MASSES, DISCRIMINANTS, AND GALOIS GROUPS OF TAME QUARTIC AND QUINTIC EXTENSIONS OF LOCAL FIELDS

CHAD AWTREY

ABSTRACT. Let K be a finite extension of the p-adic numbers with $p \neq 2, 5$ and L/K a ramified extension. We count the number of nonisomorphic extensions where the Galois group of the splitting field of L is equal to one of the ten transitive subgroups of S_4 and S_5.

1. INTRODUCTION

The study of p-adic numbers $\mathbf{Q}_p$ and their extensions has been pursued for over a century since the publication of Hensel's venerable paper [Hen01]. Of particular interest to number theorists is the following classical result [Lan94, Proposition II.5.14].

Theorem 1.1. *Let K be a finite extension of $\mathbf{Q}_p$ and let n be any positive integer. There exist only finitely many extensions of K of degree n.*

This result motivates the obvious question: if there are only finitely many extensions, how many are there? In response, several authors have developed what are known as "mass" formulas; formulas for the number of extensions of a local field which count subfields of an algebraic closure. For example, Krasner [Kra66] gives a formula for the number of totally ramified extensions of a local field of specified degree. The main tool used is his well-known lemma. As another example, Serre [Ser78] computes the number of extensions in two different ways, one using Eisenstein polynomials, the other applying Weyl's integration formula to the multiplicative group of a division algebra.

More recently, several researchers have focused on counting the number of extensions of a local field with prescribed Galois group being of a certain form. For example, Repka [Rep88] uses the norm to prove that every quartic extension of a local field with odd residue characteristic has a quadratic subfield. An immediate consequence is that A_4 and S_4 cannot occur as the Galois group of the normal closure of such a field. It is therefore natural to ask for a formula that counts the number of nonisomorphic tamely ramified quartic extensions of local fields whose normal closures have Galois group either C_4, V_4, or D_4.

One approach is to use local class field theory [Iwa55]. Another approach is to combine knowledge of subfields with the structure of the Galois group. For example, suppose L is a quartic extension of $K/\mathbf{Q}_p$ with $p > 2$, and suppose $\mathrm{Gal}(L/K) = V_4$. By Galois theory, L must contain three quadratic subfields. Since $p > 2$, a consequence of Hensel's lemma is that there are only three quadratic extensions of K. Thus, the compositum of any two of these fields produces the unique V_4 extension of K. In the case that L/K is an octic Galois extension and

2000 *Mathematics Subject Classification.* Primary 11S15, 11S20.

$K = \mathbf{Q}_p$, Naito uses a similar approach to show there is a unique D_4 extension of $\mathbf{Q}_p$ if $p \equiv 3 \pmod 4$ and none if $p \equiv 1 \pmod 4$ [Nai95]. Other authors have studied tamely ramified Galois extensions of local fields when the Galois group is Q_8, S_3, A_4, and S_4 ([Jen89], [Fuj90], [WJ07]).

In this paper, we offer a third approach to this problem, and we generalize the setting to include non-Galois extensions. In particular, we compute the number of tamely ramified degree four extensions of local fields where the Galois group of the normal closure is either C_4, V_4, or D_4. Our approach is unique in that we obtain a defining polynomial for each extension and compute the Galois group of this polynomial. Our techniques for computing Galois groups are of interest since we use only one resolvent (the discriminant) along with mass and ramification considerations. Taking this approach further, we show the same techniques can be applied to totally and tamely ramified quintic extensions of local fields. In this case, we count the number of nonisomorphic extensions where the Galois group of the normal closure is a transitive subgroup of S_5. Since Galois groups of local fields are solvable, this leaves only the cases of C_5, D_5, and $F_5 = C_5 \rtimes C_4$ [Ser79, Corollary IV.2.5].

In section 2, we give a few important definitions and state our main theorems concerning totally and tamely ramified quartic and quintic extensions of local fields. In section 3, we formulate and prove several technical lemmas, describing how they work together to yield proofs of our main theorems. In the final section, we prove the theorems.

2. Statement of the Main Theorems

For the remainder of the paper, we fix a prime $p \neq 2, 5$, an algebraic closure $\overline{\mathbf{Q}}_p$ of the p-adic numbers, and a finite extension $K/\mathbf{Q}_p$. Let e be the ramification index of K and let f be its residue degree. Thus $ef = [K : \mathbf{Q}_p]$.

Definition 2.1. We say K is of **type** $\langle \mathbf{j}, \mathbf{n}, \mathbf{k}^+, \mathbf{d} \rangle$ if $p \equiv j \pmod n$ and $f \equiv k \pmod d$. We say K is of **type** $\langle \mathbf{j}, \mathbf{n}, \mathbf{k}^-, \mathbf{d} \rangle$ if $p \equiv j \pmod n$ and $f \not\equiv k \pmod d$.

For a finite extension L/K, let L^{gal} denote its splitting field and $m(L/K)$ its mass. That is,

$$m(L/K) = [L : K]/|\text{Aut}(L/K)|,$$

where $\text{Aut}(L/K)$ denotes the automorphism group.

Let $\mathcal{L}_K^n$ consist of representatives of the isomorphism classes of degree n extensions of K. When $p \nmid n = e$, Krasner's mass formula [Kra66] gives

$$\sum_{L \in \mathcal{L}_K^n} m(L/K) = n.$$

For totally and tamely ramified extensions of local fields, we compute their individual masses explicitly (Lemma 3.2), and use this information to determine Galois groups. The determination of Galois groups is the key ingredient in the proofs of our main results, Theorems 2.2 and 2.3.

Theorem 2.2. *Let $p > 2$ be a prime number and $K/\mathbf{Q}_p$ a finite extension.*

(1) *If K is of type $\langle -1, 4, 0^-, 2 \rangle$, there are two nonisomorphic totally ramified quartic extensions of K. In both cases, the Galois group of their splitting fields is D_4.*

TABLE 1. Invariant data for the possible Galois groups of tamely ramified quintic extensions of local fields.

$\mathbf{G}$	**Parity**	$\lvert\mathbf{C}_{\mathbf{S_5}}(\mathbf{G})\rvert$
C_5	$+$	5
D_5	$+$	1
F_5	$-$	1

(2) *Otherwise, there are four nonisomorphic totally ramified quartic extensions of K; each of which is cyclic.*
(3) *Let K'/K be the unramified quadratic extension. There are two nonisomorphic quartic extensions of L/K that contain K'/K such that L/K' is totally ramified. One extension is cyclic. The other extension has Galois group equal to V_4.*

Theorem 2.3. *Let $p \neq 2, 5$ be a prime number and $K/\mathbf{Q}_p$ a finite extension.*

(1) *There are five nonisomorphic totally ramified quintic extensions of K with cyclic Galois group if one of the following conditions holds:*
   (a) $p \equiv 1 \pmod 5$
   (b) *K is of type $\langle -1, 5, 0^+, 2\rangle$*
   (c) *K is of type $\langle \pm 2, 5, 0^+, 4\rangle$*
(2) *There is a unique totally ramified quintic extension of K whose normal closure has Galois group D_5 if one of the following conditions holds:*
   (a) *K is of type $\langle -1, 5, 0^-, 2\rangle$*
   (b) *K is of type $\langle \pm 2, 5, 0^-, 4\rangle$ and $\mathbf{Q}_p(\sqrt{5}) \subset K$.*
(3) *There is a unique totally ramified quintic extension of K whose normal closure has Galois group F_5 if K is of type $\langle \pm 2, 5, 0^-, 4\rangle$ and $\mathbf{Q}_p(\sqrt{5}) \not\subset K$.*

3. Some Lemmas

In this section, we formulate several technical lemmas and describe how they fit together to yield our main theorems. First, we focus on the invariants that distinguish between the possible Galois groups for quartic and quintic extensions of local fields. One invariant is the parity of the group. To illustrate this invariant, suppose L/K is a finite extension with $n = [L : K]$, and let G be the Galois group of L^{gal}/K. The parity of G is $+$ if $G \subset A_n$ and $-$ otherwise. It corresponds to whether or not the discriminant of L/K is a square in K.

Another invariant we use is the order of the centralizer of G in S_n. This quantity is useful for computing Galois groups since it corresponds to the size of the automorphism group of L/K. It turns out that the parity and centralizer order are enough to distinguish between C_5, D_5, and F_5 (Table 1).

For quartic extensions we use one more invariant, which we refer to as the *quadratic subfield discriminant* product (*qsd*). Suppose the extension L/K has a unique quadratic subfield K', and let G be the Galois group of L^{gal}/K, as before. We write $qsd(G) = +$ if $\mathrm{disc}(L/K) \cdot \mathrm{disc}(K'/K)$ is a square in K; otherwise we write $qsd(G) = -$. The *qsd* product is useful for distinguishing between C_4 and D_4, as the following lemma shows.

TABLE 2. Invariant data for the possible Galois groups of tamely ramified quartic extensions of local fields.

G	**Parity**	$\mathbf{\lvert C_{S_4}(G)\rvert}$	**qsd(G)**
C_4	$-$	4	$+$
V_4	$+$	4	
D_4	$-$	2	$-$

Lemma 3.1. *Let L/K be a quartic extension and suppose $G = Gal(L^{gal}/K)$ is either C_4 or D_4. Then L/K has a unique quadratic subfield, up to isomorphism. Moreover, $qsd(G) = +$ if and only if $G = C_4$.*

Proof. If $G = C_4$, then L/K has a unique quadratic subfield by the fundamental theorem of Galois theory. Suppose $G = D_4$ and let $E \subset G$ be the subgroup which fixes L. The nonisomorphic subfields of L/K correspond to conjugacy classes of intermediate subgroups F such that $E \leq F \leq G$. Direct computation shows the group D_4 has one such intermediate subgroup of index two, proving that L/K has a unique quadratic subfield up to isomorphism. A well-known result on quartic Galois groups shows that $qsd(C_4) = +$ while $qsd(D_4) = -$ [KW89]. □

For each of the possible Galois groups of tamely ramified quartic extensions of local fields, Table 2 shows the parity and the order of the centralizer in S_4. For C_4 and D_4, the table also shows the *qsd* product.

Our remaining lemmas describe how to compute the mass and centralizer order invariants on the field-theoretic side. The first is a restatement of [PR01, Theorem 7.2] in our context.

Lemma 3.2. *Let $K/\mathbf{Q}_p$ be a finite extension and let n be an integer with $p \nmid n$. Let $g = \gcd(p^f - 1, n)$ and let $m = n/g$.*

(a) *There are g nonisomorphic totally ramified extensions of K of degree n; each with mass m.*
(b) *Let ζ be a primitive $(p^f - 1)$-st root of unity and let π be a uniformizer for K. Each totally and tamely ramified extension of K of degree n is isomorphic to an extension that is generated by a root of the polynomial $x^n + \zeta^r\pi$, for some $0 \leq r < g$.*

Lemma 3.3. *Let L/K be a totally ramified extension of degree n with $p \nmid n$ and let $g = \gcd(p^f - 1, n)$. Let $G = Gal(L^{gal}/K)$. Then*

$$g = |C_{S_n}(G)|.$$

Proof. From Galois theory, we know the automorphism group of L/K is isomorphic to the centralizer of G in S_n. Thus the size of $\mathrm{Aut}(L/K)$ is equal to the order of $C_{S_n}(G)$. Using this fact and the definition of the mass of L/K, we have

$$[L : K] = m(L/K) \cdot |\mathrm{Aut}(L/K)| = m(L/K) \cdot |C_{S_n}(G)|.$$

By Lemma 3.2, we also have

$$[L : K] = m(L/K) \cdot g.$$

These two equalities combine to prove the lemma. □

4. Proof of Theorems

4.1. **Proof of Theorem 2.2.**

Proof. We know the Galois group $G = \mathrm{Gal}(L^{\mathrm{gal}}/K)$ must be either C_4, V_4, or D_4. First, we consider the case when L/K is totally ramified. Let $g = \gcd(p^f - 1, 4)$. Since p is odd, g is 2 or 4. Furthermore, $g = 2$ if and only if $p \equiv -1 \pmod 4$ and f is odd if and only if K is of type $\langle -1, 4, 0^-, 2\rangle$. Otherwise, we must have $g = 4$. Since $g = |C_{S_4}(G)|$, we see that $G = D_4$ if and only if $g = 2$ if and only if K is of type $\langle -1, 4, 0^-, 2\rangle$; proving part (1). If $g = 4$, then G is either C_4 or V_4. Since $V_4 \subset A_4$ and C_4 is not, we see that G is determined by the discriminant of L/K. By Lemma 3.2, the four totally ramified quartic extensions of K are generated by the polynomials $x^4 + \zeta^r\pi$ where ζ is a primitive $(p^f - 1)$-st root of unity, $0 \le r < 4$, and π is a uniformizer for K. Now, since each extension is totally ramified, the field discriminant and the polynomial discriminant are equal. Thus

$$\mathrm{disc}(L/K) = \mathrm{disc}(x^4 + \zeta^r\pi) = 256\zeta^{3r}\pi^3,$$

which is clearly not a square in K. Thus $G = C_4$ for all four of these extensions; proving part (2).

Suppose now that L/K contains the unramified quadratic subfield K'. Since $p > 2$, L/K' is a totally and tamely ramified quadratic extension. By Lemma 3.2, there are two such extensions, generated by $x^2 - \pi$ and $x^2 - \alpha\pi$, where α is a primitive $(p^{2f} - 1)$-st root of unity and π is a uniformizer for K. We note that K'/K is generated by a root of $x^2 - N_{K'/K}(\alpha)$ where $N_{K'/K}$ represents the norm from K' down to K. Let $L_1 = K'(\sqrt{\pi})/K$ and let $L_2 = K'(\sqrt{\alpha\pi})/K$. Working up to multiplication by a square, the formula for the discriminant in towers gives

$$\mathrm{disc}(L_1/K) = N_{K'/K}(\mathrm{disc}(L/K')).$$

Since L/K' is generated by the Eisenstein polynomial $x^2 - \pi$, its field discriminant and polynomial discriminant are both equal to 4π. Since K'/K is quadratic and unramified, we have

$$\mathrm{disc}(L_1/K) = N_{K'/K}(\mathrm{disc}(x^2 - \pi)) = N_{K'/K}(4\pi) = 4^2\pi^2,$$

which is a square in K. This proves the Galois group of L_1/K is V_4.

Similarly, we have

$$\mathrm{disc}(L_2/K) = N_{K'/K}(\mathrm{disc}(x^2 - \alpha\pi)) = N_{K'/K}(4\alpha\pi) = 4^2\pi^2 N_{K'/K}(\alpha),$$

which is not a square in K since $N_{K'/K}(\alpha)$ is not. This implies that the Galois group of L^{gal}/K is either C_4 or D_4. By Lemma 3.1, we see that C_4 and D_4 are distinguished by their *qsd* product. Since each of these extensions has a unique quadratic subfield up to isomorphism, we know this subfield must be the unramified subfield, whose discriminant is $4N_{K'/K}(\alpha)$. Therefore, we have

$$\mathrm{disc}(L_2/K) \cdot \mathrm{disc}(K'/K) = 4^2\pi^2 N_{K'/K}(\alpha) \cdot 4N_{K'/K}(\alpha) = 64\pi^2 N_{K'/K}(\alpha)^2,$$

which is a square in K. This proves the Galois group of L_2/K is C_4. □

4.2. **Proof of Theorem 2.3.**

Proof. We know G must be either C_5, D_5, or $F_5 = C_5 \rtimes C_4$. Let $g = \gcd(p^f - 1, 5)$. Thus g is either 1 or 5. Furthermore, $g = 5$ if and only if $p^f \equiv 1 \pmod 5$, which occurs if either (a) $p \equiv 1 \pmod 5$, (b) K is of type $\langle -1, 5, 0^+, 2\rangle$, or (c) K is of type $\langle \pm 2, 5, 0^+, 4\rangle$. Since $g = |C_{S_5}(G)|$, we see that $G = C_5$ if and only if one the

conditions (a), (b), or (c) occurs; proving part (1). If $g = 1$, then G is either D_5 or F_5, depending on whether $\mathrm{disc}(L/K)$ is a square or not, respectively.

Suppose now $g = 1$ and that none of (a), (b), and (c) hold. By Lemma 3.2, the unique totally ramified quintic extension L/K is generated by a root of the polynomial $x^5 - \pi$ where π is a uniformizer for K. Since L/K is totally ramified, we have

$$\mathrm{disc}(L/K) = \mathrm{disc}(x^5 - \pi) = 5^5\pi^4,$$

which is a square in K if and only if 5 is. Certainly 5 is a square in K if $\mathbf{Q}_p(\sqrt{5}) \subset K$.

Suppose $\mathbf{Q}_p(\sqrt{5}) \not\subset K$, and consider the polynomial $f(x) = x^2 - 5$. Since $p \neq 2, 5$, Hensel's lemma and quadratic reciprocity show that f has a root in K if and only if $p \equiv \pm 1 \pmod 5$. Since we are supposing that (a) and (b) do not hold, it follows that 5 is a square in K if and only if $p \equiv -1 \pmod 5$ and f is odd or $\mathbf{Q}_p(\sqrt{5}) \subset K$. This proves parts (2) and (3). □

5. Acknowledgements

The author wishes to thank the anonymous reviewers for their helpful comments. This research was supported in part by an internal grant from Elon Unversity.

References

[Fuj90] Genjiro Fujisaki, *A remark on quaternion extensions of the rational p-adic field*, Proc. Japan Acad. Ser. A Math. Sci. **66** (1990), no. 8, 257–259. MR 1077609 (91m:11104)

[Hen01] Kurt Hensel, *Ueber die Entwickelung der algebraischen Zahlen in Potenzreihen*, Math. Ann. **55** (1901), no. 2, 301–336. MR MR1511153

[Iwa55] Kenkichi Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. **80** (1955), 448–469. MR 0075239 (17,714g)

[Jen89] C. U. Jensen, *On the representations of a group as a Galois group over an arbitrary field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 441–458. MR 1024582 (90k:12006)

[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)

[KW89] Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR 992075 (90i:12006)

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)

[Nai95] Hirotada Naito, *Dihedral extensions of degree* 8 *over the rational p-adic fields*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), no. 1, 17–18. MR 1326788 (96a:11133)

[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)

[Rep88] Joe Repka, *Quadratic subfields of quartic extensions of local fields*, Internat. J. Math. Math. Sci. **11** (1988), no. 1, 1–4. MR 918210 (89b:11096)

[Ser78] Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 22, A1031–A1036. MR 500361 (80a:12018)

[Ser79] ———, *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)

[WJ07] Da-Sheng Wei and Chun-Gang Ji, *On the number of certain Galois extensions of local fields*, Proc. Amer. Math. Soc. **135** (2007), no. 10, 3041–3047 (electronic). MR 2322733 (2008f:11136)

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