The number of modular extensions of odd degree of a local field

By Masakazu YAMAGISHI

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

(Communicated by Heisuke HIRONAKA, M.J.A., Sept. 12, 2008)

Abstract: The number of Galois extensions, up to isomorphism, of a local field whose Galois groups are isomorphic to the modular group $M_{p^m} = \langle x, y \mid x^{p^{m-1}} = y^p = 1, y^{-1}xy = x^{p^{m-2}+1}\rangle$, where p is an odd prime, is counted.

Key words: Local field; p-extension.

1. 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 [4] we 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 Shafarevitch's formula [3], and as an application we calculated $\nu(k,G)$ for $G = D_{2^m}, Q_{2^m}$; the dihedral group and the generalized quaternion group, respectively, of order 2^m ($m \geq 3$). In [2], using the same formula, we calculated $\nu(k,G)$ for $G = SD_{2^m}, M_{2^m}$; the semidihedral group and the modular group, respectively, of order 2^m ($m \geq 4$).

In this note, we shall do the same kind of calculation for

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

the modular group of order p^m, where p is an odd prime and $m \geq 3$. We have previously calculated $\nu(k, M_{p^3})$ (Theorem 2.2(1) and Remark 3.2(2) of [4], where we used the notation E_2 instead of M_{p^3}). We generalize this result as follows:

Theorem 1. *Let l be the residue characteristic of k, q the maximal power of p such that k contains a primitive qth root of unity, and let*

$$n = \begin{cases} 0 & (l \neq p), \\ [k : \mathbf{Q}_p] & (l = p). \end{cases}$$

We have

$$\nu(k, M_{p^m}) = \begin{cases} \dfrac{p^{mn-2n-1}(p^n-1)(p^{n+1}-1)}{p-1} & (q = 1), \\ \dfrac{p^{mn-2n-1}q(p^{n+1}-1)^2}{p-1} & (1 < q < p^{m-2}), \\ \dfrac{p^{mn+m-2n-3}(p^{2n+2}-p^{n+1}-p^n+1)}{p-1} & (q = p^{m-2}), \\ \dfrac{p^{mn+m-2n-3}(p^n-1)(p^{n+2}-1)}{p-1} & (q > p^{m-2}). \end{cases}$$

2. For the proof of the theorem, we collect some basic facts on the modular group M_{p^m}. Let C_N denote the cyclic group of order N.

Lemma 2. *Let p be an odd prime and $G = M_{p^m}$ ($m \geq 3$).*

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

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

where $a \in (\mathbf{Z}/p^{m-1}\mathbf{Z})^\times$, $b \in \mathbf{Z}/p\mathbf{Z}$ and $c \in p^{m-2}\mathbf{Z}/p^{m-1}\mathbf{Z}$. In particular, $|\mathrm{Aut}(G)| = p^m(p-1)$.

(2) *The subgroups of G containing $G^p[G,G] = \langle x^p\rangle$ are as follows:*
- *G itself,*
- *$\langle x^p, y\rangle \cong C_{p^{m-2}} \times C_p$,*
- *$\langle x^p, x^a y\rangle \cong C_{p^{m-1}}$ $\quad (a \in (\mathbf{Z}/p\mathbf{Z})^\times)$,*
- *$\langle x\rangle \cong C_{p^{m-1}}$,*
- *$\langle x^p\rangle \cong C_{p^{m-2}}$.*

(3) *There are $p^{m-3}(p^2+p-1)$ conjugacy classes of G; they are*

2000 Mathematics Subject Classification. Primary 11S20.

- $\{x^a\}$ $(a \in p\mathbf{Z}/p^{m-1}\mathbf{Z})$,
- $\{x^a y^b, x^{a+p^{m-2}} y^b, x^{a+2p^{m-2}} y^b, \ldots, x^{a+(p-1)p^{m-2}} y^b\}$ $(a \in \mathbf{Z}/p^{m-2}\mathbf{Z},\ b \in \mathbf{Z}/p\mathbf{Z}$ *such that* $\gcd(a, b, p) = 1)$.

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

(5) *The other* $p^{m-3}(p-1)$ *irreducible complex characters of* G *are the traces of the* p*-dimensional representations* ρ_j *of* G $(j \in (\mathbf{Z}/p^{m-2}\mathbf{Z})^\times)$ *defined by*

$$\rho_j(x) = \begin{pmatrix} \omega^j & & & & \\ & (\zeta\omega)^j & & & \\ & & (\zeta^2\omega)^j & & \\ & & & \ddots & \\ & & & & (\zeta^{p-1}\omega)^j \end{pmatrix},$$

$$\rho_j(y) = \begin{pmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix},$$

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

Proof. (1) Let f be an automorphism of G. Since x and $f(x)$ have the same order p^{m-1}, we see that $f(x) = x^a y^b$ for some $a \in (\mathbf{Z}/p^{m-1}\mathbf{Z})^\times$ and $b \in \mathbf{Z}/p\mathbf{Z}$, noting that $(x^a y^b)^p = x^{ap}$ holds. Similarly, $f(y) = x^c y^d$ for some $c \in p^{m-2}\mathbf{Z}/p^{m-1}\mathbf{Z}$ and $d \in \mathbf{Z}/p\mathbf{Z}$ with $(c, d) \neq (0, 0)$. From the relation $f(y)^{-1} f(x) f(y) = f(x)^{p^{m-2}+1}$, it follows that $d = 1$. These conditions on a, b, c and d are sufficient.

(2), (3) and (4) are easily verified.

(5) It is straightforward to see that $\rho_j(x)$ and $\rho_j(y)$ given above define a complex representation of G for $j \in \mathbf{Z}$. Calculating the trace, we see that

- ρ_j is irreducible if and only if j is prime to p, and
- ρ_j is equivalent to $\rho_{j'}$ if and only if $j \equiv j' \pmod{p^{m-2}}$.

Thus we obtain $p^{m-3}(p-1)$ inequivalent irreducible complex characters of G. There are no more, by (3) and (4). □

3. We briefly review the result of [4]. For a finite p-group G, we have

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

where H runs over all subgroups of G, $\mu_G(\ )$ denotes the Möbius function on the partially ordered set consisting of all subgroups of G, and $\alpha_k(H) = |\operatorname{Hom}(\mathcal{G}_k, H)|$, $\mathcal{G}_k$ being the Galois group of the maximal pro-p-extension of k.

By a classical result of P. Hall [1], we know that

$$\mu_G(H) = \begin{cases} (-1)^i p^{i(i-1)/2} & \\ \qquad \text{if } H \supset G^p[G, G] \text{ and } [G : H] = p^i, & \\ 0 \quad \text{otherwise.} & \end{cases}$$

If $q = 1$, then $\alpha_k(H) = |H|^{n+1}$ and we obtain Shafarevitch's formula [3]

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

where d is the minimal number of generators of G.

If $q > 1$, then we have

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

where χ runs over all irreducible complex characters of H. In [4], we stated this in the case $l = p$ (i.e. $n \geq 1$), but this is valid also in the case $n = 0$.

4. We give a proof of the theorem, omitting the details of the calculation.

In the case $q = 1$, the formula follows from Shafarevitch's formula.

Suppose $q > 1$. By the formula for $\nu(k, G)$ in the previous section and by Lemma 2, it is enough to know $\alpha_k(H) = |\operatorname{Hom}(\mathcal{G}_k, H)|$ for $H = C_{p^i}, C_{p^i} \times C_p$ and M_{p^m}. We have

$$\alpha_k(C_{p^i}) = \begin{cases} p^{i(n+1)} q & (q \leq p^i), \\ p^{i(n+2)} & (q \geq p^i), \end{cases}$$

$$\alpha_k(C_{p^i} \times C_p) = \begin{cases} p^{(i+1)(n+1)+1} q & (q \leq p^i), \\ p^{(i+1)(n+2)} & (q \geq p^i), \end{cases}$$

since we see by local class field theory that

$$\mathcal{G}_k / [\mathcal{G}_k, \mathcal{G}_k] \cong \mathbf{Z}_p^{n+1} \times \mathbf{Z}_p / q\mathbf{Z}_p.$$

Using the formula for $\alpha_k(H)$ in the previous section, we obtain

$$\alpha_k(M_{p^m}) = \begin{cases} p^{mn+m+1}q & (1 < q < p^{m-2}), \\ p^{mn+2m-n-3}(p^{n+2}+p-1) & (q \geq p^{m-2}), \end{cases}$$

and the result follows. □

References

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

[2] M. Ito and M. Yamagishi, The number of semi-dihedral or modular extensions of a local field, Proc. Japan Acad. Ser. A Math. Sci. **83** (2007), no. 2, 10–13.

[3] I. Shafarevitch, On p-extensions, Rec. Math. [Mat. Sbornik] N.S. **20(62)** (1947), 351–363.

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