THE PROBABILITY THAT A p-ADIC RANDOM ÉTALE ALGEBRA IS AN UNRAMIFIED FIELD

ROY SHMUELI

Abstract. We study the random étale algebra generated by a random polynomial with i.i.d. coefficients distributed according to Haar measure normalized on \( \mathbb{Z}_p \). We determine the probability that this random algebra is an unramified field, explicitly. In addition, we prove a private case of a conjecture made by Bhargava, Cremona, Fisher and Gajović. More precisely, we show that this probability is a rational function of \( p \) that is invariant under replacing \( p \) by \( 1/p \).

1. Introduction

For any positive integer \( n \), let \( f_n \) be the random polynomial

\[ f_n(X) = \xi_0 + \xi_1 X + \cdots + \xi_n X^n, \]

where \( \xi_0, \ldots, \xi_n \) are independent and identically distributed random variables taking values in \( \mathbb{Z}_p \) and distributed according to the normalized Haar measure on \( \mathbb{Z}_p \). In this paper, we study the random algebra \( A_n := \mathbb{Q}_p[X]/\langle f_n \rangle \). This algebra is étale, almost surely. Therefore, it induces a splitting type.

A splitting type of degree \( n \) is a tuple \( \sigma = (d_1^{e_1} \cdots d_k^{e_k}) \), where \( d_i \) and \( e_i \) are positive integers satisfying \( \sum_{i=1}^k d_i e_i = n \). We allow repeats in the list of symbols \( d_i^{e_i} \), but the order in which they appear does not matter.

For an étale algebra extension \( A/\mathbb{Q}_p \) of degree \( n \), we define its splitting type to be \( \sigma(A) = (d_1^{e_1} \cdots d_k^{e_k}) \) if \( p \) factors in \( A \) as \( p^{e_1} \cdots p^{e_k} \) where \( p_1, \ldots, p_k \) are primes in \( A \) having residue field degrees \( d_1, \ldots, d_k \) respectively.

In [BCFG22], Bhargava, Cremona, Fisher and Gajović study the splitting type of \( A_n := \mathbb{Q}_p[X]/\langle f_n \rangle \). They calculated the probability that \( f_n \) has exactly \( r \) roots. This event is equivalent to the event that \( 1 \) appear exactly \( r \) times in \( \sigma(A_n) \). In their research they showed that this probability is a rational function in \( p \) which is invariant under replacing \( p \) by \( p^{-1} \).

Moreover, they conjectured a more general property on the probabilities of the splitting type:

For a splitting type \( \sigma \) of degree \( n \), let \( E_\sigma \) be the event that \( A_n \) is étale over \( \mathbb{Q}_p \) and \( \sigma(A_n) = \sigma \).

We define the following probabilities:

\[ \rho(\sigma; p) = \mathbb{P}(E_\sigma), \]

\[ \alpha(\sigma; p) = \mathbb{P}(E_\sigma | f_n \text{ monic}), \quad \text{and} \]

\[ \beta(\sigma; p) = \mathbb{P}(E_\sigma | f_n \text{ monic and } f_n \equiv X^n \pmod{p}). \]

Conjecture 1. Let \( \sigma \) be any splitting type. Then \( \rho(\sigma; p), \alpha(\sigma; p) \) and \( \beta(\sigma; p) \) are rational functions of \( p \) and satisfy the identities:

(1) \[ \rho(\sigma; p) = \rho(\sigma; p^{-1}), \quad \text{and} \]

(2) \[ \alpha(\sigma; p) = \beta(\sigma; p^{-1}). \]

We establish the conjecture in the case that the algebra is an unramified field, that is when \( \sigma = (n^1) \).
Theorem 2. For any positive integer $n$ there exists a rational function $J_n^* \in \mathbb{Q}(t)$ such that for

$$\sigma = (n^1)$$

we have

(3) \quad \rho(\sigma; p) = \frac{p - 1}{p^{n+1} - 1} \left( p^n J_n^*(p) + J_n^*(p^{-1}) \right),

(4) \quad \alpha(\sigma; p) = J_n^*(p), \quad \text{and}

(5) \quad \beta(\sigma; p) = J_n^*(p^{-1}).

The function $J_n^*$ in Theorem 2 is given by explicit recursive formula: Let $J_1(u, v) = 1$ and for $n > 1$ let

(6) \quad J_n(u, v) = \frac{1}{u^{n-1} - v^{n-1}} \sum_{1 \not| \neq d| n} v^{n/d - 1} \left( \sum_{c|d} \mu\left( \frac{d}{c} \right) u^{c-1} \right) J_{n/d}(u^d, v).

Here $\mu$ is the Möbius function. We then define $J_n^*$ by

(7) \quad J_n^*(t) = \frac{1}{n} J_n(t, t^{-n/2}).

When $n$ is odd, the powers of $v$ on the right side of (6) are even except in the arguments of $J_{n/d}$, therefore an inductive argument gives that $J_n^*$ is rational.

Acknowledgements. I thank Itai Bar-Deroma and Sahar Diskin for their feedback on the research. I also thank Eli Glasner for his support in the research and my supervisor, Lior Bary-Soroker for his conversions and ideas.

This research was partially supported by grants from the Israel Science Foundation, grant no. 702/19 and grant no. 1194/19.

2. Notations and Generalities

Let $F$ be a $p$-adic field. We denote its valuation ring by $\mathcal{O}_F$ and its maximal ideal by $m_F$.

2.1. Absolute value. We denote by $|\cdot|_F$ the $p$-adic absolute value normalized such that $|\pi|_F = q^{-1}$, where $\pi$ is the uniformizer of $F$ and $q$ is the size of the residue field of $F$. In the case $F = \mathbb{Q}_p$, we abbreviate and write $|\cdot|_p$ instead of $|\cdot|_{\mathbb{Q}_p}$.

Each absolute value $|\cdot|_F$ can be extended uniquely to an absolute value on the algebraic closure of $\mathbb{Q}_p$, and all of those extensions are equivalent. For field extension $K/F$ of degree $n$, we have that $|x|_K = |x|^n_F$ for any $x$ in the algebraic closure of $\mathbb{Q}_p$.

2.2. Haar measure. We denote with $\lambda_F$ the normalized Haar measure on $F$, that is, the unique measure which is locally finite, regular, invariant to translations and satisfies $\lambda_F(\mathcal{O}_F) = 1$. We have that for any $\alpha \in F$ and a Borel set $S \subseteq F$ then $\lambda_F(\alpha S) = |\alpha|_F \lambda_F(S)$.

In this paper, all the integrals on $F$ are Lebesgue integrals according to $\lambda_F$.

2.3. Discriminant. Let $K/F$ be a field extension of degree $n$. For elements $\omega_1, \ldots, \omega_n \in K$ we define their discriminant to be

$$\Delta_{K/F}(\omega_1, \ldots, \omega_n) = \det \left( (T_{K/F}(\omega_i \omega_j))_{1 \leq i \leq n} \right),$$

where $T_{K/F}$ is the field trace. If $L$ is $F$-linear map from $K$ to $K$ and mapping $\omega_1, \ldots, \omega_n$ to $\omega_1', \ldots, \omega_n'$ then

(8) \quad \Delta_{K/F}(\omega_1', \ldots, \omega_n') = (\det L)^2 \Delta_{K/F}(\omega_1, \ldots, \omega_n).

In addition, for $x \in K$, we define the discriminant of $x$ to be $\Delta_{K/F}(x) = \Delta_{K/F}(1, x, \ldots, x^{n-1})$. We have that $K = F[x]$ if and only if $\Delta_{K/F}(x) \neq 0$. Moreover, if $K = F[x]$ then $\Delta_{K/F}(x)$ is the discriminant of the minimal polynomial over $F$.

When $\omega_1, \ldots, \omega_n$ are $\mathcal{O}_F$-basis of $\mathcal{O}_K$ then $\Delta_{K/F}(\omega_1, \ldots, \omega_n)$ is the field discriminant of $K$ relative to $F$ which we denote with $D_{K/F}$. The field discriminant is not depends on the choice of $\omega_1, \ldots, \omega_n$ up to multiplication by a unit. Therefore, the absolute value of the discriminant,
\(|D_{K/F}|_p\), is invariant to the choice of \(\omega_1, \ldots, \omega_n\). Also, we have that \(K/F\) is unramified if and only if the uniformizer of \(F\) divides \(D_{K/F}\).

3. The inversion formula

In this section we prove an inversion formula for \(J_n\):

**Proposition 3.** For any \(n \in \mathbb{N}\),

\[
J_n\left(u^{-1}, v^{-1}\right) = v^{n-1}J_n(u, v).
\]

We prove this proposition using the theory of incidence algebras which we introduce below. For more information on the subject see [SO97].

3.1. Incidence algebras. Let \((P, \leq)\) be a poset. For \(x, y \in P\), we define the interval between \(x\) and \(y\) to be the subset

\[
[x, y]_P = \{z \in P : x \leq z \leq y\}.
\]

We say that a poset \(P\) is a locally finite poset if \([x, y]_P\) is finite set for each \(x, y \in P\).

A sequence \(z = (x_0, \ldots, x_k)\) of elements in \(P\) is called a proper chain in \(P\) of length \(k + 1\) if \(x_0 < x_1 < \cdots < x_k\).

We also say that \(z\) starts at \(x_0\) and ends at \(x_k\). In addition, let \(C^k_P(x, y)\) denote the set of all proper chains of length \(k + 1\) that start at \(x\) and ends at \(y\). And, let \(C^k_P(x, y)\) denote the set of all proper chains that start at \(x\) and ends at \(y\), i.e. \(C^k_P(x, y) = \bigcup_{i=0}^{\infty} C^i_P(x, y)\).

For two chains \(z, w \in C^k_P(x, y)\) we say that \(w\) is finer than \(z\) if \(z\) is a sub-sequence of \(w\). For a proper chain \(z = (z_0, \ldots, z_k)\), we denote with \(C^m_P(z_0, \ldots, z_k)\) the set of all proper chains of length \(m + 1\) which are finer than \(z\). Note that for any non-negative integer \(m\) we have

\[
\#C^m_P(z_0, \ldots, z_k) = \sum_{m_1 + \cdots + m_k = m} \prod_{i=1}^k \#C^{m_i}_P(z_{i-1}, z_i).
\]

Let \(P\) be a locally finite poset and let \(A\) be a commutative ring with unity. The incidence \(A\)-algebra of \(P\), denoted by \(I_A(P)\), is the algebra whose elements are \(\varepsilon: P^2 \to A\) such that \(\varepsilon(x, y) = 0\) for all \(x \not< y\). The operations are defined as followed:

\[
(\varepsilon_1 + \varepsilon_2)(x, y) = \varepsilon_1(x, y) + \varepsilon_2(x, y),
\]

\[
(\varepsilon_1 \cdot \varepsilon_2)(x, y) = \sum_{x \leq z \leq y} \varepsilon_1(x, z)\varepsilon_2(z, y),
\]

\[
(a \cdot \varepsilon)(x, y) = a\varepsilon(x, y),
\]

for all \(x, y \in P, \varepsilon, \varepsilon_1, \varepsilon_2 \in I_A(P)\) and \(a \in A\).

Let

\[
\delta(x, y) = \begin{cases} 1, & x = y, \\ 0, & \text{otherwise}. \end{cases}
\]

Then \(\delta\) is the identity element of \(I_A(P)\).

We have the following lemmas describe the invertible elements in \(I_A(P)\).

**Lemma 4.** An element \(\varepsilon \in I_A(P)\) is invertible if and only if \(\varepsilon(x, x)\) is invertible in \(A\) for each \(x \in P\). In that case, \(\varepsilon^{-1}\) is defined recursively: for any \(x \in P\), we have that \(\varepsilon^{-1}(x, x) = \varepsilon(x, x)^{-1}\) and for any \(x < y\)

\[
\varepsilon^{-1}(x, y) = \varepsilon(x, x)^{-1} \sum_{x \leq z \leq y} \varepsilon(x, z)\varepsilon^{-1}(z, y).
\]

**Proof.** See [SO97, Theorem 1.2.3] and its proof. \(\square\)

**Lemma 5.** Assume that \(\varepsilon(x, x) = 1\) for all \(x \in P\). Then, for all \(x, y \in P\),

\[
\varepsilon^{-1}(x, y) = \sum_{(z_0, \ldots, z_k) \in C^k_P(x, y)} (-1)^{k-1} \prod_{i=0}^{k-1} \varepsilon(z_i, z_{i+1}).
\]
Lemma 4. We prove this with induction on \( x \). For the induction base \( x = y \), and by Lemma 4 we get that \( \varepsilon^{-1}(x, x) = 1 \). Moreover, the sum on the right side of the equation is also 1 since there is a single chain from \( x \) to \( x \).

For the induction step, let \( x < y \). By Lemma 4 we have that

\[
\varepsilon^{-1}(x, y) = - \sum_{z < y} \varepsilon(x, z) \varepsilon^{-1}(z, y).
\]

We use the induction assumption to obtain

\[
\varepsilon^{-1}(x, y) = - \sum_{z < y} \varepsilon(x, z) \sum_{(z_0, \ldots, z_k) \in \mathcal{C}_P(z, y)} (-1)^{k+1} \varepsilon(z, z_{i+1}).
\]

We rearrange the factors

\[
\varepsilon^{-1}(x, y) = \sum_{x < z \leq y} \sum_{(z_0, \ldots, z_k) \in \mathcal{C}_P(z, y)} (-1)^{k+1} \varepsilon(x, z) \prod_{i=0}^{k-1} \varepsilon(z, z_{i+1}).
\]

Running over all \( x < z \leq y \) and then over all chains \((z_0, \ldots, z_k) \in \mathcal{C}_P(z, y)\) is the same as running over all chains \((w_0, \ldots, w_k) \in \mathcal{C}_P(x, y)\) with \( z \) being the first element in the chain after \( x \). Thus,

\[
\varepsilon^{-1}(x, y) = \sum_{(w_0, \ldots, w_k) \in \mathcal{C}_P(x, y)} (-1)^{k} \prod_{i=0}^{k-1} \varepsilon(w_i, w_{i+1}). \tag{10}
\]

Let \( Q \subseteq P \), by abuse of notation we let \( Q \) denotes the poset composed of the elements of \( Q \) and the order \( \leq \) restricted to \( Q^2 \). For \( \varepsilon \in I_A(P) \) we have that \( \varepsilon|_Q \in I_A(Q) \). For \( \varepsilon, \varepsilon_1, \varepsilon_2 \in I_A(P) \), we denote with \( \varepsilon_1 \ast_Q \varepsilon_2 \) the multiplication of \( \varepsilon_1|_Q \) and \( \varepsilon_2|_Q \) in \( I_A(Q) \) and with \( \text{Inv}_Q \varepsilon \) the inverse of \( \varepsilon|_Q \) in \( I_A(Q) \).

Corollary 6. Let \( Q, Q' \subseteq P \) and \( x, y \in P \) such that \([x, y]_Q = [x, y]_{Q'}\). Then for all \( \varepsilon \in I_A(P) \)

\[
\text{Inv}_Q \varepsilon(x, y) = \text{Inv}_{Q'} \varepsilon(x, y).
\]

Proof. This is immediate from Lemma 5 since \( \mathcal{C}_Q(x, y) = \mathcal{C}_{Q'}(x, y) \). \( \square \)

We add a definition that will be useful in the next subsections.

Definition 7. Let \( x \leq y \) and let \( Q, Q' \subseteq P \), we say that \( Q \) and \( Q' \) are complementing the interval \([x, y]_P\) if \( x, y \in Q \cap Q' \) and for any \( x < z < y \) then either \( z \in Q \) or \( z \in Q' \) but not both.

3.2. The M"obius function. We define the following function \( \zeta \in I_A(P) \) by

\[
\zeta(x, y) = \begin{cases} 
1, & x \leq y, \\
0, & \text{otherwise}.
\end{cases}
\]

By Lemma 4 we have that \( \zeta \) is invertible and its inverse, \( \mu \), satisfy

\[
\mu(x, y) = - \sum_{x < z \leq y} \mu(z, y). \tag{10}
\]

Moreover, since \( \zeta(x, x) = 1 \) for all \( x \in P \), Lemma 5 gives that

\[
\mu(x, y) = \sum_{k=0}^{\infty} (-1)^k \# \mathcal{C}_P^k(x, y). \tag{11}
\]

We call \( \mu \) the M"obius function on \( P \). For \( Q \subseteq P \), we denote by \( \mu_Q \) the M"obius function on \( Q \), i.e. \( \mu_Q = \text{Inv}_Q \zeta \).

Lemma 8. Let \( x < y \) and let \( Q, Q' \subseteq P \) which are complementing the interval \([x, y]_P\). Then

\[
\text{Inv}_Q \mu(x, y) = - \mu_{Q'}(x, y).
\]
Proof. By Lemma 5 we have

\[ \text{Inv}_Q \mu(x, y) = \sum_{(z_0, \ldots, z_k) \in C^*_Q(x, y)} (-1)^k \prod_{i=1}^{k} \mu(z_{i-1}, z_i). \]

By (11) we get

\[ \text{Inv}_Q \mu(x, y) = \sum_{(z_0, \ldots, z_k) \in C^*_Q(x, y)} (-1)^k \prod_{i=1}^{k} \left( \sum_{m=0}^{\infty} (-1)^m \#C^m_P(z_{i-1}, z_i) \right). \]

We expand the multiplication and then use (9) to obtain

\[ \text{Inv}_Q \mu(x, y) = \sum_{(z_0, \ldots, z_k) \in C^*_Q(x, y)} (-1)^k \sum_{m=0}^{\infty} (-1)^m \prod_{i=1}^{k} \#C^m_P(z_{i-1}, z_i). \]

Changing the order of summation gives that

\[ \text{Inv}_Q \mu(x, y) = \sum_{m=0}^{\infty} (-1)^m \sum_{(z_0, \ldots, z_k) \in C^*_Q(x, y)} (-1)^k \#C^m_P(z_0, \ldots, z_k). \]

From the inclusion–exclusion principle we have that

\[ \#C^m_Q(x, y) = \#C^m_P(x, y) - \sum_{x < z_1 < y \atop z_1 \in Q} \#C^m_P(x, z_1, y) + \sum_{x < z_1 < z_2 < y \atop z_1, z_2 \in Q} \#C^m_P(x, z_1, z_2, y) - \ldots \]

\[ = - \sum_{(z_0, \ldots, z_k) \in C^*_Q(x, y)} (-1)^k \#C^m_P(z_0, \ldots, z_k). \]

We plug this into (12) and get that

\[ \text{Inv}_Q \mu(x, y) = - \sum_{m=0}^{\infty} (-1)^m \#C^m_Q(x, y). \]

Applying Lemma 5 on left side of the equation finishes the proof. \( \square \)

We define the function \( \Gamma_Q : P \times Q \to A \) by

\[ \Gamma_Q(x, y) = \sum_{x \leq z \leq y \atop z \in Q} \mu(x, z) \text{Inv}_Q \mu(z, y). \]

Lemma 9. Let \( Q \subseteq P \). Then for all \( x \in P \) and \( y \in Q \) we have that

\[ \Gamma_Q(x, y) = \begin{cases} - \text{Inv}_{Q \cup \{x\}} \mu(x, y), & x \notin Q, \\ 1, & x = y, \\ 0, & \text{otherwise}. \end{cases} \]

Proof. We start with the case of \( x \in Q \). In this case we can write \( \Gamma_Q(x, y) \) as multiplication in \( I_A(Q) \) as follows

\[ \Gamma_Q(x, y) = (\mu \ast_Q \text{Inv}_Q \mu)(x, y). \]

Clearly, \( \mu \ast_Q \text{Inv}_Q \mu = \delta \) and this finish the case when \( x \in Q \).

If \( x \notin Q \), then we have by Lemma 4 that

\[ - \text{Inv}_{Q \cup \{x\}} \mu(x, y) = \sum_{x \leq z \leq y \atop z \in Q \cup \{x\}} \mu(x, z) \text{Inv}_{Q \cup \{x\}} \mu(z, y). \]
From Corollary 6 we conclude that $\text{Inv}_{Q \cup \{x\}} \mu(z, y) = \text{Inv}_Q \mu(z, y)$ for all $x < z$. Hence, 

$$-\mu_{Q \cup \{y\}}(x, y) = \sum_{x \leq z \leq y} \mu(x, z) \text{Inv}_Q \mu(z, y) = \Gamma_Q(x, y).$$

\hfill \Box

3.3. The $\theta$ polynomial. Set $A_P = \mathbb{Q}[t_x : x \in P]$ where $t_x$ are algebraically independent elements over $Q$. We define the following function $\theta \in I_{A_P}(P)$ by

$$\theta(x, y) = \sum_{x \leq z \leq y} \mu(z, y) \frac{t_z}{t_x}$$

(14)

If there is no risk for ambiguity we write $\theta(x, y)$ instead of $\theta(x, y; \Gamma)$. Note that $\theta(x, x) = 1$ for all $x \in P$, hence $\theta$ is invertible by Lemma 4. We are interested in finding $\text{Inv}_Q \theta$ for different subposets $Q \subseteq P$.

**Definition 10.** Let $Q \subseteq P$. We say that a monomial $m \in A_P$ is $Q$-admissible if there exists $z_1, \ldots, z_k, y \in Q$ and $w_1, \ldots, w_k \in P$ such that

$$m = \frac{t_{w_1}}{t_{z_1}} \cdots \frac{t_{w_k}}{t_{z_k}}, \quad \text{and} \quad z_1 \leq w_1 \leq z_2 \leq w_2 \leq \cdots \leq z_k \leq w_k \leq y.$$

If $\frac{t_{w_1}}{t_{z_1}} \cdots \frac{t_{w_k}}{t_{z_k}}$ is a reduced fraction that is, $w_i \not\equiv z_j$ for all $i$ and $j$, we call it the admissible form of $m$.

We denote by $M(Q)$ the set of all $Q$-admissible monomials.

**Lemma 11.** Let $Q \subseteq P$ and let $x, y \in Q$. Then $\text{Inv}_Q \theta(x, y) \in \text{Span}_Q M\left([x, y]_Q \right)$. Moreover, let $m \in M\left([x, y]_Q \right)$ with admissible form $\frac{t_{w_1}}{t_{z_1}} \cdots \frac{t_{w_k}}{t_{z_k}}$ then the coefficient of $m$ in $\text{Inv}_Q \theta(x, y)$ is:

$$[\text{Inv}_Q \theta(x, y)]_m = \text{Inv}_Q \mu(x, z_1) \prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_{i+1}),$$

where $z_{k+1} = y$ and $Q_i = Q \cup \{w_i\}$.

**Proof.** We prove this with induction on $x$. For the induction base we have that $x = y$. In this case, $M\left([x, y]_Q \right) = \{1\}$ and $\text{Inv}_Q \theta(x, y) = 1$ so the lemma is clear.

For the induction step we have $y > x$, and we assume that for all $y \geq z > x$ we have $\text{Inv}_Q \theta(z, y) \in \text{Span}_Q M\left([z, y]_Q \right)$ and the coefficients of $\text{Inv}_Q \theta(z, y)$ are as described in this lemma.

By Lemma 4,

$$\text{Inv}_Q \theta(x, y) = -\sum_{x < z \leq y} \theta(x, z) \cdot \text{Inv}_Q \theta(z, y).$$

(16)

From definition, we have that $\theta(x, z) \in \text{Span}_Q \{t_w/t_x : x \leq w \leq z\}$. Together with the induction assumption we infer that $\theta(x, z) \cdot \text{Inv}_Q \theta(z, y) \in \text{Span}_Q M\left([x, y]_Q \right)$ for all $x < z \leq y$. Therefore, we get from (16) that $\text{Inv}_Q \theta(x, y) \in \text{Span}_Q M\left([x, y]_Q \right)$.

Next, we prove (15). Let $m \in M\left([x, y]_Q \right)$ with admissible form $\frac{t_{w_1}}{t_{z_1}} \cdots \frac{t_{w_k}}{t_{z_k}}$. Set $m' = \frac{t_{w_2}}{t_{z_2}} \cdots \frac{t_{w_k}}{t_{z_k}}$ and $C = [\text{Inv}_Q \theta(z_2, y)]_{m'}$. So by the induction’s assumption and since $\mu_Q(z_2, z_2) = 1$ we have that

$$C = \prod_{i=2}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_{i+1}).$$

(17)

We split the proof into two cases:
Case 1: When $z_1 = x$. We take a look at the sum in (16), and we identify the $z$ which contributes to the coefficient of $m$. Since $m \notin \mathcal{M}(\langle x, y \rangle_Q)$, there are two kinds of summands that contains $m$:

- Summands with $z_1 < z < w_1$. Here $m$ appears from the multiplication of the monomial $\frac{t_z}{t_{z_1}}$ in $\theta(x, z)$ and the monomial $\frac{t_{w_1}}{t_z} \cdot m'$ in $\text{Inv}_Q(z, y)$.
- Summands with $w_1 \leq z \leq z_2$. Here $m$ appears from the multiplication of the monomial $\frac{t_{w_1}}{t_z}$ in $\theta(x, z)$ and the monomial $m'$ in $\text{Inv}_Q(z, y)$.

So from (16) we get that

$$[\text{Inv}_Q \theta(x, y)]_m = - \sum_{z_1 < z < w_1, z \in Q} \left[ \theta(z_1, z) \right]_{t_{z_1}/t_z} [\text{Inv}_Q \theta(z, y)]_{t_{w_1}/t_{z}} \cdot m' - \sum_{w_1 \leq z \leq z_2, z \in Q} \left[ \theta(z_1, z) \right]_{t_{w_1}/t_z} [\text{Inv}_Q \theta(z, y)]_{m'}.$$  

And from the definition of $\theta$ (see (14)) we have that

$$(18) \quad [\text{Inv}_Q \theta(x, y)]_m = - \sum_{z_1 < z < w_1, z \in Q} [\text{Inv}_Q \theta(z, y)]_{t_{w_1}/t_{z}} \cdot m' - \sum_{w_1 \leq z \leq z_2, z \in Q} \mu(w_1, z) [\text{Inv}_Q \theta(z, y)]_{m'}.$$  

Next, we focus on the term $[\text{Inv}_Q \theta(z, y)]_{t_{w_1}/t_{z}} \cdot m'$, when $x < z < w_1$. Using the induction assumption gives

$$[\text{Inv}_Q \theta(z, y)]_{t_{w_1}/t_{z}} \cdot m' = \text{Inv}_Q \mu(z, z) \cdot \mu_Q(z_1, z, w_1) \Gamma_Q(w_1, z_2) \prod_{i=2}^{k} \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1).$$

And by (17) and $\mu_Q(z, z) = 1$ we obtain

$$(19) \quad [\text{Inv}_Q \theta(z, y)]_{t_{w_1}/t_{z}} \cdot m' = \mu_Q(z_1, z, w_1) \Gamma_Q(w_1, z_2) \cdot C.$$  

We move forward to the term $[\text{Inv}_Q \theta(z, y)]_{m'}$, when $w_1 \leq z \leq z_2$. From the induction assumption

$$[\text{Inv}_Q \theta(z, y)]_{m'} = \text{Inv}_Q \mu(z, z_2) \prod_{i=2}^{k} \mu_Q(w_i, z_i) \Gamma_Q(w_i, z_i+1).$$

And plugging in (17) gives

$$(20) \quad [\text{Inv}_Q \theta(z, y)]_{m'} = \text{Inv}_Q \mu(z, z_2) \cdot C.$$  

We plug (19) and (20) into (18) to get

$$(21) \quad [\text{Inv}_Q \theta(x, y)]_m = - \sum_{x < z < w_1, z \in Q} \mu_Q(z, w_1) \Gamma_Q(w_1, z_2) \cdot C - \sum_{w_1 \leq z \leq z_2, z \in Q} \mu(w_1, z) \text{Inv}_Q \mu(z, z_2) \cdot C.$$  

We look on the second sum of (21). So from (13) and since $\mu_Q(w_1, w_1) = 1$ we get

$$\sum_{w_1 \leq z \leq z_2, z \in Q} \mu(w_1, z) \text{Inv}_Q \mu(z, z_2) \cdot C = \mu_Q(w_1, w_1) \Gamma_Q(w_1, z_2) \cdot C.$$  

We put this in (21) and get that

$$[\text{Inv}_Q \theta(x, y)]_m = - \sum_{z_1 < z < w_1, z \in Q_1} \mu_Q(z, w_1) \cdot \Gamma_Q(w_1, z_2) C$$

Plugging (10), (17) and $\mu_Q(x, z_1) = 1$ into the last equation gives

$$[\text{Inv}_Q \theta(x, y)]_m = \mu_Q(z_1, w_1) \Gamma_Q(w_1, z_2) C$$

$$= \text{Inv}_Q \mu(x, z_1) \prod_{i=1}^{k} \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1),$$
as needed.

Case 2: When \( x < z_1 \). Since for all \( x < z \leq y \), all the monomials of \( \theta(x, z) \) contains \( t_x \) except for 1, from (16) we have

\[
[\text{Inv}_Q \theta(x, y)]_m = - \sum_{x < z \leq y} [\theta(x, z)]_1 [\text{Inv}_Q \theta(z, y)]_m.
\]

Thus, (14) implies

\[
[\text{Inv}_Q \theta(x, y)]_m = - \sum_{x < z \leq y} \mu(x, z)[\text{Inv}_Q \theta(z, y)]_m.
\]

Then, we plug in the induction assumption to obtain

\[
[\text{Inv}_Q \theta(x, y)]_m = - \sum_{x < z \leq y} \mu(x, z) \text{Inv}_Q \mu(z, z_1) \prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1),
\]

and we finish the induction by using Lemma 4.

\[\square\]

**Lemma 12.** Let \( x < y \) and let \( Q, Q' \subseteq P \) complementing the interval \([x, y]_P\), and let \( m \) be a \([x, y]_Q\)-admissible monomial. Suppose that the monomial \( m^{-1} \cdot t_y/t_x \) is \([x, y]_Q\)-admissible. Then,

\[
[\text{Inv}_Q \theta(x, y)]_m = -[\text{Inv}_{Q'} \theta(x, y)]_{m^{-1} \cdot t_y/t_x}.
\]

**Proof.** Let \( t_{w_1} \cdots t_{w_k} \) be the admissible form of \( m \). Set \( z_{k+1} = y, Q_i = Q \cup \{ w_i \} \) and \( Q_i' = Q \cup \{ z_i \} \).

So from Lemma 11,

\[
(22) \quad [\text{Inv}_Q \theta(x, y)]_m = \text{Inv}_Q \mu(x, z_1) \prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1).
\]

Next, we have that

\[
m^{-1} \cdot \frac{t_y}{t_x} = \frac{t_{z_1}}{t_x} \cdot \frac{t_{z_2}}{t_{w_1}} \cdots \frac{t_{z_k}}{t_{w_{k-1}}} \cdot \frac{t_y}{t_{w_k}}.
\]

Hence, \( w_1, \ldots, w_{k-1} \) must be in the denominator of \( m^{-1} \cdot t_y/t_x \). And since \( m^{-1} \cdot t_y/t_x \) is \([x, y]_{Q'}\)-admissible we get that \( w_1, \ldots, w_{k-1} \in Q' \). Also, \( w_k \in Q' \) since either \( w_k = y \) or \( w_k \) is in the denominator of \( m^{-1} \cdot t_y/t_x \).

Finally, we split the proof into 4 cases. In each of those cases \( m^{-1} \cdot t_y/t_x \) has a slightly different admissible form.

Case 1: When \( x = z_1 \) and \( y \neq w_k \). Since \( Q \) and \( Q' \) are complementing \([x, y]_P\) and \( x \leq z_1 < w_i \leq w_k < y \) for all \( i = 1, \ldots, k \), the elements \( w_i \notin Q \). Thus, we use Lemma 9 to get

\[
\prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1) = \prod_{i=1}^k \mu_Q(z_i, w_i) (-\text{Inv}_Q \mu(w_i, z_i+1)).
\]

The subposets \( Q_i \) and \( Q_i' \) are complementing the interval \([z_i, w_i]_P\). Moreover, \( Q_i \) and \( Q_{i+1} \) are complementing the interval \([w_i, z_{i+1}]_P\). Hence, applying Lemma 8 on the last equation gives

\[
\prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1) = \prod_{i=1}^k \text{Inv}_{Q_i} \mu(z_i, w_i) (-\mu_Q(z_{i+1}, w_i)).
\]

For all \( i = 2, \ldots, k \) we have that \( x \leq z_1 < z_i < w_k < y \), hence \( z_i \notin Q' \). So we apply Lemma 9 again:

\[
\prod_{i=1}^k \mu_Q(z_i, w_i) \Gamma_Q(w_i, z_i+1) = -\text{Inv}_{Q_i} \mu(z_1, w_1) \mu_Q(z_1, z_2) \prod_{i=2}^k \Gamma_Q(z_i, w_i) \mu_{Q_{i+1}}(w_i, z_{i+1}),
\]
and form here we get the identity

\[(23) \prod_{i=1}^{k} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) = -\text{Inv}_{Q'} \mu(x, w_1) \left( \prod_{i=1}^{k-1} \mu_{Q'_{i+1}}(w_i, z_{i+1}) \Gamma_Q(z_{i+1}, w_{i+1}) \right) \mu_{Q'_{k+1}}(w_k, z_{k+1}). \]

Next, we take a look on the admissible form of \(m^{-1} \cdot \frac{t_y}{t_x} \) which is

\[m^{-1} \cdot \frac{t_y}{t_x} = \frac{t_{z_2}}{t_{w_1}} \ldots \frac{t_{z_k}}{t_{w_{k-1}}} \cdot \frac{t_y}{t_w}.\]

From Lemma 11,

\[\text{Inv}_{Q'} \theta(x, y)|_{m^{-1} \cdot \frac{t_y}{t_x}} = \text{Inv}_{Q'} \mu(x, w_1) \prod_{i=1}^{k} \mu_{Q'_{i+1}}(w_i, z_{i+1}) \Gamma_Q(z_{i+1}, w_{i+1}),\]

where \(w_{k+1} = y \). And, by using (23), then the identities \(\text{Inv}_{Q} \mu(x, z_1) = \Gamma_{Q'}(w_{k+1}, z_{k+1}) = 1\), and then (22) to obtain

\[\text{Inv}_{Q'} \theta(x, y)|_{m^{-1} \cdot \frac{t_y}{t_x}} = \left( \prod_{i=1}^{k} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) \right) \Gamma_Q(z_{k+1}, w_{k+1}) = -\text{Inv}_{Q} \mu(x, z_1) \prod_{i=1}^{k} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) = -[\text{Inv}_{Q} \theta(x, y)]_m,\]

as needed.

**Case 2:** When \(x = z_1\) and \(y = w_k\). Similarly to proving (23), we use Lemma 9, then Lemma 8 and then Lemma 9 to get the identity

\[(24) \left( \prod_{i=1}^{k-1} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) \right) \mu_{Q_k}(z_k, w_k) = -\text{Inv}_{Q'} \mu(x, w_1) \prod_{i=1}^{k-1} \mu_{Q'_{i+1}}(w_i, z_{i+1}) \Gamma_Q(z_{i+1}, w_{i+1}).\]

Next, we focus on the admissible form of \(m^{-1} \cdot \frac{t_y}{t_x} \) is

\[m^{-1} \cdot \frac{t_y}{t_x} = \frac{t_{z_2}}{t_{w_1}} \ldots \frac{t_{z_k}}{t_{w_{k-1}}} \cdot \frac{t_y}{t_w}.\]

Using Lemma 11 gives

\[\text{Inv}_{Q'} \theta(x, y)|_{m^{-1} \cdot \frac{t_y}{t_x}} = \text{Inv}_{Q'} \mu(x, w_1) \prod_{i=1}^{k-1} \mu_{Q'_{i+1}}(w_i, z_{i+1}) \Gamma_Q(z_{i+1}, w_{i+1}).\]

Then, we use (24), then the identities \(\text{Inv}_{Q} \mu(x, z_1) = \Gamma_{Q}(w_k, z_{k+1}) = 1\), and then (22) to obtain

\[\text{Inv}_{Q'} \theta(x, y)|_{m^{-1} \cdot \frac{t_y}{t_x}} = -\left( \prod_{i=1}^{k-1} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) \right) \mu_{Q_k}(z_k, w_k) = -\text{Inv}_{Q} \mu(x, z_1) \prod_{i=1}^{k} \mu_{Q_i}(z_i, w_i) \Gamma_Q(w_i, z_{i+1}) = -[\text{Inv}_{Q} \theta(x, y)]_m,\]

as needed.

**Case 3:** When \(x \neq z_1\). In this case, \(t_x\) must be in the denominator of \(m^{-1} \cdot \frac{t_y}{t_x}\). Therefore, by replacing \(m\) with \(m^{-1} \cdot \frac{t_y}{t_x}\) and swapping \(Q\) and \(Q'\), we get one of the other cases. \(\square\)
Lemma 13. Let \( x < y \) and let \( Q, Q' \subseteq P \) complementing the interval \([x, y]_P\). Set \( \mathcal{L}^{-1} = \{(t_x^{-1})_{x \in P}\} \). Then,

\[
\text{Inv}_Q \theta(x, y; \mathcal{L}) = -\frac{t_y}{t_x} \text{Inv}_{Q'} \theta(x, y; \mathcal{L}^{-1}).
\]

Proof. Let \( m \) be some monomial in \( A_P \). It suffices to show that

\[
(25) \quad [\text{Inv}_Q \theta(x, y; \mathcal{L})]_m = -[\text{Inv}_{Q'} \theta(x, y; \mathcal{L})]_{m^{-1} \cdot t_y / t_x}.
\]

We divide the proof into four cases:

Case 1: When \( m \) is \([x, y]_{Q'}\)-admissible with admissible form \( t_x^{-1} \cdot \cdots \cdot t_x^{-1} \) and there exists \( i \) such that \( w_i \notin Q' \). In this case both sides of \((25)\) are zero. Indeed, \( w_i \neq x \) and \( w_i \neq y \) because \( x, y \in Q' \). Hence, \( m^{-1} \cdot t_y / t_x \) must contain \( t_{w_i} \), in its denominator and consequently \( m^{-1} \cdot t_y / t_x \) is not \([x, y]_{Q'}\)-admissible. Thus, by Lemma 11, the right side of \((25)\) is zero. For the left side of \((25)\), by Lemma 9 we have \( \Gamma_Q(w_i, z_{i+1}) = 0 \), then by using Lemma 11 we infer that the left side is also zero.

Case 2: When \( m \) is \([x, y]_{Q}\)-admissible with admissible form \( t_x^{-1} \cdot \cdots \cdot t_x^{-1} \) and for all \( i \) we have \( w_i \in Q' \). In this case we have that

\[
m^{-1} \cdot t_y / t_x = t_{w_1} \cdot \cdots \cdot t_{w_k} / t_{z_1} \cdot \cdots \cdot t_{z_k} t_x \times t_y,
\]

and also

\[
x \leq x \leq w_1 \leq z_1 \leq w_2 \leq \cdots \leq z_k \leq y.
\]

Hence, \( m^{-1} \cdot t_y / t_x \) is \([x, y]_{Q'}\)-admissible, and Lemma 12 implies \((25)\).

Case 3: When \( m \) is not \([x, y]_{Q}\)-admissible and \( m^{-1} \cdot t_y / t_x \) is not \([x, y]_{Q'}\)-admissible. Here by Lemma 11 both sides of \((25)\) are zeros and this equation holds.

Case 4: When \( m \) is not \([x, y]_{Q}\)-admissible and \( m^{-1} \cdot t_y / t_x \) is \([x, y]_{Q}\)-admissible. This case is either Case 1 or Case 2, after replacing \( m \) with \( m^{-1} \cdot t_y / t_x \) and swapping \( Q \) and \( Q' \) in \((25)\).

\( \square \)

3.4. The natural numbers poset. We take a look on the poset \( \mathbb{N} \) with the partial order "\( \mid \)" and on the incidence algebra \( I_{A_\mathbb{N}}(\mathbb{N}) \). In this incidence algebra we have the M"obius function and the \( \theta \) polynomial. We note that the known M"obius function from number theory is connected the M"obius function of incidence algebra over \( \mathbb{N} \) by the following relation:

\[
\mu(d, n) = \begin{cases} 
\mu\left(\frac{n}{d}\right), & d \mid n, \\
0, & \text{otherwise}.
\end{cases}
\]

In this subsection we will always set \( n = u^n \) where \( u \) is some variable or expression. Therefore, in this section we abbreviate and write \( u \) instead of \((u^n)_{n \in \mathbb{N}}\) on the third argument of elements of \( I_{A_\mathbb{N}}(\mathbb{N}) \), i.e.,

\[
\varepsilon(d, n; u) = \varepsilon(d, n; (u^n)_{n \in \mathbb{N}}) \quad \text{for all } \varepsilon \in I_{A_\mathbb{N}}(\mathbb{N}).
\]

In particular, the \( \theta \) polynomial is

\[
\theta(d, n; u) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) u^{n - d}.
\]

Lemma 14. For any positive integer \( n \geq 1 \),

\[
(27) \quad J_n(u, v) = -\frac{v^{-n+1}}{\prod_{\varepsilon \neq n} (r_\varepsilon - 1)} \sum_{1, n \in Q \subseteq [1, n]_\mathbb{N}} (-1)^{#Q} \text{Inv}_Q \theta(1, n; u) \prod_{\varepsilon \mid n, \varepsilon \notin Q} r_\varepsilon,
\]

where \( r_\varepsilon = u^{n - e} v^{n/e + 1} \).
Proof. We start with simplifying the right side of (27) which we denote with \( \tilde{J}_n(u, v) \). We use Lemma 5 on the right side of (27),

\[
\tilde{J}_n(u, v) = -\frac{v^{-n+1}}{\prod_{e \neq n} (r_e - 1)} \sum_{1, n \in Q \subseteq [1, n]_n} (-1)^{|Q|} \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n)} (-1)^k \left( \prod_{i=0}^{k-1} \theta(d_i, d_{i+1}; u) \right) \prod_{e \in n} r_e.
\]

By changing the order of summation we get that

\[
\tilde{J}_n(u, v) = -\frac{v^{-n+1}}{\prod_{e \neq n} (r_e - 1)} \sum_{Q \subseteq [1, n]_n} (-1)^{|Q|} \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n)} (-1)^k \left( \prod_{i=0}^{k-1} \theta(d_i, d_{i+1}; u) \right) \prod_{e \in n} r_e.
\]

We focus on the inner sum of (28). By changing the variable \( Q \) to \( Q \setminus \{d_0, \ldots, d_k\} \), we get

\[
\sum_{Q \subseteq [1, n]_n} (-1)^{|Q|} \prod_{e \in Q} r_e = \sum_{e \in n} (-1)^{|Q|+1} \prod_{e \in Q \setminus \{d_0, \ldots, d_k\}} r_e.
\]

For a finite sequence \((a_i)_{i \in F}\) we have the identity

\[
\prod_{i \in F} (a_i - 1) = \sum_{F' \subseteq F} (-1)^{|F'|} \prod_{i \in F \setminus F'} a_i.
\]

Using this identity on the right side of (29) gives

\[
\sum_{Q \subseteq [1, n]_n} (-1)^{|Q|} \prod_{e \in Q} r_e = -\prod_{e \in n} (r_e - 1).
\]

We put (30) in (28) to obtain

\[
\tilde{J}_n(u, v) = v^{-n+1} \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n)} \left( \prod_{i=0}^{k-1} \theta(d_i, d_{i+1}; u) \right) \prod_{e \notin \{d_0, \ldots, d_k\}} (r_e - 1).
\]

We insert the denominator inside the sum and get

\[
\tilde{J}_n(u, v) = v^{-n+1} \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n)} \left( \prod_{i=0}^{k-1} \frac{\theta(d_i, d_{i+1}; u)}{r_{d_i} - 1} \right).
\]

Plugging

\[
v^{-n+1} = \prod_{i=0}^{k-1} \frac{v^{n/d_i+1}}{v^{n/d_i}},
\]

into (31) gives

\[
\tilde{J}_n(u, v) = \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n)} \left( \prod_{i=0}^{k-1} \frac{v^{n/d_i+1} \theta(d_i, d_{i+1}; u)}{u^{n-d_i} - u^{n/d_i}} \right).
\]

Next, we prove that \( J_n(u, v) = \tilde{J}_n(u, v) \) with induction on \( n \). For \( n = 1 \), the equality is clear. For \( n > 1 \), the induction assumption and (32) gives that for any \( 1 \neq d \mid n \),

\[
J_{n/d}(u^d, v) = \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n/d)} \left( \prod_{i=0}^{k-1} \frac{v^{n/d_i+1} \theta(d_i, d_{i+1}; u)}{u^{n-d_i} - u^{n/d_i}} \right).
\]

Using (26) we have \( \theta(d_i, d_{i+1}; u^d) = \theta(dd_i, dd_{i+1}; u) \). Hence,

\[
J_{n/d}(u^d, v) = \sum_{(d_0, \ldots, d_k) \in \mathcal{C}_Q^*(1, n/d)} \left( \prod_{i=0}^{k-1} \frac{v^{n/dd_i+1} \theta(dd_i, dd_{i+1}; u)}{u^{n-dd_i} - u^{n/dd_i}} \right).
\]
We take a look on the map 

\[(d_0, \ldots, d_k) \mapsto (dd_0, \ldots, dd_k)\].

This map is a bijection from \(C^*_N(1, n/d)\) to \(C^*_N(d, n)\). Therefore, we can change the variables of the sum in (33) to get

\[
J_{n/d}(u^d; v) = \sum_{(d_0, \ldots, d_k) \in C^*_N(d, n)} \prod_{i=0}^{k-1} \frac{v^{n/d_{i+1}} \theta(d_i, d_{i+1}; u)}{\theta(v^{n/d_i}, v^{n/d_{i+1}}; u)}.
\]

Finally, we plug (26) and (34) into (6):

\[
J_n(u, v) = \frac{1}{u^{n-1} - v^{n-1}} \sum_{1 \neq d | n} v^{n/d-1} \theta(1, d; u) \sum_{(d_0, \ldots, d_k) \in C^*_N(d, n)} \prod_{i=0}^{k-1} \frac{v^{n/d_{i+1}} \theta(d_i, d_{i+1}; u)}{\theta(v^{n/d_i}, v^{n/d_{i+1}}; u)}
\]

The two sums in the last line are running over all the proper chains from 1 to \(n\), when \(d\) is chosen to be the first element in the chain after 1. Hence,

\[
J_n(u, v) = \sum_{(d_0, \ldots, d_k) \in C^*_N(1, n)} \prod_{i=0}^{k-1} \frac{v^{n/d_{i+1}} \theta(d_i, d_{i+1}; u)}{\theta(v^{n/d_i}, v^{n/d_{i+1}}; u)}.
\]

And using (32) finishes the proof. \(\square\)

**Proof of Proposition 3.** When \(n = 1\) this proposition is clear, so we assume that \(n > 1\). From Lemma 14 we have that

\[
J_n(u^{-1}, v^{-1}) = -\frac{v^{n-1}}{\prod_{e \neq n} (r_e^{-1} - 1)} \sum_{1 \neq Q \subseteq [1, n]} (-1)^{|Q|} \prod_{e \in Q} r_e^{-1}.
\]

where \(r_e = u^{-n-e} v^{-n-e+1}\). First we focus on the fraction on the right side (35):

\[
\frac{v^{n-1}}{\prod_{e \neq n} (r_e^{-1} - 1)} = \frac{v^{n-1}}{\sum_{e \neq n} (r_e^{-1} - 1)} = \frac{v^{n-1}}{\prod_{e \neq n} (1 - r_e^{-1})}.
\]

Thus,

\[
\frac{v^{n-1}}{\prod_{e \neq n} (r_e^{-1} - 1)} = (-1)^{|1, n|+1} v^{n-1} \prod_{e \neq n} r_e^{-1} \prod_{e \neq n} (r_e - 1).
\]

We put the last equation in (35),

\[
J_n(u^{-1}, v^{-1}) = \frac{v^{n-1}}{\prod_{e \neq n} (r_e^{-1} - 1)} \sum_{1 \neq Q \subseteq [1, n]} (-1)^{|1, n|+1+|Q|} \prod_{e \in Q} \theta(1, u^{-1}; \prod_{e \notin Q} r_e).
\]

Next, we focus on the sum of (36). For any \(1, n \in Q \subseteq [1, n]_{\mathbb{N}}\), set \(\tilde{Q} = ([1, n]_{\mathbb{N}} \setminus Q) \cup \{1, n\}\). Since \(Q = \left([1, n]_{\mathbb{N}} \setminus \tilde{Q}\right) \cup \{1, n\}\),

\[
\prod_{e \in Q} r_e = \prod_{e \in \tilde{Q}} r_e \prod_{e \in [1, n]} r_e
\]

and then

\[
\prod_{e \in \tilde{Q}} r_e = u^{-n-1} v^{-n+1} \prod_{e \in [1, n]} r_e.
\]
Moreover, we have that \( \#\tilde{Q} = \#[1,n]_\mathbb{N} - \#Q + 2 \). Putting that and \((37)\) in \((36)\) gives

\[
(38) \quad J_n(u^{-1}, v^{-1}) = \prod_{e \not\in n} (r_e - 1) \sum_{1, n \in \tilde{Q} \subseteq [1,n]_\mathbb{N}} (-1)^{\#\tilde{Q}} \text{Inv}_Q \theta(1,n; u^{-1}) \prod_{e \in \tilde{Q}} r_e.
\]

The posets \(Q\) and \(\tilde{Q}\) are complementing the interval \([1,n]_\mathbb{N}\), so applying Lemma 13 on \((38)\) gives

\[
(39) \quad J_n(u^{-1}, v^{-1}) = \prod_{e \not\in n} (r_e - 1) \sum_{1, n \in \tilde{Q} \subseteq [1,n]_\mathbb{N}} (-1)^{\#\tilde{Q}} \text{Inv}_Q \theta(1,n; u) \prod_{e \in \tilde{Q}} r_e.
\]

We change the variable of the sum to obtain

\[
(40) \quad J_n(u^{-1}, v^{-1}) = \prod_{e \not\in n} (r_e - 1) \sum_{1, n \in \tilde{Q} \subseteq [1,n]_\mathbb{N}} (-1)^{\#\tilde{Q}} \text{Inv}_Q \theta(1,n; u) \prod_{e \in \tilde{Q}} r_e.
\]

Finally, we use Lemma 14 in \((39)\) and get

\[
J_n(u^{-1}, v^{-1}) = v^{n-1} J_n(u,v). \quad \square
\]

4. THE ROOTS OF \(f_n\)

Let \(K\) be a \(p\)-adic field of degree \(n\) over \(\mathbb{Q}_p\). For an open set \(U \subseteq K\) we define \(R_K(U)\) to be the number of roots of \(f_n\) in the set \(U\) which also generates \(K\) i.e.

\[
R_K(U) = \#\{x \in U : f_n(x) = 0 \text{ and } K = \mathbb{Q}_p[x]\}.
\]

If \(U = K\) we abbreviate and write \(R_K = R_K(K)\).

In this section we calculate the expected value of \(R_K(U)\) for three sets \(U = K, \mathcal{O}_K, \mathfrak{m}_K\) in the case that \(K/\mathbb{Q}_p\) is unramified. More precisely,

**Proposition 15.** Let \(K\) be an unramified field extension of \(\mathbb{Q}_p\) of degree \(n\). Then

\[
(41) \quad \frac{1}{n} \mathbb{E}[R_K(\mathcal{O}_K)] = \frac{p^{n+1} - p^n}{p^{n+1} - 1} \cdot J_n^*(p),
\]

\[
(42) \quad \frac{1}{n} \mathbb{E}[R_K(\mathfrak{m}_K)] = \frac{p - 1}{p^{n+1} - 1} \cdot J_n^*(p^{-1}), \quad \text{and}
\]

\[
(43) \quad \frac{1}{n} \mathbb{E}[R_K] = \frac{p}{p^{n+1} - 1} \left( p^n J_n^*(p) + J_n^*(p^{-1}) \right).
\]

Let \(K/F\) be a finite extension of \(p\)-adic fields. Define \(\phi_{K/F} : \mathcal{O}_K \to \mathbb{R}^+\) to be the function

\[
(44) \quad \phi_{K/F}(x) = \lambda_K(\mathcal{O}_F[x]).
\]

We prove the following properties on the function \(\phi_{K/F}\).

**Lemma 16.** For all \(x \in \mathcal{O}_K\),

\[
\phi_{K/F}(x) = \frac{\Delta_{K/F}(x)}{|D_{K/F}|}. \quad \square
\]

**Proof.** If \(K \neq F[x]\) then \(\Delta_{K/F}(x) = 0\) and also \(\lambda_K(\mathcal{O}_F[x]) \leq \lambda_K(F[x]) = 0\). So we assume that \(K = F[x]\).

Let \(\mathcal{B} = (\omega_1, \ldots, \omega_n)\) is an \(\mathcal{O}_F\)-basis of \(\mathcal{O}_K\) and let \(\mathcal{B}_x = (1,x,\ldots, x^n)\) be a \(F\)-basis of \(K\). Note that \(\mathcal{B}\) is also a \(F\)-basis of \(K\). Set \(M\) to be the change of basis matrix from \(\mathcal{B}_x\) to \(\mathcal{B}\), so

\[
\phi_{K/F}(x) = \det M.F.
\]

Moreover, from \((8)\)

\[
\Delta_{K/F}(1,x,\ldots, x^n) = (\det M)^2 \Delta_{K/F}(\omega_1,\ldots, \omega_n). \]
Lemma 16 and the identity $\Delta \equiv \sigma / \pi$ which contradicts $\sigma \in O_F$ implies that $\sigma \in O_F$. We say an integer element $\zeta \in O_K$ is inertial if its degree over $\mathbb{Q}_p$ equals to the degree of $\zeta \bmod m_K$ over $\mathbb{F}_p$.

Let $L$ be the unique subfield in $K$ which is unramified over $\mathbb{Q}_p$ and of degree $m$. For each element $\zeta$ in the residue field of $K$ of degree $m$, we can lift $\zeta$ to an element $\zeta$ in $L$. It is clear that $\zeta$ is inertial. Therefore, for each residue class of $O_K/m_K$ we can choose an inertial representative.

In addition, if $\zeta \in O_K$ is inertial and $q$ is the size of the residue field of $F$ then the degree of $\zeta$ over $F$ is the same as the degree of $\zeta \bmod m_F$ over $\mathbb{F}_q$.

Lemma 19. Assume $K/F$ is an unramified extension. Let $\zeta \in O_K$ be an inertial element of degree $m$ over $F$ and $x \in m_K$. Then

$$\phi_{K/F}(\zeta + x) = \phi_{K/F}[\zeta](x).$$

Proof. Set $y = \zeta + x$ and $L = F[\zeta]$. We have that $|D_{K/F}|_F = |D_{K/L}|_L = 1$. So by Lemma 16 it is sufficed to show that $|\Delta_{K/F}(y)|_F = |\Delta_{K/L}(y)|_L$.

Let $f$ (resp. $g$) be the minimal polynomial of $y$ over $F$ (resp. $L$). We have that

$$|\Delta_{K/F}(y)|_F = |N_{K/F}(f(y))|_F = |f(y)|_K,$$

and similarly

$$|\Delta_{K/L}(y)|_L = |N_{K/L}(g(y))|_L = |g(y)|_K.$$

Moreover, $g \mid f$ so there exists $h \in L[X]$ such that $f = gh$. Since $f' = g'h + gh'$ and $g(y) = 0$ we get that $f'(y) = g'(y)h(y)$. Hence, form (45) and (46) we get that

$$|\Delta_{K/F}(y)|_F = |\Delta_{K/L}(y)|_L|h(y)|_K.$$

From the hypothesis $K/F$ is unramified, hence $K/F$ is Galois extension. We denote $G = \text{Gal}(K/F)$ and $H = \text{Gal}(K/L) \leq G$. Since

$$f(X) = \prod_{\sigma \in G} (X - \sigma(y)), \quad g(X) = \prod_{\sigma \in H} (X - \sigma(y)),$$

we have

$$h(X) = \prod_{\sigma \in G \setminus H} (X - \sigma(y)).$$

Let $\pi$ be the common uniformizer of $F, L$ and $K$. So

$$h(y) \equiv \prod_{\sigma \in G \setminus H} (\zeta - \sigma(\zeta)) \pmod{\pi}.$$

There is no $\sigma \in G \setminus H$ such that $\zeta \equiv \sigma(\zeta) \pmod{\pi}$. Indeed, if $\zeta \equiv \sigma(\zeta) \pmod{\pi}$ then $O_L = O_F[\zeta]$ implies that $\sigma|_L$ is in the inertia group of $L/F$. But since $L/F$ is unramified, we get that $\sigma|_L = \text{id}_L$ which contradicts $\sigma \not\in H$.

Therefore, we get from (48) that $h(y) \not\equiv 0 \pmod{\pi}$ and consequently $|h(y)|_K = 1$. Plugging this into (47) finish the proof. \qed
Lemma 20. Let $K/F$ be an unramified extension of degree $n$ and let $r \in \mathbb{C}$ with $\Im(r) > 0$. Assume $q$ is the size of residue field of $F$. Then

$$\int_{\mathcal{O}_K} \phi_{K/F}(x)^r \, dx = J_n(q, q^{-nr/2}).$$

Proof. We prove this with induction on $n$. For $n = 1$ we have that $K = F$ and $\phi_{F/F}(x) = 1$. So it is clear that $\int_{\mathcal{O}_F} \phi_{F/F}(x)^r \, dx = J_1(q, q^{-nr/2})$.

Assume $n > 1$. Let $\pi$ be the common uniformizer of $F$ and $K$, and let $S$ be a set of inertial representatives of the residue classes of $\mathcal{O}_K/\mathfrak{m}_K$.

We have that $\mathcal{O}_K = \bigcup_{\zeta \in S} (\zeta + \mathfrak{m}_K)$. Hence,

$$J := \int_{\mathcal{O}_K} \phi_{K/F}(x)^r \, dx = \sum_{\zeta \in S} \int_{\zeta + \mathfrak{m}_K} \phi_{K/F}(x)^r \, dx.$$

We apply change of variables $x \mapsto \zeta + \pi x$ to obtain

$$J = q^{-n} \sum_{\zeta \in S} \int_{\mathcal{O}_K} \phi_{K/F}(\zeta + \pi x)^r \, dx.$$

Since $\zeta$ is inertial for each $\zeta \in S$ we can use Lemma 19 to infer that

$$J = q^{-n} \sum_{\zeta \in S} \int_{\mathcal{O}_K} \phi_{K/F|\zeta}(\pi x)^r \, dx.$$

Also, by Lemma 17 we get that

$$J = q^{-n} \sum_{1 \neq d | n} \sum_{\deg \zeta = d} \int_{\mathcal{O}_K} \phi_{K/F|\zeta}(\pi x)^r \, dx$$

$$= q^{-n} \sum_{d | n} \sum_{\deg \zeta = d} \int_{\mathcal{O}_K} |\pi|_{F|\zeta} \phi_{K/F|\zeta}(x)^r \, dx$$

$$= q^{-n} \sum_{d | n} q^{-\frac{(n/d)}{2}} \sum_{\deg \zeta = d} \int_{\mathcal{O}_K} \phi_{K/F|\zeta}(x)^r \, dx.$$

Therefore, by the induction assumption we have that

$$J = q^{-n} \sum_{1 \neq d | n} q^{-\frac{(n/d)}{2}} \sum_{\deg \zeta = d} J_n/d \left(q^d, q^{-nr/2}\right) + q^{-\frac{(n)}{2}} \sum_{\deg \zeta = 1} J.$$

We set $\Theta_d(q) = \#\{\zeta \in S : d = \deg \zeta\}$ and then

$$J = q^{-n} \sum_{1 \neq d | n} q^{-\frac{(n/d)}{2}} \Theta_d(q) J_n/d \left(q^d, q^{-nr/2}\right) + q^{-\frac{(n)}{2}} \sum_{\deg \zeta = 1} J.$$

By simple calculations we get that

$$J = \frac{q^{-1}}{q^{n-1} - q^{-\frac{(n)}{2}}} \sum_{1 \neq d | n} q^{-\frac{(n/d)}{2}} \Theta_d(q) J_n/d \left(q^d, q^{-nr/2}\right).$$

Next, we have that

$$\Theta_d(q) = a \sum_{e | d} \mu \left(\frac{d}{e}\right) q^{e-1}.$$

Indeed, since the elements of $S$ are inertial

$$\Theta_d(q) = \#\{\zeta \in S : d = \deg \zeta\} = \#\{\zeta \in \mathbb{F}_{q^d} : d = \deg \zeta\}.$$
And since
\[ q^d = \sum_{e|d} \# \left\{ \zeta \in \mathbb{F}_{q^d} : e = \deg_{e} \zeta \right\} = \sum_{e|d} \Theta_e(q), \]
From Möbius inversion formula we obtain
\[ \Theta_d(q) = \sum_{e|d} \mu \left( \frac{d}{e} \right) q^e, \]
and (50) follows immediately.

Finally, we plug in (50) into (49) gives
\[ J = \frac{1}{q^{n-1} - q^{-\frac{1}{2}}} \sum_{1 \neq d|n} q^{-\frac{n}{2}dr} \left( \sum_{e|d} \mu \left( \frac{d}{e} \right) q^{e-1} \right) J_{n/d} \left( q^d, q^{-nr/2} \right). \]
We finish the proof by setting \( u = q \) and \( v = q^{-nr/2} \) in (6) and then comparing to the last equation. \( \square \)

Remark 21. Lemma 20 is related to Igusa’s local zeta functions (see [Den91] or [Igu07]). This relation appear in the following manner:

Let \( \omega_1, \ldots, \omega_n \) be a \( \mathcal{O}_F \)-basis of \( \mathcal{O}_K \) we define the multivariate polynomial
\[ h(X_1, \ldots, X_n) = \Delta_K(X_1 \omega_1 + \cdots + X_n \omega_n). \]
The polynomial \( h \) is a homogeneous polynomial with coefficients in \( F \). Set \( s = 2r \), so the Igusa’s zeta function of \( h \) is
\[ Z_h(s) = \int_{\mathcal{O}_F^r} \left| h(x) \right|^s_F \, dx = \int_{\mathcal{O}_K} \phi_{K/F}(x)^s \, dx. \]
It is known that \( Z_h \) is a rational function of \( q^{-1} \) and \( q^{-s} \). Lemma 20 gives this rational function explicitly. Moreover, by setting \( Z(u, v) = J_n(u^{-1}, v^n) \) and using Proposition 3 we obtain \( Z(u^{-1}, v^{-1}) = v^{(\frac{r}{2})} Z(u, v) \). This functional equation has been conjectured for by Igusa [Igu89] under certain conditions on the polynomial \( h \). One of the conditions is the existence of resolutions of singularities. Later, this conjecture was proved by Denef and Meuser [DM91].

Proof of Proposition 15. Let \( U \subseteq \mathcal{O}_K \) open set, so from [Car22, Theorem 5.8] we have
\[ \mathbb{E}[R_K(U)] = \left| D_{K/\mathbb{Q}_p} \right|_p \cdot \frac{p^{n+1} - p^n}{p^{n+1} - 1} \int_U \phi_{K/\mathbb{Q}_p}(x) \, dx. \]
Since \( K/\mathbb{Q}_p \) is unramified,
\[ \mathbb{E}[R_K(U)] = \frac{p^{n+1} - p^n}{p^{n+1} - 1} \int_U \phi_{K/\mathbb{Q}_p}(x) \, dx. \]
Therefore, (40) follows immediately from (7), (51) and Lemma 20. For (41) we set \( U = \mathfrak{m}_K \) in (51) and get
\[ \mathbb{E}[R_K(\mathfrak{m}_K)] = \frac{p^{n+1} - p^n}{p^{n+1} - 1} \int_{\mathfrak{m}_K} \phi_{K/\mathbb{Q}_p}(x) \, dx. \]
By a change of variable we get that
\[ \int_{\mathfrak{m}_K} \phi_{K/\mathbb{Q}_p}(x) \, dx = \int_{\mathcal{O}_K} \phi_{K/\mathbb{Q}_p}(px) \cdot |p|_K \, dx = p^{-n} \int_{\mathcal{O}_K} \phi_{K/\mathbb{Q}_p}(px) \, dx. \]
Next we apply Lemma 17, then Lemma 20 and then Proposition 3 we obtain
\[ \int_{m_K} \phi_{K/Q_p}(x) \, dx = p^{-(2\ell)-n} \int_{O_K} \phi_{K/Q_p}(x) \, dx \]
\[ = p^{-(2\ell)-n} J_n \left( p, p^{-n/2} \right) \]
\[ = p^{-n} J_n \left( p^{-1}, p^{n/2} \right). \]
And we get (41) by plugging the last equation and (7) into (52).

Finally, we prove (42). We have that
\[ (53) \quad E[R_K] = E[R_K(O_K)] + E[R_K(K \setminus O_K)]. \]
If \( x \in K \setminus O_K \) is a root of \( f_n \), then \( x^{-1} \) is a root of \( X^n f_n(X^{-1}) \) and \( x^{-1} \in m_K \). Moreover, \( X^n f_n(X^{-1}) \) has the same law as \( f_n \). Thus, \( E[R_K(K \setminus O_K)] = E[R_K(m_K)] \). Setting this in (53) and then plugging (40) and (41) finish the proof. \( \square \)

5. Main Proof

Set \( \sigma = (n^1) \) as in Theorem 2 and let \( K/Q_p \) be an étale extension of splitting type \( \sigma \). Then \( K \) must be a field of degree \( n \) and unramified over \( Q_p \). Moreover, all the étale extensions of \( Q_p \) with splitting type \( \sigma \) are isomorphic to \( K \).

We begin with proving the following relation between \( R_K \) and the probabilities \( \rho, \alpha \) and \( \beta \). (c.f. [Car22, Proposition 4.11]).

**Lemma 22.** Let \( C \) be an event such that \( P(\cdot | C) \) is well-defined. Then
\[ P(E_o | C) = \frac{1}{n} E[R_K | C]. \]

**Proof.** First, we prove
\[ (54) \quad P(A_n \simeq K | C) = \frac{E[R_K | C]}{\# \text{Aut}_{Q_p}(K)}. \]
This is similar to [Car22, Proposition 5.11], and we follow its proof with small adjustments.

We have that \( R_K = \# \text{Hom}_{\text{surj}}(A_n, K) \). Also, since \( A_n \) and \( K \) are both of degree \( n \) over \( Q_p \), then any surjective homomorphism is an isomorphism. Therefore,
\[ \frac{R_K}{\# \text{Aut}_{Q_p}(K)} = \mathbb{1}_{A_n \simeq K}. \]
By applying the expectation function \( E[\cdot | C] \) on both sides of the equation and using the linearity of expectation we obtain (54).

The field \( K \) is the unique (up to an isomorphism) étale algebra extending \( Q_p \) with splitting type \( \sigma \). Therefore, the event \( E_o \) is equivalent to the event that \( A_n \cong K \). Moreover, it is known that \( \# \text{Aut}_{Q_p}(K) = n \). Putting those facts in (54) finish the proof. \( \square \)

We now prove each of the equations in Theorem 2.

**Proof of (3).** This is an immediate consequence of (42) and Lemma 22. \( \square \)

**Proof of (4).** If \( f_n \) is not a primitive polynomial we can divide it with \( p \) and get a random polynomial with the same law as \( f_n \). Therefore,
\[ (55) \quad E[R_K(O_K)] = E[R_K(O_K) | f_n \text{ primitive}]. \]
Assume \( f_n \) is primitive and \( p \mid \ell_n \) occurs then \( \tilde{f}_n := f_n \mod p \) is a nonzero polynomial with degree \( < n \). From Hensel’s lemma (see [Nen99, Lemma II.4.6]) there exists \( f, g \in \mathbb{Z}_p[X] \) such that \( \deg f = \deg f_n < n, f \equiv f_n \mod p, g \equiv 1 \mod (p) \) and \( f_n = fg \).

Let \( x \in O_K \) be a root of \( f_n \), so \( f(x) = 0 \) otherwise \( g(x) = 0 \) which contradicts \( g \equiv 1 \mod (p) \). But since \( \deg f < n \) we get that \( K \not\cong Q_p[x] \). Therefore, there are no roots of \( f_n \) in \( O_K \) which are generators of \( K \) i.e. \( R_K(O_K) = 0 \).
From the assumption we have that \( \mathbb{E}[R_K(\mathcal{O}_K) \mid f_n \text{ primitive} \wedge p \mid \xi_n] = 0 \). So, using the law of total expectation on the right side of (55) gives

\[
\mathbb{E}[R_K(\mathcal{O}_K)] = \mathbb{P}(p \mid \xi_n \mid \mathcal{O}_K) \mathbb{E}[R_K(\mathcal{O}_K) \mid p \mid \xi_n]
= \frac{p^n(p-1)}{p^{n+1}-1} \cdot \mathbb{E}[R_K(\mathcal{O}_K) \mid p \mid \xi_n].
\]

Dividing the variable \( \xi_i \) with a unit does not change its law, so we can replace the condition in the expectation with \( \xi_n = 1 \) i.e.

\[
\mathbb{E}[R_K(\mathcal{O}_K)] = \frac{p^n(p-1)}{p^{n+1}-1} \cdot \mathbb{E}[R_K(\mathcal{O}_K) \mid f_n \text{ monic}].
\]

Also, under this condition all the roots of \( f_n \) are in \( \mathcal{O}_K \) and thus \( R_K(\mathcal{O}_K) = R_K \). So

\[
\mathbb{E}[R_K(\mathcal{O}_K)] = \frac{p^n+1-p^n}{p^{n+1}-1} \cdot \mathbb{E}[R_K \mid f_n \text{ monic}],
\]

Plugging (40) into the last equation gives.

\[
\frac{1}{n} \mathbb{E}[R_K \mid f_n \text{ monic}] = J^*_n(p),
\]

and the proof is finished by Lemma 22. \( \square \)

**Proof of (5).** Using similar arguments as in the proof of (4) we have that (56)

\[
\mathbb{E}[R_K(\mathcal{m}_K)] = \mathbb{E}[R_K(\mathcal{m}_K) \mid f_n \text{ primitive}].
\]

Assume \( f_n \text{ is primitive} \) and \( f_n \not\equiv uX^n \pmod{p} \) for each unit \( u \in \mathbb{F}_p^\times \). So there exists \( m < n \) and \( g \in \mathbb{F}_p[X] \) such that \( f_n \equiv X^m\bar{g} \pmod{p} \) and \( \bar{g}(0) \not\equiv 0 \pmod{p} \). By Hensel’s lemma (see [Neu99, Lemma II.4.6]) there exists \( f, \bar{g} \in \mathbb{Z}_p[X] \) such that \( \deg f = m < n \), \( f \equiv X^m \pmod{p} \), \( g \equiv \bar{g} \pmod{p} \) and \( f_n = fg \).

Let \( x \in \mathbb{m}_K \) be a root of \( f_n \), so \( f(x) = 0 \) otherwise \( \bar{g}(0) \equiv g(x) = 0 \pmod{p} \) which is contradiction for the choice of \( \bar{g} \). But since \( \deg f < n \) we get that \( K \not\equiv \mathbb{Q}_p[x] \). Therefore, there are no roots of \( f_n \) in \( \mathbb{m}_K \) which are generators of \( K \). i.e. \( R_K(\mathcal{m}_K) = 0 \).

From the assumption we have that \( \mathbb{E}[ R_K(\mathcal{O}_K) \mid \bigwedge_{u \in \mathbb{F}_p^\times} f_n \not\equiv uX^n \pmod{p} ] = 0 \). So, by applying the law of total expectation on the right of (56),

\[
\mathbb{E}[R_K(\mathcal{m}_K)]
= \mathbb{P} \left( \bigvee_{u \in \mathbb{F}_p^\times} f_n \equiv uX^n \pmod{p} \mid f_n \text{ primitive} \right) \mathbb{E} \left[ R_K(\mathcal{m}_K) \bigg| \bigg\{ \bigvee_{u \in \mathbb{F}_p^\times} f_n \equiv uX^n \pmod{p} \right] \right] 
= \frac{p^n-1}{p^{n+1}-1} \cdot \mathbb{E} \left[ R_K(\mathcal{m}_K) \bigg| \bigg\{ \bigvee_{u \in \mathbb{F}_p^\times} f_n \equiv uX^n \pmod{p} \right] \right].
\]

Dividing the variable \( \xi_i \) with a unit does not change its law, so we can replace the condition in the expectation with the condition that \( f_n \text{ monic} \) and \( f_n \equiv X^n \pmod{p} \) i.e.

\[
\mathbb{E}[R_K(\mathcal{m}_K)] = \frac{p^n-1}{p^{n+1}-1} \cdot \mathbb{E}[R_K(\mathcal{m}_K) \mid f_n \text{ monic and } f_n \equiv X^n \pmod{p}].
\]

Also, under this condition all roots of \( f_n \) are in \( \mathcal{m}_K \) and thus \( R_K(\mathcal{m}_K) = R_K \). Thus,

\[
\mathbb{E}[R_K(\mathcal{m}_K)] = \frac{p^n-1}{p^{n+1}-1} \cdot \mathbb{E}[R_K \mid f_n \text{ monic and } f_n \equiv X^n \pmod{p}].
\]

From (41) we get that

\[
\frac{1}{n} \mathbb{E}[R_K \mid f_n \text{ monic and } f_n \equiv X^n \pmod{p}] = J^*_n(p),
\]

and the proof is finished by Lemma 22. \( \square \)
The probability that a $p$-adic random étale algebra is an unramified field

References

[BCFG22] M. Bhargava, J. Cremona, T. Fisher, and S. Gajović. The density of polynomials of degree $n$ over $\mathbb{Z}_p$ having exactly $r$ roots in $\mathbb{Q}_p$. Proceedings of the London Mathematical Society, 124(5):713–736, 2022.

[Car22] X. Caruso. Where are the zeroes of a random $p$-adic polynomial? Forum of Mathematics, Sigma, 10:e55, 2022.

[Den91] J. Denef. Report on Igusa’s local zeta function. Séminaire Bourbaki, 1990(741):359–386, 1991.

[DM91] J. Denef and D. Meuser. A functional equation of Igusa’s local zeta function. American Journal of Mathematics, 113(6):1135–1152, 1991.

[Igu89] J. Igusa. Universal $p$-adic zeta functions and their functional equations. American Journal of Mathematics, 111(5):671–716, 1989.

[Igu07] J. Igusa. An introduction to the theory of local zeta functions, volume 14 of AMS/IP Studies in Advanced Mathematics. American Mathematical Soc., 2007.

[Neu99] J. Neukirch. Algebraic number theory, volume 322 of Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin, 1999.

[SO97] E. Spiegel and C. J. O’Donnell. Incidence algebras, volume 206 of Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1997.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel.

Email address: royshmueli@mail.tau.ac.il