THE FIRST DIGIT OF THE DISCRIMINANT OF EISENSTEIN POLYNOMIALS AS AN INVARIANT OF TOTALLY RAMIFIED EXTENSIONS OF P-ADIC FIELDS

CHAD AWTREY, ALEXANDER GAURA, SEBASTIAN PAULI, SANDI RUDZINSKI, ARIEL UY, AND SCOTT ZINZER

Abstract. Let K be an extension of the p-adic numbers with uniformizer π. Let φ and ψ be Eisenstein polynomials over K of degree n that generate isomorphic extensions. We show that if the cardinality of the residue class field of K divides $n(n-1)$, then $v(\operatorname{disc}(\varphi)-\operatorname{disc}(\psi)) > v(\operatorname{disc}(\varphi))$. This makes the first (non-zero) digit of the π-adic expansion of $\operatorname{disc}(\varphi)$ an invariant of the extension generated by φ. Furthermore we find that non-cyclic extensions of degree p of the field of p-adic numbers are uniquely determined by this invariant.

1. Introduction

This paper is concerned with the classification of extensions of p-adic fields using invariants. We introduce a new invariant and show how it is related to other invariants of the extension.

For a field extension of finite degree, the discriminant of an integral basis yields invariants of the extension. A change of integral basis results in the multiplication of the discriminant by the square of a unit in the base ring; namely, by the determinant of the transformation matrix. Because the only units in the ring of integers $\mathbb{Z}$ are ± 1 and because -1 is not a square, the discriminant is an invariant of an extension of the rational numbers $\mathbb{Q}$.

When we consider extensions of the p-adic field $\mathbb{Q}_p$, the ring of p-adic numbers $\mathbb{Z}_p$ takes the place of $\mathbb{Z}$. As $\mathbb{Z}_p$ contains infinitely many units, the discriminant of an integral basis is not an invariant of an extension of $\mathbb{Q}_p$. However, since changing integral bases changes the discriminant by the square of a unit, the discriminant modulo the square of units does produce an invariant of the extension; see [Cas86, chapter 7, section 6] for details. Nevertheless, commonly only the valuation of the discriminant is used as an invariant of extensions of $\mathbb{Q}_p$, since it yields information about the ramified part of the extension.

It is natural to ask whether this invariant can be refined by considering not the complete discriminant but possibly some of the digits of its p-adic expansion. To this end we restrict our investigation to discriminants of integral bases of a certain form; namely, power integral bases, which are bases of the form 1, α, α^2,$\dots$,α^{n-1} where n is the degree of the extension. In the case of totally ramified extensions, the discriminants of such a power integral bases is the same as the discriminant of the Eisenstein polynomial with root α.

We find that the first digit of the p-adic expansion of the discriminant of generating Eisenstein polynomials is an invariant for most extensions. This allows for a finer classification of totally ramified extensions. Most of our results also hold over extensions of $\mathbb{Q}_p$; in this case we consider the π-adic expansion of the discriminant where π is a uniformizing element of the base field. As an application we show that for extensions of $\mathbb{Q}_p$ of degree p this new invariant already yields the Galois group.

Notation. We introduce the notation that we use throughout the paper and recall some results about totally ramified extensions.

For a prime number p we denote by $\mathbb{Q}_p$ the completion of the rational numbers $\mathbb{Q}$ with respect to the p-adic exponential valuation v_p, by $\mathbb{Z}_p$ its valuation ring, and by $\overline{\mathbb{Q}_p}$ a fixed algebraic closure of $\mathbb{Q}_p$. By K we denote a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$, uniformizing element π, and maximal ideal (π). The exponential valuation v_π on K is normalized such that $v_\pi(\pi) = 1$. The extensions of v_p and v_π to $\overline{\mathbb{Q}_p}$ are also denoted by v_p and v_π. We write $\underline{K}$ for the residue class field $\mathcal{O}_K/(\pi)$ of K and for $\beta \in \mathcal{O}_K$ we set $\underline{\beta} = \beta + (\pi) \in \underline{K}$.

The extensions that we consider are totally ramified extensions. In the following the ground field K will either be the p-adic field $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}_p$. Totally ramified extensions L/K can be generated by an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$. For a root α of φ we have $\mathcal{O}_L = \mathcal{O}_K(\alpha)$. The discriminant $\operatorname{disc}(\varphi)$ of the generating polynomial φ is equal to the discriminant of the integral basis $1, \alpha, \ldots, \alpha^{n-1}$ of $\mathcal{O}_L/\mathcal{O}_K$ where n is the degree of φ and thus the degree of L/K. The root α is a uniformizing element of $\mathcal{O}_L$. We write v_α for the valuation on $\mathcal{O}_L$ that is normalized such that $v_\alpha(\alpha) = 1$. For $\gamma \in K$ we have $v_\alpha(\gamma) = n \cdot v_\pi(\gamma)$. The minimal polynomial of any uniformizing element of $\mathcal{O}_L$, that is of any $\beta \in \mathcal{O}_L$ with $v_\alpha(\beta) = 1$ is also a uniformizing element of L and its minimal polynomial is an Eisenstein polynomial.

2. Main Results

In this section we present our main results. The proofs can be found in the following sections. We start by investigating the number of common digits of the discriminants is related to the distance between the two polynomials.

For a given $n \in \mathbb{N}$ there are finitely many totally ramified extensions of K of degree n. Marc Krasner has presented a formula for the number of the extensions with given degree and valuation of the discriminant [Kra66]. To this end he introduces a distance function d on the set of Eisenstein polynomials of a fixed degree and valuation of the discriminant, also see [PR01, Section 4].

Definition 2.1. Let φ, $\psi \in \mathcal{O}_K[x]$ be Eisenstein of degree n with $v_\pi(\operatorname{disc}(\varphi)) = v_\pi(\operatorname{disc}(\psi))$. Let $\alpha \in \overline{\mathbb{Q}_p}$ be a root of φ and define the distance between φ and ψ as $d(\varphi, \psi) = v_\pi(\psi(\alpha))$.

This distance is symmetric with respect to the input polynomials and is independent of the choice of root. It satisfies the ultrametric inequality, and clearly $d(\varphi, \psi) = \infty$ if and only if $\varphi = \psi$.

We find that when we choose two polynomials φ and ψ that generate isomorphic extensions such that they are close enough, that is when $d(\varphi, \psi)$ is large enough, we can ensure that arbitrarily many digits of the π-adic expansion of their discriminants coincide.

Theorem 2.2. Let φ, $\psi \in \mathcal{O}_K[x]$ be Eisenstein of degree n with $v_\pi(\operatorname{disc}(\varphi)) = v_\pi(\operatorname{disc}(\psi)) = n + j - 1$. If $d(\varphi, \psi) > \frac{n+2j}{n}$, then

$$v_\pi(\operatorname{disc}(\varphi) - \operatorname{disc}(\psi)) \geq \left(1 - \frac{1}{n}\right) v_\pi(\operatorname{disc}(\varphi)) + d(\varphi, \psi).$$

From now on we concentrate on the first digit of the π-adic expansion of the discriminants of polynomials. We use this notation:

Definition 2.3. For $\beta \in \mathcal{O}_K$ we set $\operatorname{tc}(\beta) = \underline{(\beta/\pi^{v_\pi(\beta)})} \in \underline{K}$. This is the first nonzero digit (or the trailing coefficient) of the π-adic expansion of β as an element of $\underline{K}$.

Clearly we have:

Lemma 2.4. For $\alpha, \beta \in K$ we have $\operatorname{tc}(\alpha \cdot \beta) = \operatorname{tc}(\alpha) \cdot \operatorname{tc}(\beta)$.

We find that this first π-adic digit of the valuation of the generating Eisenstein polynomial is an invariant in many cases.

Theorem 2.5. Let $\varphi, \psi \in \mathcal{O}_K[x]$ be Eisenstein and of degree n such that $K[x]/(\varphi) \cong K[x]/(\psi)$. If $(\#\underline{K} - 1)|(n(n-1))$ then $\operatorname{tc}(\operatorname{disc}(\varphi)) = \operatorname{tc}(\operatorname{disc}(\psi))$.

In these cases, the trailing coefficient of the discriminant is independent of the generating Eisenstein polynomial and thus is an invariant of power integral bases of a totally ramified extension. Thus, if $(\#\underline{K} - 1)|(n(n-1))$, then the trailing coefficient of the discriminant is an invariant of the extension. Some classes of extensions always have the same invariant.

Proposition 2.6. Let p be odd and $\varphi \in \mathbb{Q}_p[x]$ be Eisenstein of degree p^m such that $\mathbb{Q}_p[x]/(\varphi)$ is cyclic. Then

$$\operatorname{tc}(\operatorname{disc}(\varphi)) = \begin{cases} 1 & \text{if } m \text{ is even} \\ -1 & \text{if } m \text{ is odd and } p \equiv 1 \bmod 4 \\ 1 & \text{if } m \text{ is odd and } p \equiv 3 \bmod 4. \end{cases}$$

We end with examples of information that can be obtained from this invariant. Extensions of $\mathbb{Q}_p$ of degree p have been described in detail, see [Ama71] or [JR06]. We show that they can also be classified using the discriminant and its trailing coefficient, that is, the first non-zero coefficient of its p-adic expansion.

Theorem 2.7. Let φ be an Eisenstein polynomial of degree p in $\mathbb{Q}_p$ such that $\operatorname{Gal}(\varphi) \not\cong C_p$ and $v_p(\operatorname{disc}(\varphi)) \neq 2p-1$. Then the isomorphism class of the extension generated by φ is uniquely determined by $v_p(\operatorname{disc}(\varphi))$ and $\operatorname{tc}(\operatorname{disc}(\varphi))$.

The Galois group of an Eisenstein polynomial φ of degree p over $\mathbb{Q}_p$ can be determined from the valuation of its discriminant $\operatorname{disc}(\varphi)$ and its trailing coefficient $\operatorname{tc}(\operatorname{disc}(\varphi))$.

Corollary 2.8. Let p be an odd prime, and let φ be an Eisenstein polynomial of degree p over $\mathbb{Q}_p$. Let $v = v_p(\operatorname{disc}(\varphi))$, $j = v - p + 1$, and $\underline{\gamma} = (\underline{-1})^{(p-1)/2} \operatorname{tc}(\operatorname{disc}(\varphi))$. Then

$$\operatorname{Gal}(\varphi) \cong \begin{cases} C_p \rtimes C_{p-1} & \text{if } v = 2p-1 \\ C_p & \text{if } v = 2p-2 \text{ and } \underline{\gamma} = \underline{p-1} \\ C_p \rtimes C_d & \text{otherwise} \end{cases}$$

where $d = \frac{p-1}{\gcd(\frac{p-1}{m}, j)}$ with m being the order of $\underline{aj}$ in $\mathbb{F}_p^\times$ for $\underline{a} = \underline{\gamma} \cdot (\underline{-1})^{j+1} \underline{j}^{-1}$.

3. Proof of Theorem 2.2

We recall some of the results from the work of Krasner (see [Kra66] or [PR01]) about the distance function d. Assume that $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in \mathcal{O}_K[x]$ and $\psi(x) = \sum_{i=0}^{n} \psi_i x^i \in \mathcal{O}_K[x]$ are Eisenstein polynomials whose discriminants have the same valuation, say $v_\pi(\operatorname{disc}(\varphi)) = v_\pi(\operatorname{disc}(\psi)) = n + j - 1$. Denote by $\alpha = \alpha_{(1)}, \dots, \alpha_{(n)}$ the roots of φ in $\overline{\mathbb{Q}_p}$.

If $d(\varphi, \psi) > \frac{n+2j}{n}$ then there is a root $\beta \in \overline{\mathbb{Q}_p}$ of ψ such that $v_\pi(\alpha - \beta) > v_\pi(\alpha - \alpha_{(i)})$ for $2 \le i \le n$. In this case Krasner's lemma implies that $K(\alpha) = K(\beta)$. So the assumption of Theorem 2.2 implies that the extensions generated by φ and ψ are isomorphic.

Furthermore, again assuming that $v_\pi(\alpha - \beta) > v_\pi(\alpha - \alpha_{(i)})$ for some $2 \le i \le n$, we obtain another expression for the distance of two polynomials:

$$d(\varphi, \psi) = \sum_{i=1}^{n} \min\{v_\pi(\alpha - \beta), v_\pi(\alpha - \alpha_{(i)})\} = v_\pi(\alpha - \beta) + \sum_{i=2}^{n} v_\pi(\alpha - \alpha_{(i)})$$

So we can write the valuation of $\alpha - \beta$ in terms of $d(\varphi, \psi)$ and $\operatorname{disc}(\varphi)$:

$$\begin{aligned} v_\pi(\alpha - \beta) &= d(\varphi, \psi) - \sum_{i=2}^{n} v_\pi(\alpha - \alpha_{(i)}) \\ &= d(\varphi, \psi) - v_\pi\left(\prod_{i=2}^{n} (\alpha - \alpha_{(i)})\right) \\ &= d(\varphi, \psi) - \frac{1}{n} v_\pi(\operatorname{disc}(\varphi)). \end{aligned} \tag{1}$$

We now are ready to prove Theorem 2.2.

Proof of Theorem 2.2. Let $\alpha = \alpha_{(1)}, \dots, \alpha_{(n)}$ and β as above. As $K(\alpha) = K(\beta)$ there is $\gamma \in K(\alpha)$ with $v_\alpha(\gamma) = 0$ such that $\beta = \alpha + \gamma\alpha^m$ where $m = v_\alpha(\alpha - \beta)$. We order the roots $\beta_{(1)}, \dots, \beta_{(n)}$ of ψ such that $\beta_{(1)} = \beta = \alpha + \gamma\alpha^m$, $\beta_{(2)} = \alpha_{(2)} + \gamma_{(2)}\alpha_{(2)}^m$ and so on. For the discriminant of ψ we get:

$$\begin{aligned} \operatorname{disc}(\psi) &= \prod_{i<j} \left(\beta_{(i)} - \beta_{(j)}\right)^2 = \prod_{i<j} \left(\left(\alpha_{(i)} + \gamma_{(i)}\alpha_{(i)}^m\right) - \left(\alpha_{(j)} + \gamma_{(j)}\alpha_{(j)}^m\right)\right)^2 \\ &= \prod_{i<j} \left(\left(\alpha_{(i)} - \alpha_{(j)}\right) + \left(\gamma_{(i)}\alpha_{(i)}^m - \gamma_{(j)}\alpha_{(j)}^m\right)\right)^2 \\ &= \prod_{i<j} \left(\alpha_{(i)} - \alpha_{(j)}\right)^2 \prod_{i<j} \left(1 - \sum_{k=1}^{m} \left(\gamma_{(j)}\alpha_{(i)}^{m-k}\alpha_{(j)}^{k-1}\right) - \alpha_{(i)}^m \frac{\gamma_{(j)} - \gamma_{(i)}}{\alpha_{(j)} - \alpha_{(i)}}\right)^2 \\ &= \operatorname{disc}(\varphi) \prod_{i<j} \left(1 - \gamma_{(j)} \sum_{k=1}^{m} \left(\alpha_{(i)}^{m-k}\alpha_{(j)}^{k-1}\right) - \alpha_{(i)}^m \frac{\gamma_{(j)} - \gamma_{(i)}}{\alpha_{(j)} - \alpha_{(i)}}\right)^2. \end{aligned}$$

Let $C_{ij} = \left(1 - \gamma_{(j)} \sum_{k=1}^{m} \left(\alpha_{(i)}^{m-k}\alpha_{(j)}^{k-1}\right) - \alpha_{(i)}^{m} \frac{\gamma_{(j)}-\gamma_{(i)}}{\alpha_{(j)}-\alpha_{(i)}}\right)^2$. We have $v_\alpha(C_{ij} - 1) \geq m - 1$. With $\operatorname{disc}(\psi) = \operatorname{disc}(\varphi)(\prod_{i<j} C_{ij})$ we get:

$$\begin{aligned}
v_\pi(\operatorname{disc}(\varphi) - \operatorname{disc}(\psi)) &= v_\pi\left(\operatorname{disc}(\varphi) - \operatorname{disc}(\varphi)\left(\prod_{i<j} C_{ij}\right)\right)\\
&= v_\pi(\operatorname{disc}(\varphi)) + v_\pi\left(1 - \left(\prod_{i<j} C_{ij}\right)\right)\\
&\geq v_\pi(\operatorname{disc}(\varphi)) + \frac{m-1}{n}.
\end{aligned}$$

With $m = v_\alpha(\alpha - \beta) = n \cdot v_\pi(\alpha - \beta)$ and (1) we obtain

$$\begin{aligned}
v_\pi(\operatorname{disc}(\varphi) - \operatorname{disc}(\psi)) &\geq v_\pi(\operatorname{disc}(\varphi)) + \frac{n \cdot v_\pi(\alpha - \beta) - 1}{n}\\
&= v_\pi(\operatorname{disc}(\varphi)) + d(\varphi, \psi) - \frac{1}{n}(v_\pi(\operatorname{disc}(\varphi)) + 1). \qquad \square
\end{aligned}$$

4. Proof of Theorem 2.5

Proof of Theorem 2.5. Let α be a root of φ. Since φ and ψ generate isomorphic extensions, there exists $\beta \in K(\alpha)$ such that $\psi(\beta) = 0$. So $\beta = \sum_{k=0}^{n-1} b_k\alpha^k$ for some $b_k \in \mathcal{O}_K$. As $v_\alpha(\beta) = v_\alpha(\alpha) = 1$ we have $v(b_1) = 0$. Let $\alpha_{(1)}, \alpha_{(2)}, \dots, \alpha_{(n)}$ be the conjugates of α and let $\sigma_1, \sigma_2, \dots, \sigma_n$ be the isomorphisms such that $\sigma_i(\alpha) = \alpha_{(i)}$. Let $\beta_{(1)}, \beta_{(2)}, \dots, \beta_{(n)}$ be the roots of ψ, defined by

$$\beta_{(i)} = \sigma_i(\beta) = \sigma_i\left(\sum_{k=0}^{n-1} b_k\alpha^k\right) = \sum_{k=0}^{n-1} \sigma_i(b_k)\sigma_i(\alpha)^k = \sum_{k=0}^{n-1} b_k\alpha_{(i)}^k.$$

We now compute the discriminant of ψ, with the goal of writing it in terms of the discriminant of φ.

$$\begin{aligned}
\operatorname{disc}(\psi) = \prod_{i<j}\left(\beta_{(i)} - \beta_{(j)}\right)^2 &= \prod_{i<j}\left(\sum_{k=1}^{n-1} b_k\left(\alpha_{(i)}^k - \alpha_{(j)}^k\right)\right)^2\\
&= \prod_{i<j}\left(\alpha_{(i)} - \alpha_{(j)}\right)^2 \prod_{i<j}\left[\sum_{k=1}^{n-1}\left(b_k \sum_{\ell=0}^{k-1} \alpha_{(i)}^{(k-1-\ell)}\alpha_{(j)}^{\ell}\right)\right]^2\\
&= \operatorname{disc}(\varphi) \cdot \prod_{i<j}\left[\sum_{k=1}^{n-1}\left(b_k \sum_{\ell=0}^{k-1} \alpha_{(i)}^{(k-1-\ell)}\alpha_{(j)}^{\ell}\right)\right]^2.
\end{aligned}$$

We write $\operatorname{disc}(\varphi) - \operatorname{disc}(\psi) = \operatorname{disc}(\varphi) \cdot (1 - \gamma)$ where

$$\gamma = \prod_{i<j}\left[\sum_{k=1}^{n-1}\left(b_k \sum_{\ell=0}^{k-1} \alpha_{(i)}^{(k-1-\ell)}\alpha_{(j)}^{\ell}\right)\right]^2.$$

Note that γ is a symmetric polynomial in $\alpha_{(1)}, \dots, \alpha_{(n)}$. Let $e_1, \dots, e_n$ denote the elementary symmetric polynomials in $\alpha_{(1)}, \dots, \alpha_{(n)}$. By the fundamental theorem of symmetric polynomials, there is a polynomial $\gamma^* \in \mathcal{O}_K[x_1, \dots, x_n]$ such that

$\gamma = \gamma^*(e_1, \ldots, e_n)$. If we expand γ^*, all terms consist of sums of products of $\alpha_{(1)}, \ldots, \alpha_{(n)}$ except for the constant term, $b_1^{n(n-1)}$. So

$$\gamma^* = m_{(1)}e_1 + m_{(2)}e_2 + \cdots + m_{(n)}e_n + m_{(n+1)}e_1^2 + m_{(n+2)}e_1e_2 + \cdots + b_1^{n(n-1)}$$

for some $m_{(1)}, \ldots, m_{(n(n-1)-1)} \in \mathcal{O}_K$. Note that $e_1, \ldots, e_n$ are exactly the coefficients of φ. Since the coefficients of φ have π-adic valuation greater than or equal to 1, π divides all of its coefficients. This implies $\underline{\gamma} = \underline{b_1^{n(n-1)}}$.

The next step is to show $\underline{b_1^{n(n-1)}} = \underline{1}$. Since both φ and ψ are Eisenstein and generate the same extension, $v_\alpha(\beta) = 1$. So

$$1 = v_\alpha(\beta) = v_\alpha\left(\sum_{k=0}^{n-1} b_k\alpha^k\right) = \min_{0 \le k \le n-1}\{v_\alpha(b_k\alpha^k)\}.$$

Equality holds because each b_k has α-adic valuation 0 or a positive multiple of n, so each term has a different valuation. For all k, $v_\alpha(b_k\alpha^k) \ge 1$. For $k \ge 1$, this is obviously true. For $k = 0$, $v_\alpha(b_0) = 0$ or a positive multiple of n. As $v_\alpha(b_0)$ must be at least 1, the lowest multiple of n it can be is n. We now have that for $k \ne 1$, $v_\alpha(b_k\alpha^k) \ge 2$. Thus $v_\alpha(b_1\alpha) = 1$, implying $v_\alpha(b_1) = 0$, i.e. $b_1 \notin (\pi)$. By the generalization of Fermat's little theorem, $b_1 \notin (\pi) \Rightarrow \underline{b_1^{\#\underline{K}-1}} = 1$. By assumption $(\#\underline{K} - 1)|n(n-1)$, so this implies $\underline{b_1^{n(n-1)}} = 1$.

We have $\underline{(1-\gamma)} = \underline{(1-b_1^{n(n-1)})} = \underline{(1-1)} = \underline{0}$. Because $\pi|(1-\gamma)$ we can write $1 - \gamma = \pi \cdot c$ for some c. So

$$\operatorname{disc}(\varphi) - \operatorname{disc}(\psi) = \operatorname{disc}(\varphi)\cdot(1-\gamma) = \operatorname{disc}(\varphi)\cdot\pi\cdot c.$$

Therefore, $v_\pi(\operatorname{disc}(\varphi) - \operatorname{disc}(\psi)) \ge v_\pi(\operatorname{disc}(\varphi)) + 1$ and thus $\operatorname{tc}(\operatorname{disc}(\varphi)) = \operatorname{tc}(\operatorname{disc}(\psi))$. □

5. Proof of Proposition 2.6

Because of Lemma 2.4 we only need to consider the trailing coefficients of the differences of roots in our considerations.

In the proof of the proposition we will use information obtained from the ramification polygon of the polynomial $\varphi \in \mathbb{Q}_p[x]$ under consideration. We recall some of the information that can be obtained from the ramification polygon, see [GP12] for details.

Let α be a root of φ. The ramification polynomial of an Eisenstein polynomial φ of degree n

$$\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^n) = \sum_{i=0}^{n} \rho_i x^i \in \mathbb{Q}_p(\alpha)[x]$$

has the roots $\frac{\alpha^* - \alpha}{\alpha}$ where α^* is a root of φ. The Newton polygon of the ramification polynomial is called the ramification polygon of φ, it is independent of the choice of α and an invariant of the extension $\mathbb{Q}_p(\alpha) \equiv \mathbb{Q}_p[x]/(\varphi)$. Its breaks can only be at powers of p and The negatives of the slopes λ of the segments are the valuations of the differences of the roots of φ. The length of the segment (in direction of the horizontal axis) with slope λ is the number of roots α^* of φ such that $v_\alpha(\alpha - \alpha^*) = \lambda + 1$.

When $\mathbb{Q}_p[x]/(\varphi)$ is normal the differences of the roots of φ are in $\mathbb{Q}_p[x]/(\varphi)$ and thus the slopes λ_i of the segments of the ramification polygon are integral.

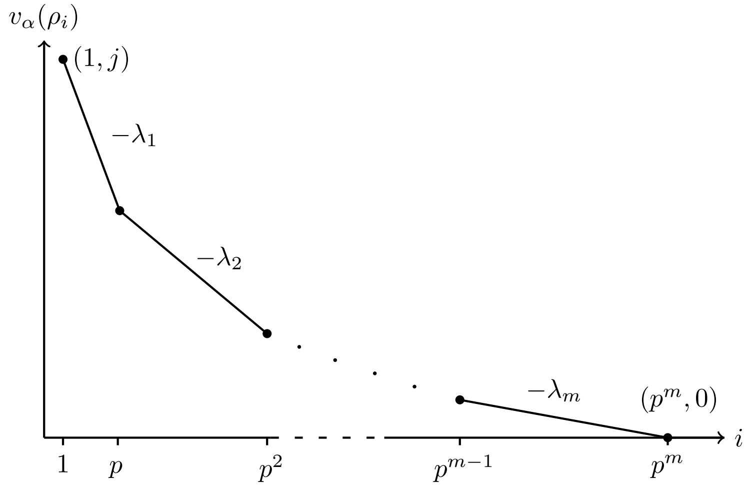

FIGURE 1. Ramification polygon of an Eisenstein polynomial $\varphi \in \mathbb{Q}_p[x]$ of degree p^m with $\operatorname{disc}(\varphi) = p^m + j - 1$ generating a normal cyclic extension, where $\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^{p^m}) = \sum_{i=0}^{p^m} \rho_i x^i \in \mathbb{Q}_p(\alpha)[x]$ with α a root of φ is the ramification polynomial of φ.

Furthermore the roots of the residual polynomials of the segment of slope λ are of the form

$$\underline{\gamma} = \underline{\left(\frac{\alpha^* - \alpha}{\alpha^{\lambda+1}}\right)}$$

and thus $\operatorname{tc}(\alpha^* - \alpha) = \underline{\gamma}$. As $\mathbb{Q}_p[x]/(\varphi)$ is normal we have $\underline{\gamma} \in \mathbb{F}_p$. The normality also implies that the lengths of the segments of the ramification polygon are $p^i - p^{i-1}$ for $1 \le i \le m$ and that all elements of $\mathbb{F}_p^\times$ are roots of the residual polynomial of each segment.

Proof of Proposition 2.6. The polynomial φ is an Eisenstein polynomial of degree p^m. As the extension generated by φ is normal, the slopes of the segments are integers. It follows from the symmetry of the roots and the normality of the extension that the breaks in the polygon are exactly at 1, p, p^2, $\dots$,p^{m-1}, see Figure 1. So the lengths of the segments with finite slope are $p-1$, p^2-p, $\dots$, $p^m - p^{m-1}$.

As $\underline{\mathbb{Q}_p^\times} = \mathbb{F}_p^\times$ only has $p-1$ distinct elements it follows from the symmetry of the roots that we get for any root α of φ that:

$$\prod_{v_p(\alpha-\alpha^*)=\lambda_1} \operatorname{tc}(\alpha - \alpha^*) = \prod_{\underline{\gamma} \in \mathbb{F}_p^\times} \underline{\gamma} = \underline{-1} \tag{2}$$

where the α^* are roots of φ and $-\lambda_1$ is the slope of the first segment of the ramification polygon from Figure 1. Similarly, again because of normality and symmetry, taking into consideration the lengths of the segment for the second to the n-th segments with slopes λ_i of length $p^i - p^{i-1}$ using that p is odd, we get:

$$\prod_{v_p(\alpha-\alpha^*)=\lambda_i} \operatorname{tc}(\alpha-\alpha^*) = \left(\prod_{\underline{\gamma}\in\mathbb{F}_p^\times} \underline{\gamma}\right)^{p^{i-1}} = (\underline{-1})^{p^{i-1}} = \underline{-1}. \tag{3}$$

Equations (2) and (3) yield:

$$\begin{aligned}\operatorname{tc}(\operatorname{disc}(\varphi)) &= (\underline{-1})^{\frac{p^m(p^m-1)}{2}} \prod_{\alpha^*\neq\alpha} \operatorname{tc}(\alpha-\alpha^*)\\ &= (\underline{-1})^{\frac{p^m(p^m-1)}{2}} \prod_{\alpha}\prod_{i=1}^{m}\prod_{v_p(\alpha-\alpha^*)=\lambda_i} \operatorname{tc}(\alpha-\alpha^*)\\ &= (\underline{-1})^{\frac{p^m(p^m-1)}{2}} ((\underline{-1})^m)^{p^m} = (\underline{-1})^{m+\frac{p^m(p^m-1)}{2}}.\end{aligned}$$

Recall that p is odd. When m is even we have $p^m \equiv 1 \bmod 4$ so $\frac{p^m-1}{2} \equiv 0 \bmod 4$ which implies $\operatorname{tc}(\operatorname{disc}(\varphi)) = 1$. Similarly, when m is odd and $p \equiv 1 \bmod 4$ then $\frac{p^m-1}{2} \equiv 0 \bmod 4$, so $\operatorname{tc}(\operatorname{disc}(\varphi)) = -1$ and when m is odd and $p \equiv 3 \bmod 4$ then $\frac{p^m-1}{2} \equiv 1 \bmod 4$, so $\operatorname{tc}(\operatorname{disc}(\varphi)) = 1$. □

6. Proof of Theorem 2.7 and Corollary 2.8

Before we get to the proof of the theorem and corollary we give some auxiliary results. In the proofs below we use that $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = \operatorname{tc}(\operatorname{disc}(\varphi))\,(\underline{-1})^{\frac{n(n-1)}{2}}$ where $\operatorname{Res}(\varphi,\varphi')$ denotes the resultant of φ and φ' and the degree of φ is n.

To determine the trailing coefficient of the discriminant of Eisenstein polynomials φ of degree p over $\mathbb{Q}_p$ for p odd we distinguish the three cases presented in Table 1. The case $v_p\operatorname{disc}(\varphi) = 2p-2$ in which $\operatorname{Gal}\varphi \cong C_p$ is covered by Proposition 2.6.

Lemma 6.1. Let p be an odd prime, and $\varphi \in \mathbb{Q}_p[x]$ be of degree p, with $v_p(\operatorname{disc}(\varphi)) = 2p-1$. Then $\operatorname{tc}(\operatorname{disc}(\varphi)) = (\underline{-1})^{\frac{p(p-1)}{2}}$.

Proof. If φ is a degree p polynomial with $v_p(\operatorname{disc}(\varphi)) = 2p-1$, it must be of the form $\varphi(x) = x^p + p(1+ap)$ for $a \in \{1,\dots,p-1\}$, or generate an isomorphic extension to such a polynomial [JR06, Table 2.1]. However, using Theorem 2.5, we can reduce to the case where the polynomials are exactly of this form since we are only concerned with the trailing coefficient of the discriminant. We compute $\varphi'(x) = px^{p-1}$. Then 0 is a root of φ' with multiplicity $p-1$. To show $\operatorname{tc}(\operatorname{disc}(\varphi)) = (\underline{-1})^{\frac{p(p-1)}{2}}$ we show $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = \underline{1}$. We have

$$\operatorname{Res}(\varphi,\varphi') = p^p(p(1+ap))^{p-1} = p^{2p-1}(1+ap)^{p-1}.$$

Thus

$$\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = \underline{(1+ap)}^{p-1} = \underline{1}^{p-1} = \underline{1}.$$ □

Lemma 6.2. Let φ be an Eisenstein polynomial in $\mathbb{Q}_p$ of the form $x^p + apx^j + p$ for $a, j \in \{1,\dots,p-1\}$ and j and a not both equal to $p-1$. Then $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = (\underline{-1})^{j+1}aj$.

Proof. As $\varphi(x) = x^p + apx^j + p$ we have $\varphi'(x) = px^{p-1} + apjx^{j-1} = px^{j-1}(x^{p-j} + aj)$. The polynomial φ' has 0 as a root with multiplicity $j-1$ and $p-j$ roots $r_0,\dots,r_{p-j-1}$ with $r_k^{p-j} = -aj$ for $0 \le k \le p-j-1$ of multiplicity 1.

Table 1. Families of generating polynomials of extensions of degree p of $\mathbb{Q}_p$ for p odd with their Galois group. We have $d = \frac{p-1}{\gcd(\frac{p-1}{m},j)}$ where m is the order of $\underline{aj}$ in $\mathbb{F}_p^\times$ for $\underline{a} = \underline{\gamma} \cdot (\underline{-1})^{j+1}\underline{j}^{-1}$. See [JR06].

$\varphi \in \mathbb{Q}_p[x]$	Parameters	$v_p(\operatorname{disc}(\varphi))$	$\operatorname{Gal}(\varphi)$
$x^p + apx^j + p$	$1 \leq a \leq p-1$ $1 \leq j \leq p-1$ $(j,a) \neq (p-1,p-1)$	$p+j-1$	$C_p \rtimes C_d$
$x^p - px^{p-1} + p(1+ap)$	$0 \leq a \leq p-1$	$2p-2$	C_p
$x^p + p(1+ap)$	$0 \leq a \leq p-1$	$2p-1$	$C_p \rtimes C_{p-1}$

Let $\xi \in \overline{\mathbb{Q}_p}$ be a primitive $(p-j)$th root of unity and fix a non zero root r_0 of φ' then the other non zero roots are of the form $r_k = \xi^k r_{p-j}$ where $k = 1, \ldots, p-j-1$. Writing $\varphi(x) = x^j(x^{p-j} + ap) + p$ and evaluating φ at the roots of φ' we obtain:

$$\operatorname{Res}(\varphi,\varphi') = p^p p^{j-1} \prod_{k=0}^{p-j-1} \left[\left(\xi^k r_0\right)^j \left(r_0^{p-j} + ap\right) + p \right].$$

Hence

$$\begin{aligned}
\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) &= \prod_{k=0}^{p-j-1} \left[\left(\underline{\xi^k}(\underline{r_0}\right)^j \cdot \left(\underline{r_0}^{p-j} + \underline{ap}\right) + \underline{p} \right] \\
&= \prod_{k=0}^{p-j-1} \left[\underline{\xi}^{kj} \cdot \underline{r_0}^{j+p-j} \right] = \underline{r_0}^{p(p-j)} \cdot \prod_{k=0}^{p-j-1} \underline{\xi}^{kj} \\
&= (\underline{r_0})^{p-j} \cdot \underline{\xi}^{j \sum_0^{p-j-1} k} = (\underline{-aj}) \cdot \underline{\xi}^{j \frac{(p-j)(p-j-1)}{2}} \\
&= \underline{-aj} \cdot (\underline{\xi^{\frac{p-j}{2}}})^{j(p-j-1)} = (\underline{-1})^{j+1}\underline{aj}.
\end{aligned}$$

□

Proof of Theorem 2.7. Let $\varphi \in \mathbb{Q}_p[x]$ be Eisenstein of degree p such that $\operatorname{Gal}(\varphi) \neq C_p$ and $v_p(\operatorname{disc}(\varphi)) \neq 2p-1$. For each of these extensions, there is exactly one polynomial of the form $x^p + apx^j + p$ for $a, j \in \{1, \ldots, p-1\}$ where $p+j-1$ is the valuation of the discriminant and j and a are both not equal to $p-1$ [JR06, Proposition 2.3.1].

Thus there exists some $\psi(x) = x^p + apx^j + p$ (for fixed a and j) that generates an extension isomorphic to φ. By Theorem 2.5, $v_p(\operatorname{Res}(\varphi,\varphi')) = v_p(\operatorname{Res}(\psi,\psi'))$ and $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = \operatorname{tc}(\operatorname{Res}(\psi,\psi'))$. With Table 1 and Lemma 6.2 we get

$$j = v_p(\operatorname{Res}(\varphi,\varphi')) - p + 1 \text{ and } a = \operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = (\underline{-1})^{j+1}\underline{j}^{-1}.$$

No two distinct $j \in \{1, \ldots, p-1\}$ have the same multiplicative inverse modulo p. Also for a fixed j, no two distinct possible values of $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi'))$ give the same value of a. Thus $v_p(\operatorname{Res}(\varphi,\varphi'))$ and $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi'))$ uniquely determine ψ, and therefore the extension. □

Proof of Corollary 2.8. If $v_p(\operatorname{Res}(\varphi,\varphi')) = 2p-1$, then $\operatorname{Gal}(\varphi) = C_p \rtimes C_{p-1}$.

Suppose $v_p(\operatorname{Res}(\varphi,\varphi')) = 2p-2$ and $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = \underline{-1}$. Then φ is either in the first or second family in Table 1, since $v_p(\operatorname{Res}(\varphi,\varphi')) = 2p-2$. By Lemma 6.2 we have $\operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) = (\underline{-1})^{j+1}\underline{aj}$. Since $j = p-1$, $\underline{-1} = \operatorname{tc}(\operatorname{Res}(\varphi,\varphi')) =$

$(\underline{-1})^p \underline{a(p-1)} = \underline{a}$. Hence φ must be in the second row of the table, that is, $\mathrm{Gal}(\varphi) = C_p$.

Otherwise, compute a and j as in Theorem 2.7. In Table 1, $d = (p-1)/\gcd(\frac{p-1}{m}, j)$ where m is the order of aj in $\mathbb{F}_p^\times$ [JR06]. The size of the Galois group is $p \cdot d$ and the Galois group is $C_p \rtimes C_d$. □

7. Acknowledgments

The results presented in this paper were obtained during the Research Experience for Undergraduates *REU Computational Research on Local Fields and Galois Groups* at Elon University in the summer of 2018 which was supported by Elon University, the National Security Agency (grant H98230-18-1-0012), and the University of North Carolina Greensboro. We also would like to thank the anonymous referee for the helpful comments.

References

[Ama71] Shigeru Amano, *Eisenstein equations of degree p in a $\mathfrak{p}$-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **18** (1971), 1–21. MR 0308086 (46 #7201)

[Cas86] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986. MR 861410

[GP12] Christian Greve and Sebastian Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, International Journal of Number Theory **8** (2012), no. 6, 1401–1424. MR 2965757

[JR06] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)

[Kra66] Marc Krasner, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, Les Tendances Géom. en Algèbre et Théorie des Nombres, Editions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 143–169. MR 0225756 (37 #1349)

[PR01] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659 (electronic). MR 1836924 (2002e:11166)

Elon University

Princeton University

University of North Carolina Greensboro

University of North Carolina Greensboro

Carnegie Mellon University

Aurora University