subalgebras attract roots; indeed, noticing that F embeds diagonally into F^2, the above principle tells us that if we are given two nearby roots in F of a random polynomial, there is a huge chance that those roots actually coincide, which exactly means that it is unlikely to get nearby distinct roots.

Another amazing benefit of working with étale extensions is the existence of mass formulas for the density functions in the spirit of Bhargava's extension to étale algebras of the classical Serre mass formula [2]. Given a finite étale F-algebra E, define $\rho_n(E)$ by the integral of Eq. (1) and let $\mathrm{Aut}_{F\text{-alg}}(E)$ denote the group of F-automorphisms of E.

Theorem G. *For any positive integers r and n with $n \geq r$, we have:*

$$\sum_{E \in \mathbf{\acute{E}t}_r} \frac{\rho_n(E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} \;=\; 1 \tag{2}$$

where the summation set $\mathbf{\acute{E}t}_r$ *consists of all isomorphism classes of étale extensions* E *of* F *of degree* r *(and the notation* $\#$ *refers to the cardinality).*

When $r = 1$, Eq. (2) reduces to $\rho_n(F) = 1$ and so asserts that a random polynomial of degree at least 1 has exactly one root in F on average; we then recover Lerario and Kulkarni's result in this case. When r grows, Theorem G roughly says that the above remarkable property continues to hold if we count (weighted) roots in extensions of a fixed degree provided that we pay attention to include all étale algebras, and not only fields! Notice however that Theorem D shows that the contribution of actual extensions to the sum in Eq. (2) is about $1/r$. The most significant part of the mass then comes from nontrivial products of smaller degree extensions.

Organization of the article. The plan of the article follows closely the progression of the introduction. In Section 1, we prove Theorems A and B. In Section 2, we study examples and obtain closed formulas for the density functions in several simple cases. In addition of treating completely the case of quadratic extension (in line with Theorem C), we obtain partial results for extensions of prime degrees and for unramified extensions. Section 3 is devoted to finding estimations of orders of magnitude of the density functions and their integrals; we notably prove Theorems D and E there. Finally, in Section 4, we present the setup of étale algebras and extend Theorems A and B to this setting. We then discuss applications to higher moments and mass formulas for density functions, establishing Theorems F and G.

Notations. Throughout the article, we fix a prime number p, a finite extension F of $\mathbb{Q}_p$ and an algebraic closure $\bar{F}$ of F. We use the letter q to denote the cardinality of the residue field of F. We write $\|\cdot\|$ for the p-adic norm on $\bar{F}$, normalized by $\|p\| = p^{-[F:\mathbb{Q}_p]}$.

We let Ω_n be the space of polynomials of degree at most n with coefficients in $\mathcal{O}_F$; we call μ_n the probability measure on Ω_n corresponding to $\lambda_F^{\otimes n+1}$ under the canonical identification $\Omega_n \simeq \mathcal{O}_F^{n+1}$. In a slight abuse of notations, we continue to write $\|\cdot\|$ for the norm on Ω_n corresponding to the sup norm on $\mathcal{O}_F^{n+1}$ (it is the so-called *Gauss norm*).

Throughout the article, all finite extensions of F are implicitely supposed to be contained in $\bar{F}$. If K is such an extension, we denote by $\mathcal{O}_K$ its ring of integers and by $\mathcal{O}_K^\times$ the group of invertible elements of $\mathcal{O}_K$. We let λ_K be the Haar measure on K normalized by $\lambda_K(\mathcal{O}_K) = 1$. Our normalization choices lead to the transformation formula $\lambda_K(aH) = \|a\|^r \cdot \lambda_K(H)$ where r is the degree of the extension K/F.

Finally, we use the notation $\#A$ to denote the cardinality of a set A.

1 Density functions

The aim of this section is to define the density functions $\rho_{K,n}$ and to prove Theorems A and B. The main ingredient we shall need is a p-adic version of the famous Kac-Rice formula which gives an integral expression for a number of roots of a polynomial. We will establish it in §1.1. In §1.2, we carry out a key computation which will allow us to construct the density functions and prove Theorem B in §1.3. We finally move to the computation of expected number of roots and prove Theorem A is §1.4.

1.1 The p-adic Kac-Rice formula

A p-adic version of the Kac-Rice formula already appears in the pioneer work of Evans [8]. Nevertheless, for the purpose of this article, it will be more convenient to use a different formulation from that of Evans (the latter being actually closer to what we usually call the "area formula"). For this reason, we prefer taking some time to establish our version of the p-adic Kac-Rice formula and giving a complete proof of it. We refer to [17, Chapter 5] for the definition of strictly differentiable functions of the p-adic variable.

Theorem 1.1. *Let K be a finite extension of F of degree r. Let U be a compact open subset of K and let $f : U \to K$ be a strictly differentiable function. We assume that $(f(x), f'(x)) \neq (0,0)$ for all $x \in U$. Then:*

$$\#f^{-1}(0) = \lim_{s\to\infty} q^{sr} \cdot \int_U \|f'(x)\|^r \cdot \mathbb{1}_{\{\|f(x)\|\leq q^{-s}\}}\, dx. \tag{3}$$

Proof. Throughout the proof, we denote by B_s the closed ball of K of radius q^{-s} and center 0. If π denotes a uniformizer of K, the set B_s can be alternatively defined by $B_s = \pi^s \mathcal{O}_K$. We deduce from the latter equality that $\lambda_K(B_s) = \|\pi\|^{sr} = q^{-sr}$.

We consider an element $a \in U$ such that $f(a) = 0$. From our assumption, we know that $f'(a) \neq 0$. Therefore, applying [6, Lemma 3.4], we get the existence of a positive integer S_a having the following property: for any integer $s \geq S_a$, the function f induces a bijection from $a + f'(a)^{-1}B_s$ to B_s. Up to enlarging S_a, we can further assume that $\|f'(x)\| = \|f'(a)\|$ for all $x \in B_{S_a}$. We deduce for these two facts that:

$$\int_{a+B_{S_a}} \|f'(x)\|^r \cdot \mathbb{1}_{\{\|f(x)\|\leq q^{-s}\}}\, dx = \|f'(a)\|^r \cdot \lambda_K\big(f'(a)^{-1}B_s\big) = q^{-sr} \tag{4}$$

for all $s \geq S_a$.

From the previous discussion, we also derive that a is the unique zero of f in B_{S_a}. In other words, the set of zeros of f is discrete. By compacity, it follows that f has only finitely many zeros in U. Let us call them $a_1, \ldots, a_m$. Set $S = \max(S_{a_1}, \ldots, S_{a_m})$ and, for $i \in \{1, \ldots, m\}$, write $U_i = a_i + B_{S_{a_i}}$. Up to enlarging again the S_{a_i}'s, we can assume that the U_i's are pairwise disjoint. Summing up the equalities (4), we find:

$$\sum_{i=1}^{m} \int_{U_i} \|f'(x)\|^r \cdot \mathbb{1}_{\{\|f(x)\|\leq q^{-s}\}}\, dx = m \cdot q^{-sr} \tag{5}$$

provided that $s \geq S$. Let V be the complement in U of $U_1 \sqcup \cdots \sqcup U_m$. It is compact and the function f does not vanish on it. Hence, if s is large enough, we have $\|f(x)\| > q^{-s}$ for all $x \in V$. For those s, we thus get:

$$\int_V \|f'(x)\|^r \cdot \mathbb{1}_{\{\|f(x)\|\leq q^{-s}\}}\, dx = 0. \tag{6}$$

Combining Eqs. (5) and (6), we find that the equality:

$$q^{sr} \cdot \int_U \|f'(x)\|^r \cdot \mathbb{1}_{\{\|f(x)\|\leq q^{-s}\}}\, dx = m$$

holds true when s is sufficiently large. Passing to the limit, we get the theorem. □

We underline that the compacity assumption in Theorem 1.1 cannot be relaxed. For example, taking simply $U = \mathbb{Z}_p \backslash \{0\}$ and $f : x \mapsto x$, one sees that f have no zero in U while the right hand side of Eq. (3) converges to 1. Roughly speaking, the integral continues to see the missing zero at the origin, which is expected because removing one point from the domain of integration does not alter the value of the integral.

Similarly, the assumption that the zeros of f are nondegenerate (*i.e.* that the derivative does not vanish at these points) is definitely necessary. For example, if we take the function $f : \mathbb{Z}_p \to \mathbb{Q}_p$, $x \mapsto x^2$, a simple calculation shows that the right hand side of Eq. (3) converges to $\frac{p}{p+1} < 1$. More generally, one can prove that, if f is a polynomial whose roots in U are $a_1, \ldots, a_m$ and have multiplicity $\mu_1, \ldots, \mu_m$ respectively, then the right hand side of Eq. (3) converges to:

$$\sum_{i=1}^{m} \frac{q^{\mu_i} - q^{\mu_i - 1}}{q^{\mu_i} - 1}.$$

In other words, a root of multiplicity μ does not contribute for 1 but for $\frac{q^\mu - q^{\mu-1}}{q^\mu - 1} < 1$.

1.2 A key computation

Let K be a finite of F of degree r and let U be an open subset of K. We aim at computing the expected value of random variable $Z_{U,n} : \Omega_n \to \mathbb{Z} \cup \{+\infty\}$ defined by:

$$\begin{aligned} Z_{U,n}(P) &= \#\left\{ x \in U \text{ s.t. } f(x) = 0 \right\} \\ &= \lim_{s \to \infty} q^{sr} \cdot \int_U \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}\, dx \end{aligned}$$

the second equality coming from Theorem 1.1. For this, roughly speaking, we would like to write down the following calculation:

$$\begin{aligned} \mathbb{E}[Z_{U,n}] = \int_{\Omega_n} Z_{U,n}(P) dP &= \int_{\Omega_n} \lim_{s \to \infty} q^{sr} \cdot \int_U \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}\, dx\, dP \\ &= \int_U \lim_{s \to \infty} q^{sr} \cdot \int_{\Omega_n} \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}\, dP\, dx \end{aligned}$$

and introduce the density function defined by:

$$x \mapsto \lim_{s \to \infty} q^{sr} \cdot \int_{\Omega_n} \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}\, dP. \tag{7}$$

However, we have to be a bit more careful because the above limit does not behave quite well everywhere: it takes infinite values on certain subspaces but it turns out that those parts lead to a finite positive contribution when we integrate. The next proposition shows that these issues are somehow localized on strict subfields.

Proposition 1.2. *If $n \geq r$ and if x lies in $\mathcal{O}_K$ and generates K over F, the limit in Eq.* (7) *exists and is equal to:*

$$\frac{\|D_K\|}{\#\big(\mathcal{O}_K / \mathcal{O}_F[x]\big)} \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r\, dQ$$

where D_K denotes the discriminant of the extension K/F.

Proof. For simplicity, write:

$$I_s = q^{sr} \cdot \int_{\Omega_n} \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}\, dP.$$

Let Z be the minimal monic polynomial of x over F. By our assumptions, Z has degree r and coefficients in $\mathcal{O}_F$. This implies that the map $\Omega_{n-r} \times \Omega_{r-1} \to \Omega_n$ taking (Q, R) to $QZ + R$ preserves the measure. Performing the corresponding change of variables, we end up with the equality:

$$\begin{aligned} I_s &= q^{sr} \cdot \int_{\Omega_{r-1}} \int_{\Omega_{n-r}} \|Q(x)Z'(x) + R'(x)\|^r \cdot \mathbb{1}_{\{\|R(x)\| \leq q^{-s}\}} \, dQ \, dR \\ &= q^{sr} \cdot \int_{\Omega_{r-1}} \left(\int_{\Omega_{n-r}} \|Q(x)Z'(x) + R'(x)\|^r \, dQ \right) \mathbb{1}_{\{\|R(x)\| \leq q^{-s}\}} \, dR \end{aligned}$$

We consider the evaluation morphism $\alpha_x : F \otimes_{\mathcal{O}_F} \Omega_{r-1} \to K$ taking a polynomial R to $R(x)$. It is F-linear and bijective since the domain of α_x is restricted to polynomials of degree strictly less than r. Its inverse α_x^{-1} is F-linear and so, it is continuous. Thus, there exists a positive constant γ such that $\|R(x)\| \geq \gamma \cdot \|R\|$ for all $R \in \Omega_{r-1}$.

Let us assume for a moment that we are given a polynomial $R \in \Omega_{r-1}$ such that $\|R(x)\| \leq q^{-s}$. By what precedes, we find that $\|R\| \leq \gamma^{-1} q^{-s}$, from what we further deduce that $\|R'(x)\| \leq \gamma^{-1} q^{-s}$. Since $Z'(x)$ does not vanish, we conclude that $Z'(x)$ must divide $R'(x)$ provided that s is large enough. One can then perform the change of variables $Q \mapsto Q - \frac{R'(x)}{Z'(x)}$ in the inner integral and get:

$$\begin{aligned} \int_{\Omega_{n-r}} \|Q(x)Z'(x) + R'(x)\|^r \, dQ &= \int_{\Omega_{n-r}} \|Q(x)Z'(x)\|^r \, dQ \\ &= \|Z'(x)\|^r \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ. \end{aligned}$$

We are then left with:

$$I_s = q^{sr} \cdot \|Z'(x)\|^r \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ \cdot \int_{\Omega_{r-1}} \mathbb{1}_{\{\|R(x)\| \leq q^{-s}\}} \, dR. \tag{8}$$

In order to estimate the last factor, we come back to the evaluation morphism α_x. Since it is a F-linear isomorphism, it must act on the measures by multiplication by some scalar (namely, its determinant). In other words, there exists a positive constant δ such that $\lambda_K(\alpha_x(H)) = \delta \cdot \mu_n(H)$ for all measurable subset H of Ω_{r-1}. Taking $H = \Omega_{r-1}$, we find

$$\delta = \lambda_K\big(\alpha_x(\Omega_{r-1})\big) = \lambda_K\big(\mathcal{O}_F[x]\big) = \frac{1}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)}.$$

As in the proof of Theorem 1.1, we let B_s be the closed ball of K of radius q^{-s} centered at 0. By definition $\alpha_x^{-1}(B_s)$ consists of polynomials R such that $\|R(x)\| \leq q^{-s}$. Moreover, if s is sufficiently large, $\alpha_x^{-1}(B_s)$ sits inside Ω_{r-1}, and so:

$$\begin{aligned} \int_{\Omega_{r-1}} \mathbb{1}_{\{\|R(x)\| \leq q^{-s}\}} \, dR &= \mu_n\big(\alpha_x^{-1}(B_s)\big) \\ &= \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) \cdot \lambda_K(B_s) = \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) \cdot q^{-sr}. \end{aligned}$$

Plugging this input in Eq. (8), we end up with:

$$I_s = \|Z'(x)\|^r \cdot \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ \tag{9}$$

when s is sufficiently large. The sequence $(I_s)_{s \geq 0}$ is then eventually constant and converges to the limit given by the above formula. In order to conclude the proof of the

proposition, it remains to relate the norm of $Z'(x)$ with that of the discriminant of K. We endow K with the symmetric F-bilinear form $b : K \times K \to F$, $(u, v) \mapsto \mathrm{Tr}_{K/F}(uv)$. Let also $\mathcal{B}_x = (1, x, \dots, x^{r-1})$ be the canonical basis of $\mathcal{O}_F[x]$ over $\mathcal{O}_F$ and set $\mathcal{B}'_x = \big(\frac{x^{r-1}}{Z'(x)}, \frac{x^{r-2}}{Z'(x)}, \dots, \frac{1}{Z'(x)}\big)$. Both $\mathcal{B}_x$ and $\mathcal{B}'_x$ are F-basis of K and it follows from [19, §III.6, Lemma 2] that the matrix of b in the basis $\mathcal{B}_x$ and $\mathcal{B}'_x$ is lower-triangular with all diagonal entries equal to 1. Its determinant is then 1 as well. Performing a change of basis, we find that:

$$\det \mathrm{Mat}_{\mathcal{B}_x}(b) = \pm\, N_{K/F}\big(Z'(x)\big)$$

where, by definition, $\mathrm{Mat}_{\mathcal{B}_x}(b)$ is the matrix of b in $\mathcal{B}_x$ and $N_{K/F}$ is the norm of K over F. We now consider a basis $\mathcal{B}$ of $\mathcal{O}_K$ over $\mathcal{O}_F$. By definition, the discriminant of K is the determinant of $\mathrm{Mat}_{\mathcal{B}}(b)$. Therefore, if P denotes the transition matrix from $\mathcal{B}$ to $\mathcal{B}_x$, we derive from the change-of-basis formula that $\det \mathrm{Mat}_{\mathcal{B}_x}(b) = (\det P)^2 \cdot D_K$ and so:

$$N_{K/F}\big(Z'(x)\big) = \pm\, (\det P)^2 \cdot D_K.$$

On the other hand, noticing that P is also the matrix of α_x in the canonical basis, we deduce that:

$$\|\det P\| = \lambda_K\big(\mathcal{O}_F[x]\big) = \frac{1}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)}.$$

Combining the two previous equalities, we end up with:

$$\|Z'(x)\|^r = \|N_{K/F}\big(Z'(x)\big)\| = \frac{1}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)^2} \cdot \|D_K\|.$$

Plugging this relation in Eq. (9), we obtain the proposition. □

1.3 Construction and properties of the density functions

In this subsection, we construct the density functions $\rho_{K,n}$ and establish Theorem B.

Definition 1.3. Let n be a positive integer and K be a finite extension of F of degree r. For $x \in \mathcal{O}_K$, we set:

$$\begin{aligned} \rho_{K,n}(x) &= \frac{\|D_K\|}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)} \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ \qquad && \text{if } n \geq r \text{ and } F[x] = K, \\ &= 0 && \text{otherwise.} \end{aligned}$$

For $x \in K$, $x \notin \mathcal{O}_K$, we set $\rho_{K,n}(x) = \|x\|^{-2r} \cdot \rho_{K,n}(x^{-1})$.

The first part of Definition 1.3 is exactly what we expect after Proposition 1.2. As for the second part, it is motivated by the observation that the transformation $P(X) \mapsto X^n P(X^{-1})$ preserves the measures on Ω_n and changes a root x into x^{-1}. In any case, we notice that, since K is a discrete valuation field, we have $x \in \mathcal{O}_K$ or $x^{-1} \in \mathcal{O}_K$ for all $x \in K$. Defintion 1.3 then makes sense and leads to a well-defined function $\rho_{K,n} : K \to \mathbb{R}^+$, which is called the *density function* on K of degree n.

The rest of this subsection is devoted to the proof of Theorem B. The vanishing property and the invariance under isomorphisms (Statements 1 and 3 respectively) are clear from the definitions. In what follows, we address the other items of Theorem B one by one (in a slightly different order).

1.3.1 Continuity

The function

$$x \mapsto \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ$$

is continuous on $\mathcal{O}_K$ as the integrand is obviously bounded, positive and continuous on $\Omega_{n-r} \times \mathcal{O}_K$.

Let $x \in \mathcal{O}_K$ such that $F[x] = K$. In this case, the index of $\mathcal{O}_F[x]$ in $\mathcal{O}_K$ is the inverse of the p-adic norm of the determinant of the matrix $M(x)$ whose i-th column is filled with the coordinates of x^i in a fixed basis of $\mathcal{O}_K$. If y is a second element of $\mathcal{O}_K$ which is congruent to x modulo p^s for some integer s, then the matrices $M(x)$ and $M(y)$ are also congruent modulo p^s and so are their determinants. In other words, if $\|x - y\| \leq \varepsilon$ for some positive real number ε, then $\|\det M(x) - \det M(y)\| \leq \varepsilon$ as well. It follows that $\|\det M(x)\| = \|\det M(y)\|$, that is $\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) = \#\big(\mathcal{O}_K/\mathcal{O}_F[y]\big)$, as soon as $\varepsilon < \|\det M(x)\|$. This proves that the function $y \mapsto \#\big(\mathcal{O}_K/\mathcal{O}_F[y]\big)$ is constant in some neighborhood of x; in particular, it is continuous at x and so is $\rho_{K,n}$.

We now consider the case where $F[x] \neq K$. Set $L = F[x]$ and let d denote the degree of the extension L/F. We consider a second element $y \in \mathcal{O}_K$ such that $F[y] = K$ and $x \equiv y \pmod{p^s}$ for some given integer s. We then have the inclusion $\mathcal{O}_F[y] \subset \mathcal{O}_L + p^s\mathcal{O}_K$, from what we derive the estimation:

$$\#\big(\mathcal{O}_K/\mathcal{O}_F[y]\big) \geq \#\big(\mathcal{O}_K/(\mathcal{O}_L + p^s\mathcal{O}_K)\big) = \|p\|^{s(d-r)} \geq \|x - y\|^{d-r}.$$

Since $d < r$, we deduce that the quantity $\#\big(\mathcal{O}_K/\mathcal{O}_F[y]\big)$ goes to ∞ when y approches x, from what we conclude that $\rho_{K,n}$ is continuous at x.

Finally, the continuity on K immediately follows from that on $\mathcal{O}_K$.

1.3.2 Transformation under homography

It is enough to prove the transformation formula for the matrices

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} (a \in \mathcal{O}_F^\times) \quad ; \quad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} (a \in \mathcal{O}_F) \quad ; \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

since they generate $\mathrm{GL}_2(\mathcal{O}_F)$. It is obvious for scalars matrices.

For the second family of matrices, we have to check $\rho_{K,n}(x + a) = \rho_{K,n}(x)$ for $x \in K$ and $a \in \mathcal{O}_F$. Let us assume first that $x \in \mathcal{O}_K$. Then $\mathcal{O}_F[x] = \mathcal{O}_F[x + a]$. Moreover, the map $\Omega_{n-r} \to \Omega_{n-r}$, $Q(X) \mapsto Q(X + a)$ preserves the measure, implying that:

$$\int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ = \int_{\Omega_{n-r}} \|Q(x + a)\|^r \, dQ$$

We conclude that the equality $\rho_{K,n}(x + a) = \rho_{K,n}(x)$ is correct in this case. We assume now that $x \notin \mathcal{O}_K$, *i.e.* $\|x\| > 1$. Since a lies in $\mathcal{O}_F$, we have $\|a\| \leq 1$ and so $\|x + a\| = \|x\|$. Setting $y = x^{-1}$ we are then reduced to prove that $\rho_{K,n}(y) = \rho_{K,n}(z)$ with $z = \frac{y}{1+ay}$. Observing that $\|y\| < 1$, we can write a series expansion for the inverse of $1 + ay$ and eventually get:

$$z = \sum_{i \geq 0} (-1)^i a^i y^{i+1} \in \mathcal{O}_F[y].$$

Similarly, we prove that $y \in \mathcal{O}_F[z]$ and hence $\mathcal{O}_F[y] = \mathcal{O}_F[z]$. We consider the transformation $\tau : \Omega_{n-r} \to \Omega_{n-r}$ defined by $\tau\big(Q(X)\big) = X^{n-r}Q(X^{-1})$. It is explicity given by the formula:

$$\tau\big(a_{n-r}X^{n-r} + \cdots + a_1X + a_0\big) = a_0X^{n-r} + a_1X^{n-r-1} + a_{n-r}$$

and hence preserves the measure. Therefore:

$$\begin{aligned}\int_{\Omega_{n-r}} \|Q(y)\|^r \, dQ &= \|y\|^{n-r} \cdot \int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ \\ &= \|y\|^{n-r} \cdot \int_{\Omega_{n-r}} \|Q(x+a)\|^r \, dQ \\ &= \|y\|^{n-r} \cdot \|x+a\|^{n-r} \cdot \int_{\Omega_{n-r}} \|Q(z)\|^r \, dQ.\end{aligned}$$

In addition, we remark that $y(x+a) = 1 + ay$ has norm 1. We then end up with:

$$\int_{\Omega_{n-r}} \|Q(y)\|^r \, dQ = \int_{\Omega_{n-r}} \|Q(z)\|^r \, dQ$$

which eventually lefts us with the desired equality $\rho_{K,n}(y) = \rho_{K,n}(z)$.

It remains to treat the case of the antidiagonal matrix, which amounts to proving that $\rho_{K,n}(x^{-1}) = \|x\|^{2r}\rho_{K,n}(x)$. It is obvious from the definition when $x \notin \mathcal{O}_K$ or $x^{-1} \notin \mathcal{O}_K$. We may then assume that x is invertible in $\mathcal{O}_K$, *i.e.* $\|x\| = 1$. In this situation, using again that τ preserves the measure, we find:

$$\int_{\Omega_{n-r}} \|Q(x)\|^r \, dQ = \int_{\Omega_{n-r}} \|Q(x^{-1})\|^r \, dQ.$$

Let Z be the minimal polynomial of x. The constant coefficient of Z is the norm of x up to a sign. Hence it has norm 1, which means that it is invertible in $\mathcal{O}_F$. It follows from this observation that x^{-1} can be expressed as a polynomial in x with coefficients in $\mathcal{O}_F$, that is $x^{-1} \in \mathcal{O}_F[x]$. Similarly, one has $x \in \mathcal{O}_F[x^{-1}]$. Combining both results, we get $\mathcal{O}_F[x] = \mathcal{O}_F[x^{-1}]$, from what we deduce the desired equality.

1.3.3 Formulas for extremal degrees

When $n = r$, the density function $\rho_{r,K}$ is defined by:

$$\rho_{r,K}(x) = \frac{\|D_K\|}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)} \cdot \int_{\mathcal{O}_F} \|t\|^r \, dt.$$

Let π be a fixed uniformizer of F and set $U_s = \pi^s\mathcal{O}_F^\times$. We observe that U_s consists exactly of elements of norm q^{-s} and that $\mathcal{O}_F\backslash\{0\}$ is the disjoint union of the U_s. It follows from these observations that:

$$\int_{\mathcal{O}_F} \|t\|^r \, dt = \sum_{s=0}^{\infty} \int_{U_s} \|t\|^r \, dt = \sum_{s=0}^{\infty} \lambda_F(U_s) \cdot q^{-sr}.$$

Besides, the measure of U_s can be computed as follows:

$$\lambda_F(U_s) = \lambda_F(\pi^s\mathcal{O}_F^\times) = \|\pi^s\| \cdot \lambda_F(\mathcal{O}_F^\times) = q^{-s} \cdot \left(1 - \frac{1}{q}\right).$$

We then conclude that:

$$\int_{\mathcal{O}_F} \|t\|^r \, dt = \left(1 - \frac{1}{q}\right) \cdot \sum_{s=0}^{\infty} q^{-sr-s} = \frac{q^{r+1} - q^r}{q^{r+1} - 1} \tag{10}$$

and the claimed formula follows.

We now move to the case $n \geq 2r-1$. We set $m = n - r$. Looking at the definition of $\rho_{K,n}$, we realize that it is enough to prove that:

$$\int_{\Omega_m} \|Q(x)\|^r \, dQ = \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) \cdot \int_{\mathcal{O}_F[x]} \|t\|^r \, dt.$$

As in the proof of Proposition 1.2, let Z denote the minimal polynomial of x and consider the measure-preserving morphism $\Omega_{m-r} \times \Omega_{r-1} \to \Omega_m$ mapping (S,T) to $SZ+T$. (We agree that $\Omega_{-1} = \{0\}$ when $m = r-1$.) Performing the corresponding change of variables, we obtain:

$$\int_{\Omega_m} \|Q(x)\|^r \, dQ = \int_{\Omega_{r-1}} \|T(x)\|^r \, dT.$$

In other words, we may assume that $m = r-1$, *i.e.* $n = 2r-1$. Following again the proof of Proposition 1.2, we consider the evaluation map $\alpha_x : \Omega_{r-1} \to \mathcal{O}_K$, $T(X) \mapsto T(x)$. We have seen that it acts on the measures by multiplication by $\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)^{-1}$. Therefore, performing the change of variables $t = \alpha_x(T)$, we obtain:

$$\int_{\Omega_{r-1}} \|T(x)\|^r \, dT = \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) \cdot \int_{\mathcal{O}_F[x]} \|t\|^r \, dt$$

which concludes the proof.

1.3.4 Monotony

From what precedes, it is clear that $\rho_{K,n}(x) = \rho_{K,n+1}(x)$ when $F[x] \neq K$ or $n < r$ or $n \geq 2r-1$. It is then enough to prove that $\rho_{K,n}(x) < \rho_{K,n+1}(x)$ in the remaining cases. Coming back to the definition of the density functions, this amounts to showing that:

$$\int_{\Omega_m} \|Q(x)\|^r \, dQ \; < \; \int_{\Omega_{m+1}} \|Q(x)\|^r \, dQ$$

provided that $0 \leq m < r-1$ and $F[x] = K$. Let $a \in \mathcal{O}_F$. By compacity, the function $\Omega_m \to \mathbb{R}$, $Q \mapsto \|ax^{m+1} + Q(x)\|$ attains its minimum. In other words, there exists a polynomial $Q_a \in \Omega_m$ such that $\|ax^{m+1} + Q_a(x)\| \leq \|ax^{m+1} + Q(x)\|$ for all $Q \in \Omega_m$. Write $\delta_a = \|ax^{m+1} + Q_a(x)\|$. Notice that $\delta_a > 0$; indeed, otherwise, x would be annihilated by a polynomial over F of degree $m+1 < r$, contradicting $F[x] = K$. Note also that δ_a depends only on the norm of a; in particular the function $a \mapsto \delta_a$ is measurable.

Lemma 1.4. *With the above notations, we have:*

$$\|ax^{m+1} + Q(x)\| = \max\big(\delta_a, \, \|(Q - Q_a)(x)\|\big)$$

for all $a \in \mathcal{O}_F$ and $Q \in \Omega_m$.

Proof. Putting $S = Q - Q_a$, the ultrametric triangle inequality gives:

$$\|ax^{m+1} + Q(x)\| \leq \max\big(\delta_a, \, \|S(x)\|\big) \tag{11}$$

with equality provided that $\|S(x)\| \neq \delta_a$. We then get the lemma under this additional assumption. On the contrary, when $\|S(x)\| = \delta_a$, we derive from the definition of Q_a that $\|ax^{m+1} + Q(x)\| \geq \delta_a$. We deduce that Eq. (11) is an equality in this case as well, which establishes the lemma. □

Separating the leading coefficient in the integral over Ω_{m+1}, we obtain:

$$\begin{aligned}\int_{\Omega_{m+1}} \|Q(x)\|^r \, dQ &= \int_{\mathcal{O}_F} \int_{\Omega_m} \|ax^{m+1} + Q(x)\|^r \, dQ \, da \\ &= \int_{\mathcal{O}_F} \int_{\Omega_m} \max\left(\delta_a^r, \, \|(Q - Q_a)(x)\|^r\right) dQ \, da \\ &= \int_{\mathcal{O}_F} \int_{\Omega_m} \max\left(\delta_a^r, \, \|Q(x)\|^r\right) dQ \, da\end{aligned}$$

which eventually shows that:

$$\int_{\Omega_{m+1}} \|Q(x)\|^r \, dQ \, \geq \, \int_{\Omega_m} \|Q(x)\|^r \, dQ$$

with strict inequality provided that the set of pairs $(a, Q) \in \mathcal{O}_F \times \Omega_m$ for which $\|Q(x)\| < \delta_a$ has positive measure. But, the latter property holds always true, being a consequence of the facts that $\delta_a = \delta_1 > 0$ for all $a \in \mathcal{O}_F^\times$ and that $\mathcal{O}_F^\times$ has positive measure in $\mathcal{O}_F$. This concludes the proof of Theorem B.

1.4 From density functions to average number of roots

We now focus on Theorem A. After Proposition 1.2, we are encouraged to treat separately roots lying in strict subextensions of K. We materialize this idea by introducing the notion of new roots.

Definition 1.5. Let K be a finite extension of F. An element $x \in \bar{F}$ is *new* in K if it is in K but not in any strict subextension of K.

Given an open subset U of a finite extension K of F together with a positive integer n, we define the random variable $Z_{U,f}^{\text{new}} : \Omega_n \to \mathbb{Z}$ taking a polynomial of P to the number of roots of P, which lie in U and are new in K. After what we have achieved so far, one strongly expects the mean value of $Z_{U,n}^{\text{new}}$ to be related to the integral of the expression of the limit which appears in Proposition 1.2.

Theorem 1.6. *Let n be a positive integer. Let K be a finite extension of F and let U be an open subset of K. Then:*

$$\mathbb{E}\big[Z_{U,n}^{\text{new}}\big] = \int_U \rho_{K,n}(x) \, dx. \tag{12}$$

Proof. As usual, let r be the degree of the extension K/F. Let K^{new} be the subset of K consisting of elements x for which $F[x] = K$. Since K contains only finitely many subextensions and each subextension is a closed subspace of K, we deduce that K^{new} is open in K. We set $\mathcal{O}_K^{\text{new}} = \mathcal{O}_K \cap K^{\text{new}}$.

To start with, we assume that U is compact and included in $\mathcal{O}_K^{\text{new}}$. We then have $Z_{U,n}^{\text{new}} = Z_{U,n}$. Since a random polynomial has almost surely only simple roots, we deduce from the p-adic Kac-Rice formula (*cf* Theorem 1.1) that:

$$\begin{aligned}\mathbb{E}[Z_{U,n}] &= \int_{\Omega_n} \lim_{s \to \infty} \int_U I_s(x, P) \, dx \, dP \\ \text{with} \quad I_s(x, P) &= q^{sr} \cdot \|P'(x)\|^r \cdot \mathbb{1}_{\{\|P(x)\| \leq q^{-s}\}}.\end{aligned}$$

It is clear that $I_s(x,P)$ is everywhere nonnegative. As in the proof of Theorem 1.1, let B_s be the closed ball of K of radius q^{-s} and center 0. From [8, Proposition 3.2], we deduce that:

$$\int_{P^{-1}(B_s)} \|P'(x)\|^r \, dx \;=\; \int_{B_s} \#P^{-1}(y)\, dy \;\leq\; n\lambda_K(B_s) \;=\; nq^{-rs}.$$

for any polynomial $P \in \Omega_n$. Hence:

$$\int_U I_s(x,P)\, dx = q^{sr} \int_{U\cap P^{-1}(B_s)} \|P'(x)\|^r \, dx \;\leq\; n.$$

We can then apply Lebesgue's dominated convergence theorem and get:

$$\mathbb{E}[Z_{U,n}] = \lim_{s\to\infty} \int_{\Omega_n}\int_U I_s(x,P)\, dx\, dP = \lim_{s\to\infty} \int_U \int_{\Omega_n} I_s(x,P)\, dP\, dx$$

the second equality coming from Fubini's theorem. We now want to use a similar argument to swap the limit on s and the integral over U. In order to proceed, we fix an element $x \in U$ and denote by $\alpha_x : F \otimes_{\mathcal{O}_F} \Omega_n \to K$ the evaluation morphism at x already considered in the proof of Proposition 1.2. Noticing that $\|P'(x)\|^r \leq 1$ for all $P \in \Omega_n$, we find:

$$\begin{aligned}\int_{\Omega_n} I_s(x,P)\, dP &\leq q^{sr} \cdot \mu_n\big(\Omega_n \cap \alpha_x^{-1}(B_s)\big) \\ &\leq q^{sr} \cdot \mu_n\big(\alpha_x^{-1}(B_s)\big) = \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big).\end{aligned}$$

We have seen in §1.3.1 that the function $x \mapsto \#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)$ is continuous; hence it is integrable on the compact set U. The dominated convergence theorem then again applies and gives:

$$\mathbb{E}[Z_{U,n}] = \int_U \lim_{s\to\infty} \int_{\Omega_n} I_s(x,P)\, dP\, dx = \int_U \rho_{K,n}(x)\, dx.$$

Theorem 1.6 is then proved when U is compact and included in $\mathcal{O}_K^{\text{new}}$.

One can extend the result to any open subset of $\mathcal{O}_K$ using a standard limit argument. Precisely, if U is open in $\mathcal{O}_K$, one can construct an increasing sequence $(U_m)_{m\geq 0}$ of compact open subsets of $\mathcal{O}_K^{\text{new}}$ such that $\bigcup_{m\geq 0} U_m = U \cap \mathcal{O}_K^{\text{new}}$. Applying what we have done before with U_m, we find:

$$\mathbb{E}[Z_{U_m,n}] = \int_{U_m} \rho_{K,n}(x)\, dx. \tag{13}$$

Moreover the sequence $Z_{U_m,n}$ is nondecreasing and simply converges to $Z_{U,n}^{\text{new}}$. By the monotone convergence theorem, we find that $\mathbb{E}[Z_{U_m,n}]$ converges to $\mathbb{E}[Z_{U,n}^{\text{new}}]$. Passing to the limit in Eq. (13), we obtain the theorem for U.

For a general U, we write $U = U_0 \sqcup U_\infty$ with $U_0 = U \cap \mathcal{O}_K$ and $U_\infty = U \backslash U_0$. Since both sides of Eq. (12) are additive with respect to U, it is enough to prove the theorem for U_∞. For this, as in §1.3.2, we consider the measure-preserving map $\tau : \Omega_n \to \Omega_n$ defined by:

$$\tau\big(a_nX^n + \cdots + a_1X + a_0\big) = a_0X^n + \cdots + a_{n-1}X + a_n.$$

An element $x \in K$ is a root of a polynomial P if and only if x^{-1} is a root of $\tau(P)$. It is also obvious that $x \in K^{\text{new}}$ if and only if $x^{-1} \in K^{\text{new}}$. Thus we get $\mathbb{E}\big[Z_{U_\infty,n}^{\text{new}}\big] = \mathbb{E}\big[Z_{V_\infty,n}^{\text{new}}\big]$ where V_∞ is the image of U_∞ under the map $x \mapsto x^{-1}$. Besides $V_\infty \subset \mathcal{O}_K$; we can then apply the theorem with V_∞ and conclude that:

$$\mathbb{E}\big[Z_{U_\infty,n}^{\text{new}}\big] = \int_{V_\infty} \rho_{K,n}(x)\, dx = \int_{U_\infty} \rho_{K,n}(x^{-1}) \cdot \|x\|^{-2r}\, dx = \int_{U_\infty} \rho_{K,n}(x)\, dx$$

which finally proves the theorem in all cases. □

We conclude this section by explaining how Theorem A can be derived from Theorem 1.6. It is actually quite easy once we have notice that, given a finite extension E of F, any root $x \in K$ of a polynomial $P \in \Omega_n$ is new in a unique subextension K' of E, namely $K' = F[x]$. Hence, if U is an open subset of E, one has:

$$Z_{U,n} = \sum_{K' \subset K} Z^{\text{new}}_{U \cap K',n}$$

and Theorem A follows by additivity of the mean.

2 Examples and closed formulas

As we have seen in Section 1, the distribution of roots in $\bar{F}$ of a random polynomial of degree n over $\mathcal{O}_F$ are governed by the density functions $\rho_{K,n}$. However, it is not clear so far how useful could be this result for deriving explicit formulas, given that the density functions are defined by somehow intricated integral expressions which do not look easily tractable at first glance.

The aim of this section is to get more familiar with those integrals and fully compute them in certain simple cases. The case of quadratic extensions will be covered in full generality in §2.1, culminating with a proof of Theorem C. Partial results in the case of prime degree extensions and unramified extensions will be given in §2.2 and §2.3 respectively.

Before getting to the heart of the matter and dealing with extensions, it is important to elucidate the case of the ground field F itself. This base case is addressed by the following proposition.

Proposition 2.1. *For all positive integer n and all $x \in F$, we have:*

$$\begin{aligned} \rho_{F,n}(x) &= \frac{q}{q+1} && \text{if } x \in \mathcal{O}_F \\ &= \frac{q}{q+1} \cdot \|x\|^{-2} && \text{otherwise.} \end{aligned}$$

Proof. It follows from Theorem B that $\rho_{F,n}$ does not depend on n provided that $n \geq 1$. The values of $\rho_{F,n}$ on $\mathcal{O}_F$ aren the given by the explicit formula for $\rho_{F,1}(x)$ which appears again in Theorem B. The values on $F \backslash \mathcal{O}_F$ are deduced from that on $\mathcal{O}_F$, coming back to Definition 1.3. □

Integrating over F, we recover (one more time) the fact that a random polynomial over $\mathcal{O}_F$ has exactly one root on average in F. In a similar fashion, if U is an open subset of $\mathcal{O}_F$, we find $\mathbb{E}[Z_{U,n}] = \frac{q}{q+1} \cdot \lambda(U)$. In particular, when $F = \mathbb{Q}_p$ and $U = \mathbb{Z}_p$, we recover Evans' theorem [8] which states that a random polynomial over the p-adics has $\frac{p}{p+1}$ roots in $\mathbb{Z}_p$ on average.

2.1 Quadratic extensions

Throughout this subsection, we fix a quadratic extension K of F together with an integer $n \geq 1$. We aim at finding a closed expression for $\rho_{K,n}(x)$ for $x \in \mathcal{O}_K$. Our starting point is Theorem B which provides us with the following expression:

- if $n = 2$, then $\rho_{K,2}(x) = \|D_K\| \cdot \dfrac{1}{\#\big(\mathcal{O}_K / \mathcal{O}_F[x]\big)} \cdot \dfrac{q^2}{q^2+q+1}$,

- if $n \geq 3$, then $\rho_{K,n}(x) = \|D_K\| \cdot \displaystyle\int_{\mathcal{O}_F[x]} \|t\|^2 \, dt$.

We now distinguish between two cases depending on the fact that K/F is ramified or not.

Proposition 2.2. *Let K be the unramified quadratic extension of F. Then, for all $x \in \mathcal{O}_K$, we have:*

$$\rho_{K,2}(x) = \frac{q^2}{q^2+q+1} \cdot \mathrm{dist}(x,F),$$
$$\textit{for } n \geq 3, \quad \rho_{K,n}(x) = \frac{q^2}{q^2+q+1} \cdot \mathrm{dist}(x,F) + \frac{q^3}{(q^2+1)\,(q^2+q+1)} \cdot \mathrm{dist}(x,F)^4$$

where $\mathrm{dist}(x,F)$ *denotes the distance from x to F.*

Proof. Since K/F is unramified, its discriminant has norm 1 and thus does not contribute. We fix an element $\zeta \in \mathcal{O}_K$ with norm 1 such that $\mathcal{O}_K = \mathcal{O}_F[\zeta]$. The family $\mathcal{B} = (1, \zeta)$ is a basis of $\mathcal{O}_K$ over $\mathcal{O}_F$. Let $x \in \mathcal{O}_K$, $x \notin \mathcal{O}_F$ and write $x = a + b\zeta$ with $a, b \in \mathcal{O}_F$, $b \neq 0$. We have $\mathcal{O}_F[x] = \mathcal{O}_F[b\zeta]$, which shows that a basis of $\mathcal{O}_F[x]$ over $\mathcal{O}_F$ is simply $\mathcal{B}_x = (1, b\zeta)$. Comparing $\mathcal{B}$ and $\mathcal{B}_x$, we find $\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) = \#\big(\mathcal{O}_F/b\mathcal{O}_F\big) = \|b\|^{-1}$. Observing in addition that a is the closest element of x in F, we can reinterpret the norm of b as the distance of x to F. Putting all ingredients together, we obtain the announced formula for $\rho_{K,2}(x)$. This formula has been established when $x \notin \mathcal{O}_F$; however, it obviously also holds true when $x \in \mathcal{O}_F$ since $\rho_{K,2}(x)$ vanishes in this case by definition.

We now move to the computation of $\rho_{K,n}$ for $n \geq 3$. We continue to consider an element $x \in \mathcal{O}_K$, $x \notin \mathcal{O}_F$ and to write $x = a + b\zeta$ with $a, b \in \mathcal{O}_F$, $b \neq 0$. Performing a change of variables or, more simply, coming back to Definition 1.3, we have:

$$\rho_{K,n}(x) = \frac{1}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)} \cdot \int_{\mathcal{O}_F^2} \|u + vx\|^2 \, du\, dv = \|b\| \cdot \int_{\mathcal{O}_F^2} \|u + vx\|^2 \, du\, dv.$$

Replacing u by $u - va$, this reduces to:

$$\rho_{K,n}(x) = \|b\| \cdot \int_{\mathcal{O}_F^2} \|u + vb\zeta\|^2 \, du\, dv = \|b\| \cdot \int_{\mathcal{O}_F^2} \max\big(\|u\|^2, \|vb\|^2\big) \, du\, dv.$$

As in §1.3.3, we decompose $\mathcal{O}_F$ as the disjoint union $\mathcal{O}_F = \{0\} \sqcup \bigcup_{s \geq 0} U_s$ where U_s consists of elements of norm q^{-s}. Decomposing the integral accordingly and writing $\|b\| = q^{-v}$, we find:

$$\rho_{K,n}(x) = \left(1 - \frac{1}{q}\right)^2 q^{-v} \cdot \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} q^{-s-t-2\min(s,t+v)}.$$

Computing the latter double sum is painful but straightforward. We split the domain of summation into three regions, namely:

$$D_1 = \big\{\, (s,t) \in \mathbb{Z}_{\geq 0}^2 \quad \text{such that} \quad s < v \,\big\},$$
$$D_2 = \big\{\, (s,t) \in \mathbb{Z}_{\geq 0}^2 \quad \text{such that} \quad v \leq s \leq t + v \,\big\},$$
$$D_3 = \big\{\, (s,t) \in \mathbb{Z}_{\geq 0}^2 \quad \text{such that} \quad s > t + v \,\big\}.$$

We then compute the double sum separately on each domain:

- over D_1: $\displaystyle\sum_{s=0}^{v-1} \sum_{t=0}^{\infty} q^{-3s-t} = \frac{q^4}{(q-1)(q^3-1)} \cdot (1 - q^{-3v})$,

- over D_2: $\displaystyle\sum_{s=v}^{\infty}\sum_{t=s-v}^{\infty} q^{-3s-t} = q^{-3v}\sum_{s=0}^{\infty}\sum_{t=s}^{\infty} q^{-3s-t} = \frac{q^5}{(q-1)(q^4-1)}\cdot q^{-3v}$,
- over D_3: $\displaystyle\sum_{t=0}^{\infty}\sum_{s=t+v+1}^{\infty} q^{-s-3t-2v} = q^{-3v-1}\sum_{t=0}^{\infty}\sum_{s=t}^{\infty} q^{-s-3t} = \frac{q^4}{(q-1)(q^4-1)}\cdot q^{-3v}$.

Summing up all contributions and noticing $q^{-v} = \|b\| = \mathrm{dist}(x,F)$, we finally find the expression given in the statement of the proposition. As previously, we notice that this formula continues to hold when $x \in \mathcal{O}_F$ given that $\rho_{K,n}(x)$ vanishes by definition in this case. □

Proposition 2.3. *Let K be a totally ramified quadratic extension of F. Then, for all $x \in \mathcal{O}_K$, we have:*

$$\frac{\rho_{K,2}(x)}{\|D_K\|} = \frac{q^{3/2}}{q^2+q+1}\cdot \mathrm{dist}(x,F),$$

$$\text{for } n \geq 3, \quad \frac{\rho_{K,n}(x)}{\|D_K\|} = \frac{q^{3/2}}{q^2+q+1}\cdot \mathrm{dist}(x,F) + \frac{1}{q\,(q+1)\,(q^2+q+1)}\cdot \mathrm{dist}(x,F)^4$$

where $\mathrm{dist}(x,F)$ *denotes the distance from x to F.*

Proof. The proof is quite similar to that of Proposition 2.2, so we only sketch the argument. We fix a uniformizer π of K. The family $(1,\pi)$ forms a basis of $\mathcal{O}_K$ over $\mathcal{O}_F$. Let $x \in \mathcal{O}_K$, $x \notin \mathcal{O}_F$ and write $x = a + b\pi$ with $a, b \in \mathcal{O}_F$, $b \neq 0$. From the fact that $(1, b\pi)$ is a $\mathcal{O}_F$-basis of $\mathcal{O}_F[x]$, we deduce that the cardinality of $\mathcal{O}_K/\mathcal{O}_F[x]$ is $\|b\|^{-1}$. Noticing that $\mathrm{dist}(x,F) = \|b\pi\| = \sqrt{q}\cdot\|b\|$, we get the announced formula for $\rho_{K,2}(x)$.

When $n \geq 3$, we start with the formula:

$$\rho_{K,n}(x) = \frac{\|D_K\|}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)}\cdot\int_{\mathcal{O}_F^2}\|u+vx\|^2\,du\,dv.$$

Decomposing the integral into slices where $\|u\|$ and $\|v\|$ are constant, we obtain:

$$\frac{\rho_{K,n}(x)}{\|D_K\|} = \left(1-\frac{1}{q}\right)^2 q^{-v}\cdot\sum_{s=0}^{\infty}\sum_{t=0}^{\infty} q^{-s-t-\min(2s,2t+2v+1)}$$

where v is defined by $\|b\| = q^{-v}$. Finally, splitting the previous double sum into three parts exactly as we did in the unramified case, we end up after some calculations with the formula displayed in the statement of the proposition. □

Theorem C can be deduced from Propositions 2.2 and 2.3 by integrating over K. For this, the first ingredient is the observation that the transformation law of Theorem B.3 permits to relate the integral of $\rho_{K,n}$ outside $\mathcal{O}_K$ to its integral over another domain sitting inside $\mathcal{O}_K$. Precisely, applying it with the homography $h : x \mapsto x^{-1}$, we get $\rho_{K,n}\big(h(x)\big) = \|x\|^4\cdot\rho_{K,n}(x)$. Noticing in addition that h maps bijectively $K\backslash\mathcal{O}_K$ to the maximal ideal $\mathfrak{m}_K$ of $\mathcal{O}_K$, we obtain:

$$\int_{K\backslash\mathcal{O}_K}\rho_{K,n}(x)\,dx = \int_{\mathfrak{m}_K}\rho_{K,n}\big(h(x)\big)\cdot\|h'(x)\|^2\,dx = \int_{\mathfrak{m}_K}\rho_{K,n}(x)\,dx.$$

Summing up the contributions over $\mathcal{O}_K$ and $K\backslash\mathcal{O}_K$, we end up with:

$$\int_K \rho_{K,n}(x)\,dx = \int_{\mathcal{O}_K}\rho_{K,n}(x)\,dx + \int_{\mathfrak{m}_K}\rho_{K,n}(x)\,dx.$$

Theorem C now easily follows from the next lemma.

Lemma 2.4. *Let d be a positive integer and set $\alpha_d = \dfrac{q-1}{q^{d+1}-1} = \dfrac{1}{q^d + q^{d-1}\cdots + 1}$.*

(i) If K/F is unramified, we have:

$$\int_{\mathcal{O}_K} \mathrm{dist}(x,F)^d\,dx = q^d\alpha_d \quad \textit{and} \quad \int_{\mathfrak{m}_K} \mathrm{dist}(x,F)^d\,dx = q^{-2}\alpha_d.$$

(ii) If K/F is totally ramified, we have:

$$\int_{\mathcal{O}_K} \mathrm{dist}(x,F)^d\,dx = q^{d/2}\alpha_d \quad \textit{and} \quad \int_{\mathfrak{m}_K} \mathrm{dist}(x,F)^d\,dx = q^{d/2-1}\alpha_d.$$

Proof. We first assume that K/F is unramified. Writing $\mathcal{O}_K = \mathcal{O}_F[\zeta]$ as in the proof of Proposition 2.2, we find:

$$\int_{\mathcal{O}_K} \mathrm{dist}(x,F)^d\,dx \;=\; \int_{\mathcal{O}_F} \|b\|^d\,db = q^d\alpha_d$$

the last equality being nothing but Eq. (10) established in §1.3.3. Similarly noticing that $x = a + b\zeta$ lies in $\mathcal{O}_K$ if and only if both a and b falls in the maximal ideal $\mathfrak{m}_F$ of $\mathcal{O}_F$, we obtain:

$$\int_{\mathfrak{m}_K} \mathrm{dist}(x,F)^d\,dx \;=\; \lambda(\mathfrak{m}_F)\cdot\int_{\mathfrak{m}_F} \|b\|^d\,db \;=\; q^{-1}\int_{\mathfrak{m}_F} \|b\|^d\,db.$$

Fixing a uniformizer π_F of F and performing the change of variables $b = \pi_F t$, we finally get:

$$\int_{\mathfrak{m}_K} \mathrm{dist}(x,F)^d\,dx \;=\; q^{-d-2}\int_{\mathcal{O}_F} \|t\|^d\,dt = q^{-2}\alpha_d.$$

The argument in the totally ramified case is similar. We pick a uniformizer π of K and writing $\mathcal{O}_K = \mathcal{O}_F[\pi]$, we find:

$$\int_{\mathcal{O}_K} \mathrm{dist}(x,F)^d\,dx \;=\; \int_{\mathcal{O}_F} \|b\pi\|^d\,db \;=\; \|\pi\|^d\cdot q^d\alpha_d \;=\; q^{d/2}\alpha_d.$$

For the integral over $\mathfrak{m}_K$, we observe that $a + b\pi \in \mathcal{O}_K$ if and only if $a \in \mathfrak{m}_F$. Therefore:

$$\int_{\mathfrak{m}_K} \mathrm{dist}(x,F)^d\,dx \;=\; \lambda(\mathfrak{m}_F)\cdot\int_{\mathcal{O}_F} \|b\pi\|^d\,db \;=\; q^{d/2-1}\alpha_d$$

which concludes the proof. □

2.2 Prime degree extensions

The strategy we have presented above in the case of quadratic extensions actually extends to all extensions of prime degree, the crucial point being that K/F does not admit any nontrivial subextension. Nonetheless, in this generality, the computations become much longer and painful although they remain feasible in theory. The case of polynomials of minimal degree remain however reasonable.

Proposition 2.5. *Let r be a prime number and let K be an extension of F of degree r.*

(i) If K/F is unramified then, for all $x \in \mathcal{O}_K$, we have:

$$\rho_{r,K}(x) = \frac{q^{r+1}-q^r}{q^{r+1}-1}\cdot \mathrm{dist}(x,F)^{r(r-1)/2}.$$

(ii) If K/F is totally ramified then, for all $x \in \mathcal{O}_K$, we have:

$$\rho_{r,K}(x) = \|D_K\| \cdot \frac{q^{(r+3)/2} - q^{(r+1)/2}}{q^{r+1} - 1} \cdot \mathrm{dist}(x, F)^{r(r-1)/2}.$$

Proof. We assume first that K/F is unramified. Let $x \in \mathcal{O}_K$, $x \notin \mathcal{O}_F$. By compacity, there exists $a \in \mathcal{O}_F$ such that $\|x - a\| = \mathrm{dist}(x, F)$. We pick such an element a and write $x - a = \pi^v \zeta$ where π is a fixed uniformizer of F and $\zeta \in \mathcal{O}_K$ has norm 1. Let k_F and k_K denote the residue fields of F and K respectively and let $\bar{\zeta}$ be the image of ζ in k_K. We claim that $\bar{\zeta} \notin k_F$; indeed, otherwise, there would exist $b \in \mathcal{O}_F$ with $b \equiv \zeta \pmod{\pi}$ and so $\|x - (a + \pi^v b)\| \leq q^{-v-1} < q^{-v} = \|x - a\|$, contradicting the minimality property of a. Given that the extension k_K/k_F has prime degree, we deduce that $k_K = k_F[\bar{\zeta}]$ and, consequently, that $\mathcal{O}_K = \mathcal{O}_F[\zeta]$. The family $(1, \zeta, \ldots, \zeta^{r-1})$ is then a basis of $\mathcal{O}_K$ over $\mathcal{O}_F$, while $(1, \pi^v\zeta, \ldots, (\pi^v\zeta)^{r-1})$ is a basis of $\mathcal{O}_F[x]$ over $\mathcal{O}_F$. This shows that:

$$\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) = q^{v+2v+\cdots+(r-1)v} = q^{vr(r-1)/2} = \mathrm{dist}(x, F)^{-r(r-1)/2}$$

from what we deduce the claimed formula for $\rho_{r,K}(x)$.

We now move to the totally ramified case. Let π_F (resp. π_K) denote a fixed uniformizer of F (resp. K). Then $\mathcal{O}_K = \mathcal{O}_F[\pi_K]$ and the family $\mathcal{B} = (1, \pi_K, \ldots, \pi_K^{r-1})$ is a $\mathcal{O}_F$-basis of $\mathcal{O}_K$. Let $x \in \mathcal{O}_K$ and let $a \in \mathcal{O}_F$ such that $\|x - a\| = \mathrm{dist}(x, F)$. Write $x - a = \pi_K^v u$ with $v \in \mathbb{Z}_{\geq 0}$ and $u \in \mathcal{O}_K^\times$. The minimality condition in the definition of a implies that $v \not\equiv 0 \pmod{r}$. Besides the family $\mathcal{B}_x = (1, \pi_K^v u, \ldots, (\pi_K^v u)^{r-1})$ is a $\mathcal{O}_F$-basis of $\mathcal{O}_F[x]$. For $i \in \{0, \ldots, r-1\}$, we decompose $(\pi_K^v u)^i$ in the basis $\mathcal{B}$, *i.e.* we write:

$$(\pi_K^v u)^i = \sum_{j=0}^{r-1} a_{ij} \pi_K^j \tag{14}$$

with $a_{ij} \in \mathcal{O}_F$. Set $c = q^{1/r}$. Taking norms in Eq. (14), we get $c^{-vi} = \max_{1 \leq j < r} \big(\|a_{ij}\| \cdot c^{-j}\big)$. In other words, $\|a_{ij}\| \leq c^{j-vi}$ for all j and the equality holds for at least one index j. On the other hand, the inequality is certainly strict as soon as r does not divides $j - vi$ because $\|a_{ij}\|$ is a negative power of $q = c^r$. Therefore, if j_i denotes the remainder in the division of vi by r, we conclude that $\|a_{ij}\| \leq c^{j-vi}$ for all j with equality if and only if $j = j_i$. Let A be the change-of-basis matrix from $\mathcal{B}$ to $\mathcal{B}_x$. By definition, its entries are exactly the a_{ij}'s. Let P be the permutation matrix associated to $i \mapsto j_i$ and define:

$$B = \begin{pmatrix} \pi_F^{-v_0} & & \\ & \ddots & \\ & & \pi_F^{-v_{r-1}} \end{pmatrix} \cdot P^{-1} \cdot A \qquad \text{with} \quad v_i = \frac{vi - j_i}{r}.$$

The estimations on $\|a_{ij}\|$ we have obtained previously shows that B has entries in $\mathcal{O}_F$ and that B mod π_F is lower-triangular with nonzero diagonal entries. Hence B is invertible over $\mathcal{O}_F$, which gives $\|\det B\| = 1$. Since P is clearly invertible as well, we conclude that:

$$\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big) = \|\det A\|^{-1} = q^{v_0+\cdots+v_r} = q^{(v-1)(r-1)/2}.$$

Remembering that $\mathrm{dist}(x, F) = \|x - a\| = \|\pi_K^v u\| = q^{-v/r}$, we finally find the formula given in the proposition. □

Extending Proposition 2.5 to larger degrees does not require more conceptual arguments but leads to much more laborious calculations. Precisely, it follows from Definition 1.3 that, for $n \geq r$ and $x \in \mathcal{O}_K \backslash \mathcal{O}_F$, one has:

$$\rho_{n,K}(x) = \frac{\|D_K\|}{\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)} \cdot \int_{\mathcal{O}_F^{m+1}} \max\big(\|u_0\|^r,\, \delta^r\|u_1\|^r,\, \ldots,\, \delta^{rm}\|u_m\|^r\big)\, du_0 \cdots du_m$$

where $\delta = \mathrm{dist}(x, F)$ and $m = \min(r-1, n-r)$. Besides, after the proof of Proposition 2.5, we know an explicit formula for $\#\big(\mathcal{O}_K/\mathcal{O}_F[x]\big)$. The computation of the integral can be carried out by splitting the domain of integration, namely $\mathcal{O}_F^{m+1}$, into $m+1$ subdomains depending on the index at which the maximum is reached. Computing separately all contributions and summing them up, we can conclude. As far as we tried, it seems that the final formula does not take a simple form in full generality.

2.3 Unramified extensions

For general unramified extensions K, it is possible to compute at a lower cost some values of $\rho_{K,n}$ (for any n).

Proposition 2.6. *Let r be a positive integer and let K be the unramified extension of F of degree r. Let $x \in \mathcal{O}_K$. We assume that $\mathcal{O}_F[x] = \mathcal{O}_K$. Then:*

$$\rho_{n,K}(x) = \frac{q^{n'+1} - q^r}{q^{n'+1} - 1} \qquad \textit{with} \quad n' = \min(n, 2r-1)$$

for all $n \geq r$.

Proof. Set $m = n' - r$. Let k_F (resp. k_K) denote the residue field of F (resp. K). Let $\xi \in k_K$ be the image of x. Our assumption implies that $k_F[\xi] = k_K$. Therefore, if an expression of the form $u_0 + u_1 x + \cdots + u_m x^m$ with $u_i \in \mathcal{O}_F$ vanishes in k_K, then all u_i have to vanish in k_F. We deduce from this property that:

$$\|u_0 + u_1 x + \cdots + u_m x^m\| = \max\big(\|u_0\|,\, \|u_1\|,\, \ldots,\, \|u_m\|\big)$$

for all $u_0, \ldots, u_m \in \mathcal{O}_F$. It then follows from Definition 1.3 and our assumptions that:

$$\rho_{n,K}(x) = \int_{\mathcal{O}_F^{m+1}} \max\big(\|u_0\|^r,\, \|u_1\|^r,\, \ldots,\, \|u_m\|^r\big)\, du_0 \cdots du_m.$$

Contrarily to what we said at the end of §2.2, it turns out that the latter integral can be easily computed. Indeed, let us fix a uniformizer π of F and, for each nonnegative integer s, set $U_s = (\pi^s \mathcal{O}_F)^{m+1}$. The U_s's then form a decreasing sequence of open subsets of $\mathcal{O}_F^{m+1}$. Moreover, it is easy to check that U_s is exactly the domain on which the integrand $\max\big(\|u_0\|^r, \ldots, \|u_m\|^r\big)$ is less than or equal to q^{-sr}. We deduce from this that:

$$\rho_{n,K}(x) = \sum_{s=0}^{\infty} \big(\lambda_F^{\otimes m+1}(U_s) - \lambda_F^{\otimes m+1}(U_{s+1})\big) \cdot q^{-sr}.$$

Observing that $\lambda_F^{\otimes m+1}(U_s) = \lambda_F(\pi^s \mathcal{O}_F)^{m+1} = q^{-s(m+1)}$, we end up with:

$$\rho_{n,K}(x) = \big(1 - q^{-m-1}\big) \cdot \sum_{s=0}^{\infty} q^{-s(m+1+r)} = \frac{q^{m+1+r} - q^r}{q^{m+1+r} - 1}$$

which is what we wanted to prove. □

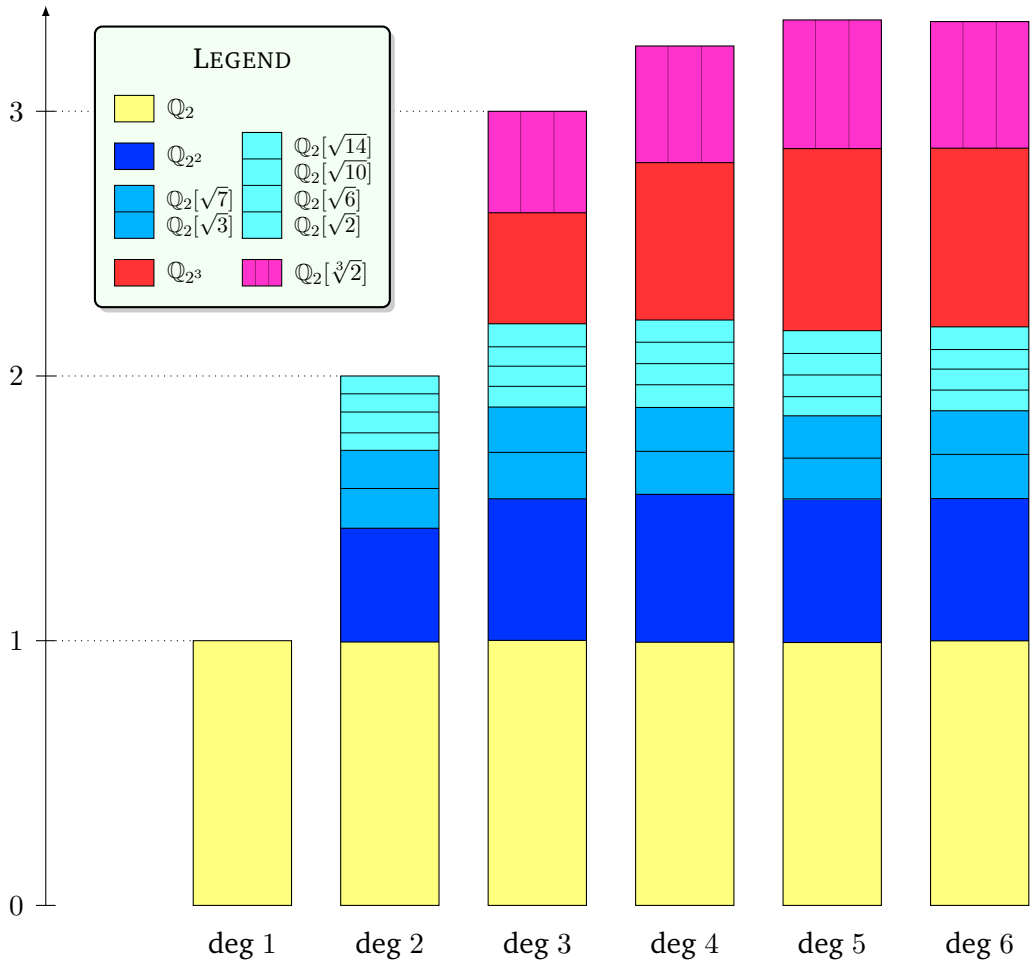

Figure 1: Average number of roots of a polynomial in various extensions. Sample of $500{,}000$ polynomials over $\mathbb{Z}_2$ picked uniformly at random.

2.4 Numerical simulations

We have conducted several numerical experiments illustrating the theoretical results obtained in §1 and §2. First of all, for $p \in \{2, 5\}$, we have picked a sample of $500,000$ random polynomials over $\mathbb{Z}_p$ of degree up to 5 and count the number of (new) roots these polynomials have in $\mathbb{Q}_p$ and all its extensions of degree 2 and 3. The results are reported on Fig. 1 for $p = 2$ and on Fig. 2 for $p = 5$. In both cases, we observe that the empirical average number of roots in $\mathbb{Q}_p$ is 1 as predicted by Proposition 2.1.

We can also check that the number of new roots heavily depends on the discriminant of the extension. When $p = 5$, for example, the discrimant of $\mathbb{Q}_{5^2}$ has norm 1 whereas the discrimant of the two other quadratic extensions, namely $\mathbb{Q}_5[\sqrt{5}]$ and $\mathbb{Q}_5[\sqrt{10}]$, has norm $1/5$; looking at the picture of Fig. 2, we see that the height of the dark blue area is roughly 5 times larger that the height of the light blue one. Similarly, when $p = 2$, the discriminant of $\mathbb{Q}_4$ has norm 1, the discrimiant of $\mathbb{Q}_2[\sqrt{3}]$ and $\mathbb{Q}_2[\sqrt{7}]$ has norm $1/4$ and that of the four remaining quadratic extensions has norm $1/8$. Again, we way check on Fig. 1 that one has approximately the same ratios for the heights of the corresponding areas.

Another property we can visualize on Fig. 1 and Fig. 2 is the monotony statement of Theorem B. Indeed, we see that the heights of the areas tend to slightly increase with the degree until they stabilize at degree 3 for quadratic extensions and degree 5 for cubic

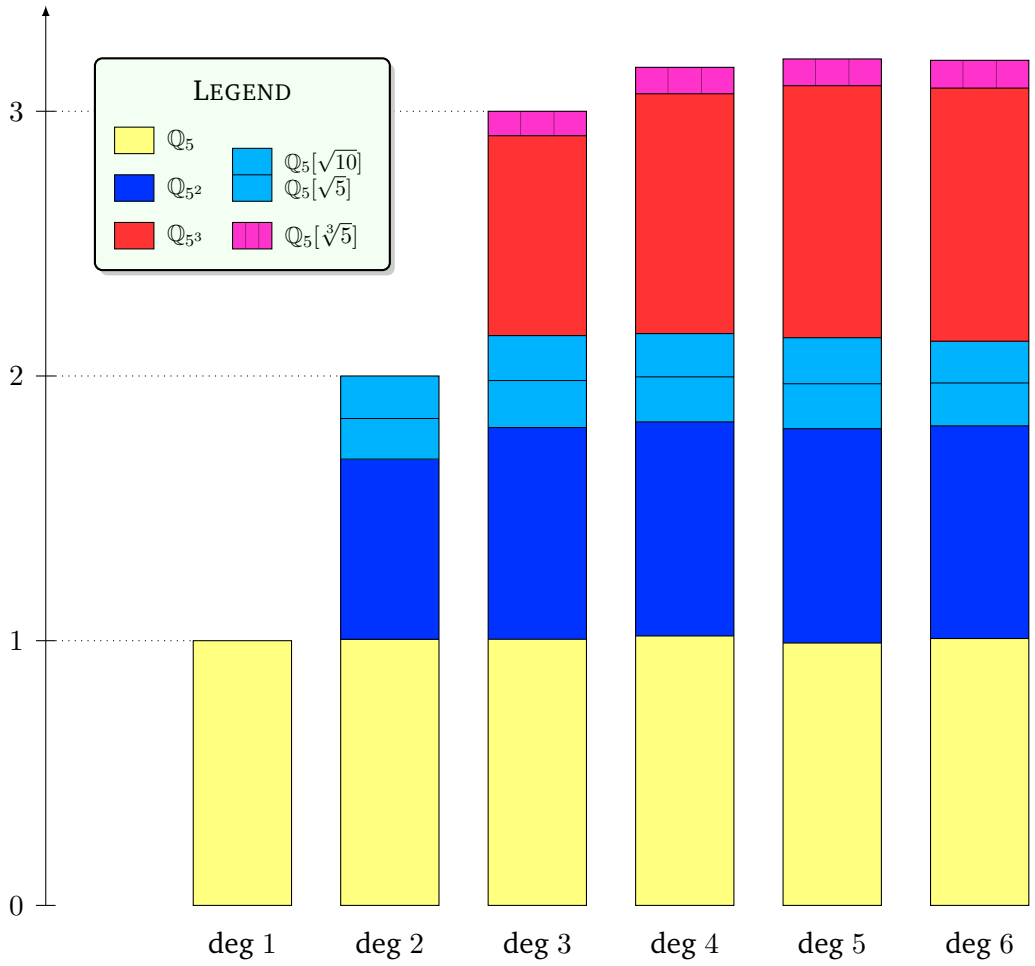

Figure 2: Average number of roots of a polynomial in various extensions. Sample of $500{,}000$ polynomials over $\mathbb{Z}_5$ picked uniformly at random.

extensions.

In a slightly different direction, Fig. 3 shows the empiric repartition of new roots of a sample of $500,000$ random polynomials of degree 5 over $\mathbb{Z}_2$ in the ring of integers of two quadratic extensions, namely $\mathbb{Z}_4$, presented as $\mathbb{Z}_2[\zeta]$ with $\zeta^2+\zeta+1=0$ (on the left) and $\mathbb{Z}_2[\pi]$ where π is a root of the Eisenstein polynomial X^2+2X-2 (on the right). In our pictures, each bullet corresponds to a class modulo 2^5. The darkness of the bullet encodes the number of roots we got in the corresponding class: the bullet is black if we observed more than 400 roots (in total, on our sample of $500,000$ polynomials), it is left white if we have not got any root and grayscale colors are used for intermediate number of hits. Moreover, on each $\mathbb{Z}_2$-line, the classes are ordered as follows:

$$0,16,8,24,4,20,12,28,2,18,10,26,6,22,14,30,$$
$$1,17,9,25,5,21,13,29,3,19,11,27,7,23,15,31,$$

i.e. the even classes come first, followed by the odd ones and inside each subgroup, the classes are gathered according to their congruence modulo 4, then modulo 8, *etc.* This organisation is appropriate for our purpose but it somehow reflects the 2-adic distance.

On each picture, it is striking that the bullets are becoming much brighter when we are approaching the $\mathbb{Z}_2$-line on the bottom. This empirical observation is in perfect compliance

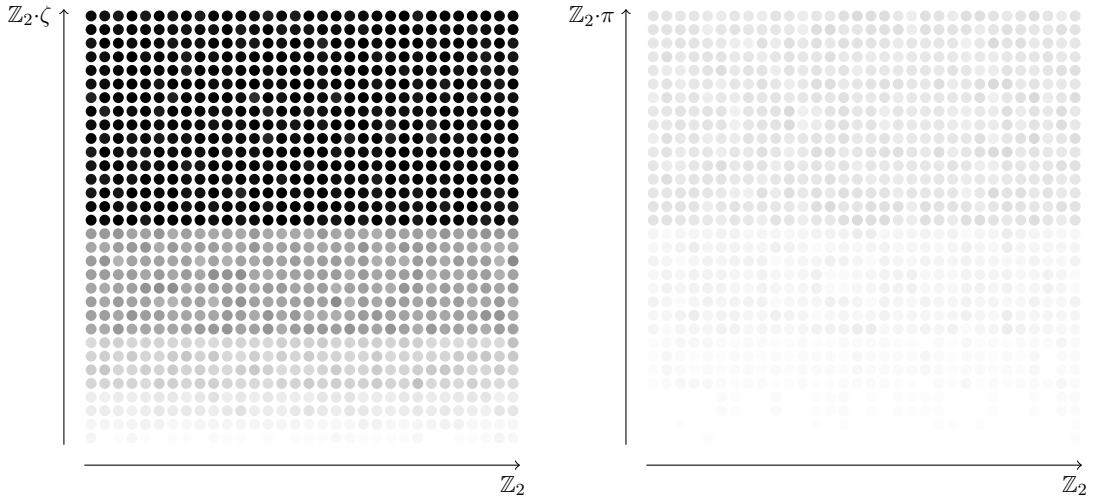

Figure 3: Repartition of new roots of a polynomial in $\mathbb{Z}_4$ (on the left) and in $\mathbb{Z}_2[\pi]$ with $\pi^2 + 2\pi - 2 = 0$ (on the right). Sample of $500{,}000$ polynomials over $\mathbb{Z}_2$ picked uniformly at random.

with the explicit formulas of Propositions 2.2 and 2.3 that clearly indicate that the size of $\rho_{K,n}(x)$ is governed by the distance of x to $\mathbb{Q}_2$. Another unmissable point is that the bullets on the picture on the right are much brighter than the bullets on the left. Again, this is due to the fact that the discriminant of $\mathbb{Q}_2[\pi]$ has a smaller norm than the discriminant of $\mathbb{Q}_4$; we then expect more roots, and so darker bullets, in the case of $\mathbb{Q}_4$.

3 Some orders of magnitude

In the previous section, we have tried to write down *exact* formulas for the density function $\rho_{K,n}$'s. However, in many cases, it is sufficient—and sometimes even more useful—to know their orders of magnitude. In this section, we focus on the quantities:

$$\rho_n(K) = \int_K \rho_{K,n}(x)\, dx$$

which counts the average number of new roots in K, *i.e.* $\rho_n(K) = \mathbb{E}[Z_{K,n}^{\text{new}}]$ (see Definition 1.5 and Theorem 1.6). We obtain sharp asymptotic estimations of them when q and r grows, proving in particular Theorems D and E.

3.1 Counting generators over finite fields

This subsection gathers several preliminary lemmas concerning the number of generators of an extension of finite fields. Write $\mathbb{F}_q$ (resp. $\bar{\mathbb{F}}_q$) for the residue field of F (resp. $\bar{F}$). It is well-known that $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. For any given a positive integer f, let $\mathbb{F}_{q^f}$ denote the unique extension of $\mathbb{F}_q$ of degree f sitting inside $\bar{\mathbb{F}}_q$. Let G_f be the number of elements $x \in \mathbb{F}_{q^f}$ such that $\mathbb{F}_q[x] = \mathbb{F}_{q^f}$. From the obvious fact that each $x \in \mathbb{F}_{q^f}$ generates some $\mathbb{F}_{q^m}$ for a divisor m of f, we deduce the relation:

$$\sum_{m|f} G_m = q^f. \tag{15}$$

This relation can be "inverted" using Moebius inversion formula. We recall that the Moebius function $\mu : \mathbb{Z}_{>0} \to \{0, 1\}$ is defined by $\mu(p_1 \dots p_s) = (-1)^s$ if $p_1, \dots, p_s$ are distinct prime numbers and $\mu(n) = 0$ as soon as n is divisible by a square. Eq. (15) then becomes:

$$G_f = \sum_{m|f} \mu\left(\frac{f}{m}\right) q^m. \tag{16}$$

From the latter formula, one easily derive that $G_f = q^f + O(q^{f/2})$. Here is an other estimation of the same type we shall need in the sequel.

Lemma 3.1. *For all positive integer f, we have:*

$$\sum_{\substack{m|f \\ m<f}} G_m q^m \leq 2q^f.$$

Proof. A strict divisor of f cannot certainly exceed $f/2$. On the other hand, it is obvious from the definition that $G_m \leq q^m$ for all m. Hence, the sum of the lemma is bounded from above by:

$$\sum_{m<f/2} q^{2m} \leq \frac{q^{f+2} - 1}{q^2 - 1} \leq \frac{q^f}{1 - q^{-2}} \leq 2q^f$$

given that $q \geq 2$. □

Let φ be the Euler's totient function. We recall that $\varphi(n)$ is by definition the number of integers which are less than n and coprime with n. If the decomposition of n in prime factors reads $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, one has the formula:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

The beautiful next lemma, which relates harmoniously the Moebius and the Euler functions, is somehow classical; we nevertheless include a proof for completeness.

Lemma 3.2. *For any positive integer n, one has the relation:*

$$\sum_{m|n} \frac{\mu(m)}{m} = \frac{\varphi(n)}{n}.$$

Proof. Write $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ where the p_i's are pairwise distinct prime numbers. The divisors m of n are exactly the integers of the form $m = p_1^{\beta_1} \cdots p_s^{\beta_s}$ with $\beta_i \leq \alpha_i$ for all i. We then deduce from the definition of the Moebius function that:

$$\sum_{m|n} \frac{\mu(m)}{m} = \sum_{\beta_1=0}^{1} \cdots \sum_{\beta_s=0}^{1} \frac{(-1)^{\beta_1 + \cdots + \beta_s}}{p_1^{\beta_1} \dots p_s^{\beta_s}} = \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) = \frac{\varphi(n)}{n}$$

which proves the lemma. □

Lemma 3.3. *For any positive integer r, one has the relation:*

$$r \cdot \sum_{f|r} \frac{G_f}{f} = \sum_{m|r} \varphi\left(\frac{r}{m}\right) q^m.$$

Proof. The lemma follows from the following sequence of equalities:

$$\begin{aligned} r \cdot \sum_{f|r} \frac{G_f}{f} &= r \cdot \sum_{m|f|r} \mu\left(\frac{f}{m}\right) \frac{q^m}{f}. && \text{by Eq. (16)} \\ &= r \cdot \sum_{m|r} \sum_{n|\frac{r}{m}} \frac{\mu(n)}{n} \cdot \frac{q^m}{m}. && \text{(change of variables } n = \tfrac{f}{m}\text{)} \\ &= \sum_{m|r} \varphi\left(\frac{r}{m}\right) q^m && \text{by Lemma 3.2.} \end{aligned}$$

□

3.2 Isolating the main contribution to $\rho_n(K)$

We come back to the p-adic situation and to our problem of finding a sharp asymptotic of $\rho_n(K)$. In what follows, we fix a finite extension K of F. We denote its degree by r and its residual degree by f. The residue field of K is then $\mathbb{F}_{q^f}$. Let $\mathcal{G}_K$ be the set of generators of $\mathcal{O}_K$, that is:

$$\mathcal{G}_K = \big\{\, x \in \mathcal{O}_K \quad \text{such that} \quad \mathcal{O}_F[x] = \mathcal{O}_K \,\big\}.$$

Similarly, for a positive integer f, we define $\mathcal{G}_f$ as the set of generators of $\mathbb{F}_{q^f}$ over $\mathbb{F}_q$. By definition, the number G_f we have introduced in §3.1 is the cardinality of $\mathcal{G}_f$. For each $\alpha \in \mathbb{F}_{q^f}$, we let U_α denote the open subset of $\mathcal{O}_K$ consisting of elements whose image in the residue field is α. The U_α's are then pairwise disjoint and $\lambda_K(U_\alpha) = q^{-f}$ for all α.

Lemma 3.4. *For $\alpha \in \mathbb{F}_{q^f}$, we have:*

$$\begin{aligned} q^{-f} \cdot \big(1 - q^{-f}\big) \;\le\; \lambda_K(\mathcal{G}_K \cap U_\alpha) \;\le\; q^{-f} \qquad & \text{if } \alpha \in \mathcal{G}_f, \\ \mathcal{G}_K \cap U_\alpha \;=\; \emptyset \qquad & \text{if } \alpha \notin \mathcal{G}_f. \end{aligned}$$

Proof. If $x \in \mathcal{O}_K$ generates $\mathcal{O}_K$ over $\mathcal{O}_F$, its image in the residue field must generate $\mathbb{F}_{q^f}$ over $\mathbb{F}_q$. This proves the lemma when $\alpha \notin \mathcal{G}_f$.

We now assume that $\alpha \in \mathcal{G}_f$. First of all, it is clear that $\lambda_K(\mathcal{G}_K \cap U_\alpha) \le \lambda_K(U_\alpha) = q^{-f}$. Let $\bar{Z}$ be the minimal polynomial of α over $\mathbb{F}_q$. Let also $a \in \mathcal{O}_K$ be a lifting of α and $Z \in \Omega_f$ be a polynomial lifting $\bar{Z}$. We fix in addition a uniformizer π of K. Then $Z(a)$ is a multiple of π and we write $Z(a) = \pi b$. Besides $\bar{Z}'(a)$ does not vanish given that $\mathbb{F}_{q^f}/\mathbb{F}_q$ is a separable extension. For $x \in \mathcal{O}_K$, the congruence:

$$Z(a + \pi x) \;\equiv\; Z(a) + Z'(a)\pi x \;\equiv\; \pi \cdot \big(b + Z'(a)\, x\big) \pmod{\pi^2}$$

shows that $Z(a + \pi x)$ is a uniformizer of K as soon as the image of x in the residue field is different from $\frac{-b}{Z'(a)}$. When this occurs, $\mathcal{O}_F[x]$ then contains a uniformizer of F together with a generator of the residue field, implying that $\mathcal{O}_F[x] = \mathcal{O}_K$. The lemma follows. □

Proposition 3.5. *For all $n \ge r$, we have:*

$$\int_{K \setminus \mathcal{G}_K} \rho_{K,n}(x)\, dx \;\le\; 4 \cdot \|D_K\| \cdot q^{-f}$$

Proof. Set $V = K \setminus \mathcal{G}_K$ and $V_\alpha = V \cap U_\alpha$ for $\alpha \in \mathbb{F}_{q^f}$. Set also $V_\infty = K \setminus \mathcal{O}_K$. The set V then appears as the disjoint union of the V_α's for α varying in $\mathbb{P}^1(\mathbb{F}_{q^f})$. We are going to bound the integral of $\rho_{K,n}$ an each V_α separately. When $\alpha \in \mathcal{G}_K$, it follows from Lemma 3.4

that $\lambda_K(V_\alpha) \leq q^{-2f}$. Besides, coming back to Definition 1.3, we remark that $\rho_{K,n}$ is upper bounded by $\|D_K\|$ on $\mathcal{O}_K$ and so, on V_α. We then deduce, in this case, that

$$\frac{1}{\|D_K\|} \cdot \int_{V_\alpha} \rho_{K,n}(x)\, dx \;\leq\; q^{-2f}.$$

We now consider the case where $\alpha \in \mathbb{F}_{q^f}$, $\alpha \notin \mathcal{G}_K$. Write $\ell = \mathbb{F}_q[\alpha]$ and let $m(\alpha)$ be the degree of the extension $\ell/\mathbb{F}_q$. By assumption $m(\alpha) < f$. On the other hand, the reduction morphism $\mathcal{O}_K \to \mathbb{F}_{q^f}$ takes $\mathcal{O}_F[x]$ to ℓ. We deduce that the cardinality of the quotient $\mathcal{O}_K/\mathcal{O}_F[x]$ is bounded from below by the cardinaly of $\mathbb{F}_{q^f}/\ell$, which is $q^{f-m(\alpha)}$. Injecting this bound in the defition of $\rho_{n,K}$, we find:

$$\frac{1}{\|D_K\|} \cdot \int_{V_\alpha} \rho_{K,n}(x)\, dx \;\leq\; \lambda_K(V_\alpha) \cdot q^{m(\alpha)-f} \;=\; q^{m(\alpha)-2f}.$$

Finally, when $\alpha = \infty$, we perform the change of variables $x \mapsto x^{-1}$, which lefts us with:

$$\int_{V_\infty} \rho_{K,n}(x)\, dx \;=\; \int_{V_0} \rho_{K,n}(x)\, dx \;\leq\; \|D_K\| \cdot q^{1-2f}.$$

Summing up all upper bounds, we find:

$$\frac{1}{\|D_K\|} \cdot \int_{K\backslash\mathcal{G}_K} \rho_{K,n}(x)\, dx \;\leq\; q^{1-2f} \;+\; G_f q^{-2f} + \sum_{\substack{m|f \\ m<f}} G_m q^{m-2f}$$

given that the number of $\alpha \in \mathbb{F}_{q^f}\backslash\mathcal{G}_K$ for which $m(\alpha) = m$ is equal to G_m by definition. Remembering that $G_f \leq q^f$ and using Lemma 3.1, we end up with:

$$\frac{1}{\|D_K\|} \cdot \int_{K\backslash\mathcal{G}_K} \rho_{K,n}(x)\, dx \;\leq\; q^{1-2f} + q^{-f} + 2q^{-f} \;\leq\; 4q^{-f}.$$

The proposition is proved. □

The next corollary can be seen as an effective version of Theorem D (use Eq. (16)).

Corollary 3.6. *We have the estimations:*

$$-q^{-f} \;\leq\; \frac{\rho_r(K)}{\|D_K\|} \;-\; \frac{q^{r+1}-q^r}{q^{r+1}-1} \cdot \frac{G_f}{q^f} \;\leq\; 4q^{-f}$$

$$\text{for } n \geq 2r-1, \qquad -q^{-f} \;\leq\; \frac{\rho_n(K)}{\|D_K\|} \;-\; \frac{q^r}{q^r+1} \cdot \frac{G_f}{q^f} \;\leq\; 4q^{-f}$$

Proof. Let $n = r$ or $n \geq 2r-1$. Recall that by definition:

$$\rho_n(K) = \int_K \rho_{K,n}(x)\, dx \;=\; \int_{\mathcal{G}_K} \rho_{K,n}(x)\, dx \;+\; \int_{K\backslash\mathcal{G}_K} \rho_{K,n}(x)\, dx.$$

By Proposition 3.5, we know that the integral over $K\backslash\mathcal{G}_K$ is upper bounded by $4q^{-f}$. It is also obviously nonnegative since the integrand is nonnegative. Therefore, it is enough to prove that:

$$0 \;\leq\; c_n \,\frac{G_f}{q^f} \;-\; \int_{\mathcal{G}_K} \frac{\rho_{K,n}(x)}{\|D_K\|}\, dx \;\leq\; q^{-f}$$

with $c_r = \frac{q^{r+1}-q^r}{q^{r+1}-1}$ and $c_n = \frac{q^r}{q^r+1}$ for $n \geq 2r-1$. On the other hand, a computation similar to the one we carried out in §1.3.3 gives:

$$\int_{\mathcal{O}_K} \|t\|^r \, dt = \frac{q^r}{q^r+1}.$$

Hence, it follows from the explicit formulas of Theorem B that $\rho_{K,n}$ is constant equal to $c_n \cdot \|D_K\|$ on $\mathcal{G}_K$. We are then reduced to check that $0 \leq q^{-f} G_f - \lambda_K(\mathcal{G}_K) \leq q^{-f} c_n^{-1}$. This follows from Lemma 3.4 after remarking that $0 \leq c_n \leq 1$. □

By the monotony result of Theorem B, the previous corollary also provides estimations of $\rho_n(K)$ when n varies between r and $2r-1$. They are however less sharp since the error term is *a priori* only in $O\big(q^{-1}\big)$ instead of $O\big(q^{-f}\big)$. We can nevertheless recover more accuracy when the extension K/F is unramified.

Theorem 3.7. *If K/F is unramified, we have the estimation:*

$$-q^{-r} \;\leq\; \frac{\rho_n(K)}{\|D_K\|} \;-\; \frac{q^{n+1}-q^r}{q^{n+1}-1} \cdot \frac{G_r}{q^r} \;\leq\; 4q^{-r}$$

for all n between r and $2r-1$.

Proof. It is exactly the same than the proof of Corollary 3.6, except that the value of $\rho_{K,n}$ on $\mathcal{G}_K$ is now given by Proposition 2.6. (Note also that $f = r$ in the unramified case.) □

Replacing G_r by its expression given by Eq. (16), we end up with the following asymptotic development in the spirit of Theorem D:

$$\rho_n(K) = \left(1 - \frac{1}{q^{n-r+1}}\right) \cdot \sum_{m|r} \mu\Big(\frac{r}{m}\Big)\, q^{m-r} \;+\; O\left(\frac{1}{q^r}\right). \tag{17}$$

This estimation holds true for any *unramified* extension K/F and an integer n in the range $[r,\ 2r-1]$; moreover, the constant hidden in the $O(-)$ is absolute.

3.3 Summing up over extensions of fixed degree

The aim of this subsection is to prove Theorem E. The strategy we will follow is quite simple: we sum up the surroundings of Corollary 3.6 over all extensions K of a fixed degree r. For this, the main new ingredient we shall need is Serre's mass formula that we recall below. If K is a finite extension of F, we write $\mathrm{Aut}_{F\text{-alg}}(K)$ for the group of automorphisms of F-algebras of K.

Theorem 3.8 (Serre's mass formula)**.** *For any positive integer r, we have:*

$$q^{r-1} \sum_K \frac{\|D_K\|}{\#\,\mathrm{Aut}_{F\text{-alg}}(K)} = 1$$

where the sum runs over all isomorphism classes of totally ramified *extensions K of F of degree r.*

Proof. See [18]. □

We need to be careful that, in the formulation of Theorem 3.8, the sum runs over *isomorphism classes* of extensions and not extensions sitting inside $\bar{F}$ as we work with usually in this article. To switch between those two viewpoints, we observe that an abstract extension K of F of degree r admits r embeddings into $\bar{F}$. However, two such embeddings have the same image (and so define the same subfield of $\bar{F}$) when they differ by an automorphism of K. The number of subfields of $\bar{F}$ which are isomorphic to K is then exactly equal to $\frac{r}{\#\,\mathrm{Aut}_{F\text{-alg}}(K)}$. Therefore, Serre's mass formula can be rewritten as follows:

$$\sum_{K \in \mathbf{Ex}_{r,1}} \|D_K\| = \frac{r}{q^{r-1}} \tag{18}$$

where the indexation set $\mathbf{Ex}_{r,1}$ consists of all subfields K of $\bar{F}$ which are totally ramified extensions of F of degree r. More generally, given an auxiliary positive integer f dividing r, we define $\mathbf{Ex}_{r,f}$ as the set of embedded extensions of F of degree r and residual degree f. Serre's mass formula extends without difficulty to extensions in $\mathbf{Ex}_{r,f}$.

Proposition 3.9. *For all positive integers r and all divisors f or r, we have:*

$$\sum_{K \in \mathbf{Ex}_{r,f}} \|D_K\| = \frac{r}{q^r} \cdot \frac{q^f}{f}.$$

Proof. Let F_f be the unique unramified extension of F sitting inside $\bar{F}$. Its residue field is $\mathbb{F}_{q^f}$ and the normalized norm on F_f is the f-th power of $\|\cdot\|$. Moreover, any extension K in $\mathbf{Ex}_{r,f}$ canonically contains F_f and then appears uniquely as a totally ramified extension of F_f. In addition, the discriminant of K/F, still denoted by D_K, is the f-th power of the discriminant D_{K/F_f} of K/F_f. Hence $\|D_{K/F_f}\|^f = \|D_K\|$. The formula (18) applied with the base field F_f then gives:

$$\sum_{K \in \mathbf{Ex}_{r,f}} \|D_K\| = \sum_{K \in \mathbf{Ex}_{r,f}} \|D_{K/F_f}\|^f = \frac{r}{f} \cdot \frac{1}{(q^f)^{r/f-1}} = \frac{r}{q^r} \cdot \frac{q^f}{f}$$

which establishes the proposition. □

We now fix two positive integers r and n with $n \geq 2r-1$. For a given divisor f or r, observing that:

$$1 - \frac{1}{q^f} \leq 1 - \frac{1}{q^r} \leq \frac{q^r}{q^r+1} \leq 1$$

we derive from Corollary 3.6 that:

$$\left| \frac{\rho_n(K)}{\|D_K\|} - \frac{G_f}{q^f} \right| \leq \frac{5}{q^f}$$

for any extension $K \in \mathbf{Ex}_{r,f}$. Summing up over all such extensions, we find:

$$\left| \sum_{K \in \mathbf{Ex}_{r,f}} \rho_n(K) \; - \; \frac{G_f}{q^f} \sum_{K \in \mathbf{Ex}_{r,f}} \|D_K\| \right| \leq \frac{5}{q^f} \sum_{K \in \mathbf{Ex}_{r,f}} \|D_K\|$$

which gives after Proposition 3.9:

$$\left| \sum_{K \in \mathbf{Ex}_{r,f}} \rho_n(K) \; - \; \frac{r}{q^r} \cdot \frac{G_f}{f} \right| \leq \frac{5}{q^r} \cdot \frac{r}{f}.$$

Writing that $\mathbf{Ex}_r$ is the disjoint union of the $\mathbf{Ex}_{r,f}$'s for f varying in the set of divisors of r and summing up all the above estimations, we end up with:

$$\left| \sum_{K \in \mathbf{Ex}_r} \rho_n(K) \; - \; \frac{r}{q^r} \sum_{f|r} \frac{G_f}{f} \right| \; \leq \; \frac{5}{q^r} \sum_{f|r} \frac{r}{f} \; = \; \frac{5}{q^r} \sum_{f|r} f. \tag{19}$$

Finally, the error term is controlled thanks to the following classical result:

$$\sum_{f|r} f \; = \; O\big(r \cdot \log\log r\big)$$

(see for instance [9]). Injecting it in Eq. (19) and using the summation formula of Lemma 3.3, we finally get Theorem E.

Remark 3.10. It is amusing to observe that Theorems D and E have a very similar shape, except that former involves the Moebius function whereas the latter implicates the Euler function. Comparing both results and writing $\delta = \varphi - \mu$, we obtain:

$$\sum_{K \in \mathbf{Ex}_r^{\text{ram}}} \rho_n(K) = \sum_{m|r} \delta\Big(\frac{r}{m}\Big)\, q^{m-r} \; + \; O\left(\frac{r \cdot \log\log r}{q^r}\right)$$

where the indexation set $\mathbf{Ex}_r^{\text{ram}}$ consists of all *ramified* extensions of F of degree r sitting inside $\bar{F}$. Since $\delta(1) = 0$, the dominant term of the sum in the right hand side is obtained for $m = r/\ell$ where ℓ is the smallest divisor of m. Its value is $\delta(\ell)\, q^{-r(1-\frac{1}{\ell})}$. Since ℓ is necessarily prime, we have moreover $\mu(\ell) = -1$ and $\varphi(\ell) = \ell - 1$, giving $\delta(\ell) = \ell$. As a consequence, we obtain the approximation:

$$\sum_{K \in \mathbf{Ex}_r^{\text{ram}}} \rho_n(K) \; \approx \; \ell \cdot q^{-r(1-\frac{1}{\ell})}.$$

For example, when $r = 2$, we find that the order of magnitude of $\sum_{K \in \mathbf{Ex}_2^{\text{ram}}} \rho_n(K)$ is $2/q$. If q is odd, the set $\mathbf{Ex}_2^{\text{ram}}$ consists exactly of two elements (namely the extensions $F\big[\sqrt{\pi}\big]$ and $F\big[\sqrt{a\pi}\big]$ where π is a uniformizer of F and a is an element of $\mathcal{O}_F$ which is not a square in the residue field) and each corresponding summand contributes for $1/q$.

4 The setup of étale algebras

In the previous section, we have exclusively focused our interest on the *mean* of the $Z_{U,n}$'s. However, it is evident that the mean captures only a small part of the complexity of the phenomena and, beyond it, we would like to study higher moments or correlations between the $Z_{U,n}$'s to get a more precise picture of the situation.

In this section, we propose to attack these questions by applying the same methods as before in some suitable enlarged framework, which is that of finite étale algebras (that are finite products of finite extensions of F). On the one hand, allowing this flexibility is somehow harmless because all the techniques we have developed in the previous sections extend without difficulty. However, on the other hand, it is also quite interesting because it sheds new lights on many natural questions. For instance, it turns out that the average number of roots in power algebras of the form K^m is closely related to higher moments of the random variables $Z_{U,n}$ for $U \subset K$. Similarly, studying the average number of roots in

products of type $K_1 \times K_2$ provides valuable information on the correlations between $Z_{K_1,n}$ and $Z_{K_2,n}$.

This section is organized as follows. In §4.1, we introduce the random variables $Z_{E,n}$ and $Z_{E,n}^{\text{new}}$ for a finite étale algebra E and relate them to products of the $Z_{K,n}$'s. In §4.2, we extend Theorems A and B to our new setup. In §4.3, we spend some time on the special case of the étale algebra F^2, making everything explicit in this example. We then derive from our calculations precise information about the variance and the correlations between the $Z_{U,n}$'s where U is an open subset of F, proving in particular Theorem F. Finally, we prove Theorem G in §4.4.

4.1 Roots and new roots

Before getting to the heart of the matter, we gather basic standard facts about finite étale F-algebras. To begin with, let us recall that a finite étale algebra over F is defined as an finite algebra over F without nilpotent elements [7, Definition 2.1.2]. It is well known (see [7, Corollary 2.1.6]) that any finite étale algebra over F can be decomposed as a product $K_1 \times K_2 \times \cdots \times K_m$ where each K_i is a finite extension of E. In what follows, we will often pick such a decomposition and work with it. The two next (classical) results will be quite useful to check that all our forthcoming constructions are intristic, *i.e.* do not depend on the choice of a decomposition as above.

Lemma 4.1. *Let $K, K_1, \ldots, K_m$ be finite extensions of F and set $E = K_1 \times \cdots \times K_m$. Let $f : E \to K$ be a surjective morphism of F-algebras. Then there exists an index i such that $f = \varphi \circ \text{pr}_i$ where $\varphi : K_i \to K$ is an isomorphism and pr_i denotes the projection on the i-th factor.*

Proof. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in E$ with the 1 in i-th position. If x lies in the kernel of f, so does $e_i x$ for all i. This proves that $\ker f$ decomposed as $I_1 \times \cdots \times I_m$ where I_i is some ideal of K_i. Since K_i is a field, one must have $I_i = 0$ or $I_i = K_i$. Moreover, since f is surjective, $\ker f$ is a maximal ideal. This shows that there exists a special index i such that $I_i = 0$ and $I_j = K_j$ for all $j \neq i$. Hence f factors through pr_i and the lemma follows. □

Corollary 4.2. *Let $K_1, \ldots, K_m$ be pairwise nonisomorphic finite extensions of F. Let $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ be two tuple of nonnegative integers. Let:*

$$f : K_1^{a_1} \times \cdots \times K_m^{a_m} \longrightarrow K_1^{b_1} \times \cdots \times K_m^{b_m}$$

be a surjective morphism of F-algebras. Then, for each $i \in \{1, \ldots, m\}$, there exists an injection $\sigma_i : \{1, \ldots, b_i\} \to \{1, \ldots, a_i\}$ and a tuple $(\varphi_{i,1}, \ldots, \varphi_{i,b_i})$ of automorphisms of K_i such that:

$$f\big((x_{i,j})_{1 \leq i \leq m, 1 \leq j \leq a_i}\big) = \big(\varphi_{i,j}(x_{i,\sigma_i(j)})\big)_{1 \leq i \leq m, 1 \leq j \leq b_i}.$$

Proof. Write $x = (x_{i,j})_{1 \leq i \leq m, 1 \leq j \leq a_i}$. Given $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, b_i\}$, Lemma 4.1 tells us that the (i,j) coordinate of $f(x)$ must be of the form $\varphi_{i,j}(x_{i,\sigma_i(j)})$ for some automorphism $\varphi_{i,j}$ of K_i and some $\sigma_i(j) \in \{1, \ldots, b_i\}$. This establishes the shape we have given for f. Finally, the fact that the σ_j's are injective follows from the surjectivity of f. □

When $a_i = b_i$ for all i, Corollary 4.2 indicates that the group of automorphisms of F-algebras of $E = K_1^{a_1} \times \cdots \times K_m^{a_m}$, denoted by $\text{Aut}_{F\text{-alg}}(E)$, is canonically isomorphic to

$$\prod_{i=1}^{m} \big(\mathfrak{S}_{a_i} \rtimes \text{Aut}_{F\text{-alg}}(K_i)^{a_i}\big)$$

where $\mathfrak{S}_{a_i}$ is the symmetric group on a_i letters and it acts on $\mathrm{Aut}_{F\text{-alg}}(K_i)^{a_i}$ by permuting the automorphisms. In particular we deduce that:

$$\#\mathrm{Aut}_{F\text{-alg}}(E) = \prod_{i=1}^{m} a_i! \left(\#\mathrm{Aut}_{F\text{-alg}}(K_i)\right)^{a_i}.$$

Another property of étale algebras it will be important to keep in mind in the sequel is recorded in the next proposition.

Proposition 4.3. *Any F-subalgebra of a finite étale F-algebra is finite étale.*

Proof. It is obvious from the definition. □

We now go back to our topic. Given a polynomial $P \in F[X]$, a root of P in a finite étale F-algebra E is, by definition, an element $x \in E$ such that $P(x) = 0$. It is a standard fact that the datum of a root of P in E is equivalent to the datum of a morphism of F-algebras $F[X]/P \to E$: to a root x, we associate the morphism taking X to x and, conversely, to a morphism $\varphi : F[X]/P \to E$, we associate the root $\varphi(X)$.

The notion of new elements we have introduced in the case of extensions in Definition 1.5 extends immediately to finite étale algebras.

Definition 4.4. Let E be a finite étale algebra over F. An element $x \in E$ is *new* in E if it does not belong to any strict sub-F-algebra of E, *i.e.* if $F[x] = E$.

Lemma 4.5. *Let P is a polynomial over F. Let $x \in E$ is a root of P and $\varphi : F[X]/P \to E$ be its associated morphism. Then x is new in E if and only if φ is surjective.*

Proof. It follows from the fact that the image of φ is the F-algebra generated by x. □

Given a positive integers n, a finite étale F-algebra E and an open subset $U \subset E$, we define the random variables $Z_{U,n} : \Omega_n \to \mathbb{Z}$ and $Z^{\mathrm{new}}_{U,n} : \Omega_n \to \mathbb{Z}$ by:

$$\begin{aligned} Z_{U,n}(P) &= \text{number of roots of } P \text{ in } U \\ Z^{\mathrm{new}}_{U,n}(P) &= \text{number of roots of } P \text{ in } U\text{, which are new in } E. \end{aligned}$$

It follows from Lemma 4.5 that $Z_{U,n}(P)$ (resp. $Z^{\mathrm{new}}_{U,n}(P)$) is also the number of morphisms (resp. surjective morphisms) of F-algebras $\varphi : F[X]/P \to E$ such that $\varphi(X) \in U$. In particular $Z_{E,n}(P) = \#\operatorname{Hom}_{F\text{-alg}}\big(F[X]/P, E\big)$ and $Z^{\mathrm{new}}_{E,n}(P) = \#\operatorname{Hom}^{\mathrm{surj}}_{F\text{-alg}}\big(F[X]/P, E\big)$ (where the notations are transparent). This reformulation shows directly that $Z^{\mathrm{new}}_{E,n}$ identically vanishes when $n < [E : F]$. Besides, the random variables $Z_{U,n}$ and $Z^{\mathrm{new}}_{U,n}$ are related by the formula:

$$Z_{U,n} = \sum_{E' \subset E} Z^{\mathrm{new}}_{E' \cap U,n} \tag{20}$$

which simply comes from the observation that an element $x \in E$ is new in a unique subalgebra E' of E, namely $E' = F[x]$. This algebra is moreover necessarily étale over F by Proposition 4.3. We note furthermore that the construction $Z_{U,n}$ is multiplicative with respect to the parameter U, *i.e.* that:

$$Z_{U_1 \times U_2,n} = Z_{U_1,n} \cdot Z_{U_2,n}$$

for any positive integer n, any finite étale F-algebras E_1 and E_2 and any open subsets U_1 and U_2 of E_1 and E_2 respectively. This property is interesting for us because it implies the formula:

$$\mathrm{Cov}\big(Z_{U_1,n},\, Z_{U_2,n}\big) = \mathbb{E}\big[Z_{U_1 \times U_2,n}\big] - \mathbb{E}\big[Z_{U_1,n}\big] \cdot \mathbb{E}\big[Z_{U_2,n}\big] \tag{21}$$

which shows that the covariance of $Z_{U_1,n}$ and $Z_{U_2,n}$ can be computed in terms of means of random variables of the form $Z_{U,n}$. The next proposition highlights a similar property for the higher (factorial) moments of certain random variables $Z_{U,n}^{\text{new}}$.

Proposition 4.6. *Let K be a finite extension of F and set $a = \#\operatorname{Aut}_{F\text{-alg}}(K)$. Let m, n be two positive integers and let U be an open subset of K stable by all morphisms in $\operatorname{Aut}_{F\text{-alg}}(K)$. Then:*

$$Z_{U^m,n}^{\text{new}} = Z_{U,n}^{\text{new}} \cdot \big(Z_{U,n}^{\text{new}} - a\big) \cdot \big(Z_{U,n}^{\text{new}} - 2a\big) \cdots \big(Z_{U,n}^{\text{new}} - (m-1)a\big).$$

Proof. Write $r = [K : F]$ and pick a polynomial $P \in \Omega_n$. Let $x = (x_1, \dots, x_m) \in U^m$. We claim that x is a new root of P in E if and only if x_i is a new root of P in K for all i and the x_i's are pairwise nonconjugate. To prove to claim, we let Z be the minimal polynomial of x over F and, similarly, for all $i \in \{1, \dots, m\}$, we denote by Z_i the minimal polynomial of x_i over F. We then have $Z = \operatorname{lcm}(Z_1, \dots, Z_m)$. Notice moreover that all the Z_i's are irreducible since we have assumed that K is a field. On the other hand, the fact that x is new in E (resp. x_i is new in K) is equivalent to the equality $\deg Z = rm$ (resp. $\deg Z_i = r$). We deduce from this that x is new in E if and only if x_i is new in K for all i and the Z_i's are pairwise coprime. By irreducibility, the coprimality condition is equivalent to the fact that the Z_i's are pairwise distinct, which is further equivalent to the fact that the x_i's are pairwise nonconjugate. This establishes our claim.

We are now ready to count the number of new roots of P in U^m. Indeed, by what precedes, it is equivalent to count the number of tuples $(x_1, \dots, x_m) \in U^m$ of new roots in K which are pairwise nonconjugate. By definition of $Z_{U,n}^{\text{new}}$, we have $Z_{U,n}^{\text{new}}(P)$ possibilities for x_1. The fact that x_2 cannot be conjugate to x_1 eliminates exactly a possibilities because we have assumed that U is stable under the action of $\operatorname{Aut}_{F\text{-alg}}(K)$. It then remains $Z_{U,n}^{\text{new}}(P) - a$ possibilities for x_2. Similarly, we have $Z_{U,n}^{\text{new}}(P) - 2a$ possibilities for x_3 because it has to be nonconjugate to both x_1 and x_2. Repeating this argument m times, we end up with the formula of the proposition. □

4.2 Density functions

In this subsection, we aim at extending the definition of density functions to the setting of étale algebras and at proving variants of Theorems A and B in this framework. For this, the first step is to find an adequate generalization of the p-adic Kac-Rice.

Kac-Rice formula

If E is a finite étale algebra over F presented as $E = K_1 \times K_2 \times \cdots \times K_m$ (where the K_i's are finite extensions of F), we endow it with the norm $\|\cdot\|$ defined by:

$$\|(x_1, x_2, \dots, x_m)\| = \max\big(\|x_1\|, \|x_2\|, \dots, \|x_m\|\big) \qquad (x_i \in K_i).$$

We deduce from Corollary 4.2 and the discussion just after that the above definition is intrinsic in the sense that it does not depend on the chosen identification $E \simeq K_1 \times \cdots \times K_m$. We let $\mathcal{O}_E$ be the subring of E consisting of elements of norm at most 1. When E is presented as $E = K_1 \times \cdots \times K_m$, we have $\mathcal{O}_E = \mathcal{O}_{K_1} \times \cdots \times \mathcal{O}_{K_m}$.

Given E as above, we also define the norm map $N_{E/F} : E \to F$ taking an element $x \in E$ to its so-called norm which is, by definition, the determinant of the F-linear mapping $E \to E$, $y \mapsto xy$. When $E = K_1 \times \cdots \times K_m$, we have:

$$N_{E/F}\big((x_1, \dots, x_m)\big) = N_{K_1/F}(x_1) \cdots N_{K_m/F}(x_m)$$

for what we derive:

$$\begin{aligned}\|N_{E/F}\big((x_1,\dots,x_m)\big)\| &= \|N_{K_1/F}(x_1)\|\cdots\|N_{K_m/F}(x_m)\| \\ &= \|x_1\|^{[K_1:F]}\dots\|x_m\|^{[K_m:F]}.\end{aligned}$$

The latter formula shows in particular that $N_{E/F}$ maps $\mathcal{O}_E$ to $\mathcal{O}_F$.

With the above preparation, the extension of the p-adic Kac-Rice formula to our new setting can be formulated as follows.

Theorem 4.7. *Let E be a finite étale algebra over F and set $r=[E:F]$. Let U be a compact open subset of E and let $f:U\to E$ be a strictly differentiable function. We assume that $f'(x)$ is invertible in E for all $x\in E$ such that $f(x)=0$. Then:*

$$\#f^{-1}(0)=\lim_{s\to\infty} q^{sr}\cdot\int_U \|N_{E/F}(f'(x))\|\cdot\mathbb{1}_{\{\|f(x)\|\le q^{-s}\}}\,dx.$$

Proof. It is entirely similar to that of Theorem 1.1. □

Density functions

We define the discriminant D_E of a finite étale F-algebra $E=K_1\times\cdots\times K_m$ as the product $D_{K_1}\cdots D_{K_m}$. One checks that D_E is also the discriminant of the bilinear form $E\times E\to F$, $(x,y)\mapsto \mathrm{Tr}_{E/F}(xy)$ where $\mathrm{Tr}_{E/F}$ is the trace map of E over F. This alternative definition shows in particular that D_E does not depend (up to multiplication by an invertible element) on the choice of the presentation $E=K_1\times\cdots\times K_m$.

In the case of étale algebras, the density functions cannot be defined exactly the same way as for extensions (see Definition 1.3) because it may happen that neither x nor x^{-1} falls in the ring of integers. We will then proceed in a slightly different manner. We denote by λ_E the Haar measure on E normalized by $\lambda_E(\mathcal{O}_E)=1$. If $E=K_1\times\cdots\times K_m$, we simply have $\lambda_E=\lambda_{K_1}\otimes\cdots\otimes\lambda_{K_m}$. A second important ingredient we will need is a *height* function $H:E\to\mathbb{R}$; writing again $E=K_1\times\cdots\times K_m$, it is defined as follows:

$$H\big((x_1,\dots,x_m)\big)=\prod_{i=1}^m \max\Big(1,\ \|x_i\|^{[K_i:F]}\Big)\qquad (x_i\in K_i).$$

Using again Corollary 4.2, we conclude that this notion does not depend on the choice of the identification $E=K_1\times\cdots\times K_m$.

Given a positive integer n and a finite étale F-algebra E of degree r, we set:

$$\rho_{E,n}(x)=\frac{\|D_E\|\cdot\lambda_E\big(\mathcal{O}_F[x]\big)}{H(x)^{n+1}}\cdot\int_{\Omega_{n-r}}\|N_{E/F}(Q(x))\|\,dQ$$

The main benefit of the above expression is its validity for any $x\in E$. In particular, when x is not new in E, we observe that $\mathcal{O}_F[x]$ is included in a strict F-linear subalgebra of E and thus has measure zero; $\rho_{E,n}(x)$ then vanishes as well in this case. In a similar fashion, when x is new in $\mathcal{O}_E$, the height of x is 1 and the measure of $\mathcal{O}_F[x]$ is the inverse of the cardinality of $\mathcal{O}_E/\mathcal{O}_F[x]$; we then get in this case:

$$\rho_{E,n}(x)=\frac{\|D_E\|}{\#\big(\mathcal{O}_E/\mathcal{O}_F[x]\big)}\cdot\int_{\Omega_{n-r}}\|N_{E/F}(Q(x))\|\,dQ$$

which is exactly the formula of Definition 1.3. Theorems A and B now extend almost *verbatim* with, however, one notable exception: the monotony property of Theorem B no longer holds in the framework of étale algebras; only remains the fact that the sequence $(\rho_{E,n})_{n\ge1}$ is eventually constant.

Theorem 4.8. *For any positive integer n, any finite étale F-algebra E and any open subset U of E, we have:*

$$\begin{aligned}\mathbb{E}\big[Z_{U,n}^{\mathrm{new}}\big] &= \int_U \rho_{E,n}(x)\,dx \\ \mathbb{E}[Z_{U,n}] &= \sum_{E'\subset E}\int_{U\cap E'}\rho_{E',n}(x)\,dx\end{aligned}$$

where the latter sum runs over all F-subalgebras E' of E. Moreover, writing $r=[E:F]$, the function $\rho_{E,n}$ satisfies the following list of properties, in which x denotes an element of E.

1. (Vanishing) *If $F[x]\neq E$ or $n<r$, then $\rho_{E,n}(x)=0$.*
2. (Continuity) *The function $\rho_{E,n}$ is continuous on K.*
3. (Transformation under homography) *For $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{GL}_2(\mathcal{O}_F)$, we have:*

$$\rho_{E,n}\left(\frac{ax+b}{cx+d}\right)=\|N_{E/F}(cx+d)\|^2\cdot\rho_{E,n}(x).$$

4. (Ultimate constancy) *If $n\geq 2r-1$, then $\rho_{E,n}=\rho_{E,2r-1}$.*
5. (Formulas for extremal degrees) *If $F[x]=E$ and $x\in\mathcal{O}_E$, then*

$$\rho_{E,r}(x)=\|D_K\|\cdot\frac{1}{\#\big(\mathcal{O}_E/\mathcal{O}_F[x]\big)}\cdot\frac{q^{r+1}-q^r}{q^{r+1}-1}$$

$$\text{for } n\geq 2r-1,\quad \rho_{E,n}(x)=\|D_K\|\cdot\int_{\mathcal{O}_F[x]}\|N_{E/F}(t)\|\,dt.$$

Proof. The proof follows the same pattern than in the case of extensions. The first step is to extend Proposition 1.2 and show that:

$$\lim_{s\to\infty}\int_{\Omega_n} q^{sr}\cdot\|N_{E/F}(P(x))\|\cdot\mathbb{1}_{\{\|P(x)\|\leq q^{-s}\}}\,dP \;=\; \rho_{E,n}(x) \tag{22}$$

when x is new in E. As in the proof of Proposition 1.2, we write I_s for the above integral. Let Z be the minimal monic polynomial of x; it does not need to be irreducible but it has degree r since x is assumed to be new in E. Let $c\in\mathcal{O}_F$ be the *content* of Z that is, by definition, the gcd of the coefficients of Z. Using that the content of a product is the product of the contents, we find that a product $QZ\in\mathcal{O}_F[x]$ if and only if $Q\in c^{-1}\mathcal{O}_F[X]$. Moreover, we have seen in the proof of Proposition 1.2 that there exists a positive constant γ such that $\|R(x)\|\geq\gamma\cdot\|R\|$ for all polynomial R of degree at most $r-1$. We deduce from these facts, for any fixed R with $\|R\|\leq\gamma$, the property $QZ+R\in\Omega_n$ is equivalent to $Q\in c^{-1}\Omega_{n-r}$. Remarking in addition that the mapping $(Q,R)\mapsto QZ+R$ preserves the measure (it is linear and has determinant one in the canonical bases), we obtain the equality:

$$I_s=q^{sr}\cdot\int_{\Omega_{r-1}}\int_{c^{-1}\Omega_{n-r}}\|N_{E/F}\big(Q(x)Z'(x)+R'(x)\big)\|\cdot\mathbb{1}_{\{\|R(x)\|\leq q^{-s}\}}\,dQ\,dR$$

which holds true provided that s is sufficiently large. Repeating now the argument presented in the proof of Proposition 1.2, we end up with:

$$\begin{aligned} I_s &= \|D_E\| \cdot \lambda_E\big(\mathcal{O}_F[x]\big) \cdot \int_{c^{-1}\Omega_{n-r}} \|N_{E/F}(Q(x))\| \cdot dQ \\ &= \|D_E\| \cdot \lambda_E\big(\mathcal{O}_F[x]\big) \cdot \|c\|^{-n-1} \int_{\Omega_{n-r}} \|N_{E/F}(Q(x))\| \cdot dQ \end{aligned}$$

for s large enough. Consider a decomposition $E = K_1 \times \cdots \times K_m$ and write $x = (x_1, \ldots, x_m)$ accordingly. For each index i, set $r_i = [K_i : F]$ and let Z_i be the minimal monic polynomial of x_i. Then Z is the lcm of the Z_i's and comparing degrees, we get $Z = Z_1 \cdots Z_m$. On the other hand, using relations between coefficients and roots, we find that the coefficient on Z_i in X^j has norm at most $\|x_i\|^{r_i - j}$ and equality is reached for $j \in \{0, r_i\}$. Therefore, the content c_i of Z_i is 1 when $x_i \in \mathcal{O}_{K_i}$ and it is equal to $N_{K_i/F}(x_i)$ otherwise. Hence $\|c_i\| = \max\big(1, \|x_i\|^{r_i}\big)$ in all cases. By the multiplicativity property of contents, we conclude that $\|c\| = H(x)$, which finally establishes Eq. (22). After this result, the proof of the first part of the theorem is totally similar to that of Theorem 1.6.

It remains to establish the properties of the density functions. Continuity and formulas for extremal degrees are derived exactly as in the case of extensions (see §1.3.1 and §1.3.3 respectively). Although the transformation formula under homography can be tackled as in §1.3.2, it is probably easier, in the case of étale algebras, to use a different argument that we present now. First of all, we remark that, thanks to continuity, the set of equalities:

$$\mathbb{E}\big[Z_{U,n}^{\text{new}}\big] \;=\; \int_U \rho_{E,n}(x)\, dx$$

(when U varies) entirely determines the density function $\rho_{E,n}$. Given an homography $h : t \mapsto \frac{at+b}{ct+d}$, it is then enough to prove that $\mathbb{E}\big[Z_{U,n}^{\text{new}}\big] = \mathbb{E}\big[Z_{h(U),n}^{\text{new}}\big]$ for any open subset U of E, which follows from the fact that the transformation:

$$\Omega_n \to \Omega_n, \quad P(X) \mapsto (cX+d)^n \cdot P\left(\frac{aX+b}{cX+d}\right)$$

preserves the measure.

It finally only remains to prove that $\rho_{E,n} = \rho_{E,2r-1}$ as soon as $n \geq 2r-1$. Let x be a new element in E. As in the first part of the proof, we consider the minimal monic polynomial $Z \in \mathcal{O}_F[X]$ of x and let $c \in \mathcal{O}_F$ be its content. We pick a decomposition $E = K_1 \times \cdots \times K_m$ and we let E_0 (resp. E_∞) be the product of the K_i's in which x falls in the ring of integers (resp. outside the ring of integers). We thus have the decomposition $E = E_0 \times E_\infty$ and we write $x = (x_0, x_\infty)$ accordingly. It follows from the definition of the height function that $H(x) = \|N_{E_\infty/F}(x_\infty)\|$. For $t \in \{0, \infty\}$, set $r_t = [E_t : F]$ and let Z_t be the minimal monic polynomial of x_t. From the fact that x is new in E, we find $\deg Z = r$, from what we deduce that $\deg Z_t = r_t$ and $Z = Z_0 Z_\infty$. Besides, both polynomials Z_0 and $c^{-1}Z_\infty$ have integral coefficients. Even better, if we write:

$$c^{-1}Z_\infty = \lambda_0 + \lambda_1 X + \cdots + \lambda_{r_\infty} X^{r_\infty} \tag{23}$$

the constant coefficient λ_0 is invertible in $\mathcal{O}_F$ while the next ones lie in the maximal ideal of $\mathcal{O}_F$, *i.e.* $\|\lambda_0\| = 1$ and $\|\lambda_i\| < 1$ for $i \in \{1, \ldots, r_\infty\}$. For a polynomial $Q \in \Omega_n$, we define $Q \,\%\, Z_0$ as the remainder of the division of Q by Z_0 and $Q \,\%^\tau\, Z_\infty$ as the remainder of the division by *increasing power order* of Q by Z_∞. The notation $\%^\tau$ comes from the fact that:

$$Q \,\%^\tau\, Z_\infty = \tau\big(\tau(Q) \,\%\, \tau(Z_\infty)\big)$$

where τ is the involution of Ω_n taking $P(X)$ to $X^n P(X^{-1})$. We derive from the fact that $Z_0 \in \mathcal{O}_F[X]$ (resp. from Eq. (23)) that $Q \,\%\, Z_0$ (resp. $Q \,\%^\tau\, Z_\infty$) has integral coefficients when Q has. We consider the $\mathcal{O}_F$-linear mapping:

$$\begin{array}{rccc} \varphi: & \Omega_n & \longrightarrow & (\Omega_{r_0-1}) \times (X^{n-r_\infty+1}\Omega_{r_\infty-1}) \\ & Q & \mapsto & \big(Q \,\%\, Z_0,\, Q \,\%^\tau\, Z_\infty\big) \end{array}$$

We claim that φ is surjective. Given $P \in \Omega_{r_0-1}$, checking that $(P, 0)$ is in the image of φ amounts to proving that there exists a polynomial which is divisible by Z_∞ and congruent to P modulo Z_0. This follows from the fact that Z_∞ is invertible in the quotient $\mathcal{O}_F[X]/Z_0$, which is itself a consequence of Eq. (23) which implies that the series $\sum_{i=1}^{\infty} \big(1 - c^{-1} Z_\infty\big)^i$ converges in $\mathcal{O}_F[X]/Z_0$. Twisting by τ, we prove similarly that all elements of the form $(0, X^{n-r_\infty+1}B)$ with $B \in \Omega_{r_\infty-1}$ are attained by φ. This gives the surjectivity.

We deduce that Ω_n can be decomposed (noncanonically) as follows:

$$\Omega_n \simeq \big(\ker \varphi\big) \times \big(\Omega_{r_0-1}\big) \times \big(X^{n-r_\infty+1}\Omega_{r_\infty-1}\big).$$

This isomorphism moreover preserves the measure since it is $\mathcal{O}_F$-linear. Thus, if we set:

$$J_t = \int_{\Omega_{r_t-1}} \|N_{E_t/F}(Q(x_t))\|\, dQ \qquad (t \in \{0, \infty\})$$

we get:

$$\begin{aligned} \frac{1}{H(x)^{n+1}} \int_{\Omega_n} \|N_{E/F}(Q(x))\|\, dQ \;&=\; \frac{\|N_{E_\infty/F}(x_\infty)\|^{n-r_\infty+1}}{H(x)^{n+1}} \cdot J_0 \cdot J_\infty \\ &=\; \frac{1}{H(x)^{r_\infty}} \cdot J_0 \cdot J_\infty \end{aligned}$$

which shows that the latter quantity does not depend on n (provided that $n \geq 2r-1$) and so neither does $\rho_{n,E}(x)$. □

4.3 The case of F^2

The algebra $E = F^2$ is the simplest example of finite étale algebra which is not a field, but it already leads to nontrivial and interesting results about the repartition of roots in F of a random polynomial. Precisely, it allows us to compute the second momemt and the covariances between the random variables $Z_{U,n}$ when U is an open subset of F. In what follows, we present a panorama of results in this direction.

Proposition 4.9. *For $x, y \in \mathcal{O}_F$, we have:*

$$\begin{aligned} &\rho_{F^2,2}(x,y) = \frac{q^2}{q^2+q+1} \cdot \|x-y\| \\ \textit{for } n \geq 3, \quad &\rho_{F^2,n}(x,y) = \frac{q^2}{q^2+q+1} \cdot \|x-y\| - \frac{q^3}{(q+1)^2\,(q^2+q+1)} \cdot \|x-y\|^4. \end{aligned}$$

Proof. First of all, observe that $\|D_{F^2}\| = \|D_F\|^2 = 1$. Set $h = x - y$ and let A be the $\mathcal{O}_F$-subalgebra of $\mathcal{O}_F^2$ generated by (x, y). A basis of A is formed by the vectors $e_1 = (1, 1)$ and $e_2 = (0, h)$. Hence $\#(\mathcal{O}_{F^2}/A) = \|h\|^{-1}$ and the proposition follows when $n = 2$ using the explicit formulas of Theorem 4.8. For $n \geq 3$, we have to compute the integral of $\|N_{F^2/F}(t)\|$

over A. Applying the linear change of variables $\mathcal{O}_F^2 \xrightarrow{\sim} A$, $(u,v) \mapsto ue_1 + ve_2 = (u, u+hv)$, we obtain:

$$\int_A \|N_{F^2/F}(t)\|\, dt = \|h\| \int_{\mathcal{O}_F^2} \|u\| \cdot \|u+hv\|\, du\, dv. \tag{24}$$

In order to compute the latter integral, we first integrate with respect to the variable v. For a fixed $u \in \mathcal{O}_F$, we claim that:

$$\begin{aligned} \int_{\mathcal{O}_F} \|u+hv\|\, dv &= \|u\| && \text{if } \|u\| > \|h\| \\ &= \frac{q}{q+1} \cdot \|h\| && \text{otherwise.} \end{aligned}$$

Indeed, when $\|u\| > \|h\|$, the integrand is constant equal to $\|u\|$. On the contrary, when $\|u\| \leq \|h\|$, we can perform the change to variables $v \mapsto v - h^{-1}u$ and conclude by using Eq. (10). Injecting the above result in Eq. (24) and decomposing the integral according to the values of $\|u\|$, we obtain:

$$\int_A \|N_{F^2/F}(t)\|\, dt = \|h\| \cdot \left(1 - \frac{1}{q}\right) \cdot \left(\sum_{s=0}^{v-1} q^{-3s} \; + \; \frac{q}{q+1} \cdot \|h\| \cdot \sum_{s=v}^{\infty} q^{-2s} \right)$$

where v is defined by $\|h\| = q^{-v}$. A straightforward computation now gives:

$$\int_A \|N_{F^2/F}(t)\|\, dt = \frac{q^2}{q^2+q+1} \cdot \|h\| - \frac{q^3}{(q+1)^2\,(q^2+q+1)} \cdot \|h\|^4.$$

which concludes the proof thanks to the formulas for extremal degrees of Theorem 4.8. □

Using the transformation formulas reported in Theorem 4.8, we can derive from Proposition 4.9 the values of $\rho_{F^2,n}$ on the whole domain F^2. Indeed, if $x \in \mathcal{O}_F$ and $y \in F \backslash \mathcal{O}_F$, considering the homography $t \mapsto \frac{1}{1-x+t}$, we get

$$\rho_{F^2,n}(x,y) = \|1-x+y\|^{-2} \cdot \rho_{F^2,n}(1,y') = \|y\|^{-2} \cdot \rho_{F^2,n}(1,y')$$

with $y' = \frac{1}{1-x+y}$. From the fact that $1 - x + y' \notin \mathcal{O}_F$, we deduce that y' is in the maximal ideal of F and so $\|1 - y'\| = 1$. Applying Proposition 4.9, we finally find:

$$\begin{aligned} \rho_{F^2,2}(x,y) &= \frac{q^2}{q^2+q+1} \cdot \|y\|^{-2} \\ \text{for } n \geq 3, \quad \rho_{F^2,n}(x,y) &= \frac{q^2}{(q+1)^2} \cdot \|y\|^{-2} \end{aligned}$$

in this case. Similarly when both x and y do not belong to $\mathcal{O}_F$, we use the homography $t \mapsto t^{-1}$ and get:

$$\begin{aligned} \rho_{F^2,2}(x,y) &= \frac{q^2}{q^2+q+1} \cdot \frac{\|x-y\|}{\|x\|^2 \cdot \|y\|^2} \\ \text{for } n \geq 3, \quad \rho_{F^2,n}(x,y) &= \frac{q^2}{q^2+q+1} \cdot \frac{\|x-y\|}{\|x\|^2 \cdot \|y\|^2} - \frac{q^3}{(q+1)^2\,(q^2+q+1)} \cdot \frac{\|x-y\|}{\|x\|^5 \cdot \|y\|^5}. \end{aligned}$$

Applications to covariances

Proposition 4.6 tells us that the integral of $\rho_{F^2,n}$ over F^2 gives twice the second factorial of the random variable $Z_{F,n}^{\text{new}} = Z_{F,n}$ (which was already computed in [3]; it is the value called $\rho(2,n)$ in *loc. cit.*). Similarly, it turns out that we can obtain information about the variances and covariances of the random variables $Z_{U,n}$ for $U \subset F$ by integrating over smaller domains.

Proposition 4.10. *For any positive integer n and any open subsets U and V of F, we have:*

$$\mathbb{E}\big[Z_{U,n}{\cdot}Z_{V,n}\big] \;=\; \int_U \int_V \rho_{F^2,n}(x,y)\,dx\,dy \;+\; \int_{U\cap V} \rho_{F,n}(x)\,dx.$$

Proof. The étale algebra F^2 admits a unique subalgebra, which is F embedded diagonally. Hence, applying Theorem 4.8 with the open subset $W = U \times V \subset F^2$, we get:

$$\mathbb{E}\big[Z_{U,n}{\cdot}Z_{V,n}\big] = \mathbb{E}\big[Z_{W,n}\big] = \int_W \rho_{F^2,n}(x)\,dx \;+\; \int_{W\cap F} \rho_{F,n}(x)\,dx.$$

Given that F is embedded diagonally in F^2, the intersection $W \cap F$ is the set of elements $x \in F$ such that $(x,x) \in W = U \times V$, *i.e.* $W \cap F = U \cap V$. The proposition follows. □

When U and V are open balls of $\mathcal{O}_F$, one can fully compute the integrals of Proposition 4.10 and come up with closed formulas for the mean of $Z_{U,n}{\cdot}Z_{V,n}$ and then for the covariance of $Z_{U,n}$ and $Z_{V,n}$. The easiest case occurs when U are V are disjoint; indeed, under this additional assumption, the distance $\|x-y\|$ does not vary when x runs over U and V runs over V. According to Proposition 4.9, the function $\rho_{F^2,n}$ is then constant over $U \times V$ and it is easy to integrate it. Doing so, we end up with the formula given in Theorem F (in the introduction).

On the contrary, when $V \subset U$, the computation is a bit more painful but can nevertheless be carried out without trouble. For $n \geq 3$, the final result we obtain reads:

$$\begin{aligned}\mathbb{E}\big[Z_{U,n}{\cdot}Z_{V,n}\big] \;=\; &\frac{q}{q+1}{\cdot}\lambda(V) \;+\; \frac{q^3}{(q+1)\,(q^2+q+1)}{\cdot}\lambda(U)^2{\cdot}\lambda(V) \\ &-\; \frac{q^7}{(q+1)^2\,(q^2+q+1)\,(q^4+q^3+q^2+q+1)}{\cdot}\lambda(U)^5{\cdot}\lambda(V)\end{aligned}$$

where we recall that λ denotes the Haar measure on F.

Numerical simulations

As we did in §2.4, we conducted some numerical experients illustrating the results of this subsection: we picked a sample of $500,000$ random polynomials over $\mathbb{Z}_2$ and located the pairs of *distincts* roots of those polynomials (which are exactly their new roots in $\mathbb{Q}_2^2$) in the 2-adic plane. The results we obtained are reported on Fig. 4; we refer to §2.4 for some explanations on the way of reading this figure. In agreement with Proposition 4.9, we observe that pairs of roots are less and less numerous when we gettting closer to the diagonal.

Beyond this, it is also quite interesting to compare Fig. 4 with Fig. 3 (on page 24). Indeed, given than $\mathbb{Q}_2^2$ and $\mathbb{Q}_4$ have both discriminant of norm 1, we might expect at first glance the number of new roots in both algebras to be comparable. However, looking at the pictures, we clearly see that Fig. 4 is much brighter than its counterpart. In other words,

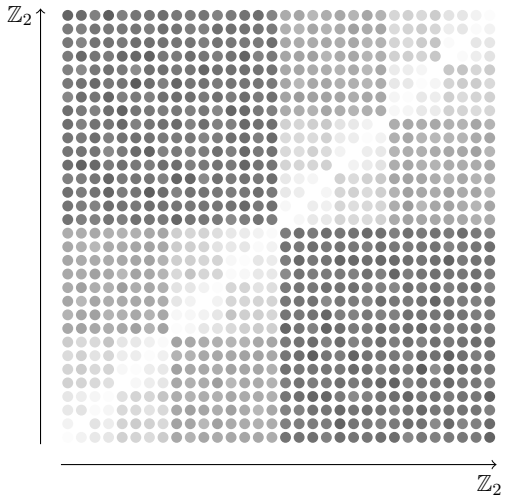

Figure 4: Repartition of pairs of distinct roots of a polynomial. Sample of $500{,}000$ polynomials over $\mathbb{Z}_2$ picked uniformly at random.

the conclusion of our numerical experiments is that there are significantly much more new roots in $\mathbb{Q}_4$ than in $\mathbb{Q}_2^2$. Coming back to Propositions 2.2 and 4.9, we realize that the aforementioned phenomenon can be explained by looking at the term of higher order (that is the term in $\mathrm{dist}(x,\mathbb{Q}_2)^4$ in the case of $\mathbb{Q}_4$ and the term in $\|x-y\|^4$ in the case of $\mathbb{Q}_2^2$); indeed, this term contributes positively (*i.e.* it comes with a plus sign) in the case of $\mathbb{Q}_4$ whereas it contributes negatively in the case of $\mathbb{Q}_2^2$. When we are sufficiently far away from $\mathbb{Q}_2$, this error term is no longer negligible and the change of sign makes a big difference.

4.4 A mass formula

In this last subsection, we prove Theorem G. For a positive integer r, we denote by $\mathbf{\acute{E}t}_r$ the set of isomorphism classes of étale algebras of degree r over F. To simplify notation, we set:

$$\Sigma(r,n) = \sum_{E \in \mathbf{\acute{E}t}_r} \frac{\rho_n(E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)}$$

for all integers r and n. Our goal is to prove that $\Sigma(r,n) = 1$ provided that $n \geq r$. We first consider the extreme case where $n = r$, for which we have the following nice reinterpretation of the summands above.

Proposition 4.11. *For a finite étale F-algebra E of degree r, we have:*

$$\frac{\rho_r(E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} = \int_{\Omega_r} \mathbb{1}_{\{F[X]/P \simeq E\}}\, dP.$$

Proof. From Theorem 4.8, we know that:

$$\rho_r(E) = \mathbb{E}\big[Z_{E,r}^{\mathrm{new}}\big] = \int_{\Omega_r} \#\mathrm{Hom}_{F\text{-alg}}^{\mathrm{surj}}\big(F[X]/P,\, E\big)\, dP. \tag{25}$$

If P is a polynomial of degree r, the quotient algebra $F[X]/P$ has degree r as well and so, any surjective homomorphism of F-algebras $F[X]/P \to E$ has to be an isomorphism. Consequently, the integrand in Eq. (25) is equal to $\#\mathrm{Aut}_{F\text{-alg}}(E)$ if $F[X]/P \simeq E$, and it vanishes otherwise. The proposition follows. □

Proposition 4.11 tells us that $\rho_r(E)/\#\mathrm{Aut}_{F\text{-alg}}(E)$ is exactly the probability that a random polynomial $P \in \Omega_r$ satisfies $F[X]/P \simeq E$. On the other hand, note that the quotient $F[X]/P$ is an étale F-algebra of degree r as soon as P is separable. This event then occurs almost surely. Therefore the probabilities that $F[X]/P \simeq E$ sum up to 1 when E runs over $\mathbf{Ét}_r$, *i.e.* $\Sigma(r,r) = 1$. Theorem G is then proved when $n = r$.

For higher n, the key ingredient of the proof is the following symmetry result.

Lemma 4.12. *For $n > r$, we have $\Sigma(r,n) = \Sigma(n-r,n)$.*

Proof. Unrolling the definitions of $\Sigma(r,n)$ and $\rho_n(E)$, we obtain:

$$\Sigma(r,n) = \int_{\Omega_n} \sum_{E \in \mathbf{Ét}_r} \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(F[X]/P,\, E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)}\, dP.$$

Pick a separable polynomial $P \in \Omega_n$ and set $E_P = F[X]/P$; it is an étale F-algebra of degree n. Define $\mathbf{Ét}_r[P]$ as the subset of $\mathbf{Ét}_r$ consisting of étale algebras E for which there exists a surjective morphism of F-algebras $E_P \to E$. Let $E \in \mathbf{Ét}_r[P]$ and choose writings $E_P = K_1^{a_1} \times \cdots \times K_m^{a_m}$ and $E = K_1^{b_1} \times \cdots \times K_m^{b_m}$ where the K_i's are pairwise nonisomorphic finite extensions of F and $a_i, b_i \in \mathbb{Z}_{\geq 0}$. From Corollary 4.2, we deduce that $a_i \geq b_i$ for all $i \in \{1,\dots,m\}$ and that:

$$\frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} = \binom{a_1}{b_1} \cdot \binom{a_2}{b_2} \cdots \binom{a_m}{b_m}.$$

Hence, if we define $E^\vee = K_1^{a_1-b_1} \times \cdots \times K_m^{a_m-b_m}$, we find:

$$\frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} = \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E^\vee)}{\#\mathrm{Aut}_{F\text{-alg}}(E^\vee)}.$$

Moreover, it follows again from Corollary 4.2 that the association $E \mapsto E^\vee$ induces a well-defined function $\mathbf{Ét}_r[P] \to \mathbf{Ét}_{n-r}[P]$. This function is moreover bijective because its inverse can be built in a similar fashion. We conclude that, for a fixed separable polynomial $P \in \Omega_n$, we have:

$$\sum_{E \in \mathbf{Ét}_r[P]} \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} = \sum_{E^\vee \in \mathbf{Ét}_{n-r}[P]} \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E^\vee)}{\#\mathrm{Aut}_{F\text{-alg}}(E^\vee)}$$

which further gives:

$$\sum_{E \in \mathbf{Ét}_r} \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E)}{\#\mathrm{Aut}_{F\text{-alg}}(E)} = \sum_{E^\vee \in \mathbf{Ét}_{n-r}} \frac{\#\mathrm{Hom}^{\mathrm{surj}}_{F\text{-alg}}(E_P,\, E^\vee)}{\#\mathrm{Aut}_{F\text{-alg}}(E^\vee)}$$

since all the additional summands which appear in both sums are zero. Taking finally the integral over Ω_n and remembering that a polynomial in Ω_n is almost surely separable, we obtain the lemma. □

After Lemma 4.12, it is easy to conclude the proof of Theorem G by induction on n. When $n = 1$, the condition $n \geq r$ indicates that $r = 1$ as well and we fall in the case where $n = r$, which has been already treated. We now pick an integer $n > 1$ and assume that $\Sigma(r,m) = 1$ provided that $1 \leq r \leq m < n$. Let also $r \in \{1,\dots,n\}$. If $n = r$, we have

already seen that $\Sigma(r,n)=1$ and there is nothing more to prove. If $r \leq n/2$, it follows from the fourth property of Theorem 4.8 that $\Sigma(r,n)=\Sigma(r,2r-1)$, from what we deduce that $\Sigma(r,n)=1$ thanks to our induction hypothesis. Finally, if $n/2 \leq r < n$, we use Lemma 4.12 to write $\Sigma(r,n)=\Sigma(n-r,n)$ and, observing that $0 < n-r \leq n/2$, we conclude by applying the previous case.

References

[1] R. Ait El Mannsour, A. Lerario, *Probabilisitc enumerative geometry over p-adic numbers: linear spaces on complete intersections*, preprint (2020)

[2] M. Bhargava, *Mass Formulae for Extensions of Local Fields, and Conjectures on the Density of Number Field Discriminants*, Int. Math. Res. Notices (2007)

[3] M. Bhargava, J. Cremona, T. Fisher, S. Gajović, *The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$*, preprint (2021)

[4] A. Bloch, G. Pólya, *On the roots of certain algebraic equations*, Proc. Lond. Math. Soc **33** (1932), 102–114

[5] J. Buhler, D. Goldstein, D. Moews, J. Rosenberg, *The probability that a random monic p-adic polynomial splits*, Exper. Math. **15** (2006), 21–32

[6] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (2014), 274–294

[7] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics **193** (2000), Springer Verlag

[8] S. Evans, *The expected number of zeros of a random system of p-adic polynomials*, Electron. Comm. Probab. **11** (2006), 278–290

[9] T. Gronwall, *Some Asymptotic Expressions in the Theory of Numbers*, Trans. Amer. Math. Soc. **14** (1913), 113–122

[10] M. Kac, *On the average number of real roots of a random algebraic equation*, Bull. Math. Amer. Soc **49** (1943), 314–320

[11] A. Lerario, A. Kulkarni, *p-adic integral geometry*, SIAM J. Appl. Algebra Geom. **5** (2020), 28–59

[12] D. Limmer, *Measure-equivalence of quadratic forms*, Ph.D. Thesis, Oregon State University (1999)

[13] J. Littlewood, A. Offord, *On the number of real roots of a random algebraic equation (i)*, J. London Math. Soc **13** (1938), 288–295

[14] J. Littlewood, A. Offord, *On the number of real roots of a random algebraic equation (ii)*, Proc. Camb. Phil. Soc. **39** (1959), 133–148

[15] J. Littlewood, A. Offord, *On the number of real roots of a random algebraic equation (iii)*, Rec. Math. (Mat. Sbornik) **54** (1943), 277–286

[16] S. Rice, *Mathematical analysis of random noise*, Bell Syst. Tech. J. **23** (1944), 282–332

[17] A. Robert, *A course in p-adic analysis*. Springer Science & Business Media **198** (2000)

[18] J.-P. Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris **286** (1978), 1031–1036

[19] J.-P. Serre, *Local fields*, Graduate Texts in Math. **67** (1979), Springer New York

[20] R. Shmueli, *The expected number of roots over the field of p-adic numbers*, preprint (2021)