Comm. Korean Math. Soc. **11** (1996), No. 3, pp. 563–568

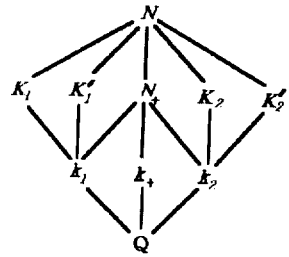
RAMIFICATION OF PRIME IDEALS IN THE DIHEDRAL OCTIC EXTENSION OVER Q

SOUN-HI KWON

ABSTRACT. In this paper we study the ramification of prime ideals in the dihedral octic extension N over Q and estimate the possible discriminants of the octic number field N.

Let N be a dihedral octic number field, G the Galois group of the extension N/Q. We write $G =< r, s; r^4 = s^2 = I, srs = r^3 >$. We have the following lattice of subfields of N, where

$$
\begin{aligned}
&Gal(N/N_+) = \{I, r^2\},\\
&Gal(N/k_+) = \{I, r, r^2, r^3\},\\
&Gal(N/K_1) = \{I, s\},\\
&Gal(N/K_1') = \{I, sr^2\} = r\{I, s\}r^{-1},\\
&Gal(N/K_2) = \{I, sr\},\\
&Gal(N/K_2') = \{I, sr^3\} = r\{I, sr\}r^{-1},\\
&Gal(N/k_1) = \{I, s, r^2, sr^2\},\\
&Gal(N/k_2) = \{I, sr, r^2, sr^3\},
\end{aligned}
$$



K_1, K_1', K_2', K_2' are non-normal quartic subfields of N. K_1 and K_1' are conjugates each other over Q. K_2 and K_2' are conjugates each other over Q. G has five conjugacy classes : $C_1 = \{I\}, C_2 = \{r^2\}, C_3 = \{r, r^3\}, C_4 = \{s, sr^2\}$ and $C_5 = \{sr, sr^3\}$. Hence, there are five complex irreducible characters of G. Let $\Psi_i, 1 \leq i \leq 4$ be the four characters of degree one and Ψ_0 be the character of degree 2. As in [1, pp. 52-52], the irreducible characters of G are as in Table 1.

Received December 23, 1995. Revised March 11, 1996.

1991 AMS Subject Classification: 11R21, 11R32.

Key words and phrases: decomposition group of prime ideal, inertia group and different of an extension.

Table 1

	C_1	C_2	C_3	C_4	C_5
Ψ_0	2	-2	0	0	0
Ψ_1	1	1	1	1	1
Ψ_2	1	1	1	-1	-1
Ψ_3	1	1	-1	1	-1
Ψ_4	1	1	-1	-1	1

Let M be an intermediate field between N and $\mathbf{Q}$. $H = Gal(N/M)$. Let χ_0 be the principal character of H and let $\chi_M = \chi_0^*$ be the induced character of G. Hence

$$\chi_M(g) = \frac{1}{\sharp H} \sharp\{x \in G : g \in x^{-1}Hx\}, \ g \in G.$$

Using this fact, we can obtain the induced characters of G as in Table 2. ([2])

Table 2

	C_1	C_2	C_3	C_4	C_5
χ_N	8	0	0	0	0
χ_{N_+}	4	4	0	0	0
χ_{k_+}	2	2	2	0	0
χ_{K_1}	4	0	0	2	0
χ_{k_1}	2	2	0	2	0
χ_{K_2}	4	0	0	0	2
χ_{k_2}	2	2	0	0	2
χ_Q	1	1	1	1	1

Hence, we have

$$\chi_N = 2\Psi_0 + \Psi_1 + \Psi_2 + \Psi_3 + \Psi_4,$$
$$\chi_{N_+} = \Psi_1 + \Psi_2 + \Psi_3 + \Psi_4,$$
$$\chi_{k_+} = \Psi_1 + \Psi_2,$$
$$\chi_{K_1} = \Psi_0 + \Psi_1 + \Psi_3, \qquad \chi_{K_2} = \Psi_0 + \Psi_1 + \Psi_4.$$

$\chi_{k_1} = \Psi_1 + \Psi_3, \qquad \chi_{k_2} = \Psi_1, +\Psi_4, \qquad \chi_Q = \Psi_1.$

For an intermediate field M, let d_M be the absolute discriminant of $M/Q, N_{M/Q}$ the norm. For $Q \subset L \subset M \subset N$, let $\delta_{M/L}$ be the discriminant of the extension M/L. For a character Ψ_i we denote by $F(\Psi_i)$ the conductor of Ψ_i.

PROPOSITION 1. *We have* $d_{N_+} = d_{k_+} d_{k_1} d_{k_2}$, $d_N = d_{N_+} F(\Psi_0)^2$, $d_{K_1} = F(\Psi_0) d_{k_1}$, $d_{K_2} = F(\Psi_0) d_{k_2}$. *In particular*, $\frac{d_{K_1}}{d_{k_1}} = \frac{d_{K_2}}{d_{k_2}} = F(\Psi_0)$.

PROOF. By Prop. 6 §3. chapter V in [3], we have

$d_N = F(\Psi_0)^2 F(\Psi_1) F(\Psi_2) F(\Psi_3) F(\Psi_4),$
$d_{N_+} = F(\Psi_1) F(\Psi_2) F(\Psi_3) F(\Psi_4),$
$d_{k_+} = F(\Psi_1) F(\Psi_2),$
$d_{k_2} = F(\Psi_1) F(\Psi_4), \qquad d_{k_1} = F(\Psi_1) F(\Psi_3)$
$d_{K_1} = F(\Psi_0) F(\Psi_1) F(\Psi_3),$
$d_{K_2} = F(\Psi_0) F(\Psi_1) F(\Psi_4)$ and $F(\Psi_1) = (1)$. □

COROLLARY 2. *We have*

$$N_{k_1/Q}(\delta_{K_1/k_1})^2 = \frac{d_{k_+} d_{k_2}}{d_{k_1}} N_{N_+/Q}(\delta_{N/N_+}).$$

PROOF. $d_{K_1} = {d_{k_1}}^2 N_{k_1/Q}(\delta_{K_1/k_1}) = d_{k_1} F(\Psi_0) = d_{k_1} \sqrt{\frac{d_N}{d_{N_+}}}$
$d_N = {d_{N_+}}^2 N_{N_+/Q}(\delta_{N/N_+})$. □

REMARK. d_{N_+} and $N_{N_+/Q}(\delta_{N/N_+})$ are squares in $\mathbb{Z}$.

Let Z_N be the ring of algebraic integres in N. Let p be a prime ideal of N lying above a prime p. $G_{-1}(p)$ the decomposition group of p, $G_0(p)$ the inertia group of p, and $G_i(p)$ $i-th$ ramification group of p, $i \geq 0$, that is,

$G_{-1}(p) = \{\sigma \in G | \sigma p = p\}$
$G_0(p) = \{\sigma \in G_{-1} | \sigma(x) \equiv x \mod p \text{ for all } x \in Z_N\}$
$G_i(p) = \{\sigma \in G_{-1} | \sigma(x) \equiv x \mod p^{i+1} \text{ for all } x \in Z_N\}$

Let e be the ramification index of p, f the degree of the residue class field.

THEOREM 3. *The ramification groups* $G_i = G_i(p)$, $i = -1, 0, 1, \cdots$, *have the following properties*

(1) $|G_{-1}| = ef$ *and* $|G_0| = e$.
(2) *For* $i \geq 0$, G_i *is a normal subgroup of* G_{-1}.
(3) G_{-1}/G_0 *is a cyclic group.*
(4) G_0/G_1 *is cyclic and* $(\frac{|G_0|}{|G_1|}, p) = 1$. *Thus* G_1 *is a* $p-$*Sylow subgroup of* G_0.
(5) *For* $i \geq 1$, G_i/G_{i+1} *is an elementary abelian* $p-$*group.*
(6) *The integers* $i \geq 1$ *such that* $G_i \neq G_{i+1}$ *are all congruent one another mod* p.

PROOF. See [3] chapter IV. □

Let $v_p(x)$ be the valuation of x at p.

PROPOSITION 4. *If* $D_{N/Q}$ *denotes the different of* N/Q, *then*

$$v_p(D_{N/Q}) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

PROOF. See Prop. 4 §1 chapter IV. in [3]. □

PROPOSITION 5. *If* $p \neq 2$ *and* $G_{-1} = Gal(N/Q)$, *then* $G_0 = Gal(N/k_+)$, $G_1 = (I)$ *and* $v_p(d_N) = 6$.

PROOF. By th. 3 iii), $G_0 = Gal(N/k_+)$ or $G_0 = Gal(N/N_+)$.

Suppose $G_0 = Gal(N/N_+)$. Then the factor group G_{-1}/G_0 is not cyclic.

Hence $G_0 = Gal(N/k_+)$ and $f = 2$. Now $v_p(d_N) = 6$ follows from $f = 2$. □

PROPOSITION 6.

(1) *If* $p \neq 2$ *and* $G_{-1} = Gal(N/k_1)$, *then* $G_0 = Gal(N/K_1)$, $G_0 = Gal(N/K_1')$ *or* $G_0 = Gal(N/N_+)$.
(2) *If* $p \neq 2$ *and* $G_{-1} = Gal(N/k_2)$, *then* $G_0 = Gal(N/K_2), G_0 = Gal(N/K_2')$ *or* $G_0 = Gal(N/N_+)$.

In these two cases, $v_p(d_N) = 4$.

PROOF. $G_{-1} \cong Z_2 \oplus Z_2$ and $G_1 = (I)$.
Thus the assertion is immediate.

PROPOSITION 7. *If* $p \neq 2$, $G_{-1} = Gal(N/k_+)$, *then*
$G_0 = Gal(N/N_+)$ *with* $v_p(d_N) = 4$,
$G_0 = Gal(N/k_+)$ *with* $v_p(d_N) = 6$,
or $G_0 = (I)$.

PROOF. If $G_0 = Gal(N/k_+)$, then we have $e = 4$, $f = 1$ and $v_p(D_{N/Q}) = 3$.
Thus $v_p(d_N) = 6$.
If $G_0 = Gal(N/N_+)$, then $e = 2$, $f = 2$, $v_p(D_{N/q}) = 1$ and $v_p(d_N) = 4$. □

PROPOSITION 8. *If* $p = 2$ *and* $G_{-1} = Gal(N/Q)$, *then the filtration of the* G_i *is one of the following :*

(1) $G_{-1} = G_0 = G_1 = Gal(N/Q)$ and $v_2(d_N) \geq 20$,
(2) $G_0 = G_1 = Gal(N/k_+)$ and $v_2(d_N) \geq 16$,
(3) $G_0 = G_1 = Gal(N/k_1)$ and $v_2(d_N) \geq 12$,
(4) $G_0 = G_1 = Gal(N/k_2)$ and $v_2(d_N) \geq 12$.

PROOF. If $G_{-1} = G_0$, then we must have $G_0 = G_1$, $G_2 \neq (I)$ and $G_2 = G_3$. Note that 2 is totally ramified in N/Q and that $Gal(N/Q)$ is a transitive even subgroup of S_8 , symmetric group of degree 8, i.e. $Gal(N/Q) \subset A_8$, alternating group of degree 8. Thus $v_2(d_{N_+}) = 8$ and $v_2(d_N) \geq 16 + 1 + 1 + 1 + 1$. ii) iii) and iv) It suffices to remark that the only normal subgroups of $Gal(N/Q)$ with cyclic factor group are $Gal(N/k_+), Gal(N/k_1)$ and $Gal(N/k_2)$.
Note that $G_1 = G_0$. If $G_0 = Gal(N/k_+)$, then $G_2 \neq (I)$, $G_2 = G_3$ and $v_2(d_N) \geq 2 \times (3+3+1+1)$. If $G_0 = Gal(N/k_1)$ or $G_0 = Gal(N/k_2)$, then $v_2 \geq 2 \times (3+3)$. □

PROPOSITION 9.

(1) *If* $p = 2$ *and* $G_{-1} = Gal(N/k_1)$,
then $G_{-1} = G_0 = G_1$ *with* $v_2(d_N) \geq 12$,
$G_0 = G_1 = Gal(N/N_+)$ *with* $v_2(d_N) \geq 8$,
$G_0 = G_1 = Gal(N/K_1)$ *with* $v_2(d_N) \geq 8$,

or $G_0 = G_1 = Gal(N/K_1')$ with $v_2(d_N) \geq 8$.

(2) If $p = 2$ and $G_{-1} = Gal(N/k_+)$,
then $G_{-1} = G_0 = G_1$, $G_2 \neq (I)$, $G_2 = G_3$ with $v_2(d_N) \geq 16$,
$G_0 = G_1 = Gal(N/N_+)$ with $v_2(d_N) \geq 8$,
or $G_0 = (I)$ with $v_2(d_N) = 0$.

PROOF. By Theorem 3, the assertion is obvious. □

PROPOSITION 10. *If $p = 2$ and $G_{-1} = G_0$ is subgroup of order 2 of $Gal(N/Q)$, then $v_2(d_N) \geq 8$.*

PROOF. By theorem 3. iv), we have $G_1 = G_0$ and $v_2(d_N) \geq 4 \times (1+1)$. □

References

1. J. -P. Serre, *Linear Representations of Finite groups*, Springer-Verlag, 1977.
2. S. Louboutin, *On the class number one problem for non-quartic CM-fields*, Tohoku Math. J. **46** (1994), 1-12.
3. J. -P. Serre, *Local fields*, Springer-Verlag, 1979.

Department of Mathematics Education
Korea University
136-701 Seoul, Korea