PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 8, August 1995

ON THE NUMBER OF GALOIS p-EXTENSIONS OF A LOCAL FIELD

MASAKAZU YAMAGISHI

(Communicated by William Adams)

ABSTRACT. Let p be a prime, k a finite extension of the p-adic field $\mathbb{Q}_p$, and G a finite p-group. Let $\nu(k, G)$ denote the number of non-isomorphic Galois extensions of k whose Galois groups are isomorphic to G. When k does not contain a primitive p-th root of unity, I. R. Šafarevič gave an explicit formula for $\nu(k, G)$. In this note, we treat the case when k contains a primitive p-th root of unity. After giving a general formula for $\nu(k, G)$ (Theorem 1), we calculate $\nu(k, G)$ explicitly for some special p-groups (Theorem 2.2).

INTRODUCTION

As is well known, a p-adic field k has only a finite number of non-isomorphic algebraic extensions with given degree (cf. [Kr]). Therefore the number of Galois extensions of k with prescribed finite Galois group G is also finite; we denote this number by $\nu(k, G)$. In this note, we are interested in giving $\nu(k, G)$ explicitly.

Suppose in the following that G is a p-group (p a prime). Let k be of residue characteristic p, and n be the degree of k over the p-adic field $\mathbb{Q}_p$. Let μ_p denote the set of p-th roots of unity. I. R. Šafarevič [Ša] proved that if $k \not\supset \mu_p$, then the Galois group of the maximal pro-p-extension of k is a free pro-p-group with exactly $n+1$ generators. And he gave an explicit formula for $\nu(k, G)$ in this case:

$$\nu(k, G) = \frac{1}{|\operatorname{Aut}(G)|}\left(\frac{|G|}{p^d}\right)^{n+1}\prod_{i=0}^{d-1}(p^{n+1} - p^i),$$

where d is the minimal number of generators of G. An analogous formula had already been obtained by E. Witt [Wi], but in a different context.

If $k \supset \mu_p$, then the Galois group of the maximal pro-p-extension of k is a one-relator group called Demuškin group, and the relation is completely determined by S. P. Demuškin, J.-P. Serre, and J. Labute (cf. [La]). Our first aim

Received by the editors December 20, 1993.
1991 *Mathematics Subject Classification*. Primary 11S15.
Key words and phrases. Local field, Demuškin group, p-extension.
Supported in part by JSPS Fellowships for Japanese Junior Scientists, and by Grant-in-Aid for Scientific Research, The Ministry of Education, Science and Culture.

is to give a general formula for $\nu(k, G)$ in this case, by using the classification theorem of Demuškin groups and a well-known enumeration argument.

Theorem 1. *Let p be a prime, k a finite extension of $\mathbb{Q}_p$ containing μ_p, and G a finite p-group. Then we have*

$$\nu(k, G) = \frac{1}{|\operatorname{Aut}(G)|} \sum_{H \le G} \mu_G(H)\alpha(H),$$

where $\mu_G(\ )$ is the Möbius function on the partially ordered set consisting of all subgroups of G (see Lemma 1.3 for the precise formula), and $\alpha(H)$ will be given in Lemma 1.8. In particular, for $p \ge 3$,

$$\alpha(H) = |H|^n \sum_{\chi} \frac{1}{\chi(1)^n} \sum_{h \in H} \chi(h^{q-1})\chi(h),$$

where $n = [k : \mathbb{Q}_p]$, q is the maximal power of p such that $k \supset \mu_q$, and χ runs over all irreducible complex characters of H.

We shall prove this theorem in §1.

Our second aim is to calculate $\nu(k, G)$ explicitly for some special p-groups (Theorem 2.2):

(1) the two non-abelian groups of order p^3 ($p \ge 3$),
(2) the dihedral and the generalized quaternion groups of 2-power orders ($p = 2$).

In the case $|G| = p^3$, our result is not new; the formula is originally due to R. Massy and T. Nguyen-Quang-Do [Ma-Ng] when $p \ge 3$, and to C. Jensen and N. Yui [Je-Yu] when $p = 2$ (cf. Remark 3.1). But our method of proof is different from theirs. Indeed, our proof of Theorem 1 (or, directly, Lemma 1.8) is significantly inspired by a work of Y. Ihara [Ih]. See Remark 1.6 below.

The following notation will be used throughout this note:

$\operatorname{Gal}(L/k)$: the Galois group of a Galois extension L/k,
$\operatorname{Aut}(G)$: the automorphism group of a group G,
$H \le G$ means that H is a subgroup of a group G,
$[a, b] := a^{-1}b^{-1}ab$,
μ_N : the group of N-th roots of unity,
$|\ \ |$: the cardinality of a set.

1. Proof of Theorem 1

1.1. Let k be a field and G a finite group. A G-extension of k is, by definition, a Galois extension of k whose Galois group is isomorphic to G. There is a one-to-one correspondence between the set of G-extensions of k in a fixed separable closure $\bar{k}$ of k and the set of surjective homomorphisms $\operatorname{Gal}(\bar{k}/k) \twoheadrightarrow G$ modulo automorphisms of G. Let $\nu(k, G)$ denote the cardinality of any one of these two sets. We thus have

$$\nu(k, G) = \frac{|\{\operatorname{Gal}(\bar{k}/k) \twoheadrightarrow G : \text{surjective homomorphism}\}|}{|\operatorname{Aut}(G)|},$$

assuming the finiteness of each factor. If G is a p-group (p a prime), then we may replace $\bar{k}$ by the maximal pro-p-extension $k(p)$ of k.

1.2. Let $\mathscr{G}$ be a fixed group. For any finite group G, let us denote

$$\alpha(G) = \alpha_{\mathscr{G}}(G) := |\{\mathscr{G} \to G : \text{homomorphism}\}|,$$
$$\beta(G) = \beta_{\mathscr{G}}(G) := |\{\mathscr{G} \twoheadrightarrow G : \text{surjective homomorphism}\}|.$$

Assume that $\alpha(H)$ (hence also $\beta(H)$) is finite for any subgroup H of a group G. Then it is clear that

$$\alpha(G) = \sum_{H \leq G} \beta(H),$$

and by the Möbius inversion formula, it follows that

$$\beta(G) = \sum_{H \leq G} \mu_G(H)\alpha(H).$$

Here $\mu_G(\ )$ is the Möbius function on the partially ordered set consisting of all subgroups of G, and is uniquely determined by the following two properties:

$$\mu_G(G) = 1,$$
$$\sum_{H \leq K \leq G} \mu_G(K) = 0, \quad \text{for any } H \lneq G.$$

Lemma 1.3. *If G is a p-group and $H \leq G$ with $[G:H] = p^i$, then we have*

$$\mu_G(H) = \begin{cases} (-1)^i p^{\frac{1}{2}i(i-1)} & \text{if } H \geq G^p[G, G], \\ 0 & \text{otherwise.} \end{cases}$$

Proof. See [Ha, p.142]. □

1.4. Suppose that $\mathscr{G}$ is finitely presented (in the category of abstract, profinite, or pro-p-groups) as:

$$\mathscr{G} = \langle x_1, x_2, \dots, x_n ; R_1 = R_2 = \cdots = R_m = 1\rangle,$$

where each $R_i = R_i(x_1, x_2, \dots, x_n)$ is a *finite* word in symbols $x_1, x_2, \dots, x_n$. Then for any finite group G (we assume that G is a p-group if $\mathscr{G}$ is a pro-p-group), we have

$$\alpha(G) = |\{(g_1, g_2, \dots, g_n) \in G^n ; R_i(g_1, g_2, \dots, g_n) = 1, \ i = 1, 2, \dots, m\}|.$$

In particular, both $\alpha(G)$ and $\beta(G)$ are finite. By the second orthogonality relation of irreducible characters [Cu-Re, 31.13], we have

$$R_i(g_1, \dots, g_n) = 1 \iff \sum_{\chi} \chi(1)\chi(R_i(g_1, \dots, g_n)) = |G|,$$
$$R_i(g_1, \dots, g_n) \neq 1 \iff \sum_{\chi} \chi(1)\chi(R_i(g_1, \dots, g_n)) = 0,$$

where χ runs over all irreducible complex characters of G. Thus we obtain

$$\alpha(G) = \frac{1}{|G|^m} \sum_{(g_1, g_2, \dots, g_n) \in G^n} \prod_{i=1}^{m} \sum_{\chi} \chi(1)\chi(R_i(g_1, \dots, g_n)). \tag{1.4.1}$$

1.5. As an important example, here we refer to the case of compact Riemann surfaces. Let $\mathscr{G} = \pi_1(X)$ be the fundamental group of a compact Riemann surface X with genus g. It is well known that $\mathscr{G}$ has the following presentation as an abstract group:

$$\mathcal{G} = \langle x_1, x_2, \dots, x_{2g}; [x_1, x_2][x_3, x_4]\cdots[x_{2g-1}, x_{2g}] = 1\rangle.$$

For this group $\mathcal{G}$, the expression (1.4.1) becomes

$$\alpha(G) = |G|^{2g-1}\sum_{\chi}\frac{1}{\chi(1)^{2g-2}}. \tag{1.5.1}$$

See [Se, 7.2], [Jo, Theorem 1] for the proof. As is mentioned in [Jo], this formula seems to be classically known.

Remark 1.6. Y. Ihara [Ih] used (1.5.1) to give an explicit formula for the number of $SL_2(\mathbb{F}_p)$-étale coverings of X, calculating $\mu_G(H)$ explicitly for all subgroups H of $G = SL_2(\mathbb{F}_p)$.

1.7. We shall generalize (1.5.1) to the case of Demuškin groups. Let k be a finite extension of the p-adic field $\mathbb{Q}_p$ with degree n, and let $\mathcal{G} = \mathrm{Gal}(k(p)/k)$, where $k(p)$ is the maximal pro-p-extension of k. Assume $k \supset \mu_p$. Then $\mathcal{G}$ is a Demuškin group. Let q be the maximal power of p such that $k \supset \mu_q$. By the classification theorem of Demuškin groups (cf. [La]), there exist generators $x_1, x_2, \dots, x_{n+2}$ of $\mathcal{G}$ such that the unique relation R takes the following form: if $q \neq 2$ (n is even in this case), then

$$R = x_1^q[x_1, x_2][x_3, x_4]\cdots[x_{n+1}, x_{n+2}]; \tag{1.7.1}$$

if $q = 2$ and n is odd, then

$$R = x_1^2x_2^4[x_2, x_3][x_4, x_5]\cdots[x_{n+1}, x_{n+2}]; \tag{1.7.2}$$

if $q = 2$ and n is even, then either

$$R = x_1^{2+2^f}[x_1, x_2][x_3, x_4]\cdots[x_{n+1}, x_{n+2}], \quad \text{or} \tag{1.7.3}$$

$$R = x_1^2[x_1, x_2]x_3^{2^f}[x_3, x_4]\cdots[x_{n+1}, x_{n+2}]. \tag{1.7.4}$$

Here, under the canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_2(\mu_{2^\infty})/\mathbb{Q}_2) \cong \mathbb{Z}_2^\times$$

induced by the Galois action on $\mu_{2^\infty} := \bigcup_i \mu_{2^i}$, the invariant $f \geq 2$ is defined by

$$\mathrm{Gal}(\mathbb{Q}_2(\mu_{2^\infty})/k \cap \mathbb{Q}_2(\mu_{2^\infty})) \cong \begin{cases} \langle -1 + 2^f\rangle & (\text{Case } 1.7.3), \\ \{\pm 1\} \times (1 + 2^f\mathbb{Z}_2) & (\text{Case } 1.7.4). \end{cases}$$

Lemma 1.8. *Let $\mathcal{G} = \mathrm{Gal}(k(p)/k)$ be as in 1.7 and G a p-group. We have*

$$\alpha(G) = \begin{cases} |G|^n \sum_{\chi} \frac{1}{\chi(1)^n} \sum_{g\in G} \chi(g^{q-1})\chi(g) & (\mathit{Case}\ 1.7.1), \\ |G|^{n-1} \sum_{\chi} \frac{1}{\chi(1)^{n-1}} \sum_{g,h\in G} \chi(g^2h^3)\chi(h) & (\mathit{Case}\ 1.7.2), \\ |G|^n \sum_{\chi} \frac{1}{\chi(1)^n} \sum_{g\in G} \chi(g^{2^f+1})\chi(g) & (\mathit{Case}\ 1.7.3), \\ |G|^{n-1} \sum_{\chi} \frac{1}{\chi(1)^{n-1}} \sum_{g,h\in G} \chi(g)\chi(gh^{2^f-1})\chi(h) & (\mathit{Case}\ 1.7.4), \end{cases}$$

where χ runs over all irreducible complex characters of G.

Proof. Substitute the explicit forms of R into (1.4.1), and use the following identity:

$$\sum_{b,c\in G} \chi(a[b,c]) = \left(\frac{|G|}{\chi(1)}\right)^2 \chi(a), \quad \text{for all } a \in G,$$

which is a consequence of Schur's lemma (cf. [Se, 7.2]). □

1.9. Putting all together, we obtain Theorem 1. □

Remark 1.10. Let $\mathcal{G}$ be a free pro-p-group with $n+1$ generators. Then $\alpha(H) = |H|^{n+1}$ for any p-group H. If we substitute this (in place of Lemma 1.8) into Theorem 1, we obtain Šafarevič's formula cited in Introduction.

2. Some special cases

2.1. **Notations on groups.** For each prime $p \geq 3$, there exist exactly two non-abelian groups of order p^3 up to isomorphism (cf. [Hu, Kapitel I, Satz 14.10]). After [Ma-Ng], we denote them by

$$E_1 := \langle x, y;\ x^p = y^p = [x, y]^p = 1,\ [x, [x, y]] = [y, [x, y]] = 1\rangle,$$
$$E_2 := \langle x, y;\ x^{p^2} = y^p = 1,\ yxy^{-1} = x^{p+1}\rangle.$$

For each integer $N \geq 2$, let D_{2N} denote the dihedral group of order $2N$ and Q_{4N} the generalized quaternion group of order $4N$:

$$D_{2N} := \langle x, y;\ x^N = y^2 = 1,\ yxy^{-1} = x^{-1}\rangle,$$
$$Q_{4N} := \langle x, y;\ x^{2N} = 1,\ y^2 = x^N,\ yxy^{-1} = x^{-1}\rangle.$$

D_8 and Q_8 are the two non-abelian groups of order 8.

Theorem 2.2. *Let the situation and the notation p, k, n, q, and f be the same as in* 1.7.

(1) (cf. [Ma-Ng]) *For* $p \geq 3$,

$$\nu(k, E_1) = \frac{p^n(p^{n+2}-1)(p^n-1)}{(p^2-1)(p-1)},$$

$$\nu(k, E_2) = \begin{cases} \frac{p^n(p^{2n+2}-p^{n+1}-p^n+1)}{p-1} & \text{if } k \not\supset \mu_{p^2}, \\ \frac{p^n(p^{n+2}-1)(p^n-1)}{p-1} & \text{if } k \supset \mu_{p^2}. \end{cases}$$

(2) *Let* $p = 2$ *and* $m \geq 3$. (a) *If* $k \supset \mu_4$, *then*

$$\nu(k, D_{2^m}) = 2^{m(n-1)-2n+3}(2^n-1)(2^{n+2}-1),$$

$$\nu(k, Q_{2^m}) = \begin{cases} 2^{m(n-1)-2n+3}(2^n-1)(2^{n+2}-1) & \text{if } m \geq 4, \\ \frac{1}{3}2^{m(n-1)-2n+3}(2^n-1)(2^{n+2}-1) & \text{if } m = 3. \end{cases}$$

(b) *If* $k \not\supset \mu_4$ *and* n *is odd, then*

$$\nu(k, D_{2^m}) = \begin{cases} 2^{m(n-1)-n+5}(2^n-1) & \text{if } m \geq 4, \\ 2^n(2^{n+1}-1)^2 & \text{if } m = 3, \end{cases}$$

$$\nu(k, Q_{2^m}) = \begin{cases} 2^{m(n-1)-n+5}(2^n-1) & \text{if } m \geq 5, \\ 2^{2n}(2^{2n+1}-2^{n+1}+1) & \text{if } m = 4, \\ \frac{1}{3}2^n(2^{n+1}-1)^2 & \text{if } m = 3. \end{cases}$$

(c) *If $k \not\ni \mu_4$ and n is even, then*

$$\nu(k, D_{2^m}) = \begin{cases} 2^{m(n-1)-2n+1}(2^n-1)\{2^{f+1}+8(2^{n+1}-1)\} & \text{if } m \geq f+2, \\ 2^{m(n-1)-2n+1}(2^{n+1}-1)\{2^{m-1}+8(2^n-1)\} & \text{if } m \leq f+1, \end{cases}$$

$$\nu(k, Q_{2^m}) = \begin{cases} 2^{m(n-1)-2n+1}(2^n-1)\{2^{f+1}+8(2^{n+1}-1)\} & \text{if } m \geq f+2, \\ 2^{m(n-1)-2n+1}(2^{n+1}-1)\{2^{m-1}+8(2^n-1)\} & \text{if } 4 \leq m \leq f+1, \\ \frac{1}{3}2^n(2^{2n+2}-2^{n+1}+1) & \text{if } m=3. \end{cases}$$

Proof. We shall give an explicit expression of $\alpha(\ )$. First note that, if H is abelian, then we have

$$\alpha(H) = |H|^{n+1} \times |\{h \in H;\, h^q = 1\}|.$$

In fact, one has only to consider the abelianization of $\mathcal{G}$;

$$\mathcal{G}/[\mathcal{G}, \mathcal{G}] \cong \mathbb{Z}_p^{n+2}/q\mathbb{Z}_p.$$

It is therefore enough to consider the cases $H = E_1$, E_2, D_M, and Q_M, where $M \geq 8$ is a power of 2. We apply Lemma 1.8. But since it is an exercise in group theory to make the character tables of such groups (for D_M and Q_M, see [Cu-Re, §47]), we shall omit the details and just state the results of calculation.

(1) We are in Case 1.7.1. We have

$$\alpha(E_1) = \alpha(E_2) = p^{3n+5} + (p-1)p^{2n+3}.$$

(2) (a) We are in Case 1.7.1. We have

$$\alpha(D_M) = \alpha(Q_M) = \begin{cases} M^{n+1}\left\{4 + \frac{1}{2^n}\left(\frac{M}{4} - 1\right)\right\} & \text{if } M \leq 2q, \\ M^{n+1}\left\{4 + \frac{1}{2^n}\left(\frac{q}{2} - 1\right)\right\} & \text{if } M \geq 2q. \end{cases}$$

(b) We are in Case 1.7.2. We have

$$\alpha(D_M) = \alpha(Q_M) = M^{n+1}\left(4 + \frac{1}{2^n}\right),$$

with the only exception that

$$\alpha(Q_8) = 8^{n+1}\left(4 - \frac{1}{2^n}\right).$$

(c) We are in Case 1.7.3 or Case 1.7.4. In either case, we have

$$\alpha(D_M) = \alpha(Q_M) = \begin{cases} M^{n+1}\left\{4 + \frac{1}{2^n}\left(\frac{M}{4} - 1\right)\right\} & \text{if } M \leq 2^{f+1}, \\ M^{n+1}\left\{4 + \frac{1}{2^n}(2^{f-1} - 1)\right\} & \text{if } M \geq 2^{f+1}. \end{cases}$$ □

Example 2.3.

$$\nu(\mathbb{Q}_2, D_{2^m}) = \begin{cases} 16 & \text{if } m \geq 4, \\ 18 & \text{if } m = 3, \end{cases}$$

$$\nu(\mathbb{Q}_2, Q_{2^m}) = \begin{cases} 16 & \text{if } m \geq 5, \\ 20 & \text{if } m = 4, \\ 6 & \text{if } m = 3. \end{cases}$$

Remark 2.4. G. Fujisaki [Fu] determined all the six Q_8-extensions of $\mathbb{Q}_2$, and H. Naito [Na] recently determined all the eighteen D_8-extensions of $\mathbb{Q}_2$.

3. Remarks

3.1. We mention here two related works by other authors.

(1) R. Massy and T. Nguyen-Quang-Do [Ma-Ng] investigated when and how an abelian extension of type (p, p) of k is embeddable into a Galois extension of degree p^3, by using Kummer theory. As an application they gave a formula for $\nu(k, G)$ when G is non-abelian of order p^3. Their result for $p = 2$ seems to be incorrect, as is pointed out in [Je-Yu, Remark (II.3.9)].

(2) C. Jensen and N. Yui [Je-Yu] investigated quaternion extensions of general fields, using Witt's theorem [Wi] and the theory of quadratic forms. Among others they gave a formula for $\nu(k, G)$ when $G = Q_8, D_8$.

3.2. If $|G|$ is prime to the residue characteristic of k, then a G-extension of k is tamely ramified. The structure of the Galois group $\mathcal{G}$ of the maximal tamely ramified extension of k is well known (cf. [Iw]): as a profinite group,

$$\mathcal{G} = \langle x, y; yxy^{-1} = x^q \rangle,$$

where q is the cardinality of the residue field of k. We can apply our method to this $\mathcal{G}$. For example, we can prove the following :

(1) If q is odd, $N \geq 2$, and $(q, N) = 1$, then we have

$$\nu(k, D_{2N}) = \begin{cases} 1 & \text{if } q \equiv -1 \bmod N, \\ 0 & \text{otherwise}, \end{cases}$$

$$\nu(k, Q_{4N}) = \begin{cases} 1 & \text{if } q \equiv -1 \bmod 2N, \\ 0 & \text{otherwise}. \end{cases}$$

(2) For p odd, let E_1, E_2 be as in §2. If $(p, q) = 1$, then we have

$$\nu(k, E_1) = 0,$$

$$\nu(k, E_2) = \begin{cases} p & \text{if } q \equiv p + 1 \bmod p^2, \\ 0 & \text{otherwise}. \end{cases}$$

However, it is easier to show these directly, and it is also easy to determine all desired extensions:

(i) if $q \equiv -1 \bmod N$, then $k(\zeta_N, \sqrt[N]{\pi})/k$ is the only D_{2N}-extension of k,

(ii) if $q \equiv -1 \bmod 2N$, then $k(\zeta_{2N}, \xi \sqrt[2N]{\pi})/k$ is the only Q_{4N}-extension of k, where π is a uniformizer in k, ζ_N (resp. ζ_{2N}) is a primitive N-th (resp. $2N$-th) root of unity, and ξ is a root of unity such that $k(\xi)/k$ is the quartic unramified extension of k. A similar description is possible for E_2-extensions. See also [Fe].

Acknowledgment

I wish to express my hearty thanks to Professor Shōichi Nakajima for warm encouragement and valuable comments, and to Professor Yasutaka Ihara, who kindly allowed me to see his handwritten notes on $SL_2(\mathbb{F}_p)$-coverings of a compact Riemann surface.

References

[Cu-Re] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York and London, 1962.

[Fe] W. Feit, *On p-regular extensions of local fields*, Proc. Amer. Math. Soc. **10** (1959), 592–595.

[Fu] G. Fujisaki, *A remark on quaternion extensions of the rational p-adic field*, Proc. Japan Acad. Ser. A Math. Sci. **66** (1990), 257–259.

[Ha] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. Oxford Ser. (2) **7** (1936), 134–151.

[Hu] B. Huppert, *Endliche Gruppen* I, Springer-Verlag, Berlin and Heidelberg, 1967.

[Ih] Y. Ihara, *Note of the lecture at Algebra Colloquium*, University of Tokyo, June, 1983.

[Iw] K. Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. **80** (1955), 448–469.

[Je-Yu] C. Jensen and N. Yui, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra, Kinokuniya, Tokyo, 1988, pp. 155–182.

[Jo] G. A. Jones, *Enumeration of homomorphisms and surface-coverings*, Preprint, University of Southampton, 1993.

[Kr] M. Krasner, *Nombres des extensions d'un degré donné d'un corps $\mathfrak{P}$-adique*, Les Tendances Géom. en Algèbre et Théorie des Nombres, Édition du Centre National de la Recherche Scientifique, Paris, 1966, pp. 143–169.

[La] J. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132.

[Ma-Ng] R. Massy and T. Nguyen-Quang-Do, *Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale*, J. Reine Angew. Math. **291** (1977), 149–161.

[Na] H. Naito, *Dihedral extensions of degree* 8 *over the rational p-adic fields*, Proc. Japan Acad. Ser. A. Math. Sci. **71** (1995).

[Ša] 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; see also Collected Mathematical Papers 6–19.

[Se] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett, Boston and London, 1992.

[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237–245.

DEPARTMENT OF MATHEMATICS, NAGOYA INSTITUTE OF TECHNOLOGY, GOKISO, SHOWA, NAGOYA 466, JAPAN

E-mail address: `yamagisi@kyy.nitech.ac.jp`