PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 10, October 2007, Pages 3041–3047
S 0002-9939(07)08905-8
Article electronically published on May 10, 2007

ON THE NUMBER OF CERTAIN GALOIS EXTENSIONS OF LOCAL FIELDS

DA-SHENG WEI AND CHUN-GANG JI

(Communicated by Ken Ono)

Abstract. In this paper, we will calculate the number of Galois extensions of local fields with Galois group A_n or S_n.

1. Introduction

Let p be a prime, F a finite extension of p-adic field $\mathbb{Q}_p$ with $[F : \mathbb{Q}_p] = m$. Let k be its residue field with $[k : \mathbb{Z}/p\mathbb{Z}] = f$. It's easy to see that $f|m$. Let π be a uniformizer of F and e the absolute ramification index of F/Q_p. Then $m = ef$. In this paper let μ_l denote the set of l-th roots of unity. All notations are standard if not explained.

Since the number of the extensions of local fields with a given degree inside the fixed algebraic closure is finite, see [2], one can ask for a formula that gives the number of extensions of a given degree. Krasner [1] gave such a formula, and Serre [6] also computed the number of extensions using a different method. Pauli and Roblot [3] gave the third proof for that formula. Similarly one can also ask for a formula that gives the number of Galois extensions of a given degree. In particular, it is possible to ask for a formula that gives the number of the Galois extensions with the prescribed finite Galois group G. We denote this number by $\nu(F, G)$. If G is a p-group with $\mu_p \nsubseteq F$, Šafarevič [4] gave an explicit formula for the number of the G-extensions over F:

$$\nu(F, G) = \frac{1}{|Aut(G)|}(\frac{|G|}{p^d})^{m+1} \prod_{i=1}^{d-1}(p^{m+1} - p^i),$$

where d is the minimal number of generators of G. If G is a p-group, and $\mu_p \subset F$, Yamagishi [7] obtained a formula for $\nu(F, G)$.

In this paper, we will calculate the number of S_n-extensions and A_n-extensions over F, where S_n is the n-th symmetric group and A_n is the n-th alternating group.

The cases for $n \geq 5$ that are quickly dismissed as S_n and A_n are not solvable in these cases, and the Galois groups of extensions of local fields are always solvable. So we only need to handle the remaining cases, $n \leq 4$.

Received by the editors June 13, 2006.
2000 *Mathematics Subject Classification.* Primary 11S15, 11S20.
Key words and phrases. Local fields, Galois closure, ramified extensions.
This work was partially supported by grants #10171046 and #10201013 from NNSF of China and Jiangsu planned projects for postdoctoral research funds.

Theorem 1.1. *Let F be a finite extension over $\mathbb{Q}_p$ with $[F:\mathbb{Q}_p]=m$, $\nu(F,G)$ the number of the Galois extensions K/F with $Gal(K/F)=G$.*

(1) *Suppose the prime $p\neq 3$; then*

$$\nu(F,S_3)=\begin{cases}0 & \text{if } \mu_3\subset F,\\ 3 & \text{if } \mu_3\not\subset F.\end{cases}$$

(2) *Suppose $p=3$; then*

$$\nu(F,S_3)=\begin{cases}3^{m+1}-3 & \text{if } \mu_3\subset F,\\ 3^m+\frac{3^{m+1}}{2}-\frac{3}{2} & \text{if } \mu_3\not\subset F.\end{cases}$$

Theorem 1.2. *Let F be a finite extension over $\mathbb{Q}_p$ with $[F:\mathbb{Q}_p]=m$, $\nu(F,G)$ the number of the Galois extensions K/F with $Gal(K/F)=G$.*

(1) *Suppose the prime $p\geqslant 3$; then*

$$\nu(F,S_4)=\nu(F,A_4)=0.$$

(2) *Suppose $p=2$; then*

$$\nu(F,A_4)=\begin{cases}4(2^{2m}-1)/3 & \text{if } \mu_3\subset F,\\ (2^{2m}-1)/3 & \text{if } \mu_3\not\subset F;\end{cases}$$

$$\nu(F,S_4)=\begin{cases}0 & \text{if } \mu_3\subset F,\\ 2^{2m+1}-1 & \text{if } \mu_4\not\subseteq F \text{ and } m \text{ is even and } f=1,\\ 2^{2m}-1 & \text{otherwise.}\end{cases}$$

2. Some lemmas

The number of S_2-extensions and A_3-extensions of local fields is specified by well-known results of local class field theory. So we only need to calculate the number of Galois extensions over F with Galois group S_3, S_4 and A_4. The following lemma plays an important role in our calculation.

Lemma 1. *Let K be a Galois extension over F with the Galois group G. For any subgroup A of G, let F_A be the field fixed by A. Then the Galois closure $cl(F_A)$ of F_A is a subfield of K and $Gal(K/cl(F_A))=\bigcap_{g\in G} gAg^{-1}$.*

We can get some Galois extensions from some non-Galois extensions by taking their Galois closure. For example, if G=S_3, D_8, A_4 and S_4, we can choose A to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and S_3, which is the non-normal subgroup of G respectively, and where D_8 is the 2-sylow subgroup of S_4. By the above lemma, the Galois extensions of F with Galois group S_3 can be gotten by the Galois closure of extensions of degree 3 of F, and the Galois extensions of F with Galois group D_8, A_4 and S_4 can be gotten by the Galois closure of extensions of degree 4 of F.

Let $M(n)$ denote the set of all extensions of degree n of F. Let $Ab(n)$ denote the set of abelian extensions of degree n of F. Also, let $M(G)$ denote the set of Galois extensions of F with the Galois group G. Let K be the Galois closure of an extension of degree n of F . The Galois group Gal(K/F) is a subgroup of S_n. Obviously the order of Gal(K/F) must be divided by n. So there are the following two maps:

$$f:\quad M(3)\to Ab(3)\cup M(S_3)$$

and

$$g: \quad M(4) \to Ab(4) \cup M(D_8) \cup M(A_4) \cup M(S_4)$$

by

$$L \to cl(L).$$

The two maps are surjective. Any inverse image L of an element K in $M(G)$ is a subfield of K, and L is not a Galois extension of F if G is not an abelian group. In these cases, the Galois group $\mathrm{Gal}(K/L)$ is not a normal subgroup of G. For $G = S_3, D_8, A_4$ and S_4, we consider respectively the number of non-normal subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z}$,$\mathbb{Z}/2\mathbb{Z}$,$\mathbb{Z}/3\mathbb{Z}$ and S_3. The subgroups are non-normal except there is an order-2 normal subgroup in D_8. So the number of inverse images of any element in $M(S_3), M(D_8), M(A_4)$ and $M(S_4)$ are $3, 4, 4, 4$ respectively. Let $|S|$ denote cardinality of a finite set S. Let $\nu(F, G)$ denote the number of $M(G)$. So there is the following result.

Lemma 2.

$$|M(3)| = |Ab(3)| + 3\nu(F, S_3),$$
$$|M(4)| = |Ab(4)| + 4\nu(F, D_8) + 4\nu(F, A_4) + 4\nu(F, S_4).$$

3. The proof of Theorem 1.1

In the following, we denote $m = [F : \mathbb{Q}_p]$, and e is the absolute ramification index of F and $q = p^f$ is the number of elements of the residue field of F.

Proof. (1) For $p \neq 3$,

$$M(3) = \{K|\ [K : F] = 3, K \text{ is a tamely ramified extension of } F\}.$$

(i) If 3rd roots of unity are contained in F, then $M(3) = Ab(3)$. By Lemma 2

$$\nu(F, S_3) = 0.$$

(ii) If 3rd roots of unity are not contained in F, then $|M(3)| = 10$, $|Ab(3)| = 1$. By Lemma 2

$$\nu(F, S_3) = 3.$$

(2) For $p = 3$, by Krasner's theorem [3],

$$|M(3)| = 3q^e + 6(q-1)(\sum_{a=0}^{e-1} q^a) + 1 = 9q^e - 5.$$

Suppose $\mu_3 \not\subset F$; then

$$|Ab(3)| = \frac{1}{2}(\frac{3}{3})^{m+1}(3^{m+1} - 1) = \frac{3^{m+1} - 1}{2} = \frac{3q^e - 1}{2}.$$

Suppose $\mu_3 \subset F$; then

$$|Ab(3)| = 4.$$

By Lemma 2

$$\nu(F, S_3) = \begin{cases} \frac{5q^e - 3}{2} & \text{if } \mu_3 \not\subset F, \\ 3q^e - 3 & \text{if } \mu_3 \subset F. \end{cases}$$

□

4. The proof of Theorem 1.2

First we give some propositions.

Proposition 4.1. *Let the prime $p \geqslant 3$. Then*

$$\nu(F, S_4) = \nu(F, A_4) = 0.$$

Proof. Suppose K is a Galois extension over F with Galois group S_4. There must exist intermediate fields F^{tr} and F^{ur} such that $\mathrm{Gal}(K/F^{tr})$ is a p-group, and $\mathrm{Gal}(F^{tr}/F^{ur})$ and $\mathrm{Gal}(F^{ur}/F)$ are cyclic groups. By Galois theory, there is a p-group S' which is a normal subgroup of S_4. Since $p \geqslant 3$, S' must be (1). Since S_4 does not have a cyclic normal subgroup S such that S_4/S is also cyclic, this is a contradiction.

Similarly we get $\nu(F, A_4) = 0$. □

Proposition 4.2. *Let $p = 2$. Then*

$$\nu(F, A_4) = \begin{cases} 4(2^{2m} - 1)/3 & \text{if } \mu_3 \subset F, \\ (2^{2m} - 1)/3 & \text{if } \mu_3 \not\subset F. \end{cases}$$

Proof. Let K be an A_4-extension over F. Since K_4 is a normal subgroup of A_4, there exists a (unique) Galois subfield F' of degree 3 over F, where $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By [2],

$$|F'^*/(F'^*)^2| = 4q^{3e},$$
$$|F^*/(F^*)^2| = 4q^e.$$

It is clear that the natural map of $F^*/(F^*)^2 \to F'^*/(F'^*)^2$ is an injection since $[F' : F] = 3$. We consider the action on $F'^*/(F'^*)^2$ of the Galois group $\mathrm{Gal}(F'/F)$.

(1) Denote $G' = \mathrm{Gal}(F'/F)$. Then the following result holds:

$$(F'^*/(F'^*)^2)^{G'} \cong F^*/(F^*)^2.$$

As we've already noted injectivity, it remains to show that the natural map is surjective. Let $a \in F'^*/(F'^*)^2$ be a fixed point of $\mathrm{Gal}(F'/F)$ and $a \neq 1$ in $F'^*/(F'^*)^2$. Then $F'(\sqrt{a'})$ is a Galois extension over F, where a' represents a lifting of a in F'^*. There isn't an order-2 normal subgroup in S_3, so

$$\mathrm{Gal}(F'(\sqrt{a'})/F) \cong \mathbb{Z}/6\mathbb{Z}.$$

Let F'' be the fixed field of the normal subgroup $\mathbb{Z}/3\mathbb{Z}$. There exists an element $b \in F^*/(F^*)^2$ such that

$$F'' = F(\sqrt{b}).$$

Then

$$F'(\sqrt{a'}) = F'(\sqrt{b}).$$

So $a = b$ in $F'^*/(F'^*)^2$.

(2) Let σ be a generator of G'. Assume $x \in F'^*/(F'^*)^2 - F^*/(F^*)^2$; then there are the following two cases:

(i) $N_{F'/F}(x) = 1$ in $F^*/(F^*)^2$,

(ii) $N_{F'/F}(x) \neq 1$ in $F^*/(F^*)^2$.

In (i), the field $F'(\sqrt{x}, \sqrt{\sigma x})$ is an A_4-extension over F since the Galois group of $F'(\sqrt{x}, \sqrt{\sigma x})/F$ isomorphic to $K_4 \rtimes \mathbb{Z}/3\mathbb{Z}$, where $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In (ii),

$$F'(\sqrt{x}, \sqrt{\sigma x}, \sqrt{\sigma^2 x}) = F'(\sqrt{x/\sigma(x)}, \sqrt{\sigma x/\sigma^2 x}, \sqrt{N_{F'/F}(x)}),$$

So $F'(\sqrt{x}, \sqrt{\sigma x}, \sqrt{\sigma^2 x})$ is an $(A_4 \times \mathbb{Z}/2\mathbb{Z})$-extension over F. Any $(A_4 \times \mathbb{Z}/2\mathbb{Z})$-extension K is generated by an A_4-extension over F and an extension of degree 2 over F. Denote the unique extension of degree 3 by F'; then there exist $x \in F'^*/(F'^*)^2$ and $a \in F^*/(F^*)^2$ satisfying $x \notin F^*/(F^*)^2$, $N_{F'/F}(x) \in (F^*)^2$ and $a \notin (F^*)^2$, such that $K = F'(\sqrt{x}, \sqrt{\sigma x}, \sqrt{a})$. It is easy to see that

$$K = F'(\sqrt{ax/\sigma x}, \sqrt{a\sigma x/\sigma^2 x}, \sqrt{a\sigma^2 x/x})$$

since $N_{F'/F}(x) = x\sigma x\sigma^2 x = 1$ in $F^*/(F^*)^2$. Then $\sigma x/\sigma^2 x = x\sigma^2 x/\sigma^2 x = x$ in $F'^*/(F'^*)^2$. Consider K as an extension over F'; there exist 7 subfields with order 2 over F' which are one-to-one correspondents to $\{y, \sigma y, \sigma^2 y, y\sigma y, \sigma y\sigma^2 y, y\sigma^2 y, N_{F'/F}(y)\}$, where $y = ax/\sigma x$. And $N_{F'/F}(y) = a \neq 1$ in $F^*/(F^*)^2$. The $\mathrm{Gal}(F'/F)$-orbits are $\{y, \sigma y, \sigma^2 y\}$, $\{y\sigma y, \sigma y\sigma^2 y, y\sigma^2 y\}$, and $\{N_{F'/F}(y)\}$. So any $(A_4 \times \mathbb{Z}/2\mathbb{Z})$-extension over F is in form of (ii) and

$$\nu(F, A_4 \times \mathbb{Z}/2\mathbb{Z}) = \nu(F, A_4)\nu(F, \mathbb{Z}/2\mathbb{Z}).$$

(i) Suppose $\mu_3 \not\subset F$, F' is the unique unramified extension of degree 3 over F, so

$$3\nu(F, A_4) + 3\nu(F, A_4 \times \mathbb{Z}/2\mathbb{Z}) = 4q^{3e} - 4q^e,$$
$$\nu(F, A_4 \times \mathbb{Z}/2\mathbb{Z}) = \nu(F, A_4)(4q^e - 1).$$

Then

$$\nu(F, A_4) = (q^{2e} - 1)/3.$$

(ii) Suppose $\mu_3 \subset F$, F' is the unique unramified extension and 3 totally ramified extensions of degree 3 over F, so

$$3\nu(F, A_4) + 3\nu(F, A_4 \times \mathbb{Z}/2\mathbb{Z}) = 4(4q^{3e} - 4q^e),$$
$$\nu(F, A_4 \times \mathbb{Z}/2\mathbb{Z}) = \nu(F, A_4)(4q^e - 1).$$

Then

$$\nu(F, A_4) = 4(q^{2e} - 1)/3.$$

□

Proposition 4.3. *Let $p = 2$. Then*

$$\nu(F, S_4) = \begin{cases} 0 & \text{if } \mu_3 \subset F, \\ 2^{2m+1} - 1 & \text{if } \mu_4 \not\subseteq F \text{ and } m \text{ is even and } f = 1, \\ 2^{2m} - 1 & \text{otherwise.} \end{cases}$$

Proof. By Krasner's theorem [3],

$$|M(4)| = 16q^{3e} - 4q^{2e} - 5.$$

By the local class field theory and the dual theory of the finite abelian group, the following equation holds:

$$|Ab(4)| = |\{S : \ S \text{ is the subgroup of order 4 of } F^*/(F^*)^4\}|.$$

Let T_1 be the set consisting of the elements of order $\leqslant 2$ in $F^*/(F^*)^4$, and let T_2 be the set consisting of the elements of order 4 in $F^*/(F^*)^4$. The sequence

$$0 \to T_1 \to F^*/(F^*)^4 \to (F^*)^2/(F^*)^4 \to 0$$

is exact. The third map is $a \mapsto a^2$. So

$$|T_1| = |F^*/(F^*)^4|/|(F^*)^2/(F^*)^4|.$$

Suppose $\mu_4 \nsubseteq F$; then

$$|T_1| = 4q^e,$$
$$|T_2| = 8q^{2e} - 4q^e.$$

Then

$$|Ab(4)| = |T_2|/2 + (|T_1| - 1)(|T_1| - 2)/6 = 20q^{2e}/3 - 4q^e + 1/3.$$

Suppose $\mu_4 \subset F$; then

$$|T_1| = 4q^e,$$
$$|T_2| = 16q^{2e} - 4q^e.$$

Then

$$|Ab(4)| = |T_2|/2 + (|T_1| - 1)(|T_1| - 2)/6 = 32q^{2e}/3 - 4q^e + 1/3.$$

Since D_8 is a 2-group, by Theorem 2.2 of [7],

$$\nu(F, D_8) = \begin{cases} q^e(q^e - 1)(4q^e - 1) & \text{if } \mu_4 \subset F \text{ or } \mu_4 \nsubseteq F \text{ and } m \text{ is even and } f = 1, \\ q^e(2q^e - 1)^2 & \text{otherwise.} \end{cases}$$

By Lemma 2,

(i) If $\mu_4 \subset F$, then

$$\nu(F, S_4) = (|M(4)| - |Ab(4)|)/4 - \nu(F, A_4) - \nu(F, D_8) = 4(q^{2e} - 1)/3 - \nu(F, A_4).$$

(ii) If $\mu_4 \nsubseteq F$, and m is odd or m is even and $f \geqslant 2$, then

$$\nu(F, S_4) = (|M(4)| - |Ab(4)|)/4 - \nu(F, A_4) - \nu(F, D_8) = 4(q^{2e} - 1)/3 - \nu(F, A_4).$$

(iii) If $\mu_4 \nsubseteq F$ and m is even and $f = 1$, then

$$\nu(F, S_4) = (|M(4)| - |Ab(4)|)/4 - \nu(F, A_4) - \nu(F, D_8) = (7q^{2e} - 4)/3 - \nu(F, A_4).$$

By Proposition 4.2, we have

$$\nu(F, S_4) = \begin{cases} 0 & \text{if } \mu_3 \subset F, \\ 2q^{2e} - 1 & \text{if } \mu_4 \nsubseteq F \text{ and } n \text{ is even and } f = 1, \\ q^{2e} - 1 & \text{otherwise.} \end{cases}$$

□

Remark. Since K_4 is a normal subgroup of S_4 and $S_4/K_4 \cong S_3$, there exists an S_3-subextension in an S_4-extension of F by Galois theory. If $\mu_3 \subset F$ and $p \neq 3$, then $\nu(F, S_3) = 0$. So $\nu(F, S_4) = 0$. This gives another proof for a case of $\nu(F, S_4)$.

Using these propositions, the proof of Theorem 1.2 is obtained. This completes the proof of Theorem 1.2.

5. Examples

Example 5.1. Let $F = \mathbb{Q}_p$. Then

(1)
$$\nu(\mathbb{Q}_p, S_3) = \begin{cases} 6 & \text{if } p = 3, \\ 0 & \text{if } p \equiv 1 \mod 3, \\ 3 & \text{if } p \equiv 2 \mod 3. \end{cases}$$

(2)
$$\nu(\mathbb{Q}_p, A_4) = \begin{cases} 1 & \text{if } p = 2, \\ 0 & \text{if } p > 2. \end{cases}$$

(3)
$$\nu(\mathbb{Q}_p, S_4) = \begin{cases} 3 & \text{if } p = 2, \\ 0 & \text{if } p > 2. \end{cases}$$

(4)
$$\nu(\mathbb{Q}_p, S_n) = \nu(\mathbb{Q}_p, A_n) = 0 \quad (n \geqslant 5).$$

References

[1] M. Krasner, Nombre des extensions d'un degré donné d'un corps p-adique, les Tendances Géométriques en algébre et Théorie des Nombres, ED. CNRS, Paris, 1966, 143-169. MR0225756 (37:1349)

[2] S. Lang, Algebraic Number Theory, Second edition. GTM, 110. Springer-Verlag, New York, 1994. MR1282723 (95f:11085)

[3] S. Pauli and X. F. Roblot, On the computation of all extensions of a p-adic field of a given degree, Math. Comp. **70** (2001), no. 236, 1641-1659. MR1836924 (2002e:11166)

[4] I. R. Šafarevič, On p-extensions, Mat. Sb. **20**(62)(1947), 351-363; English transl., Amer. Math. Soc. Transl. Ser. 2 **4** (1956), 59-72. MR0020546 (8:560e)

[5] J. -P. Serre, Corps Locaux, Hermann, Paris, 1963. MR0354618 (50:7096)

[6] J. -P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, C. R. Acad. Sci. Pairs Sér. A-B **286** (1978), A1031-A1036. MR500361 (80a:12018)

[7] M. Yamagishi, On the number of Galois p-extensions of a local field, Proc. Amer. Math. Soc. **123** (1995), 2373-2380. MR1264832 (95j:11109)

Department of Mathematics, the University of Science and Technology of China, Hefei, People's Republic of China 230026

E-mail address: dshwei@ustc.edu

Department of Mathematics, Nanjing Normal University, Nanjing, People's Republic of China 210097

E-mail address: cgji@njnu.edu.cn