Commun. Korean Math. Soc. **20** (2005), No. 4, pp. 641–644

A GALOIS EXTENSION WITH GALOIS GROUP DIHEDRAL GROUP OR GENERALIZED QUATERNION GROUP

Yoon Sung Hwang

Abstract. Let L/F be a Galois quadratic extension such that F contains a primitive n-th root of 1. Let $N = L(\alpha^{\frac{1}{n}})$ where $\alpha \in L^*$. We show that if $N_{L/F}(\alpha) \in L^n \cap F$, and $[N : L] = m$, then $G(N/F) \cong D_m$ or generalized quaternion group whether $N_{L/F}(\alpha) \in F^n$ or $\notin F^n$, respectively.

There has been much work on the realization of groups of Galois groups. This is still a very active topic of research (See, e.g. [3] and [6]). The work here can be thought as the following problem : Given a Galois field extension L/F, when can we find a field $M \supseteq L$ Galois over F with $G(M/F)$ a given group that has $G(L/F)$ as a homomorphic image. Now we start with lemma.

Lemma 1. *Let m, n be positive integers with $m|2n$ and $n > 2$. Let $G =< \tau, \sigma >$ be a group given by the relations $\tau^n = 1$ $(o(\tau) = n)$, $\sigma^m = 1$ $(o(\sigma) = m)$, $\sigma\tau = \tau^{-1}\sigma$, and $\sigma^2 = \tau^{\frac{2n}{m}}$. Then,*

(1) $|G| = 2n$.
(2) $< \tau >$ *is a normal subgroup of* G *of index 2.*
(3) $m = 2$ or 4, *i.e.,* $G \cong D_n$ *or generalized quaternion group of order* $2n$.

Proof. First we check that σ^2 and $\tau^{\frac{2n}{m}}$ have the same order. (If m is even, then $o(\sigma^2) = \frac{m}{2} = o(\tau^{\frac{2n}{m}})$, and if m is odd, then $o(\sigma^2) = m = o(\tau^{\frac{2n}{m}})$.) The relations show every element of G has the form $\tau^i\sigma^j$ where $0 \le i \le n-1$ and $0 \le j \le 1$. So $|G| \le 2n$. But $\sigma \notin < \tau >$ since σ and τ do not commute. (Otherwise, $\tau = \tau^{-1}$ but $o(\tau) > 2$.) Therefore, $|G| = 2n$. $< \tau >$ is a normal subgroup of G since $\sigma\tau\sigma^{-1} = \tau^{-1}$. Note

Received January 26, 2005.
2000 Mathematics Subject Classification: 12F10.
Key words and phrases: Galois extension, Kummer extension.
This author was supported by Korea University Grant.

that $m > 1$ is a consequence of the relations since $m = 1$ implies $\sigma = 1$, $\tau^2 = 1$, and $n \leq 2$, a contradiction to assumption $n > 2$. Since $\tau^{\frac{2n}{m}} = \sigma^2$, $\sigma\tau^{\frac{2n}{m}}\sigma^{-1} = \tau^{\frac{2n}{m}}$. But $\sigma\tau^{\frac{2n}{m}}\sigma^{-1} = (\sigma\tau\sigma^{-1})^{\frac{2n}{m}} = \tau^{\frac{-2n}{m}}$, so $\tau^{\frac{2n}{m}} = \tau^{\frac{-2n}{m}}$ and $\tau^{\frac{4n}{m}} = 1$. Hence $n|\frac{n}{m}$ and $m|4$. Therefore, $m = 2,\ 4$. □

Let N/F be a Galois extension with Galois group $G(N/F) = G$ where G is the group constructed above. Let L be the fixed field of $< \tau >$. Assume *char* $F \not| n$ and assume that F contains a primitive n-th root of 1. Then $N = L(\alpha^{\frac{1}{n}})$ for some $\alpha \in L^*$ since N/L is a cyclic extension of degree n. Here, $\alpha^{\frac{1}{n}}$ denotes a fixed n-th root of α in N. We have $\sigma|_L$ has order 2 since $\sigma \notin < \tau >$. Note that $N = L(\alpha^{\frac{1}{n}}) = L(\sigma(\alpha)^{\frac{1}{n}})$ since N/F is a Galois extension. Kummer theory implies $\sigma(\alpha) = \alpha^j\beta^n$ for some $\beta \in L$ and $gcd(j, n) = 1$. (cf. [2, Th.8.24, p.497])

Since $G(N/L) =< \tau >$, $\tau(\alpha^{\frac{1}{n}}) = \zeta^i\alpha^{\frac{1}{n}}$ where ζ is a primitive n-th root of 1 and $gcd(i, n) = 1$. By relabeling, we may assume $i = 1$. Thus $\tau(\alpha^{\frac{1}{n}}) = \zeta\alpha^{\frac{1}{n}}$. Since $\sigma(\alpha^{\frac{1}{n}})$, $\alpha^{\frac{j}{n}}\beta$ are roots of $x^n - \sigma(\alpha)$, $\sigma(\alpha^{\frac{1}{n}}) = \alpha^{\frac{j}{n}}\beta\zeta^i$ for some i, $0 \leq i \leq n-1$. We may replace β by $\beta\zeta^i$, since $\beta^n = (\beta\zeta^i)^n$. Thus, we may assume $\sigma(\alpha^{\frac{1}{n}}) = \alpha^{\frac{j}{n}}\beta$. Now we consider the equation $\sigma\tau(\alpha^{\frac{1}{n}}) = \tau^{-1}\sigma(\alpha^{\frac{1}{n}})$; $\sigma\tau(\alpha^{\frac{1}{n}}) = \sigma(\zeta\alpha^{\frac{1}{n}}) = \zeta\alpha^{\frac{j}{n}}\beta$, and $\tau^{-1}\sigma(\alpha^{\frac{1}{n}}) = \tau^{-1}(\alpha^{\frac{j}{n}}\beta) = \beta\tau^{-1}(\alpha^{\frac{j}{n}}) = \beta\tau^{-1}(\alpha^{\frac{1}{n}})^j = \beta(\zeta^{-1}\alpha^{\frac{1}{n}})^j = \beta\zeta^{-j}\alpha^{\frac{j}{n}}$. Thus, $\zeta = \zeta^{-j}$ and so $j \equiv -1 \mod n$. We may assume $j = -1$ and conclude $\sigma(\alpha) = \alpha^{-1}\beta^n$ for a possibly different $\beta \in L$. Therefore, $N_{L/F}(\alpha) = \alpha\sigma(\alpha) = \beta^n \in L^n \cap F$, where $N_{L/F}$ is the norm map.

LEMMA 2. *Let L/F be any Galois quadratic extension and let $\sigma \in G(L/F)$, $\sigma \neq id$. Assume F contains all n-th roots of 1. Then*

$$L^n \cap F = \begin{cases} F^n \cup a^{\frac{n}{2}}F^n & \text{if } n \text{ is even and } L = F(\sqrt{a}), \text{ where } a \in F, \\ F^n & \text{if } n \text{ is even and char } F = 2, \\ F^n & \text{if } n \text{ is odd.} \end{cases}$$

PROOF. Clearly "$\supseteq$" holds. Let $\lambda \in L$, and $\lambda^n \in L^n \cap F$. Then $\sigma(\lambda^n) = \lambda^n$ and $\sigma(\lambda) = \zeta\lambda$ where ζ is some n-th root of 1. Since $\frac{\sigma(\lambda)}{\lambda} \in F$, we have $\frac{\sigma(\lambda)}{\lambda} = \sigma\left(\frac{\sigma(\lambda)}{\lambda}\right) = \frac{\sigma^2(\lambda)}{\sigma(\lambda)} = \frac{\lambda}{\sigma(\lambda)}$. Thus $\lambda^2 = \sigma(\lambda)^2 = \sigma(\lambda^2)$ and so $\lambda^2 \in F$. If $\lambda \in F$, then $\lambda^n \in F^n$. If $\lambda \notin F$, then $L = F(\sqrt{b})$ where $\lambda^2 = b \in F$. So, *char* $F \neq 2$. We must have n even for if n is odd then $\lambda^2, \lambda^n \in F$ would imply $\lambda \in F$. Now $\lambda^n = (\lambda^2)^{\frac{n}{2}} = b^{\frac{n}{2}} \in b^{\frac{n}{2}}F^n$. Suppose L also equals $F(\sqrt{a})$. Then $\frac{a}{b} \in F^2$ and $\frac{a^{\frac{n}{2}}}{b^{\frac{n}{2}}} \in F^n$. This implies $a^{\frac{n}{2}}F^n = b^{\frac{n}{2}}F^n$ and the proof is complete. □

Assume n is even and $L = F(\sqrt{a})$, the fixed field of $< \tau >$ in $N = L(\alpha^{\frac{1}{n}})$ given in after Lemma 1. We now determine when $N_{N/F}(\alpha) \in F^n$.

PROPOSITION 3. *If n is even and the fixed field of $< \tau >$, $L = F(\sqrt{a})$, then $N_{N/F}(\alpha) \in F^n$ if and only if $m = 2$.*

PROOF. $\sigma^2(\alpha^{\frac{1}{n}}) = \sigma(\alpha^{-\frac{1}{n}}\beta) = \sigma(\alpha^{-\frac{1}{n}})\sigma(\beta) = \alpha^{\frac{1}{n}}\beta^{-1}\sigma(\beta)$. So, $m = 2$ iff $\sigma^2 = id_N$ iff $\sigma^2(\alpha^{\frac{1}{n}}) = \alpha^{\frac{1}{n}}$ (since $N = L(\alpha^{\frac{1}{n}})$ and $\sigma^2|_L = id_L$) iff $\beta^{-1}\sigma(\beta) = 1$, i.e., $\sigma(\beta) = \beta$ iff $\beta \in F$ (since $\beta \in L$ and $\sigma|_L \neq id_L$) iff $\beta^n \in F^n$ (since F contains all n-th roots of 1) iff $N_{L/F}(\alpha) \in F^n$ (since $N_{L/F}(\alpha) = \beta^n$). □

REMARK 1. The above proposition can be proved by computing the corestriction of a symbol algebra $(\alpha,\ x;\ L(x))_n$ from $L(x)$ to $F(x)$ where $L(x)$ is the rational function field over F, using the formula of corestriction given in [1, (1.3)] and Projection Formula ([1, Prop.1.4] or [4, Th.3.1])

Now, we are ready to give our main theorem.

THEOREM 4. *Let L/F be a Galois quadratic extension of fields such that F contains a primitive n-th root of 1. Let $\alpha \in L^*$ and assume $N_{L/F}(\alpha) \in L^n \cap F$. Let $N = L(\alpha^{\frac{1}{n}})$ where $\alpha^{\frac{1}{n}}$ denotes a fixed n-th root of α. Let $m = [N : L]$. Then N/F is a Galois extension and*
(i) *$G(N/F) \cong D_m$ if $N_{L/F}(\alpha) \in F^n$,*
(ii) *$G(N/F) \cong$ generalized quaternion group of order $2m$ if $N_{L/F}(\alpha) \notin F^n$, and m is even.*

PROOF. Let $G(N/F) = \{\mathrm{id_L},\ \sigma\}$. By assumption, $\alpha\sigma(\alpha) = N_{L/F}(\alpha) = \beta^n$ for some $\beta \in L^*$. So $\sigma(\alpha) = \alpha^{-1}\beta^n$. By Kummer theory ([2, Th. 8.24, pp.497]) $L(\alpha^{\frac{1}{n}}) = L(\sigma(\alpha)^{\frac{1}{n}})$ and so N/F is a Galois extension as N is the composite of L and a splitting field of $(x^n - \alpha)(x^n - \sigma(\alpha))$ over F. Let $G = G(N/F)$. As L contains a primitive n-th root of 1, N/L is a cyclic extension. Let $G(N/L) =< \tau >$. Then $o(\tau) = m$. Denote an automorphism of N extending σ by σ, again. Then $\sigma(\alpha^{\frac{1}{n}}) = \alpha^{-\frac{1}{n}}\beta\zeta$ where $\zeta^n = 1$. As $\beta^n = (\beta\zeta)^n$, we can replace β by $\beta\zeta$ to assume $\sigma(\alpha^{\frac{1}{n}}) = \alpha^{-\frac{1}{n}}\beta$. Then $\sigma^2(\alpha^{\frac{1}{n}}) = \sigma(\alpha^{-\frac{1}{n}}\beta) = \sigma(\beta)\alpha^{\frac{1}{n}}\beta^{-1}$.

(i) If $N_{L/F}(\alpha) = \beta^n \in F^n$, then $\beta \in F$ as F contains a primitive n-th root of 1. It follows $\sigma^2(\alpha^{\frac{1}{n}}) = \alpha^{\frac{1}{n}}$. This implies $\sigma^2 = id_N$ as $N = L(\alpha^{\frac{1}{n}})$. As $\tau(\alpha^{\frac{1}{n}}) = \zeta_1\alpha^{\frac{1}{n}}$ for some primitive m-th root ζ_1 of 1 in F, $\sigma\tau(\alpha^{\frac{1}{n}}) = \zeta_1\sigma(\alpha^{\frac{1}{n}}) = \zeta_1\alpha^{-\frac{1}{n}}\beta = \tau^{-1}\sigma(\alpha^{\frac{1}{n}})$. Also, $\sigma\tau|_L = \tau^{-1}\sigma|_L$. So,

$\sigma\tau = \tau^{-1}\sigma$, $o(\sigma) = 2$, and $o(\tau) = m$. Hence $G(N/F) =<\tau, \sigma> \cong D_m$.
(ii) If $N_{L/F}(\alpha) = \beta^n \notin F^n$, then $\beta^n \in a^{\frac{n}{2}} F^n$ where $L = F(\sqrt{a})$ by Lemma 2 as $\beta^n = N_{L/F}(\alpha) \in L^n \cap F$. So $\beta \in \sqrt{a}F$, and $\sigma(\beta)\beta^{-1} = -1$. It follows $o(\sigma) = 4$. Also, $o(\tau) = m$, $\sigma\tau = \tau^{-1}\sigma$, and $\sigma^2 = \tau^{\frac{m}{2}}$ as $\sigma^2(\alpha^{\frac{1}{n}}) = -\alpha^{\frac{1}{n}} = \zeta_1^{\frac{m}{2}} \alpha^{\frac{1}{n}} = \tau^{\frac{m}{2}}(\alpha^{\frac{1}{n}})$ since m is even. Hence, $G(N/F) =<\tau, \sigma> \cong$ generalized quaternion group of order $2m$. □

Acknowledgements. We wish to thank David B. Leep for helpful suggestions.

References

[1] Y.-S. Hwang, *The corestrictions of valued division algebras of Henselian Fields I*, Pacific J. Math. **170** (1995), 53–81.
[2] N. Jacobson, *Basic Algebra II*, Freeman and Company, 1980.
[3] G. Maile and B. H. Matzat, *Inverse Galois Theory*, Springer, Berlin, 1999.
[4] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.
[5] J.-P. Tignol, *On the corestriction of central simple algebras*, Math. Z. **194** (1987), 267-274.
[6] H. Völklein, *Groups as Galois Groups: An Introduction*, Cambridge Univ. Press, Cambridge, England, 1996.

Department of Mathematics
Korea University
Seoul 136-701, Korea
E-mail: yhwang@korea.ac.kr