International Journal of Pure and Applied Mathematics
Volume 70 No. 6 2011, 855-863

ON GALOIS GROUPS OF TOTALLY AND TAMELY RAMIFIED SEXTIC EXTENSIONS OF LOCAL FIELDS

Chad Awtrey
Department of Mathematics and Statistics
Elon University
Campus Box 2320, Elon, NC 27244, USA

Abstract: Let K be a finite extension of the p-adic numbers with $p > 3$ and L/K a totally ramified sextic extension. For each of the sixteen transitive subgroups G of S_6, we count the number of nonisomorphic extensions where the Galois group of the splitting field of L is equal to G. The technique is new and is based on the mass formulas of Krasner and Serre.

AMS Subject Classification: 11S15, 11S20
Key Words: local fields, Galois groups

1. Introduction

Since the number of extensions of a local field of a given degree inside a fixed algebraic closure is finite [11, p.54], it is natural to ask for a formula that counts the number of extensions. In his paper [10], Krasner gives a formula for the number of totally ramified extensions of a local field – his well-known lemma is the main tool. Serre computes the number of extensions in two different ways; one using Eisenstein polynomials and the other applying Weyl's integration formula to the multiplicative group of a division algebra. Pauli and Roblot [13] use Krasner's results to develop an algorithm for computing all extensions of local fields. Their algorithm provides a generating set of polynomials that is guaranteed to cover all possible extensions. Generalizing Serre's results, Bhargava [1] gives a formula for the number of etale algebra extensions of a local field.

Received: March 10, 2011

It is also natural to ask for a formula that counts the number of extensions with a given Galois group. One approach is to use class field theory by studying the absolute Galois group. This approach is applied to p-extensions in [16] and tamely ramified extensions in [8]. Relatedly, Wei and Ji study the number of Galois extensions of local fields when the Galois group is equal to either S_3, A_4, or S_4 [18].

Another approach, more classical in nature, is to study Galois groups of finite extensions through their arithmetic invariants. This idea has been used to study Galois extensions of local fields when the Galois group is Q_8 and D_4 ([9], [4], [14]). In particular, Naito uses this approach to show there is a unique totally and tamely ramified D_4 extension of $\mathbf{Q}_p$ if $p \equiv 3 \pmod 4$ and none if $p \equiv 1 \pmod 4$ [12].

In this paper, we follow the classical approach and study totally and tamely ramified sextic extensions of local fields by Galois group. For each of the sixteen transitive subgroups G of S_6, we count the number of nonisomorphic extensions where the Galois group of the normal closure is equal to G. In particular, we show that unless G is cyclic of order six or dihedral of order twelve, the number of extensions is zero. For the remaining two cases, we show the number depends only on the prime p and the residue degree of the base field.

Our approach combines Krasner's mass formula with the results of Pauli and Roblot to obtain the number of nonisomorphic extensions. We then determine the Galois group of each of these extensions. Our techniques for computing Galois groups are of interest, since they do not rely on computing and factoring resolvent polynomials (which is the traditional approach [17], [7], [3]). Instead, we use a combination of Krasner's mass formula, ramification phenomena, and the Galois theory of totally and tamely ramified cubic fields.

In Section 2, we give a few important definitions and state our main theorem concerning totally and tamely ramified sextic extensions of local fields. In Section 3, we formulate several technical lemmas and describe how they work together to yield a proof of our main theorem. In the final sections, we prove the lemmas and the main theorem.

2. Statement of the Main Theorem

For the remainder of the paper, we fix a prime $p > 3$, 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 1. We say K is of **type** $\langle \mathbf{1}, \mathbf{n} \rangle$ if either $p \equiv 1 \pmod n$ or f is

even. We say K is of **type** $\langle -\mathbf{1}, \mathbf{n}\rangle$ if both $p \equiv -1 \pmod{n}$ and f is odd.

Since we are concerned with sextic extensions of K and $p > 3$, observe that K is either of type $\langle 1, 6\rangle$ or of type $\langle -1, 6\rangle$.

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

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

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

Let $\mathcal{L}_K^n$ consist of representatives of the isomorphism classes of degree n extensions of K. Observe that $\mathcal{L}_K^n$ is necessarily finite. For totally and tamely ramified extensions, i.e. $p \nmid n = e$, Krasner's mass formula [10] gives

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

For each $L \in \mathcal{L}_K^n$, we compute its mass explicitly (Lemma 4), and use this information to determine Galois groups. The determination of Galois groups is the key ingredient in the proof of our main result, Theorem 2.

Theorem 2. *Let $p > 3$ be a prime number and $K/\mathbf{Q}_p$ a finite extension.*

1. *If K is of type $\langle 1, 6\rangle$, there are six nonisomorphic totally ramified sextic extensions of K; each of which is cyclic.*
2. *If K is of type $\langle -1, 6\rangle$, there are two nonisomorphic totally ramified extensions of K. For both of these extensions, the Galois group of their splitting fields is D_6.*

3. Some Lemmas

In this section, we formulate several lemmas that will aid in the proof of Theorem 2. The first lemma shows how the theory of ramification groups gives structural information about the Galois group of a local field.

Lemma 3. *Let L/K be a Galois extension with Galois group G. Let $\mathfrak{p}$ denote the unique maximal ideal of the integers in L. For $i \geq -1$, let G_i be the i-th ramification group. Let U_0 be the units in L and for $i \geq 1$, let $U_i = 1 + \mathfrak{p}^i$.*

(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 L. 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.*

Specializing to the case when $[L : K] = 6$ and $G = \mathrm{Gal}(L^{\mathrm{gal}}/K)$, we see that G is a solvable transitive subgroup of S_6; of which there are twelve [2]. Furthermore, G contains a solvable normal subgroup G_0 such that G/G_0 is cyclic of order dividing six and such that G_0 is cyclic of order dividing $p^{[G:G_0]}-1$. Direct computation (using [5] for example) on the twelve candidates shows that only four are possible Galois groups of tamely ramified sextic extensions. These are

$$C_6 = 6T1 \quad S_3 = 6T2 \quad D_6 = 6T3 \quad S_3C_3 = 6T5.$$

We use two invariants to distinguish between these four groups. One is the order of their centralizer in S_6. This quantity is useful for computing Galois groups since it corresponds to the size of the automorphism group of L/K. The other invariant corresponds to the list of the Galois groups of the Galois closures of the proper nontrivial subfields of L, where the subfields are considered up to isomorphism. We call this invariant the *subfield Galois group* content (*sgg*).

The *sgg* content of an extension is an invariant of its Galois group. Indeed, suppose the normal closure of L/K has Galois group G and let $E = G \cap S_{n-1}$ where $n = [L : K]$. Then E is the subgroup fixing $K(\alpha)/K$ where α is a primitive element for L/K. By the fundamental theorem of Galois theory, the nonisomorphic subfields of $K(\alpha)/K$ correspond to the intermediate subgroups F, up to conjugation, such that $E \leq F \leq G$. Specifically, if K' is a subfield of $K(\alpha)/K$ and F is its corresponding intermediate group, then the Galois group of the normal closure of K' is equal to the permutation representation of G acting on the cosets of F in G. Consequently, it makes sense to speak of the *sgg* content of a transitive subgroup as well.

For each of the four possible Galois groups of tamely ramified sextic extensions of local fields, Table 3 shows the *sgg* content, the order of the centralizer in S_6, and the transitive number. Observe that the centralizer order distinguishes all groups except C_6 vs. S_3. Knowledege of the Galois group of the cubic subfield distinguishes between these two groups.

Our remaining three lemmas describe how to compute these two invariants on the field-theoretic side.

$\mathbf{G}$	$\mathbf{T}$	$\lvert\mathbf{C}_{\mathbf{S_6}}(\mathbf{G})\rvert$	$\mathbf{sgg}(\mathbf{G})$
C_6	6T1	6	2T1, 3T1
S_3	6T2	6	2T1, 3T2
D_6	6T3	2	2T1, 3T2
S_3C_3	6T5	3	2T1

Table 1: Invariant data for the four possible Galois groups of tamely ramified sextic extensions of local fields

Lemma 4. *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) If L/K is a totally ramified extension of degree n and $d \mid n$, then L has a totally ramified subfield F such that $[F : K] = d$.

Lemma 5. *Let L/K be a totally ramified extension of degree n with $p \nmid n$ and let $g = \gcd(p^f - 1, n)$ (as in Lemma 4). Let $G = Gal(L^{\mathrm{gal}}/K)$. Then*

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

Part (b) of Lemma 4 shows that totally ramified sextic extensions have a cubic subfield. Our final lemma discusses how to compute the Galois group of the normal closure of this subfield.

Lemma 6. *Let $p > 3$ and $K/\mathbf{Q}_p$ be a finite extension.*

1. *If K is of type $\langle 1, 3\rangle$, there are three nonisomorphic totally ramified cubic extensions of K; each of which is cyclic.*

2. *If K is of type $\langle -1, 3\rangle$, there is a unique totally ramified cubic extension of K. The Galois group of its splitting field is S_3.*

4. Proof of Theorem 2

Let L/K be a totally ramified sextic extension and let $G = \mathrm{Gal}(L^{\mathrm{gal}}/K)$. By Lemma 3, G must be either C_6, S_3, D_6, or S_3C_3. By Lemma 4, the number of nonisomorphic totally ramified sextic extensions of K is equal to $g = \gcd(p^f -$

$1, 6\rangle$. Since $p > 3$, we must have $p \equiv \pm 1 \pmod 6$. This implies that $g = 2$ or $g = 6$. Furthermore, we have $g = 6$ if and only if f is even or $p \equiv 1 \pmod 6$ if and only if K is of type $\langle 1, 6\rangle$. Similarly, $g = 2$ if and only if K is of type $\langle -1, 6\rangle$. By Lemma 5, we know that the centralizer order of G is equal to g. Thus S_3C_3 cannot occur as the Galois group. Moreover, we know the Galois group is D_6 if and only if $g = 2$. This proves part (2) of the theorem. If $g = 6$, we must distinguish between the two possibilities C_6 and S_3. By Table 3, these two groups are distinguished by their sgg content.

Suppose $g = 6$. By part (b) of Lemma 4, we see that L has a cubic subfield K'. Since $g = 6$, this implies that either f is even or $p \equiv 1 \pmod 6$. Reducing p modulo 3, we see that K is of type $\langle 1, 3\rangle$. By Lemma 6, the Galois group of K' is cyclic of order 3. Thus, $sgg(G)$ must contain $C_3 = 3T1$. According to Table 3, this proves $G = C_6$. □

5. Proof of the Lemmas

Proof of Lemma 3. We note that U_0/U_1 is isomorphic to the multiplicative group of the residue field of L. For $i \geq 1$, U_i/U_{i+1} is isomorphic to the additive group of the residue field.

Part (a) follows from Proposition 4.2.7 in [15]. Part (b) follows from part (a). Since every subgroup of the residue field is a vector space over $\mathbf{Z}/p$, 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 [6, Theorem 15.2.2], 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. □

Proof of Lemma 4. Part (a) follows from [13, Theorem 7.2]. For part (b), let ζ be a primitive $(p^f - 1)$-st root of unity, $g = \gcd(p^f - 1, n)$, and let π be a uniformizer for K. Since $p \nmid n$, L is a totally and tamely ramified extension of K. Thus L can be chosen so that it is generated by a root of the polynomial $x^n + \zeta^r\pi$ for some $0 \leq r < g$ ([13, Theorem 7.2]). Let d be a divisor of n. Thus L has a subfield K' of degree d that is generated by a root of $x^d + \zeta^r\pi$; proving part (b). □

$\mathbf{G}$	$\lvert\mathbf{C}_{\mathbf{S_3}}(\mathbf{G})\rvert$
C_3	3
S_3	1

Table 2: Distinguishing transitive subgroups of S_3 by centralizer order

Proof of Lemma 5. As mentioned previously, the size of the automorphism group of L/K is equal to the order of the centralizer in S_n of the Galois group of the normal closure of L/K,

$$|\mathrm{Aut}(L/K)| = |C_{S_n}(G)|$$

By definition,

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

By Lemma 4, we also have

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

Thus we have shown $g = |\mathrm{Aut}(L/K)| = |C_{S_n}(G)|$, proving the result. □

Proof of Lemma 6. Let L/K be a totally ramified cubic extension and let $G = \mathrm{Gal}(L^{\mathrm{gal}}/K)$. For cubic extensions, the possible Galois groups are the transitive subgroups of S_3; which are $C_3 = A_3$ and S_3. It turns out that these two groups are distinguished by the orders of their centralizers (Table 5).

By Lemma 4, the number of nonisomorphic totally ramified cubic extensions of K is equal to $g = \gcd(p^f - 1, 3)$. Thus we have $g = 3$ if and only if f is even or $p \equiv 1 \pmod 3$ if and only if K is of type $\langle 1, 3\rangle$. Similarly, $g = 1$ if and only if K is of type $\langle -1, 3\rangle$. By Lemma 5, we know that the centralizer order of G is equal to g. Using Table 5, we see that $G = C_3$ if and only if $g = 3$ if and only if K is of type $\langle 1, 3\rangle$. Likewise, $G = S_3$ if and only if $g = 1$ if and only if K is of type $\langle -1, 3\rangle$. □

References

[1] Manjul Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not. IMRN*, No. 17 (2007).

[2] Gregory Butler, John McKay, The transitive groups of degree up to eleven, *Comm. Algebra*, **11**, No. 8 (1983).

[3] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Volume 138, Springer-Verlag, Berlin (1993).

[4] Genjiro Fujisaki, A remark on quaternion extensions of the rational p-adic field, *Proc. Japan Acad. Ser. A Math. Sci.*, **66**, No. 8 (1990), 257-259.

[5] The GAP Group, *GAP - Groups, Algorithms, and Programming*, Version 4.4.12 (2008).

[6] Marshall Hall, Jr., *The Theory of Groups*, The Macmillan Co., New York, N.Y. (1959).

[7] Alexander Hulpke, Techniques for the computation of Galois groups, *Algorithmic Algebra and Number Theory*, Heidelberg, 1997, Springer, Berlin (1999), 65-77.

[8] Kenkichi Iwasawa, On Galois groups of local fields, *Trans. Amer. Math. Soc.*, **80** (1955), 448-469.

[9] C.U. Jensen, On the representations of a group as a Galois group over an arbitrary field, In: *Théorie des Nombres*, Quebec, PQ, 1987, de Gruyter, Berlin (1989), 441-458.

[10] 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), 143-169.

[11] Serge Lang, *Algebraic Number Theory*, Second Edition, Graduate Texts in Mathematics, Volume 110, Springer-Verlag, New York (1994).

[12] Hirotada Naito, Dihedral extensions of degree 8 over the rational p-adic fields, *Proc. Japan Acad. Ser. A Math. Sci.*, **71**, No. 1 (1995), 17-18.

[13] Sebastian Pauli, Xavier-François Roblot, On the computation of all extensions of a p-adic field of a given degree, *Math. Comp.*, **70**, No. 236 (2001), 1641-1659, Electronic.

[14] Joe Repka, Quadratic subfields of quartic extensions of local fields, *Internat. J. Math. Math. Sci.*, **11**, No. 1 (1988), 1-4.

[15] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics, Volume 67, Springer-Verlag, New York (1979), Translated from the French by Marvin Jay Greenberg.

[16] I. Shafarevitch, On p-extensions, *Rec. Math. (Mat. Sbornik)*, **20**, No. 62 (1947), 351-363.

[17] Richard P. Stauduhar, The determination of Galois groups, *Math. Comp.*, **27** (1973), 981-996.

[18] Da-Sheng Wei, Chun-Gang Ji, On the number of certain Galois extensions of local fields, *Proc. Amer. Math. Soc.*, **135**, No. 10 (2007), 3041-3047, Electronic.

864