DIHEDRAL p-ADIC FIELDS OF PRIME DEGREE

CHAD AWTREY AND TREVOR EDWARDS

ABSTRACT. Let p and n be odd prime numbers. We study degree n extensions of the p-adic numbers whose normal closures have Galois group equal to D_n, the dihedral group of order $2n$. If $p \nmid n$, the extensions are tamely ramified and are straightforward to classify; there is a unique such extension if $n \mid p+1$ and none otherwise. If $p = n$, we follow Amano and show there are six such extensions if $p = 3$ and three otherwise. For each extension, we provide a defining polynomial and compute its inertia subgroup.

1. INTRODUCTION

The p-adic numbers $\mathbf{Q}_p$ are foundational to much of 20th and 21st century number theory (e.g., number fields, elliptic curves, and L-functions) and are connected to many practical applications in physics, chemistry, and cryptography. Their fundamental importance is supported by the fact that p-adic numbers play a significant role in computational attacks on two of the seven Clay Mathematics Million Dollar Millennium Problems; namely the Riemann Hypothesis and the Birch and Swinnerton-Dyer conjecture.

The Riemann Hypothesis concerns the distribution of prime numbers, and the truth of its generalized version would assert the correctness of the best algorithms for constructing large prime numbers, which are used daily for internet public-key cryptosystems. The Birch and Swinnerton-Dyer conjecture deals with elliptic curves, and it connects the structure of the group of rational points on an elliptic curve to properties of its corresponding L-function. The

2000 *Mathematics Subject Classification.* Primary 11S05, 11S15; Secondary 11S20, 20B35.

Key words and phrases. p-adic, extension fields, Galois group, dihedral, inertia, ramification.

The first author was supported in part by an Elon University FRD grant.

most famous application occurs in the proof of Fermat's Last Theorem [7], where the key step is to prove that every semistable elliptic curve is modular.

In all instances, experimentations and computations are routinely done in p-adic fields, using p-adic methods. Therefore, classifying p-adic fields through their arithmetic invariants would provide computational support to investigations concerning these two famous unsolved problems, as well as numerous other unproven conjectures in number theory (e.g., Bloch-Kato and Stark's).

Classifying extensions of $\mathbf{Q}_p$ means gathering explicit data that uniquely determines the extensions, including,

(1) the number of extensions for a given degree, prime, and discriminant (necessarily finite by a classical result [4, p.54]),
(2) defining polynomials for each extension,
(3) the Galois group of the extension's polynomial (a difficult computational problem in general), and
(4) the inertia subgroup (useful in number field analyses).

In this paper, we study extensions of $\mathbf{Q}_p$ of prime degree n. If $n \neq p$, then all extensions are tamely ramified and items (1)-(4) are well-understood. We include this case for completeness. If $n = p$, then Amano has given defining polynomials for each nonisomorphic extension [1]. We describe his methods and the tamely ramified case in Section 3, after giving an overview of p-adic numbers and their extensions in Section 2. In Section 4, we study the ramification groups of prime degree p-adic fields to show that the Galois groups of the polynomials in Section 3 must be solvable with very special subnormal series. In the final section, we solve items (1), (2), and (4) for extensions whose normal closures have dihedral Galois group.

2. Background

In this section, we give a brief overview of p-adic numbers and their extensions, introducing only those definitions and results that are used in the sequel. For more details, we refer the reader to [2], which contains a good elementary account of p-adic numbers. More advanced treatments can be found in [4] and [6].

2.1. **The P-adic Numbers.**

The p-adic numbers are constructed from the rationals in much the same way the reals are constructed.

In particular, consider the map $v_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ defined by

$$v_p(x) = \begin{cases} n & \text{if } x = p^n a/b \text{ with } p \nmid ab \\ \infty & \text{if } x = 0 \end{cases}$$

The function v_p is called the *p-adic valuation* and it gives rise to the *p-adic absolute value* $|\cdot|_p$ in the following way,

$$|x|_p = \frac{1}{p^{v_p(x)}} \qquad \text{for all } x \in \mathbf{Q}$$

The p-adic numbers are defined as the completion of $\mathbf{Q}$ with respect to this absolute value. The field $\mathbf{Q}_p$ has characteristic 0 and is a locally compact, totally disconnected Hausdorff topological space [2, p.63].

The ring of *p-adic integers* $\mathbf{Z}_p$ is defined as

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$$

The ring $\mathbf{Z}_p$ is compact and has a unique maximal ideal; namely $p\mathbf{Z}_p$. The *residue field* is defined as $\mathbf{Z}_p/p\mathbf{Z}_p$ and is isomorphic to the finite field with p elements $\mathbf{F}_p$. Every element of $\mathbf{Q}_p$ can be written in the form x/p^n for some $x \in \mathbf{Z}_p$ and some nonnegative integer n. Moreover, every element of $\mathbf{Z}_p$ can be represented uniquely as an infinite sum in "base p" [2, p.68]

$$\mathbf{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k : a_k \in \mathbf{Z} \text{ with } 0 \leq a_k \leq p-1 \right\}$$

2.2. **Extensions of $\mathbf{Q}_p$.** By an *extension field* of $\mathbf{Q}_p$, we mean any field K containing $\mathbf{Q}_p$. Notice that this implies K is a vector space over $\mathbf{Q}_p$, and we say K is a *finite extension* if its dimension as a $\mathbf{Q}_p$ vector space is finite. We write

$$[K : \mathbf{Q}_p] = \dim_{\mathbf{Q}_p} K$$

and call this number the *degree* of the extension.

Let $K/\mathbf{Q}_p$ be a finite extension. The set of all automorphisms on K which induce the identity on $\mathbf{Q}_p$ forms a group under function composition, called the *automorphism group* of K. The *mass* of $K/\mathbf{Q}_p$ is defined as the degree of the extension divided by the size of its automorphism group,

$$m(K) = [K : \mathbf{Q}_p]/|\mathrm{Aut}(K/\mathbf{Q}_p)|$$

If $m(K) = 1$, then K is called a *Galois extension* and $\mathrm{Aut}(K/\mathbf{Q}_p)$ is called the *Galois group* of K.

Since $\mathbf{Q}_p$ has characteristic 0, an extension field arises by adjoining to $\mathbf{Q}_p$ the root of some monic irreducible polynomial over $\mathbf{Z}_p$. By Krasner's Lemma [4, p.43], this polynomial can be chosen to have integer coefficients. Indeed, the polynomials in the next section will all lie in $\mathbf{Z}[x]$. For an extension $K/\mathbf{Q}_p$ with $n = [K : \mathbf{Q}_p]$ and an element $x \in K$, let $f(y) = y^d + a_{d-1}y^{d-1} + \cdots + a_1 y + a_0$ be its minimal polynomial. We define the *norm* of x from K down to $\mathbf{Q}_p$ as,

$$N_{K/\mathbf{Q}_p}(x) = (-1)^n f(0)^{n/d}$$

The norm is used to define the p-adic absolute value on K that extends the p-adic absolute value on $\mathbf{Q}_p$ [2, p.151]. For $x \in K$, we define

$$|x| = \sqrt[n]{\left|N_{K/\mathbf{Q}_p}(x)\right|_p}$$

The p-adic absolute value on an extension K gives rise to the corresponding p-adic valuation v_p on K by using the equation

$$|x|_p = \frac{1}{p^{v_p(x)}}$$

where $v_p(0) = \infty$.

The p-adic valuation is a homomorphism from the multiplicative group K^* to the addivite group $\mathbf{Q}$. Its image is of the form $(1/e)\mathbf{Z}$ where $e \mid [K : \mathbf{Q}_p]$ [2, p.159]. We call e the *ramification index* of $K/\mathbf{Q}_p$. Let $f = [K : \mathbf{Q}_p]/e$. We call f the *residue degree* of $K/\mathbf{Q}_p$. Any element in K whose p-adic valuation equals e is called a *uniformizer*. If $e = 1$, the extension is called *unramified*. If $e = [K : \mathbf{Q}_p]$, the extension is called *totally ramified*. If $p \nmid e$, the extension is called *tamely ramified*.

The ring of integers in $K/\mathbf{Q}_p$ is defined as

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\} = \{x \in K : v_p(x) \geq 0\}$$

It is compact with a unique maximal ideal, given by

$$\mathcal{P}_K = \{x \in K : |x|_p < 1\} = \{x \in K : v_p(x) > 1\}$$

The *residue field* of $K/\mathbf{Q}_p$ is equal to $\mathcal{O}_K/\mathcal{P}_K$ and is isomorphic to the finite field with p^f elements $\mathbf{F}_{p^f}$, where f is the residue degree of K. Moreover, $p\mathcal{O}_K = \pi^e\mathcal{O}_k = \mathcal{P}_K^e$, where π is any uniformizer and e is the ramification index of K.

3. Defining Polynomials

In this section, we give defining polynomials for prime degree extensions of $\mathbf{Q}_p$. Such extensions are either unramified or totally ramified. The unramified extensions are easy to describe, there being a unique one for each degree. This extension is cyclic, and a defining polynomial can be obtained by extending the residue field $\mathbf{F}_p$ [4, p.48]. Therefore we focus on totally ramified extensions of prime degree n, which are given by Eisenstein polynomials [2, p.164]. There are two cases to consider; $p = n$ and $p \neq n$.

If $p \neq n$, the totally ramified extensions of $\mathbf{Q}_p$ of degree n are necessarily tamely ramified and are completely classified by the following well-known result [4, p.52].

Theorem 3.1 (Tamely Ramified Polynomials)**.** *Let $n \neq p$ be prime numbers and let $g = \gcd(n, p-1)$. Let ζ be a primitive $(p-1)$-st root of unity. There are g totally ramified degree n extensions of $\mathbf{Q}_p$, each with mass n/g. These extensions are defined by the the polynomials*

$$x^n - \zeta^r p$$

where $0 \leq r \leq g-1$.

If $p = n$, the totally ramified extensions of $\mathbf{Q}_p$ of degree p are classified by the following result due to Amano [1].

Theorem 3.2 (Amano Polynomials)**.** *Let $p > 2$ be a prime number. There are p^2 totally ramified degree p extensions of $\mathbf{Q}_p$. Polynomials defining these extensions can be grouped into three families.*

(i) $x^p - px^{p-1} + ap^2 + p$, *where* $0 \leq a \leq p-1$,
(ii) $x^p + ap^2 + p$, *where* $0 \leq a \leq p-1$, *and*
(iii) $x^p + apx^b + p$, *where* $1 \leq a, b \leq p-1$ *and* $ab \neq (p-1)^2$.

4. Ramification Groups

The aim of this section is to introduce the basic properties of ramification groups and use those to deduce structural information about Galois groups of the polynomials in Section 3. A more detailed exposition can be found in [6].

Suppose $K/\mathbf{Q}_p$ is a Galois extension with Galois group G. For an integer $i \geq -1$, we define the *i-th ramification group* of G to be

the following set,

$$G_i = \{\sigma \in G : v_p(\sigma(x) - x) \geq i + 1 \text{ for all } x \in \mathcal{O}_K\}$$

The ramification groups form a decreasing sequence of normal subgroups of G which are eventually trivial. We note that $G_{-1} = G$, and we call G_0 the *inertia subgroup* of G. The ramification groups give structural information about the Galois group G.

Lemma 4.1. *Let $K/\mathbf{Q}_p$ be a Galois extension with Galois group G, and let G_i denote the i-th ramification group. Let U_0 denote the units in K. That is $U_0 = \{x \in K : v_p(x) = 0\}$. For $i \geq 1$, let $U_i = 1 + \mathcal{P}_K^i$.*

(a) *For $i \geq 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1}.*
(b) *The group G_0/G_1 is cyclic and isomorphic to a subgroup of the group of roots of unity in the residue field of K. Its order is prime to p.*
(c) *The quotients G_i/G_{i+1} for $i \geq 1$ are abelian groups and are direct products of cyclic groups of order p. The group G_1 is a p-group.*
(d) *The group G_0 is the semi-direct product of a cyclic group of order prime to p with a normal subgroup whose order is a power of p.*
(e) *The groups G_0 and G are both solvable.*

Proof. We note that U_0/U_1 is isomorphic to the multiplicative group of the residue field of K. For $i \geq 1$, U_i/U_{i+1} is isomorphic to the additive group of the residue field. Let π be a uniformizer for K. Part (a) follows from considering the map $f : G_i/G_{i+1} \to U_i/U_{i+1}$ defined by $f(\sigma) = \sigma(\pi)/\pi$. It follows that f is an injective homomorphism, independent of choice of uniformizer. Part (b) follows from part (a). Since every subgroup of the residue field is a vector space over $\mathbf{F}_p$, every subgroup of U_i/U_{i+1} is a direct sum of cyclic groups of order p. That G_1 is a p-group follows since

$$|G_1| = \prod_{i=1} |G_i/G_{i+1}|,$$

which proves part (c). Since G_0 and G_1 have relatively prime order, there exists a subgroup of G_0 that projects isomorphically onto G_0/G_1 ([3, p.230]), proving part (d). Since G/G_0 is isomorphic to the Galois group of the residue field, it is cyclic. Part (e) follows from general results on solvability. □

Using Lemma 4.1, the fundamental theorem of Galois theory, and the classification of solvable transitive subgroups of prime degree [5, p.195], we have the following.

Corollary 4.2. *Suppose $K/\mathbf{Q}_p$ is Galois with ramification index e, residue degree f, and ramification groups G_i. Let K^u be the fixed field of G_0 and K^t be the fixed field of G_1. Then we have,*

1. *$|G/G_0| = [K^u : \mathbf{Q}_p] = f$ and $|G_0| = [K : K^u] = e$,*
2. *$K^u/\mathbf{Q}_p$ is unramified, K^t/K^u is tamely ramified, and K/K^u is totally ramified,*
3. *if $K/\mathbf{Q}_p$ is tamely ramified, then G_1 is trivial and G_0 is cyclic, and*
4. *the Galois group G of an irreducible polynomial over $\mathbf{Q}_p$ of prime degree n is a solvable transitive subgroup of S_n and is therefore of the form $C_n : C_d$ where $d \mid n-1$.*

5. Dihedral P-adic Fields

In this section we compute the number of nonisomorphic extensions of $\mathbf{Q}_p$ of prime degree whose Galois groups are dihedral. In each case, we also compute the inertia subgroup. First we consider the tamely ramified extensions. We end with a discussion of the dihedral p-adic fields of degree p.

Theorem 5.1 (Tamely Ramified Galois and Inertia Groups)**.** *Let $n \neq p$ be prime numbers and let $K/\mathbf{Q}_p$ be a finite extension of degree n. The Galois group of the normal closure of K is D_n if and only if $p \equiv -1 \pmod{n}$. In this case, the extension is unique up to isomorphism, defined by the polynomial $x^n - p$, and the inertia subgroup is cyclic of order n.*

Proof. By Theorem 3.1, there are $g = \gcd(p-1, n)$ nonisomorphic extensions of $\mathbf{Q}_p$ of degree n, each with mass n/g. If $p \equiv 1 \pmod{n}$, then there are n degree n extensions of $\mathbf{Q}_p$, each with mass 1. This implies that all extensions are Galois of prime degree n, hence cyclic. Thus if the Galois group of the normal closure of $K/\mathbf{Q}_p$ is D_n, it is necessary that $n \nmid p-1$. In this case, there will be a unique extension, and its defining polynomial can be chosen as $x^n - p$. Let ζ be a primitive n-th root of unity. Then $K = \mathbf{Q}_p(\sqrt[n]{p})$ and the normal closure K^{gal} of K is given by $K(\zeta)$. It follows that $K(\zeta)/K$ is unramified and generated by the Frobenius element which sends x to x^p [6, p.77]. Thus $[K(\zeta) : K] = d$ where d is the multiplicative

order of p modulo n; that is, d is the smallest positive integer such that $p^d \equiv 1 \pmod{n}$. Thus the ramification index of K^{gal} is n and the residue degree is d. By Corollary 4.2, the Galois group of $K^{\text{gal}}/\mathbf{Q}_p$ is $C_n : C_d$ and the inertia subgroup is C_n. It follows that the Galois group of the normal closure of $K/\mathbf{Q}_p$ is dihedral if and only if $d = 2$ if and only if $p \equiv -1 \pmod{n}$. □

Theorem 5.2 (Dihedral P-adic Fields of Degree P)**.** *Let $p > 2$ be a prime number.*

1. *If $p = 3$, there are six nonisomorphic cubic extensions of $\mathbf{Q}_3$ whose normal closures have Galois group equal to D_3. Polynomials defining these extensions can be chosen to be the Amano polynomials of type (ii) and (iii) in Theorem 3.2. The inertia subgroups for these fields are all D_3 with the exception of the field defined by $x^3 + 3x^2 + 3$, whose inertia subgroup is cyclic of order 3.*
2. *If $p > 3$, there are three nonisomorphic degree p extensions of $\mathbf{Q}_p$ whose normal closures have Galois group equal to D_p. These extensions are defined by the polynomials $x^p + px^{p-1} + p$, $x^p + 2px^{(p-1)/2} + p$, and $x^p + (p-2)px^{(p-1)/2} + p$. The inertia subgroup of the field defined by $x^p + px^{p-1} + p$ is cyclic of order p. The other two fields have inertia subgroup equal to D_p.*

Proof. Let $K/\mathbf{Q}_p$ be one of the p^2 degree p extensions. Then $K = \mathbf{Q}_p(\pi)$ where π is a root of one of the polynomials in Theorem 3.2. Let G be the Galois group of this polynomial, and let G_i be the ramification groups. Then [1] proves the normal closure K^{gal} of K is equal to $\mathbf{Q}_p(\pi, \alpha)$ where $\mathbf{Q}_p(\alpha)$ is the fixed field of G_1 and $\alpha^{p-1} \in \mathbf{Q}_p$. Since $\mathbf{Q}_p$ contains the $(p-1)$-st roots of unity [2, p.72], the extension $\mathbf{Q}_p(\alpha)/\mathbf{Q}_p$ is cyclic and $G_1 = C_p$. If π is the root of a type (i) Amano polynomial, [1] proves that $[\mathbf{Q}_p(\alpha) : \mathbf{Q}_p] = 1$, and therefore K is Galois of degree p with $G = G_0 = C_p$. If π is the root of a type (ii) Amano polynomial, [1] proves that α can be chosen to be a primitive p-th root of unity, and $K^{\text{gal}}/\mathbf{Q}_p$ is totally ramified with $G = G_0 = C_p : C_{p-1}$.

Suppose now that π is a root of a type (iii) Amano polynomial, and let $d = [\mathbf{Q}_p(\alpha) : \mathbf{Q}_p]$. Let $g = \gcd(p-1, b)$ and let r be the multiplicative order of ab modulo p. Then [1] proves the maximal unramified subextension of $K^{\text{gal}}/\mathbf{Q}_p$ is given by $\mathbf{Q}_p(\beta)$ where $\beta^g = ab$ and $\alpha^{(p-1)/g} = \beta p^{b/g}$. Thus $|G_0/G_1| = [\mathbf{Q}_p(\alpha) : \mathbf{Q}_p(\beta)] = (p -$

$1)/g$. This proves the inertia subgroup $G_0 = C_p : C_{(p-1)/g}$. Since $\gcd(p, ab) = 1$, it follows that ab is a $(p-1)/r$ power of a generator of $\mathbf{F}_p^*$. This proves $|G/G_0| = [\mathbf{Q}_p(\beta) : \mathbf{Q}_p] = g/\gcd(g, (p-1)/r)$. Thus $d = |G/G_1| = |G/G_0||G_0/G_1| = (p-1)/\gcd(g, (p-1)/r)$, and the Galois group $G = C_p : C_d$.

If $p = 3$, we see that of the nine cubic extensions of $\mathbf{Q}_p$, only the six polynomials of type (ii) and (iii) give rise to dihedral extensions. These polynomials are x^3+3, x^3+12, x^3+21, x^3+3x+3, x^3+6x+3, and x^3+3x^2+3. Computing inertia groups for these six polynomials shows that all have inertia group equal to D_3 except the polynomial $x^3 + 3x^2 + 3$, which has cyclic inertia group.

Suppose now that $p > 3$. Dihedral extensions arise precisely when the Galois group of the normal closure is $C_p : C_2$; i.e., if and only if K is defined by a type (iii) Amano polynomial with $d = 2$. Thus, we are led to consider polynomials of the form $x^p + apx^b + p$. In order that $d = 2$, it is necessary and sufficient that $(p-1)/2 = \gcd(g, (p-1)/r)$, where $g = \gcd(p-1, b)$ and r is the multiplicative order of ab modulo p. There are three cases to consider: (1) $r = 2$ and $g = p - 1$, (2) $r = 2$ and $g = (p-1)/2$, and (3) $r = 1$ and $g = (p-1)/2$.

Case (1) is equivalent to $r = 2$ and $b = p - 1$. Since the only element of order 2 in $\mathbf{F}_p^*$ is congruent to -1 modulo p, we must have $a = 1$. This produces the pair $[a, b] = [1, p-1]$. Case (2) is equivalent to $r = 2$ and $b = (p-1)/2$, and therefore $a = 2$. This produces the pair $[a, b] = [2, (p-1)/2]$. Case (3) is equivalent to $r = 1$ and $b = (p-1)/2$. Since $b \equiv -1/2 \pmod{p}$, it must be the case that $a \equiv -2 \pmod{p}$. Taking $a = p - 2$ produces the pair $[a, b] = [p-2, (p-1)/2]$.

Together these three cases produce the polynomials listed in the statement of the theorem. Thus there are precisely three degree p extensions of $\mathbf{Q}_p$ whose normal closures have dihedral Galois group $D_p = C_p : C_2$. Since the inertia subgroups for these field are $C_p : C_{(p-1)/g}$, it follows that the field arising from Case (1) has cyclic inertia group, while the fields arising from Cases (2) and (3) have dihedral inertia groups. □

References

1. 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 MR0308086 (46 #7201)
2. Fernando Q. Gouvêa, *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction. MR 1488696 (98h:11155)

3. Marshall Hall, Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959. MR 0103215 (21 #1996)
4. Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)
5. Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 1357169 (96f:20001)
6. Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)
7. Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR 1333036 (96d:11072)

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: cawtrey@elon.edu

Department of Mathematics and Statistics, Elon University, Campus Box 4541, Elon, NC 27244
E-mail address: tedwards8@elon.edu