The number of semidihedral or modular extensions of a local field

By Makoto ITO*) and Masakazu YAMAGISHI**)

(Communicated by Heisuke HIRONAKA, M.J.A., Feb. 13, 2007)

Abstract: We calculate the number of Galois extensions, up to isomorphism, of a local field whose Galois groups are isomorphic to the semidihedral (resp. modular) group of order 2^m $(m \geq 4)$.

Key words: Local field; 2-extension.

1. Introduction. For a field k and a finite group G, let $\nu(k, G)$ denote the number of Galois extensions, up to isomorphism, of k with Galois group G. It is well known that $\nu(k, G)$ is finite when k is a local field (in this note, a local field means a finite extension of the l-adic field $\mathbf{Q}_l$, where l is a prime).

In a previous paper [4], the second author obtained a general formula for $\nu(k, G)$ when k is a local field and G is a p-group (p a prime), which generalizes Šafarevič's formula, and as an application he calculated $\nu(k, D_{2^m})$ and $\nu(k, Q_{2^m})$ for $m \geq 3$, where

$$D_{2^m} = \langle x, y \,|\, x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{-1} \rangle$$

is the dihedral group of order 2^m and

$$Q_{2^m} = \langle x, y \,|\, x^{2^{m-1}} = 1, y^2 = x^{2^{m-2}}, y^{-1}xy = x^{-1} \rangle$$

is the generalized quaternion group of order 2^m.

In this note, using the formula for $\nu(k, G)$ obtained in [4], we calculate $\nu(k, SD_{2^m})$ and $\nu(k, M_{2^m})$ for $m \geq 4$, where

$$SD_{2^m} = \langle x, y \,|\, x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{2^{m-2}-1} \rangle$$

is the semidihedral group of order 2^m and

$$M_{2^m} = \langle x, y \,|\, x^{2^{m-1}} = y^2 = 1, y^{-1}xy = x^{2^{m-2}+1} \rangle$$

is the modular group of order 2^m.

These four types of groups are the only finite non-abelian 2-groups of order 2^m which have elements of order 2^{m-1}.

2000 Mathematics Subject Classiffcation. Primary 11S20.

*) Field of Mathematics and Mathematical Science, Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466–8555, Japan.

**) Department of Mathematics, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466–8555, Japan.

2. Semidihedral (resp. modular) groups. We state some basic facts on the groups SD_{2^m} and M_{2^m}, which we need later. We omit the proofs since they are elementary. We denote the cyclic group of order 2^m by C_{2^m}.

Lemma 1. *Let $G = SD_{2^m}$ $(m \geq 4)$.*

(1) *An automorphism of G is described as*

$$x \mapsto x^a, \quad y \mapsto x^b y$$

where a is odd and b is even. In particular, $|\mathrm{Aut}(G)| = 2^{2m-4}$.

(2) *The subgroups of G containing $G^2[G, G] = \langle x^2 \rangle$ are as follows:*

subgroup	$G = \langle x, y \rangle$	$\langle x^2, y \rangle$	$\langle x^2, xy \rangle$	$\langle x \rangle$	$\langle x^2 \rangle$
isom. to	SD_{2^m}	$D_{2^{m-1}}$	$Q_{2^{m-1}}$	$C_{2^{m-1}}$	$C_{2^{m-2}}$

(3) *There are $2^{m-2} + 3$ conjugacy classes of G; they are*

- $\{1\}$,
- $\{x^a, x^{-a}\}$ $(a = 2, 4, 6, \ldots, 2^{m-2} - 2)$,
- $\{x^{2^{m-2}}\}$,
- $\{x^a, x^{-a+2^{2^{m-2}}}\}$ $(a = \pm 1, \pm 3, \pm 5, \ldots, \pm(2^{m-3} - 1))$,
- $\{y, x^2y, \ldots, x^{2^{m-1}-2}y\}$,
- $\{xy, x^3y, \ldots, x^{2^{m-1}-1}y\}$.

(4) *$[G, G] = \langle x^2 \rangle$, $G/[G, G] \cong C_2 \times C_2$. In particular, the number of 1-dimensional complex characters of G is 4.*

(5) *The other $2^{m-2} - 1$ irreducible complex characters of G are the traces of the 2-dimensional representations ρ_k of G defined by*

$$\rho_k(x) = \begin{pmatrix} \omega^k & 0 \\ 0 & (-\omega^{-1})^k \end{pmatrix}, \quad \rho_k(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $\omega = \exp\dfrac{2\pi\sqrt{-1}}{2^{m-1}}$, *and*

$k \in \{2, 4, 6, \dots, 2^{m-2}-2\} \cup \{\pm1, \pm3, \pm5, \dots, \pm(2^{m-3}-1)\}$.

Lemma 2. *Let* $G = M_{2^m}$ $(m \geq 4)$.

(1) *An automorphism of* G *is described as*

$$x \mapsto x^a \text{ or } x^a y, \quad y \mapsto y \text{ or } x^{2^{m-2}} y$$

where a *is odd. In particular,* $|\mathrm{Aut}(G)| = 2^m$.

(2) *The subgroups of* G *containing* $G^2[G,G] = \langle x^2\rangle$ *are as follows:*

subgroup	$G = \langle x, y\rangle$	$\langle x^2, y\rangle$	$\langle x^2, xy\rangle$	$\langle x\rangle$	$\langle x^2\rangle$
isom. to	M_{2^m}	$C_{2^{m-2}} \times C_2$	$C_{2^{m-1}}$	$C_{2^{m-1}}$	$C_{2^{m-2}}$

(3) *There are* $5 \cdot 2^{m-3}$ *conjugacy classes of* G*; they are*

- $\{x^a\}$ $\quad (a = 0, 2, 4, \dots, 2^{m-1}-2)$,
- $\{x^a, x^{a+2^{m-2}}\}$ $(a = 1, 3, 5, \dots, 2^{m-2}-1)$,
- $\{x^a y, x^{a+2^{m-2}} y\}$ $(a = 0, 1, 2, \dots, 2^{m-2}-1)$.

(4) $[G,G] = \langle x^{2^{m-2}}\rangle$, $G/[G,G] \cong C_{2^{m-2}} \times C_2$. *In particular, the number of* 1*-dimensional complex characters of* G *is* 2^{m-1}.

(5) *The other* 2^{m-3} *irreducible complex characters of* G *are the traces of the* 2*-dimensional representations* ρ_k *of* G *defined by*

$$\rho_k(x) = \begin{pmatrix} \omega^k & 0 \\ 0 & (-\omega)^k \end{pmatrix}, \quad \rho_k(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $\omega = \exp\dfrac{2\pi\sqrt{-1}}{2^{m-1}}$ *and* $k = 1, 3, 5, \dots, 2^{m-2}-1$.

3. Tame case. In general, let k be a field, $\mathcal{G} = \mathcal{G}_k$ the Galois group of the maximal pro-2-extension of k. By Galois theory, there is a one-to-one correspondence between the set of Galois extensions of k whose Galois group is isomorphic to a given finite 2-group G and the set of surjective homomorphisms from $\mathcal{G}$ to G, up to automorphisms of G. Thus the calculation of $\nu(k, G)$ reduces to the enumeration of surjective homomorphisms from $\mathcal{G}$ to G.

We first consider the case where the residue field of k has characteristic different from 2. The following result (together with the proof) is more or less well known (cf. e.g. [3]).

Theorem 3. *Let* k *be a local field,* q *the cardinality of the residue field of* k*. Suppose* q *is odd. Then we have for all* $m \geq 4$,

$$\nu(k, SD_{2^m}) = \begin{cases} 2 & (q \equiv 2^{m-2}-1 \pmod{2^{m-1}}), \\ 0 & (\textit{otherwise}), \end{cases}$$

$$\nu(k, M_{2^m}) = \begin{cases} 0 & (q \equiv 1 \pmod{2^{m-1}}), \\ 2^{m-2} & (q \equiv 2^{m-2}+1 \pmod{2^{m-1}}), \\ 2^{c-1} & (q \equiv 2^c+1 \pmod{2^{c+1}}, \ 1 \leq c \leq m-3). \end{cases}$$

Proof. The Galois group $\mathcal{G} = \mathcal{G}_k$ has the presentation

$$\mathcal{G} = \langle \sigma, \tau \,;\, \sigma\tau\sigma^{-1} = \tau^q\rangle$$

as a pro-2-group, where σ is a lift of the Frobenius automorphism and τ is a generator of the inertia subgroup. There is a bijective mapping between the set of surjective homomorphisms from $\mathcal{G}$ to G and the set

$$\{(X, Y) \in G \times G \,;\, \langle X, Y\rangle = G,\ YXY^{-1} = X^q\},$$

given by $\pi \mapsto (\pi(\tau), \pi(\sigma))$.

First let $G = SD_{2^m}$. A pair $(X, Y) \in G \times G$ generates G if and only if

(1) $X = x^a$, $Y = x^b y$ where a is odd,

(2) $X = x^a y$, $Y = x^b$ where b is odd, or

(3) $X = x^a y$, $Y = x^b y$ where $a - b$ is odd.

In each case, we verify whether $X^q Y X^{-1} Y^{-1} = 1$ holds.

(1) We have $X^q Y X^{-1} Y^{-1} = x^{a(q-2^{m-2}+1)}$. Since a is odd, $X^q Y X^{-1} Y^{-1} = 1$ holds if and only if $q \equiv 2^{m-2}-1 \pmod{2^{m-1}}$.

(2) We have $X^q Y X^{-1} Y^{-1} = x^{2^{m-3}a(q-1)+2^{m-2}-2b} \neq 1$.

(3) We have $X^q Y X^{-1} Y^{-1} = x^{2^{m-3}a(q-1)+2^{m-2}+2(a-b)} \neq 1$.

Thus the number of surjective homomorphisms from $\mathcal{G}$ to G is 2^{2m-3} if $q \equiv 2^{2m-2}-1 \pmod{2^{m-1}}$, 0 otherwise. Since $|\mathrm{Aut}(G)| = 2^{2m-4}$, we obtain the result.

Let next $G = M_{2^m}$. The three conditions that a pair $(X, Y) \in G \times G$ should generate G are literally the same as in the case of SD_{2^m}.

(1) We have $X^q Y X^{-1} Y^{-1} = x^{a(q-2^{m-2}-1)}$. Since a is odd, $X^q Y X^{-1} Y^{-1} = 1$ holds if and only if $q \equiv 2^{m-2}+1 \pmod{2^{m-1}}$.

(2) We have $X^qYX^{-1}Y^{-1} = x^{(2^{m-3}+1)a(q-1)+2^{m-2}}$, which is equal to 1 if and only if $a(q-1) \equiv 2^{m-2} \pmod{2^{m-1}}$.

(3) The same conclusion as (2).

Let 2^c be the maximal power of 2 dividing $q-1$, i.e.,

$$q \equiv 2^c + 1 \pmod{2^{c+1}}.$$

The number of a's satisfying

$$0 \leq a < 2^{m-1},\ a(q-1) \equiv 2^{m-2} \pmod{2^{m-1}}$$

is 2^c if $c \leq m-2$, 0 otherwise. Therefore, the number of surjective homomorphisms from $\mathcal{G}$ to G is

$$\begin{cases} 0 & (c > m-2), \\ 2^{2m-2} & (c = m-2), \\ 2^{c+m-1} & (c < m-2). \end{cases}$$

Since $|\mathrm{Aut}(G)| = 2^m$, we obtain the result. □

Remark 4. *Fardoux* [1] *gave a detailed description of semidihedral* (*resp. modular*) *extensions in the tame case. One can easily deduce Theorem* 3 *from his result.*

Remark 5. *The first author* [2] *gave an alternative proof of Theorem* 3 *by using the same method as in the wild case.*

4. Wild case. We consider the case where the residue field of k has characteristic 2. For a positive integer N, we denote the group of Nth roots of unity by μ_N.

Theorem 6. *Let k be a finite extension field of $\mathbf{Q}_2$ with degree n, q the maximal power of 2 such that $k \supset \mu_q$. Let U be the image of $\mathcal{G}_k$ in $\mathbf{Z}_2^\times$ under the canonical isomorphism*

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

induced by the Galois action on $\mu_{2^\infty} := \bigcup_i \mu_{2^i}$.

(1) *If $q \geq 4$, then*

$$\nu(k, SD_{2^m}) = 2^{mn-m-2n+4}(2^n-1)(2^{n+2}-1) \quad (m \geq 4).$$

(2) *If $q = 2$ and n is odd, then*

$$\nu(k, SD_{2^m}) = \begin{cases} 2^{mn-m-n+6}(2^n-1) & (m \geq 5), \\ 2^{2n}(2^{n+1}-1)^2 & (m = 4). \end{cases}$$

(3) *If $q = 2$, n is even and $U = \langle -1+2^f \rangle$ $(f \geq 2)$, then*

$$\nu(k, SD_{2^m}) = \begin{cases} 2^{mn-m-2n+5}(2^n-1)(2^{n+1}+2^{f-2}-1) \\ \quad (m \geq f+3), \\ 2^{mn-m-2n+5}(2^n-1)(2^{n+1}+2^{m-4}-1) \\ \quad +2^{mn-n+1} \quad (m = f+2), \\ 2^{mn-m-2n+5}(2^n-1)(2^{n+1}+2^{m-4}-1) \\ \quad (4 \leq m \leq f+1). \end{cases}$$

(4) *If $q = 2$, n is even and $U = \{\pm 1\} \times (1 + 2^f\mathbf{Z}_2)$ $(f \geq 2)$, then*

$$\nu(k, SD_{2^m}) = \begin{cases} 2^{mn-m-2n+5}(2^n-1)(2^{n+1}+2^{f-2}-1) \\ \quad (m \geq f+2), \\ 2^{mn-m-2n+5}(2^n-1)(2^{n+1}+2^{m-4}-1) \\ \quad (4 \leq m \leq f+2). \end{cases}$$

(5) *We have*

$$\nu(k, M_{2^m}) = \begin{cases} 2^{mn-2n-1}(2^{n+1}-1)^2 q \\ \quad (2^m \geq 8q), \\ 2^{mn+m-2n-3}\left((2^{n+1}-1)^2 + 2^n\right) \\ \quad (16 \leq 2^m = 4q), \\ 2^{mn+m-2n-3}(2^n-1)(2^{n+2}-1) \\ \quad (16 \leq 2^m \leq 2q). \end{cases}$$

Proof. Instead of finding surjective homomorphisms, we use a formula in [4]. For a finite 2-group G, we have

$$\nu(k, G) = \frac{1}{|\mathrm{Aut}(G)|} \sum_H \mu_G(H)\alpha(H),$$

where H runs over all subgroups of G, $\mu_G(\ )$ is the Möbius function on the partially ordered set consisting of all subgroups of G, and $\alpha(H) = \alpha_k(H) = |\mathrm{Hom}(\mathcal{G}_k, H)|$. See [4] for the details about $\mu_G(H)$ and $\alpha(H)$. We recall the following

- $\mu_G(H) = \begin{cases} (-1)^i 2^{i(i-1)/2} \\ \quad \text{if } H \supset G^2[G,G] \text{ and } [G:H] = 2^i, \\ 0 \quad \text{otherwise.} \end{cases}$
- If H is abelian, then $\alpha(H) = |H|^{n+1} \times |\{h \in H\,;\, h^q = 1\}|$.
- $\alpha(H)$ is expressed as a sum over the irreducible complex characters of H, this is the reason why we need irreducible characters of SD_{2^m} and M_{2^m}.

Let $G = SD_{2^m}$ or M_{2^m}. We must calculate $\alpha(H)$ for non-abelian subgroups H of G such that $H \supset G^2[G,G]$. We shall omit the details of the calculation, but just exhibit the result. (We have already done in [4] for $H = D_{2^m}, Q_{2^m}$.)

(1) In this case, we have

$$\alpha(D_{2^m}) = \alpha(Q_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{q/2-1}{2^n}\right) \\ \quad (2^m \geq 2q), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-2}-1}{2^n}\right) \\ \quad (8 \leq 2^m \leq 2q), \end{cases}$$
$$\alpha(SD_{2^m}) = \alpha(D_{2^m}) = \alpha(Q_{2^m}) \quad (m \geq 4).$$

(2) In this case, we have

$$\alpha(D_{2^m}) = (2^m)^{n+1}\left(4 + \frac{1}{2^n}\right) \quad (m \geq 3),$$
$$\alpha(Q_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{1}{2^n}\right) \\ \quad (m \geq 4), \\ 8^{n+1}\left(4 - \dfrac{1}{2^n}\right) \\ \quad (m = 3), \end{cases}$$
$$\alpha(SD_{2^m}) = \alpha(D_{2^m}) = \alpha(Q_{2^m}) \quad (m \geq 4).$$

(3) In this case, we have

$$\alpha(D_{2^m}) = \alpha(Q_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{2^{f-1}-1}{2^n}\right) \\ \quad (m \geq f+1), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-2}-1}{2^n}\right) \\ \quad (3 \leq m \leq f+1), \end{cases}$$
$$\alpha(SD_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{2^{f-1}-1}{2^n}\right) \\ \quad (m \geq f+3), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-2}-1}{2^n}\right) \\ \quad (m = f+2), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-3}-1}{2^n}\right) \\ \quad (4 \leq m \leq f+1). \end{cases}$$

(4) In this case, we have

$$\alpha(D_{2^m}) = \alpha(Q_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{2^{f-1}-1}{2^n}\right) \\ \quad (m \geq f+1), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-2}-1}{2^n}\right) \\ \quad (3 \leq m \leq f+1), \end{cases}$$
$$\alpha(SD_{2^m}) = \begin{cases} (2^m)^{n+1}\left(4 + \dfrac{2^{f-1}-1}{2^n}\right) \\ \quad (m \geq f+2), \\ (2^m)^{n+1}\left(4 + \dfrac{2^{m-3}-1}{2^n}\right) \\ \quad (4 \leq m \leq f+1). \end{cases}$$

(5) We have

$$\alpha(M_{2^m}) = \begin{cases} (2^m)^{n+1} \cdot 2q \\ \quad (2^m \geq 8q), \\ (2^m)^{n+1} \cdot 2^{m-3}\left(4 + \dfrac{1}{2^n}\right) \\ \quad (16 \leq 2^m \leq 4q). \end{cases}$$

□

Example 7 (cf. [2]).

$$\nu(\mathbf{Q}_2, SD_{2^m}) = \begin{cases} 32 & (m \geq 5), \\ 36 & (m = 4), \end{cases}$$
$$\nu(\mathbf{Q}_2, M_{2^m}) = 9 \cdot 2^{m-2} \quad (m \geq 4).$$

Remark 8. *Let k be as in Theorem 6. Comparing Theorem* 6 *with* [4, Theorem 2.2], *we remark that*

$$\nu(k, SD_{2^m}) = 2\nu(k, D_{2^m}) = 2\nu(k, Q_{2^m})$$

holds for $m \geq 4$, $m \geq 5$, $m \geq f+3, m \geq f+2$ in (1), (2), (3), (4), *respectively.*

Acknowledgment. The authors are grateful to the referee for useful comments and suggestions.

References

[1] G. Fardoux, Sur les extensions pseudodiédrales d'un corps local, C. R. Acad. Sci. Paris Sér. A-B **277** (1973), A145–A148.

[2] M. Ito, On 2-extensions of a local field, Master's thesis, Nagoya Institute of Technology, 2007. (in Japanese).

[3] C. U. Jensen, Finite groups as Galois groups over arbitrary fields, in *Proceedings of the International Conference on Algebra, Part* 2 (*Novosibirsk,* 1989), 435–448, Contemp. Math., Part 2, Amer. Math. Soc., Providence, RI, 1992.

[4] M. Yamagishi, On the number of Galois p-extensions of a local field, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2373–2380.