Dihedral Extensions of Degree 8 over the Rational p-adic Fields

By Hirotada NAITO

Department of Mathematics, Faculty of Education, Kagawa University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1995)

0. Introduction. We denote by $\boldsymbol{Q}_p$ the rational p-adic field for a prime p. It is well-known that there exist only finitely many extensions of a fixed degree over $\boldsymbol{Q}_p$ in a fixed algebraic closure of $\boldsymbol{Q}_p$ (cf. Weil [4] p. 208). Fujisaki [1] exhibited all extensions over $\boldsymbol{Q}_p$ whose Galois group is isomorphic to the quaternion group of order 8. In this note, we shall exhibit all extensions L over $\boldsymbol{Q}_p$ whose Galois group is isomorphic to the dihedral group D_4 of order 8. We call such extensions D_4-extensions. We shall show that there exist no such extension for $p \equiv 1 \bmod 4$, one extension for $p \equiv 3 \bmod 4$ and eighteen extensions for $p = 2$.

We denote by K the quadratic extension over $\boldsymbol{Q}_p$ such that L/K is a cyclic extension of degree 4. We denote by K_1 and K_2 the other two quadratic extensions over $\boldsymbol{Q}_p$ in L. We denote by M the compositum of K_1 and K_2. We denote by M_i and M_i' the quadratic extensions over K_i in L which are not Galois extensions over $\boldsymbol{Q}_p$. We deal with the case of odd primes in § 1. We exhibit all D_4-extensions over $\boldsymbol{Q}_2$ in § 2 by getting all such M_i and M_i'.

We remark that Yamagishi [3] computed the number of extensions K over a finite extension $k/\boldsymbol{Q}_p$ whose Galois group $Gal(K/k)$ is isomorphic to a fixed finite p-group (cf. see also cited papers in [3]).

1. The case $p \neq 2$. Let $L/\boldsymbol{Q}_p$ be a D_4-extension. $L/\boldsymbol{Q}_p$ has four intermediate fields M_1, M_1', M_2, M_2' of degree 4 which are not Galois extensions over $\boldsymbol{Q}_p$. We see that they are totally and tamely ramified, because p is an odd prime. We see by Serre [2] that $\boldsymbol{Q}_p$ has four totally and tamely ramified extensions of degree 4. Therefore we see that $\boldsymbol{Q}_p$ has at most one D_4-extension. In the case $p \equiv 1 \bmod 4$, we see that $\boldsymbol{Q}_p$ has no D_4-extension, because $\boldsymbol{Q}_p(\sqrt[4]{p})/\boldsymbol{Q}_p$ is a totally and tamely ramified Galois extension of degree 4. In the case $p \equiv 3 \bmod 4$, we see that $\boldsymbol{Q}_p(\sqrt{-1}, \sqrt[4]{p})/\boldsymbol{Q}_p$ is a D_4-extension.

2. The case $p = 2$. Let $L/\boldsymbol{Q}_2$ be a Galois extension of degree 8. We see that the Galois group of $L/\boldsymbol{Q}_2$ is isomorphic to D_4 if and only if L contains an intermediate field of degree 4 which is not a Galois extension over $\boldsymbol{Q}_2$. Thus it is sufficient to construct all quadratic extensions over K_i which are not Galois extensions over $\boldsymbol{Q}_2$, where K_i is a quadratic extension over $\boldsymbol{Q}_2$. We get $M_i = K_i(\sqrt{\varepsilon})$ for an $\varepsilon \in K_i^\times$ such that $\varepsilon^\sigma/\varepsilon$ is not square in K_i for the generator σ of the Galois group of $K_i/\boldsymbol{Q}_2$. We see $M_i' = K_i(\sqrt{\varepsilon^\sigma})$, $L = K_i(\sqrt{\varepsilon}, \sqrt{\varepsilon^\sigma})$ and $M = K_i(\sqrt{\varepsilon\varepsilon^\sigma})$. So we examine a representative system of $K_i^\times/(K_i^\times)^2$. We take all pairs $\{\varepsilon, \varepsilon^\sigma\}$ of the system such that $\varepsilon \not\equiv \varepsilon^\sigma \bmod (K_i^\times)^2$. By putting $L = K_i(\sqrt{\varepsilon}, \sqrt{\varepsilon^\sigma})$, we get all D_4-extensions $L/\boldsymbol{Q}_2$.

It is well-known that all quadratic extensions over $\boldsymbol{Q}_2$ are $\boldsymbol{Q}_2(\sqrt{-1})$, $\boldsymbol{Q}_2(\sqrt{-5})$, $\boldsymbol{Q}_2(\sqrt{5})$, $\boldsymbol{Q}_2(\sqrt{2})$, $\boldsymbol{Q}_2(\sqrt{-2})$, $\boldsymbol{Q}_2(\sqrt{10})$ and $\boldsymbol{Q}_2(\sqrt{-10})$. Next we examine all possible cases for K_i. We denote by $\mathfrak{o}$ the ring of integers of K_i.

2-1. $K_i = \boldsymbol{Q}_2(\sqrt{m})$ for$m = \pm 2, \pm 10$.

In this case, $\mathfrak{p} = (\sqrt{m})$ is the prime ideal of K_i. We see that all elements of $1 + \mathfrak{p}^5$ are square in K_i. Therefore we get $K_i^\times/(K_i^\times)^2 \cong (\langle\sqrt{m}\rangle/\langle m\rangle) \times (\mathfrak{o}^\times/\langle 1 + m + 2\sqrt{m}, 1 + \mathfrak{p}^5\rangle)$ by $1 + m + 2\sqrt{m} = (1 + \sqrt{m})^2$. For constructing D_4-extensions, it is sufficient to examine elements ε and $\varepsilon\sqrt{m}$, where $\varepsilon = a + b\sqrt{m}$ for $a = 1,3,5,7$ and $b = 0,1,2,3$. We take ε(resp. $\varepsilon\sqrt{m}$) such that ε, ε^σ, $\varepsilon(1 + m + 2\sqrt{m})$ and $\varepsilon^\sigma(1 + m + 2\sqrt{m})$ (resp. ε, $-\varepsilon^\sigma$, $\varepsilon(1 + m + 2\sqrt{m})$ and $-\varepsilon^\sigma(1 + m + 2\sqrt{m})$) are different modulo $\mathfrak{p}^5$ each other. Then we get D_4-extensions as follows:

$A_1 = \{\boldsymbol{Q}_2(\sqrt{1+\sqrt{2}}, \sqrt{-1}), \boldsymbol{Q}_2(\sqrt{3+\sqrt{2}}, \sqrt{-1}),$
$\boldsymbol{Q}_2(\sqrt{\sqrt{2}}, \sqrt{-1}), \boldsymbol{Q}_2(\sqrt{3\sqrt{2}}, \sqrt{-1})\}$,

$A_2 = \{\boldsymbol{Q}_2(\sqrt{\sqrt{-2}}, \sqrt{-1}), \boldsymbol{Q}_2(\sqrt{3\sqrt{-2}}, \sqrt{-1})\}$,

$B_1 = \{\boldsymbol{Q}_2(\sqrt{1+\sqrt{-2}}, \sqrt{-5}), \boldsymbol{Q}_2(\sqrt{5+\sqrt{-2}},$
$\sqrt{-5})\}$,

$C_1 = \{\boldsymbol{Q}_2(\sqrt{\sqrt{-2}(1+\sqrt{-2})}, \sqrt{5}),$
$\boldsymbol{Q}_2(\sqrt{\sqrt{-2}(1+3\sqrt{-2})}, \sqrt{5})\}$,

$C_2 = \{\boldsymbol{Q}_2(\sqrt{\sqrt{-10}(1+\sqrt{-10})}, \sqrt{5}),$