

# GALOIS GROUPS OF ORDER $2n$ THAT CONTAIN A CYCLIC SUBGROUP OF ORDER $n$

Y.-S. HWANG, DAVID B. LEEP, AND ADRIAN R. WADSWORTH

ABSTRACT. Let  $n$  be any integer with  $n > 1$ , and let  $F \subseteq L$  be fields such that  $[L : F] = 2$ ,  $L$  is Galois over  $F$ , and  $L$  contains a primitive  $n^{\text{th}}$  root of unity  $\zeta$ . For a cyclic Galois extension  $M = L(\alpha^{1/n})$  of  $L$  of degree  $n$  such that  $M$  is Galois over  $F$ , we determine, in terms of the action of  $\text{Gal}(L/F)$  on  $\alpha$  and  $\zeta$ , what group occurs as  $\text{Gal}(M/F)$ . The general case reduces to that where  $n = p^e$ , with  $p$  prime. For  $n = p^e$ , we give an explicit parametrization of those  $\alpha$  which lead to each possible group  $\text{Gal}(M/F)$ .

## 1. INTRODUCTION

Let  $F \subseteq L$  be fields with  $[L : F] = 2$  and  $L$  Galois over  $F$ , and let  $n > 1$  be a positive integer. Assume  $L$  contains a primitive  $n^{\text{th}}$  root of unity. Let  $M$  be a cyclic Galois field extension of  $L$  of degree  $n$ . So  $M = L(\alpha^{1/n})$  for some  $\alpha \in L^*$ , by Kummer theory. Let  $\text{Gal}(L/F) = \{\sigma, 1\}$ . It is easy to verify that  $M$  is Galois over  $F$  just when  $\sigma(\alpha) = \alpha^t \beta^n$  for some  $\beta \in L^*$  with  $t^2 \equiv 1 \pmod{n}$  (that is, the cyclic group  $\langle \alpha L^{*n} \rangle \subseteq L^*/L^{*n}$  is stable under the action of  $\text{Gal}(L/F)$ ). The goal of this paper is to describe explicitly in terms of  $\alpha$ ,  $\beta$ , and  $t$  what group arises for  $\text{Gal}(M/F)$ .

To do this, we first classify in § 2 the possible groups that can arise as  $\text{Gal}(M/F)$ . These are the groups of order  $2n$  containing a cyclic group of order  $n$ . There are too many of them for arbitrary  $n$  (the number is given in Proposition 2.7.) We show in § 3 that the general question of determining  $\text{Gal}(M/F)$  can be reduced to the same question when  $n$  is a prime power. When  $n = p^e$  with  $p$  an odd prime, there are just two groups: cyclic and dihedral. When  $n = 2^e$  with  $e \geq 3$  there are six groups: one cyclic, four semidirect products, and a generalized quaternion group. We give in Theorem 3.4 a general description of the group  $\text{Gal}(M/F)$  in terms of  $\alpha$ ,  $\beta$ , and  $t$ . Since we assume that the group  $\mu_n$  of  $n^{\text{th}}$  roots of unity lies in  $L$ , but not necessarily in  $F$ , we must take into account the action of  $\text{Gal}(L/F)$  on  $\mu_n$ . In order to make the determination of  $\text{Gal}(M/F)$  more explicit, we obtain in § 4 precise descriptions of the  $\alpha$  satisfying  $\sigma(\alpha) = \alpha^t \beta^n$ . This allows us in §§ 5 and 6 to pin down in detail the circumstances under which a given group arises.

There has been much work over the years on the realization of groups as Galois groups. This is still a very active topic of research (see, e.g., [V], [MM]). For

---

The first author was supported by BK-21 and a Korea University grant.

larger groups the question has often been whether the group can be realized at all over a given field. For small groups, there are criteria for exactly when the group appears as a Galois extension, see, e.g., [GSS]. For nonsimple groups one approach has been to examine the embedding problem: Given a Galois field extension  $L/F$ , when can we find a field  $M \supseteq L$  Galois over  $F$  with  $\text{Gal}(M/F)$  a given group that has  $\text{Gal}(L/F)$  as a homomorphic image. Most often in this approach  $M/L$  is of prime degree (as in [K], [GSS]). The work here can be thought of as analyzing an extension problem, but now with  $[L : F]$  as small as possible, and  $[M : L]$  arbitrarily large, but  $M$  cyclic Galois over  $L$ .

In the papers by Damey et. al. [D<sub>1</sub>], [D<sub>2</sub>], [DP], [DM], there is an examination of when dihedral and quaternion groups of 2-power order appear as Galois groups; the 2-power case of Proposition 5.2 below appears as Prop. 1 and Cor. 1 in [D<sub>1</sub>]. The focus in those papers is primarily on when a quaternion group can occur as a Galois group, particularly over an algebraic number field. Also, the paper by Jensen, [J], especially pp. 447–449, considers all four nonabelian groups of order  $2^{e+1}$  containing a cyclic subgroup of order  $2^e$ ; but, while Jensen is primarily interested in when the groups of order  $2^e$  are realizable over a given base field, we give a full classification of the fields  $M \supseteq L$  which yield these groups as  $\text{Gal}(M/F)$ , assuming  $L$  contains all  $2^{e\text{th}}$  roots of unity.

## 2. GROUPS OF ORDER $2n$ THAT CONTAIN A CYCLIC SUBGROUP OF ORDER $n$

In this section we classify groups of order  $2n$  that contain a cyclic subgroup of order  $n$ . When  $n$  is a power of 2, this classification is well-known. A good reference for this case is [G], pp. 191-193. The general case of describing finite metacyclic groups has been considered in [B].

**Proposition 2.1.** *Let  $G$  be a group of order  $2n$  which contains a cyclic subgroup of order  $n$ . Then there exist  $\tau, \sigma \in G$  and nonnegative integers  $j, l$  such that  $G = \langle \tau, \sigma \rangle$  and*

1.  $|\tau| = n, \sigma \notin \langle \tau \rangle,$
2.  $\sigma\tau\sigma^{-1} = \tau^j, \sigma^2 = \tau^l,$
3.  $j^2 \equiv 1 \pmod{n}$  and  $l(j-1) \equiv 0 \pmod{n}.$

*Proof.* Let  $\tau$  be an element of order  $n$  and let  $\sigma \in G$ , but  $\sigma \notin \langle \tau \rangle$ . Then  $G = \langle \tau, \sigma \rangle$  and  $\langle \tau \rangle \triangleleft G$ . Thus  $\sigma\tau\sigma^{-1} = \tau^j$  for some  $j \geq 0$ , and  $\sigma^2 \in \langle \tau \rangle$  since  $G/\langle \tau \rangle$  has order 2. Let  $\sigma^2 = \tau^l$ , where  $0 \leq l \leq n-1$ . Since

$$\tau = \sigma^2\tau\sigma^{-2} = \sigma(\sigma\tau\sigma^{-1})\sigma^{-1} = \sigma\tau^j\sigma^{-1} = (\sigma\tau\sigma^{-1})^j = \tau^{j^2},$$

it follows  $j^2 \equiv 1 \pmod{n}$ . Since

$$\tau^l = \sigma^2 = \sigma\tau^l\sigma^{-1} = (\sigma\tau\sigma^{-1})^l = (\tau^j)^l = \tau^{jl},$$

it follows  $jl \equiv l \pmod{n}$  and thus  $l(j-1) \equiv 0 \pmod{n}$ . □

**Definition 2.2.** Let  $(G, j, l)$  denote a group of order  $2n$  as described in Proposition 2.1. We always assume that  $j$  and  $l$  satisfy the conditions in Proposition 2.1(3).

For each ordered pair  $(j, l) \bmod n$  satisfying condition (3) of Proposition 2.1, there does in fact exist a group  $G$  as in Proposition 2.1 with such an ordered pair  $(j, l)$ . A quick construction of such a group is to take any field  $k$  containing a primitive  $n^{\text{th}}$  root of unity  $\zeta_n$ , and let  $G$  be the subgroup of  $GL_2(k)$  generated by  $\tau = \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^j \end{pmatrix}$  and  $\sigma = \begin{pmatrix} 0 & 1 \\ \zeta_n^l & 0 \end{pmatrix}$ .

The groups  $(G, j, l)$  are clearly determined up to isomorphism by  $j$  and  $l \bmod n$ , but different values of  $l$  can yield isomorphic groups. In the rest of this section, we will determine the isomorphism classes of the  $(G, j, l)$ . Let us note immediately the obvious isomorphisms arising from different choices of generators of  $(G, j, l)$ .

*Remark 2.3.* If for the group  $(G, j, l)$  described in Proposition 2.1 we replace the generator  $\sigma$  by  $\sigma' = \sigma\tau^k$ , for any integer  $k$ , then  $\sigma'\tau(\sigma')^{-1} = \tau^j$  and  $(\sigma')^2 = \tau^{l'}$ , where  $l' = k(j+1) + l$ . Of course also,  $\tau^l = \tau^{sn+l}$  for any integer  $s$ . Hence,  $(G, j, l) \cong (G, j, l')$  whenever  $l' = k(j+1) + sn + l$ , i.e., whenever  $l' \equiv l \pmod{\gcd(j+1, n)}$ . On the other hand, if we take another generator  $\tilde{\tau}$  of  $\langle \tau \rangle$ , say  $\tau = (\tilde{\tau})^u$ , where  $\gcd(u, n) = 1$ , then  $\sigma\tilde{\tau}\sigma^{-1} = (\tilde{\tau})^j$  and  $\sigma^2 = (\tilde{\tau})^{\tilde{l}}$ , where  $\tilde{l} = ul$ . So,  $(G, j, l) \cong (G, j, \tilde{l})$ . But this is an isomorphism we already have, since in fact  $\tilde{l} \equiv l \pmod{\gcd(j+1, n)}$ . To see this congruence, let  $d = \gcd(j+1, n)$ . Then,  $d | n | (j-1)l$  and  $d | (j+1) | (j+1)l$ , so  $d | 2l$ . If  $u$  is odd, then  $d | (u-1)l = \tilde{l} - l$ . If  $u$  is even, then  $n$  must be odd, so  $d$  is odd. Then  $d | 2l$  implies  $d | l$ ; likewise,  $d | \tilde{l}$ , so again  $d | (\tilde{l} - l)$ .

Let  $n = p_0^{e_0} p_1^{e_1} \cdots p_m^{e_m}$  be the prime decomposition of  $n$  where  $2 = p_0 < p_1 < \cdots < p_m$ ,  $m \geq 0$ ,  $e_0 \geq 0$ , and  $e_i \geq 1$  for all  $i \geq 1$ . Then, the Chinese Remainder Theorem shows,

$$j^2 \equiv 1 \pmod{n} \text{ if and only if } \begin{cases} j^2 \equiv 1 \pmod{2^{e_0}} \\ j^2 \equiv 1 \pmod{p_i^{e_i}}, & 1 \leq i \leq m. \end{cases}$$

If  $p_i$  is an odd prime, then  $j-1$  or  $j+1$  must be a unit of the ring  $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ , so

$$j^2 \equiv 1 \pmod{p_i^{e_i}} \text{ if and only if } j \equiv \pm 1 \pmod{p_i^{e_i}}.$$

For  $p_0 = 2$ , since  $j-1$  or  $j+1$  is not a multiple of 4,

$$j^2 \equiv 1 \pmod{2^{e_0}} \text{ if and only if } \begin{cases} j \equiv 1 \pmod{2}, & \text{if } e_0 = 1, \\ j \equiv 1, 3 \pmod{4}, & \text{if } e_0 = 2, \\ j \equiv \pm 1, 2^{e_0-1} \pm 1 \pmod{2^{e_0}} & \text{if } e_0 \geq 3. \end{cases}$$

Now, fix  $j$  with  $j^2 \equiv 1 \pmod{n}$ . To see how many different groups  $(G, j, l)$  might exist for different choices of  $l$ , let  $A = \{l \in \mathbb{Z} \mid lj \equiv l \pmod{n}\}$  and  $B = \{l \in \mathbb{Z} \mid \gcd(j+1, n) \mid l\}$ .

**Lemma 2.4.** *With the notation above,*

1.  $B \subseteq A$  and  $|A/B| = \begin{cases} 2, & \text{if } n \text{ is even and } j \equiv \pm 1 \pmod{2^{e_0}}, \\ 1, & \text{otherwise.} \end{cases}$
2. *The number of isomorphism classes of groups  $(G, j, l)$  with given  $j$  (and  $n$ ) is at most  $|A/B|$ .*

*Proof.* (1) If  $l \in B$ , then  $l \equiv k(j+1) \pmod{n}$ , for some  $k \in \mathbb{Z}$ . Then,  $l(j-1) \equiv k(j+1)(j-1) \equiv 0 \pmod{n}$ , so  $l \in A$ . Thus,  $B \subseteq A$ .

Let  $d_1 = \gcd(j-1, n)$  and  $d_2 = \gcd(j+1, n)$ . Then,  $l \in A \Leftrightarrow n \mid l(j-1) \Leftrightarrow n/d_1 \mid l(j-1)/d_1 \Leftrightarrow n/d_1 \mid l$ . But,  $l \in B$  just when  $d_2 \mid l$ . So,  $A/B \cong (n/d_1)\mathbb{Z}/d_2\mathbb{Z}$ , and  $|A/B| = d_1 d_2 / n$ . For  $p_i$  an odd prime, we have  $p_i^{e_i} \mid n \mid (j^2 - 1)$ , but  $p_i$  cannot divide both  $j-1$  and  $j+1$ . Hence, the power of  $p_i$  in one of  $d_1, d_2$  is  $p_i^{e_i}$  and the power of  $p_i$  in the other is  $p_i^0$ . So,  $p_i \nmid (d_1 d_2 / n)$ . Thus, if  $n$  is odd, we have  $d_1 d_2 / n = 1$ . If  $n$  is even and  $j \equiv \pm 1 \pmod{2^{e_0}}$ , then the power of 2 in one of  $d_1, d_2$  is  $2^{e_0}$ , and the power of 2 in the other is 2; thus  $d_1 d_2 / n = 2$ . The only remaining case is  $e_0 \geq 3$  and  $j \equiv 2^{e_0-1} \pm 1$ . In this case, the power of 2 in one of  $d_1, d_2$  is  $2^{e_0-1}$ , and in the other is  $2^1$ ; then  $d_1 d_2 / n = 1$ .

(2) is clear from Proposition 2.1 and Remark 2.3.  $\square$

**Proposition 2.5.** *Let  $G = (G, j, l)$ .*

1.  *$G$  is abelian if and only if  $j \equiv 1 \pmod{n}$ . Suppose this occurs.*
  - (a) *If  $n$  is odd, then  $G \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2n\mathbb{Z}$ .*
  - (b) *If  $n$  is even, then*

$$G \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if } l \text{ is even,} \\ \mathbb{Z}/2n\mathbb{Z}, & \text{if } l \text{ is odd.} \end{cases}$$

2. *Suppose  $j \equiv -1 \pmod{n}$ .*
  - (a) *If  $n$  is odd, then  $l \equiv 0 \pmod{n}$  and  $G \cong D_n$ , the dihedral group of order  $2n$ .*
  - (b) *If  $n$  is even, then  $n/2 \mid l$  and*

$$G \cong \begin{cases} (G, -1, 0) \cong D_n, & \text{if } l \equiv 0 \pmod{n}, \\ (G, -1, n/2) = Q_n, & \text{if } l \equiv n/2 \pmod{n}, \end{cases}$$

where  $Q_n$  is the generalized quaternion group of order  $2n$ .

*Proof.* (1)  $G$  is abelian just when  $\tau$  and  $\sigma$  commute, which occurs if and only if  $j \equiv 1 \pmod{n}$ . Assume this holds. If  $n$  is odd, there is only one abelian group of order  $2n$  containing a cyclic group of order  $n$ . Now, suppose  $n$  is even. If  $l$  is even, then Remark 2.3 shows that  $G \cong (G, j, 0) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ; if  $l$  is odd, then  $G \cong (G, j, 1)$ , which is cyclic, as  $\sigma$  then has order  $2n$ .

(2) Assume  $j \equiv -1 \pmod n$ . the condition  $lj \equiv l \pmod n$  of Proposition 2.1 forces  $n \mid 2l$ . If  $n \mid l$ , then  $G \cong (G, -1, 0) \cong D_n$ . This always holds if  $n$  is odd. But, if  $n$  is even, we have  $n/2 \mid l$ . So, when  $n \nmid l$ , we have  $l \equiv n/2 \pmod n$ , and Remark 2.3 shows that  $G \cong (G, -1, n/2) \cong Q_n$ . (Our terminology in calling this a generalized quaternion group follows [CR], p. 23. Unlike some authors, we do not require a generalized quaternion group to be a 2-group.)  $\square$

We are going to show how the study of the groups described in Proposition 2.1 can be reduced to the case where  $n$  is a prime power. But let us first observe the (well-known) classification of these groups in the prime power situation. If  $n = p^e$ , where  $p$  is an odd prime, then  $j \equiv \pm 1 \pmod n$ , so the two possible groups  $(G, j, l)$  are described in Proposition 2.5; one is abelian, the other is dihedral. The classification for  $n$  a power of 2 is given in [G], Th. 4.3, p. 191 and Th. 4.4, p. 193: If  $n = 2^{e_0}$  with  $e_0 \leq 2$ , then again  $j \equiv \pm 1 \pmod n$ , and the possibilities for  $(G, j, l)$  are given in Proposition 2.5. If  $n = 2^{e_0}$  with  $e_0 \geq 3$ , there are two further groups besides the four given in Proposition 2.5. There is one group (and only one, by Lemma 2.4) with  $j \equiv 2^{e_0-1} + 1 \pmod{2^{e_0}}$ , which we write  $(G, 2^{e_0-1} + 1, 0)$  and is denoted  $M_{e_0+1}(2)$  in [G]. There is also exactly one group with  $j \equiv 2^{e_0-1} - 1 \pmod{2^{e_0}}$ , which we write  $(G, 2^{e_0-1} - 1, 0)$  and Gorenstein calls the semidihedral group  $S_{e_0+1}$ . He proves in [G], Th. 4.3(iii), p. 191 that no two of the four nonabelian groups with  $n = 2^{e_0}$  are isomorphic. This clearly applies to the two abelian groups, as well.

For any group  $G = (G, j, l) = \langle \tau, \sigma \rangle$  as in Proposition 2.1, let  $H_i$  be the unique subgroup of  $\langle \tau \rangle$  of order  $n/p_i^{e_i}$ ,  $0 \leq i \leq m$ . Then, each  $H_i \triangleleft G$  and  $|G/H_i| = 2p_i^{e_i}$ . Furthermore, if we let  $\bar{\tau} = \tau H_i$  and  $\bar{\sigma} = \sigma H_i$ , then  $G/H_i = \langle \bar{\tau}, \bar{\sigma} \rangle$ , where  $\langle \bar{\tau} \rangle$  is a cyclic subgroup of order  $p_i^{e_i}$ ,  $\bar{\sigma} \bar{\tau} \bar{\sigma}^{-1} = \bar{\tau}^j$ ,  $\bar{\sigma}^2 = \bar{\tau}^l$ , and  $\bar{\sigma} \notin \langle \bar{\tau} \rangle$ . Thus,  $G/H_i$  is a group of the type described in Proposition 2.1, with  $n$  replaced by  $n' = p_i^{e_i}$ . Note that every element of  $G$  of odd order has trivial image in  $G/\langle \tau \rangle$ , so must lie in  $\langle \tau \rangle$ . Thus,  $H_0$  consists of all the elements of  $G$  of odd order.

**Theorem 2.6.** *Suppose  $(G, \langle \tau \rangle, \sigma, j, l)$  and  $(G', \langle \tau' \rangle, \sigma', j', l')$  are each groups of order  $2n$  as in Proposition 2.1 and with all the previous notation. Assume  $(j, l)$  and  $(j', l')$  satisfy condition (3) in Proposition 2.1. Let  $H_i$  and  $H'_i$ ,  $0 \leq i \leq m$ , be the subgroups of  $\langle \tau \rangle$  and  $\langle \tau' \rangle$  defined before. Then the following statements are equivalent.*

1.  $G \cong G'$ .
2.  $j \equiv j' \pmod n$  and  $l \equiv l' \pmod{\gcd(j+1, n)}$ .
3.  $G/H_i \cong G'/H'_i$ ,  $0 \leq i \leq m$ .
4.  $j \equiv j' \pmod{n/2^{e_0}}$  and  $G/H_0 \cong G'/H'_0$ .

*Proof.* (2)  $\Rightarrow$  (1): This was done in Remark 2.3.

(1)  $\Rightarrow$  (4): Let  $\alpha: G \rightarrow G'$  be an isomorphism. Since  $H_0$  (resp.  $H'_0$ ) consists of all the elements of  $G$  (resp.  $G'$ ) of odd order,  $\alpha(H_0) = H'_0$ . Therefore,  $\alpha$  induces an isomorphism  $G/H_0 \cong G'/H'_0$ . Let  $h$  be any generator of  $H_0$ , and let  $h' = \alpha(h)$ ,

which generates  $H'_0$ . The conjugacy class of  $h$  in  $G$  is  $\{h, h^j\}$ , which must be mapped bijectively to the conjugacy class  $\{h', (h')^{j'}\}$  of  $h'$  in  $G'$ . If these classes contain only one element each, then  $j \equiv 1 \equiv j' \pmod{n/2^{e_0}}$ . If the classes contain two elements each, then  $(h')^{j'} = \alpha(h^j) = \alpha(h)^j = (h')^j$ , so again  $j \equiv j' \pmod{n/2^{e_0}}$ .

(3)  $\Leftrightarrow$  (4): For  $i \geq 1$ , since  $|\langle \tau \rangle / H_i|$  is a power of an odd prime, we have  $G/H_i$  is either abelian or dihedral. The first case occurs just when  $j \equiv 1 \pmod{p_i^{e_i}}$ , and the second just when  $j \equiv -1 \pmod{p_i^{e_i}}$ . Thus,  $G/H_i \cong G/H'_i$  if and only if  $j \equiv j' \pmod{p_i^{e_i}}$ . By the Chinese Remainder Theorem, this occurs for all  $i \geq 1$  if and only if  $j \equiv j' \pmod{n/2^{e_0}}$ .

(3)  $\Rightarrow$  (2): As observed above,  $G/H_i$  is a group of type  $(j, l)$  with  $n$  replaced by  $p_i^{e_i}$ . For  $p_i$  odd, we noted in the previous paragraph that  $G/H_i \cong G'/H'_i$  implies  $j \equiv j' \pmod{p_i^{e_i}}$ ; then Lemma 2.4 shows that the conditions  $lj \equiv l$  and  $l'j' \equiv l' \pmod{p_i^{e_i}}$  from Proposition 2.1 imply that  $l \equiv l' \pmod{\gcd(j+1, p_i^{e_i})}$ . For  $i = 0$ , [G], Th. 4.3(iii), p. 191, together with Proposition 2.5, shows that  $G/H_0 \cong G'/H'_0$  implies  $j \equiv j' \pmod{2^{e_0}}$  and that if  $j \equiv \pm 1$ , then  $l$  and  $l'$  must lie in the same congruence class  $\pmod{\gcd(j+1, 2^{e_0})}$ . (There are just two possible congruence classes, by Lemma 2.4.) When  $e_0 \geq 3$  and  $j \equiv 2^{e_0-1} \pm 1 \pmod{2^{e_0}}$ , Lemma 2.4 shows that the conditions  $j \equiv j'$ ,  $lj \equiv l$ , and  $l'j' \equiv l' \pmod{2^{e_0}}$  already imply  $l \equiv l' \pmod{\gcd(j+1, 2^{e_0})}$ . Thus, the Chinese Remainder Theorem yields that  $j \equiv j' \pmod{n}$  and  $l \equiv l' \pmod{\gcd(j+1, n)}$ , as desired.  $\square$

We can now count the number of isomorphism classes of groups of order  $2n$  containing a cyclic subgroup of order  $n$ . Let  $n = 2^{e_0} p_1^{e_1} \dots p_m^{e_m}$ , as usual. Let  $G$  be any such group, let  $H_0$  be its unique (cyclic) subgroup of order  $n/2^{e_0}$ , and let  $S$  be any 2-Sylow subgroup of  $G$ . Since  $H_0 \triangleleft G$ ,  $|H_0 \cap S| = 1$  (as  $\gcd(|H_0|, |S|) = 1$ ), and  $G = H_0 S$  (as  $|G| = |H_0| |S| / |H_0 \cap S|$ ),  $G$  is the semidirect product of  $H_0$  by  $S$ . (We thank R. Guralnick for pointing out this semidirect product decomposition to us.) So,  $G$  is determined by  $H_0$ ,  $S$ , and the map  $\gamma: S \rightarrow \text{Aut}(H_0)$ ,  $s \mapsto$  conjugation by  $s$ . The image of  $\gamma$  consists of the identity map and the  $j^{\text{th}}$  power map. Theorem 2.6(4) shows that  $G$  is determined up to isomorphism by the isomorphism class of  $S$  ( $\cong G/H_0$ ) and by  $j \pmod{n/2^{e_0}}$ . By the results in [G] quoted above, the number of possible choices of  $S$  is  $2^{e_0}$  if  $0 \leq e_0 \leq 2$  and is 6 if  $e_0 \geq 3$ . The number of possible choices of  $j \pmod{n/2^{e_0}}$  is  $2^m$  since we must have  $j \equiv \pm 1 \pmod{p_i^{e_i}}$  for  $1 \leq i \leq m$ . Every such choice of  $S$  and  $j$  yields a semidirect product which is a group of the desired type. (For, we obtain a cyclic group of order  $n$  in the semidirect product as the direct product of  $H_0$  with a cyclic subgroup of  $S$  of order  $2^{e_0}$  lying in  $\ker(\gamma)$ .) Theorem 2.6 shows that different isomorphism classes of  $S$  or different choices of  $j \pmod{n/2^{e_0}}$  yield nonisomorphic groups. Thus, we have proved,

**Proposition 2.7.** *Let  $n$  have prime factorization  $n = 2^{e_0} p_1^{e_1} \cdots p_m^{e_m}$ . The number of isomorphism classes of groups  $G$  of order  $2n$  containing a cyclic subgroup of order  $n$  is*

$$\begin{cases} 2^{e_0+m}, & \text{if } 0 \leq e_0 \leq 2, \\ 6 \cdot 2^m, & \text{if } e_0 \geq 3. \end{cases}$$

### 3. GALOIS EXTENSIONS WITH GROUP $G$

Let  $F$  be a field with  $\text{char } F \nmid n$  and let  $L/F$  be a Galois quadratic extension. That is, if  $2 \nmid n$  and  $\text{char } F = 2$ , assume that the quadratic extension  $L/F$  is also a separable extension.

Let  $G$  be a group of order  $2n$  that contains a cyclic subgroup of order  $n$ . We shall continue to use the notation from Section 2.

In this section, we shall determine when there exists a cyclic extension  $M/L$  of degree  $n$  such that  $M/F$  is a Galois extension with  $\text{Gal}(M/F) \cong G$ . For most of this section, we shall assume that  $L$  contains a primitive  $n^{\text{th}}$  root of unity.

**Proposition 3.1.** *Let  $G$  be a group of order  $2n$  as in Proposition 2.1. Let  $\langle \tau \rangle$  be a cyclic subgroup of  $G$  of order  $n$  and let  $H_i$ ,  $0 \leq i \leq m$ , be the subgroups of  $\langle \tau \rangle$  defined in Section 2. Let  $L/F$  be a Galois quadratic extension. Then the following statements are equivalent.*

1.  $L/F$  extends to a Galois extension  $M/F$  with  $\text{Gal}(M/F) \cong G$ .
2. For each  $i$ ,  $0 \leq i \leq m$ ,  $L/F$  extends to a Galois extension  $M_i/F$  with  $\text{Gal}(M_i/F) \cong G/H_i$  and  $\text{Gal}(M_i/L) \cong \langle \tau \rangle / H_i$ .

*Proof.* It is clear that (1) implies (2) by letting  $M_i$  be the fixed field of  $H_i$  and recalling that  $H_i \triangleleft G$ .

Now assume (2) holds. Then  $M_i/L$  is a cyclic Galois extension with  $[M_i : L] = p_i^{e_i}$ , since  $[\langle \tau \rangle : H_i] = p_i^{e_i}$ . Let  $M = M_0 \cdots M_m$ . Then  $M/L$  is a cyclic Galois extension with  $[M : L] = p_0^{e_0} \cdots p_m^{e_m} = n$  and  $M/F$  is a Galois extension since  $M_i/F$  is a Galois extension,  $0 \leq i \leq m$ . Let  $G' = \text{Gal}(M/F)$ ,  $\langle \tau' \rangle = \text{Gal}(M/L)$ , and  $H'_i = \text{Gal}(M/M_i)$ . Then  $G/H_i \cong \text{Gal}(M_i/F) \cong G'/H'_i$ ,  $0 \leq i \leq m$ . Theorem 2.6 implies  $G \cong G'$ .  $\square$

Let  $\zeta$  denote a primitive  $n^{\text{th}}$  root of unity. From here on, assume that  $\zeta \in L$ . Let  $\alpha \in L^*$  and let  $k \mid n$ . Let  $L(\alpha^{1/k})$  denote a field obtained by adjoining to  $L$  a root of the equation  $x^k - \alpha = 0$ . Since  $\text{char } L \nmid k$  and  $L$  contains a primitive  $k^{\text{th}}$  root of unity, it follows  $L(\alpha^{1/k})$  is a splitting field of  $x^k - \alpha$  over  $L$  and hence  $L(\alpha^{1/k})/L$  is a Galois extension. In particular, the field  $L(\alpha^{1/k})$  does not depend on which  $k^{\text{th}}$  root of  $\alpha$  is chosen. If  $[L(\alpha^{1/k}) : L] = k$ , then  $\text{Gal}(L(\alpha^{1/k})/L) \cong \mathbb{Z}/k\mathbb{Z}$ . However, when we write  $\alpha^{1/k}$ , we will assume some specified  $k^{\text{th}}$  root of  $\alpha$  has been selected and fixed throughout the discussion. Then  $\alpha^{s/k}$  will mean  $(\alpha^{1/k})^s$  for the given choice of  $\alpha^{1/k}$ .

**Lemma 3.2.** *Let  $\alpha, \beta \in L$ . Let  $r, s$  be positive integers with  $\gcd(r, s) = 1$  and assume  $rs \mid n$ . Then  $L(\alpha^{1/r}, \beta^{1/s}) = L(\gamma^{1/(rs)})$  where  $\gamma = \alpha^s \beta^r$ .*

*Proof.* We have  $L(\gamma^{1/(rs)}) \subseteq L(\alpha^{1/r}, \beta^{1/s})$  since

$$\gamma^{1/(rs)} = \alpha^{1/r} \beta^{1/s} \in L(\alpha^{1/r}, \beta^{1/s}).$$

Choose  $a, b \in \mathbb{Z}$  such that  $ar + bs = 1$ . Then

$$\begin{aligned} \alpha^{1/r} &= \alpha^{(ar+bs)/r} = \alpha^a \alpha^{bs/r} = \alpha^a \beta^{-b} \alpha^{bs/r} \beta^b \\ &= \alpha^a \beta^{-b} (\alpha^s \beta^r)^{b/r} = \alpha^a \beta^{-b} \gamma^{b/r} = \alpha^a \beta^{-b} (\gamma^{1/(rs)})^{bs} \in L(\gamma^{1/(rs)}) \end{aligned}$$

Similarly,  $\beta^{1/s} \in L(\gamma^{1/(rs)})$ . □

Let  $\text{Gal}(L/F) = \{1, \sigma\}$ . Since  $\zeta \in L$  is a primitive  $n^{\text{th}}$  root of unity, we have

$$\sigma(\zeta) = \zeta^r,$$

where  $\gcd(r, n) = 1$ . This equation defines  $r \pmod{n}$ , which will be a significant invariant from here on. Note that  $r^2 \equiv 1 \pmod{n}$  since  $\zeta = \sigma^2(\zeta) = \sigma(\zeta^r) = \zeta^{r^2}$ .

**Definition 3.3.** *If  $L \subseteq M$ , we will say that  $M/F$  realizes  $(G, j, l)$  if  $M/F$  is a Galois extension and  $\text{Gal}(M/F) = \langle \tau, \sigma \rangle$ , where  $\text{Gal}(M/L) = \langle \tau \rangle$ ,  $\sigma$  denotes an extension of  $\sigma \in \text{Gal}(L/F)$  to an automorphism in  $\text{Gal}(M/F)$ ,  $\sigma\tau\sigma^{-1} = \tau^j$ , and  $\sigma^2 = \tau^l$ .*

**Theorem 3.4.** *Assume  $\zeta \in L$ . Let  $M = L(\alpha^{1/n})$ , where  $\alpha \in L$ , and assume  $[M : L] = n$ . Then the following statements hold.*

1.  *$M/F$  is a Galois extension if and only if  $\sigma(\alpha) = \alpha^t \beta^n$ , where  $\beta \in L$ ,  $\gcd(t, n) = 1$ . When this occurs, for any  $t' \equiv t \pmod{n}$  there is  $\beta' \in L$  with  $\sigma(\alpha) = \alpha^{t'} (\beta')^n$ .*
2. *If  $M/F$  is a Galois extension, then there exist integers  $j, l$  such that  $M/F$  realizes  $(G, j, l)$ .*
3. *The following statements are equivalent.*
  - (a)  *$M/F$  realizes  $(G, j, l)$ .*
  - (b)  *$\sigma(\alpha) = \alpha^t \beta^n$ , with  $t \equiv jr \pmod{n}$  and  $\alpha^{(t^2-1)/n} \beta^t \sigma(\beta) = \zeta^{l_1}$  where  $l_1 \equiv l \pmod{\gcd(j+1, n)}$ .*
4. *If  $M/F$  realizes  $(G, j, l)$  and we choose  $\zeta$  so that  $\tau(\alpha^{1/n}) = \zeta \alpha^{1/n}$  and  $\beta$  so that  $\sigma(\alpha^{1/n}) = \alpha^{t/n} \beta$ , then  $\alpha^{(t^2-1)/n} \beta^t \sigma(\beta) = \zeta^l$ . If we let  $\beta' = \zeta^i \beta$ , then  $\alpha^{(t^2-1)/n} (\beta')^t \sigma(\beta') = \zeta^{l+ir(j+1)}$ .*

*Proof.* (1)  $M/F$  is a Galois extension  $\Leftrightarrow (x^n - \alpha)(x^n - \sigma(\alpha))$  splits completely in  $M \Leftrightarrow M = L(\alpha^{1/n}, \sigma(\alpha)^{1/n}) \Leftrightarrow L(\alpha^{1/n}) = L(\sigma(\alpha)^{1/n})$ , since  $M = L(\alpha^{1/n})$  and  $[L(\alpha^{1/n}) : L] = [L(\sigma(\alpha)^{1/n}) : L]$ ,  $\Leftrightarrow \sigma(\alpha) = \alpha^t \beta^n$  with  $\gcd(t, n) = 1$  and  $\beta \in L$ , by Kummer Theory. Finally, if  $t' = t + dn$  and  $\sigma(\alpha) = \alpha^t \beta^n$ , then  $\sigma(\alpha) = \alpha^{t'} (\beta')^n$  where  $\beta' = \alpha^{-d} \beta$ .

(2) Assume  $M/F$  is a Galois extension and let  $G = \text{Gal}(M/F)$ . Since  $|G| = [M : F] = 2n$  and  $M/L$  is a cyclic extension of degree  $n$ , it follows that  $\text{Gal}(M/L)$  is a cyclic subgroup of  $G$  of order  $n$  and thus  $G$  is a group as in Proposition 2.1. Let  $\text{Gal}(M/L) = \langle \tau \rangle$  and let  $\sigma$  denote an extension of  $\sigma \in \text{Gal}(L/F)$  to an automorphism  $\sigma$  in  $\text{Gal}(M/F)$ . Then  $G = \langle \tau, \sigma \rangle$  since  $\sigma|_L \neq 1$ . Since  $[G : \langle \tau \rangle] = 2$ , we have  $\sigma\tau\sigma^{-1} \in \langle \tau \rangle$  and  $\sigma^2 \in \langle \tau \rangle$ . Thus  $\sigma\tau\sigma^{-1} = \tau^j$  and  $\sigma^2 = \tau^l$  and  $M/F$  realizes  $(G, j, l)$ .

(3) and (4) Assume  $M/F$  realizes  $(G, j, l)$ . Then  $\sigma(\alpha) = \alpha^t \beta^n$  with  $\beta \in L$ , from the proof of (1). This equation implies  $\sigma(\alpha^{1/n}) = \alpha^{t/n} \beta \omega$  where  $\omega$  is an  $n^{\text{th}}$  root of unity. We may replace  $\beta \omega$  by  $\beta$  so that we may assume that  $\sigma(\alpha^{1/n}) = \alpha^{t/n} \beta$ . We have  $\tau(\alpha^{1/n}) = \zeta^l \alpha^{1/n}$ , where  $\zeta^l$  is a primitive  $n^{\text{th}}$  root of unity, since  $\tau$  has order  $n$  and  $M = L(\alpha^{1/n})$  is a cyclic extension of degree  $n$ . We can assume that  $\zeta = \zeta^l$ . We now apply the equation  $\sigma\tau = \tau^j \sigma$  to  $\alpha^{1/n}$ .

$$\sigma\tau(\alpha^{1/n}) = \sigma(\zeta \alpha^{1/n}) = \zeta^r \sigma(\alpha^{1/n}) = \zeta^r \alpha^{t/n} \beta.$$

$$\tau^j \sigma(\alpha^{1/n}) = \tau^j(\alpha^{t/n} \beta) = \tau^j(\alpha^{1/n})^t \tau^j(\beta) = (\zeta^j \alpha^{1/n})^t \beta = \zeta^{jt} \alpha^{t/n} \beta.$$

Thus  $\zeta^{jt} = \zeta^r$  and  $jt \equiv r \pmod{n}$ . Since  $j^2 \equiv 1 \pmod{n}$ , it follows  $t \equiv jr \pmod{n}$  and  $t^2 \equiv j^2 r^2 \equiv 1 \pmod{n}$ .

Next we apply the equation  $\sigma^2 = \tau^l$  to  $\alpha^{1/n}$ . Since

$$\sigma^2(\alpha^{1/n}) = \tau^l(\alpha^{1/n}) = \zeta^l \alpha^{1/n}$$

and

$$\sigma^2(\alpha^{1/n}) = \sigma(\alpha^{t/n} \beta) = \sigma(\alpha^{1/n})^t \sigma(\beta) = \alpha^{t^2/n} \beta^t \sigma(\beta),$$

it follows  $\alpha^{(t^2-1)/n} \beta^t \sigma(\beta) = \zeta^l$ . We have now proved the first sentence of (4). For the rest of (4), observe that if  $\beta' = \zeta^i \beta$ , then

$$\alpha^{(t^2-1)/n} (\beta')^t \sigma(\beta') = (\alpha^{(t^2-1)/n} \beta^t \sigma(\beta)) \zeta^{i(t+r)} = \zeta^{l+ir(j+1)},$$

since  $t + r \equiv jr + r \equiv r(j + 1) \pmod{n}$ .

To show 3(a)  $\Rightarrow$  3(b) we must see what happens if we make different choices of  $\beta$  and  $\zeta$ . But, if  $\sigma(\alpha^{1/n}) = \alpha^{t/n} \beta \omega$  and  $\tau(\alpha^{1/n}) = \zeta^l \alpha^{1/n}$ , then there is another generator  $\tau_1$  of  $\langle \tau \rangle$  and a  $\sigma_1 = \sigma \tau^i$  such that  $\sigma_1(\alpha^{1/n}) = \alpha^{t/n} \beta$  and  $\tau_1(\alpha^{1/n}) = \zeta \alpha^{1/n}$ . Then, the calculation made above (using  $\sigma_1$  and  $\tau_1$  and noting that  $\sigma_1(\beta) = \sigma(\beta)$ ) shows that  $\alpha^{(t^2-1)/n} \beta^t \sigma(\beta) = \zeta^{l_1}$ , where  $\sigma_1^2 = \tau_1^{l_1}$ . But, we saw in Remark 2.3 that  $l_1 \equiv l \pmod{\text{gcd}(j+1, n)}$ , so we have 3(b).

Now assume the equations in (3)(b) hold. Then  $M/F$  is a Galois extension by (1). Choose a generator  $\tau$  of  $\text{Gal}(M/L)$  such that  $\tau(\alpha^{1/n}) = \zeta \alpha^{1/n}$  and choose  $\sigma \in \text{Gal}(M/F)$  extending  $\sigma \in \text{Gal}(L/F)$  such that  $\sigma(\alpha^{1/n}) = \alpha^{t/n} \beta$ . Then, (2) implies that  $M/F$  realizes  $(G, j', l')$ , where  $\sigma\tau\sigma^{-1} = \tau^{j'}$ , so  $(j')^2 \equiv 1 \pmod{n}$ , and  $\sigma^2 = \tau^{l'}$ . The equation  $\sigma\tau(\alpha^{1/n}) = \tau^{j'} \sigma(\alpha^{1/n})$  shows that  $\zeta^{j't} = \zeta^r$ , so  $j't \equiv r \equiv jt \pmod{n}$ . Hence,  $j' \equiv j \pmod{n}$ . Also, the calculation above for  $\sigma^2(\alpha^{1/n})$  shows

that  $\alpha^{(t^2-1)/n}\beta^t\sigma(\beta) = \zeta^{l'}$ . Hence,  $l' \equiv l_1 \equiv l \pmod{\gcd(j+1, n)}$ . But then, since  $M/F$  realizes  $(G, j', l')$ , it also realizes  $(G, j, l)$  with a different choice of  $\sigma$ , by Remark 2.3.  $\square$

#### 4. CALCULATIONS IN QUADRATIC EXTENSIONS

Let  $L/F$  be a Galois quadratic extension and assume  $\zeta \in L$  is a primitive  $n^{\text{th}}$  root of unity. Thus  $\text{char } F \nmid n$ . Let  $\sigma \in \text{Gal}(L/F)$  with  $\sigma \neq 1$ . Then  $\sigma(\zeta) = \zeta^r$  where  $r^2 \equiv 1 \pmod{n}$ . If  $\text{char } F \neq 2$ , let  $L = F(\sqrt{a})$ ,  $a \in F$ .

In this section we study the problem of describing elements  $\alpha \in L^*$  with the property  $\sigma(\alpha) = \alpha^t\beta^n$ ,  $\beta \in L$ , for a given integer  $t$  satisfying  $t^2 \equiv 1 \pmod{n}$ . By Theorem 3.4(1), this is equivalent to describing elements  $\alpha \in L^*$  with the property that  $L(\alpha^{1/n})$  is a Galois extension of  $F$ . These results will be applied in Sections 5 and 6 to the problem of constructing the Galois extensions discussed in Section 3 with a given group as described in Proposition 2.1. Keeping in mind the intended applications in Sections 5 and 6, we shall consider only the cases  $t \equiv \pm 1 \pmod{n}$  and  $t \equiv \pm 1, 2^{e-1} \pm 1 \pmod{2^e}$ ,  $e \geq 3$ , when  $n = 2^e$ .

We begin with a lemma to be used in the case  $t \equiv 1 \pmod{n}$ .

**Lemma 4.1.** 1. *If  $\delta, \delta' \in L^*$  and  $\sigma(\delta)/\delta = \sigma(\delta')/\delta'$ , then  $\delta' = b\delta$  with  $b \in F$ .*  
2. *Suppose  $\gamma = \sigma(\delta)/\delta$  with  $\gamma, \delta \in L$ . Then there exists  $b \in F$  such that*

$$\delta = \begin{cases} b(1 + \sigma(\gamma)), & \text{if } \gamma \neq -1, \\ b\sqrt{a}, & \text{if } \gamma = -1, \text{ char } F \neq 2, \\ b & \text{if } \gamma = -1, \text{ char } F = 2. \end{cases}$$

*Proof.* The equation in (1) implies  $\sigma(\delta'/\delta) = \delta'/\delta$  and thus  $\delta'/\delta \in F$ . This implies (1).

For (2), first assume  $\gamma \neq -1$ . Then  $1 + \sigma(\gamma) \neq 0$ . Since  $\gamma\sigma(\gamma) = N_{L/F}(\gamma) = 1$ , it follows  $\sigma(\delta)/\delta = \gamma = \frac{1 + \gamma}{1 + \sigma(\gamma)} = \frac{\sigma(1 + \sigma(\gamma))}{1 + \sigma(\gamma)}$ . Now (1) implies that  $\delta = b(1 + \sigma(\gamma))$  with  $b \in F$ . Now assume  $\gamma = -1$ . If  $\text{char } F \neq 2$ , then  $\sigma(\sqrt{a})/\sqrt{a} = -1$ , and so (1) implies that  $\delta = b\sqrt{a}$  with  $b \in F$ . If  $\text{char } F = 2$ , then  $\sigma(\delta)/\delta = -1 = 1$  and hence  $\delta \in F$ .  $\square$

The following proposition covers the case  $t \equiv 1 \pmod{n}$ .

**Proposition 4.2.** *Let  $n$  be a positive integer and let  $\alpha \in L$ . Then  $\sigma(\alpha) = \alpha\beta^n$ ,  $\beta \in L$ , if and only if there exists  $b \in F$  such that*

$$\alpha = \begin{cases} b(1 + \gamma^n), & \text{if } \sigma(\alpha)/\alpha \neq -1, \\ b\sqrt{a}, & \text{if } \sigma(\alpha)/\alpha = -1, \text{ char } F \neq 2, \text{ and } -1 \in L^n, \\ b, & \text{if } \sigma(\alpha)/\alpha = -1, \text{ char } F = 2, \end{cases}$$

where in the first case above,  $\gamma \in L$  and  $N_{L/F}(\gamma)^n = 1$ .

*Proof.* First suppose  $\sigma(\alpha) = \alpha\beta^n$ ,  $\beta \in L$ . Then  $\beta^n = \sigma(\alpha)/\alpha$  and Lemma 4.1(2) implies there exists  $b \in F$  such that

$$\alpha = \begin{cases} b(1 + \sigma(\beta^n)), & \text{if } \sigma(\alpha)/\alpha \neq -1, \\ b\sqrt{a}, & \text{if } \sigma(\alpha)/\alpha = -1, \text{ char } F \neq 2, \\ b, & \text{if } \sigma(\alpha)/\alpha = -1, \text{ char } F = 2. \end{cases}$$

If  $\sigma(\alpha)/\alpha \neq -1$ , let  $\gamma = \sigma(\beta)$ . Then

$$N_{L/F}(\gamma)^n = N_{L/F}(\sigma(\beta)^n) = N_{L/F}(\beta^n) = N_{L/F}(\sigma(\alpha)/\alpha) = 1.$$

If  $\sigma(\alpha)/\alpha = -1$  and  $\text{char } F \neq 2$ , then  $-1 = \beta^n \in L$ . Therefore the stated formula for  $\alpha$  holds.

Now assume that  $\alpha$  is given by the formula in the statement of this Proposition. If  $\alpha = b(1 + \gamma^n)$  and  $N_{L/F}(\gamma)^n = 1$ , then

$$\frac{\sigma(\alpha)}{\alpha} = \frac{b(1 + \sigma(\gamma)^n)}{b(1 + \gamma^n)} = \sigma(\gamma)^n.$$

Thus  $\sigma(\alpha) = \alpha\beta^n$ , where  $\beta = \sigma(\gamma)$ . If  $\alpha = b\sqrt{a}$  and  $-1 = \beta^n \in L^n$ , then  $\sigma(\alpha)/\alpha = -1 = \beta^n$ . If  $\alpha = b$ , then  $\sigma(\alpha) = \alpha \cdot 1^n$ .  $\square$

If  $t \equiv -1 \pmod{n}$  and  $\sigma(\alpha) = \alpha^{-1}\beta^n$ , then  $N_{L/F}(\alpha) = \alpha\sigma(\alpha) = \beta^n \in F \cap L^n$ . Thus to treat the case  $t \equiv -1 \pmod{n}$ , we shall first study  $F \cap L^n$  in Propositions 4.3 – 4.5. There does not seem to be a good description of  $F \cap L^n$  when  $L = F(\sqrt{-1})$  and  $n = 2^e$ ,  $e \geq 3$ , but the result in Proposition 4.5 is sufficient for our purposes.

**Proposition 4.3.** *If  $n$  is odd, then  $F \cap L^n = F^n$ .*

*Proof.* It is clear that  $F^n \subseteq F \cap L^n$ . Now let  $\lambda \in L$  and suppose  $\lambda^n = b \in F$ . Then  $b^2 = N_{L/F}(b) = N_{L/F}(\lambda)^n \in F^n$ . Since  $b^2$  and  $b^n$  lie in  $F^n$ , it follows that  $b \in F^n$ . Thus  $F \cap L^n \subseteq F^n$ .  $\square$

**Proposition 4.4.** *Assume  $n$  is even and let  $n = 2^e m$ ,  $m$  odd,  $e \geq 1$ . If  $a \notin -F^2$  (i.e.,  $L \neq F(\sqrt{-1})$ ), then  $F \cap L^n = F^n \cup a^{n/2}F^n$ .*

*Proof.* Recall that if  $s$  and  $t$  are any two relatively prime integers and  $A$  is any abelian group (written additively) then  $sA \cap tA = stA$ . Consequently, if  $E$  is any field, then  $E^s \cap E^t = E^{st}$  (by taking  $A = E^*$ ).

It is clear that  $F^n \cup a^{n/2}F^n \subseteq F \cap L^n$  since  $a^{n/2} = (\sqrt{a})^n$ . To prove the other inclusion take any nonzero  $b \in F \cap L^n = F \cap L^{2^e} \cap L^m = (F \cap L^{2^e}) \cap F^m$  (by Proposition 4.3). Then,  $b = \beta^{2^e} = \sigma(\beta)^{2^e}$  for some  $\beta \in L^*$ . Let  $\omega = \sigma(\beta)/\beta$ . So,  $\omega^{2^e} = 1$  and  $1 = N_{L/F}(\omega) = \omega\sigma(\omega)$ . So,  $\sigma(\omega) = \omega^{-1}$ . If  $\omega = 1$ , then  $\beta \in F$ , so  $b \in F^{2^e} \cap F^m = F^n$ . If  $\omega = -1$  then  $\sigma(\beta) = -\beta$ , so  $\beta = c\sqrt{a}$  for some  $c \in F$ . Then,  $b = \beta^{2^e} \in a^{2^{e-1}}F^{2^e} = a^{2^{e-1}m}F^{2^e}$ , so  $b \in F^m \cap a^{2^{e-1}m}F^{2^e} = a^{2^{e-1}m}(F^m \cap F^{2^e}) = a^{n/2}F^n$ . If  $\omega \neq \pm 1$ , then  $\omega^k = \sqrt{-1}$  for some integer  $k$ , so  $\sigma(\sqrt{-1}) = (\sqrt{-1})^{-1} = -\sqrt{-1}$ . But then,  $\sqrt{-1} = d\sqrt{a}$  for some  $d \in F^*$ , yielding

$-a = d^{-2} \in F^2$ , contrary to our hypothesis. Thus, in every case that can occur,  $b \in F^n \cup a^{n/2}F^n$ , as desired.  $\square$

**Proposition 4.5.** *Let  $L = F(\sqrt{-1})$  and assume  $\zeta \in L$  is a primitive  $(2^e)^{\text{th}}$  root of unity,  $e \geq 2$ . Then  $F \cap L^{2^{e-1}} = F^{2^{e-1}} \cup -F^{2^{e-1}}$ .*

*Proof.* The proof is by induction on  $e$ . The case  $e = 2$  is well known to be true. Now assume  $e \geq 3$ . We have  $F^{2^{e-1}} \cup -F^{2^{e-1}} \subseteq F \cap L^{2^{e-1}}$ , since  $-1 = \zeta^{2^{e-1}}$ . Suppose  $\lambda^{2^{e-1}} \in F$ , with  $\lambda \in L$ . Then  $(\lambda^{2^{e-2}})^2 \in F$  and this implies  $\lambda^{2^{e-2}} \in F \cup \sqrt{-1}F = F \cup \zeta^{2^{e-2}}F$ .

First suppose  $\lambda^{2^{e-2}} \in F$ . Then  $\lambda^{2^{e-2}} \in F \cap L^{2^{e-2}} = F^{2^{e-2}} \cup -F^{2^{e-2}}$ , by induction. Thus  $\lambda^{2^{e-2}} = \pm b^{2^{e-2}}$ ,  $b \in F$ , and this implies  $\lambda^{2^{e-1}} = b^{2^{e-1}} \in F^{2^{e-1}}$ .

On the other hand, if  $\lambda^{2^{e-2}} \in \zeta^{2^{e-2}}F$ , then  $(\lambda/\zeta)^{2^{e-2}} \in F$ . The argument in the first part implies  $(\lambda/\zeta)^{2^{e-1}} \in F^{2^{e-1}}$ . Thus  $\lambda^{2^{e-1}} \in -F^{2^{e-1}}$ , since  $-1 = \zeta^{2^{e-1}}$ .  $\square$

*Remark 4.6.* Under the hypotheses of Proposition 4.5, there does not seem to be a simple description of  $F \cap L^{2^e}$ . As already noted, for  $e = 1$  we have  $F \cap L^2 = F^2 \cup -F^2$ . For  $e = 2$  it is easy to show  $F \cap L^4 = F^4 \cup -4F^4$ . For  $e \geq 3$ , the descriptions become more awkward.

The next proposition characterizes the condition  $N_{L/F}(\alpha) \in F^n$  and  $N_{L/F}(\alpha) \in a^{n/2}F^n$  when  $n$  is even. In light of Propositions 4.3 and 4.4, this covers the case  $t \equiv -1 \pmod{n}$ , except when  $L = F(\sqrt{-1})$  and  $n$  is even.

**Proposition 4.7.** *Let  $\alpha \in L$ ,  $\alpha \neq 0$ .*

1.  $N_{L/F}(\alpha) \in F^n$  if and only if there exist  $b \in F$  and  $\beta, \gamma \in L$  such that

$$\alpha = \begin{cases} b^{n/2}N_{L/F}(\gamma)/\gamma^2, & \text{if } n \text{ is even } (e_0 \geq 1), \\ N_{L/F}(\beta)^{(n-1)/2}\beta, & \text{if } n \text{ is odd } (e_0 = 0). \end{cases}$$

2.  $N_{L/F}(\alpha) \in a^{n/2}F^n$  if and only if there exist  $b \in F$  and  $\gamma, \delta \in L$  such that

$$\alpha = \begin{cases} (b\sqrt{a})^{n/2}N_{L/F}(\gamma)/\gamma^2, & \text{if } n \equiv 0 \pmod{4} (e_0 \geq 2), \\ (b\sqrt{a})^{n/2}\delta, \text{ with } N_{L/F}(\delta) = -1, & \text{if } n \equiv 2 \pmod{4} (e_0 = 1). \end{cases}$$

*Proof.* The proofs of each of the cases are very similar and straight-forward. We will give one of the proofs. Suppose  $N_{L/F}(\alpha) = a^{n/2}b^n$ , with  $n \equiv 2 \pmod{4}$ . Let  $\delta = \alpha/(b\sqrt{a})^{n/2}$ . So,  $\alpha = (b\sqrt{a})^{n/2}\delta$  and

$$N_{L/F}(\delta) = N_{L/F}(\alpha/(b\sqrt{a})^{n/2}) = a^{n/2}b^n/(b^n(-a)^{n/2}) = (-1)^{n/2} = -1.$$

The converse is easy as are the other cases. Note that for (1), if  $N_{L/F}(\alpha) = b^n \in F^n$ , then when  $n$  is even we can (by Hilbert 90) choose  $\gamma$  so that  $\alpha b^{-n/2} = \sigma(\gamma)/\gamma$ ; when  $n$  is odd, choose  $\beta = \alpha b^{-(n-1)/2}$ . For (2), if  $N_{L/F}(\alpha) = a^{n/2}b^n$  with  $n \equiv 0 \pmod{4}$ , then choose  $\gamma$  so that  $\alpha a^{-n/4}b^{-n/2} = \sigma(\gamma)/\gamma$ .  $\square$

Now we assume  $n = 2^e$ , with  $e \geq 3$ . If  $t^2 \equiv 1 \pmod{2^e}$ , then  $t \in \{\pm 1, 2^{e-1} \pm 1\} \pmod{2^e}$ . The case  $t \equiv 1 \pmod{2^e}$  is covered in Proposition 4.2 and the case  $t \equiv -1 \pmod{2^e}$  is covered in Propositions 4.3 – 4.7, with a small gap in the case  $L = F(\sqrt{-1})$ . These cases do not depend on  $r$ , where  $\sigma(\zeta) = \zeta^r$ . Since  $r^2 \equiv 1 \pmod{n}$ , in general, we have  $r \in \{\pm 1, 2^{e-1} \pm 1\} \pmod{2^e}$  when  $n = 2^e$ ,  $e \geq 3$ . The next two results characterize the value of  $r$  when  $t \equiv 2^{e-1} \pm 1 \pmod{2^e}$ ,  $e \geq 3$ .

**Proposition 4.8.**  $L \neq F(\sqrt{-1})$  (i.e.,  $\sqrt{-1} \in F$ ) if and only if  $r \equiv 1 \pmod{2^{e-1}}$ . When this occurs,  $\zeta^2 \in F$ ; furthermore,  $\zeta \in F$  if and only if  $r \equiv 1 \pmod{2^e}$ .

*Proof.* Recall that  $r \equiv \pm 1 \pmod{2^{e-1}}$ . If  $r \equiv -1 \pmod{2^{e-1}}$ , then  $\sigma(\zeta^2) = (\zeta^2)^{-1}$ , so  $\sigma(\sqrt{-1}) = (\sqrt{-1})^{-1} = -\sqrt{-1}$ , as  $\sqrt{-1} = \pm(\zeta^2)^{2^{e-3}}$ . Hence,  $\sqrt{-1} \notin F$ , so  $L = F(\sqrt{-1})$ . On the other hand, if  $r \equiv 1 \pmod{2^{e-1}}$  then  $\sigma(\zeta^2) = \zeta^2$ , so  $\zeta^2 \in F$ . Then,  $\sqrt{-1} = \pm(\zeta^2)^{2^{e-3}} \in F$ , so  $L \neq F(\sqrt{-1})$ . Clearly,  $\zeta \in F$  if and only if  $\zeta = \sigma(\zeta) = \zeta^r$ , if and only if  $r \equiv 1 \pmod{2^e}$ .  $\square$

**Proposition 4.9.** Assume  $L = F(\sqrt{-1})$ . Then  $r \equiv -1 \pmod{2^{e-1}}$  and the following statements hold.

1. The following statements are equivalent.
  - (a)  $r \equiv -1 \pmod{2^e}$ .
  - (b)  $N_{L/F}(\zeta) = 1$ .
  - (c)  $\zeta \in F \cdot L^2$ .
2. The following statements are equivalent.
  - (a)  $r \equiv 2^{e-1} - 1 \pmod{2^e}$ .
  - (b)  $N_{L/F}(\zeta) = -1$ .
  - (c)  $\zeta \notin F \cdot L^2$ .

*Proof.* Since  $L = F(\sqrt{-1})$ , Proposition 4.8 shows that  $r \equiv -1 \pmod{2^{e-1}}$ .

If  $r \equiv -1 \pmod{2^e}$ , then  $\sigma(\zeta) = \zeta^{-1}$ . This is equivalent to  $N_{L/F}(\zeta) = 1$  and hence  $\zeta \in F \cdot L^2$ .

If  $r \equiv 2^{e-1} - 1 \pmod{2^e}$ , then  $\sigma(\zeta) = \zeta^{2^{e-1}-1} = -\zeta^{-1}$  and this is equivalent to  $N_{L/F}(\zeta) = -1$ . Since  $-1 \notin F^2$ , it follows that  $\zeta \notin F \cdot L^2$ .  $\square$

**Proposition 4.10.** Assume  $t \equiv 2^{e-1} + 1 \pmod{2^e}$ ,  $e \geq 3$ , and let  $\alpha \in L$ ,  $\alpha \neq 0$ . Suppose  $\sigma(\zeta) = \zeta^r$ . Then  $\sigma(\alpha) = \alpha^{2^{e-1}+1}\beta^{2^e}$ ,  $\beta \in L$ , if and only if there exist  $\gamma, \eta \in L^*$  with  $\eta^2 \in F$  such that

$$\alpha = \varphi N_{L/F}(\gamma)\eta^2/\gamma^{2^{e-1}},$$

where

$$\varphi = \begin{cases} 1, & \text{if } r \equiv 1, -1, \text{ or } 2^{e-1} - 1 \pmod{2^e}, \\ 1 \text{ or } \zeta, & \text{if } r \equiv 2^{e-1} + 1 \pmod{2^e}. \end{cases}$$

*Proof.* Let  $k = 2^{e-1}$ . Let

$$A = \{\alpha \in L^* \mid \sigma(\alpha) = \alpha^{k+1}\beta^{2^k} \text{ for some } \beta \in L\}$$

and let

$$B = \{ \alpha \in L^* \mid \alpha = N_{L/F}(\gamma)\eta^2/\gamma^{2^{e-1}} \text{ where } \gamma, \eta \in L^* \text{ and } \eta^2 \in F \}.$$

Clearly  $A$  and  $B$  are groups.

Let  $\alpha = \varphi N_{L/F}(\gamma)\eta^2/\gamma^{2^{e-1}}$  and let  $\beta = \gamma^{2^{e-2}}/\sigma(\gamma)\eta$ . Then  $\alpha\beta^2 = \varphi\gamma/\sigma(\gamma)$ . We have  $\sigma(\varphi) = \varphi^{2^{e-1}+1}$  in all cases since the case  $r \equiv 2^{e-1} + 1 \pmod{2^e}$  and  $\varphi = \zeta$  implies  $\sigma(\zeta) = \zeta^r = \zeta^{2^{e-1}+1}$ . It now follows that

$$\sigma(\alpha)/\alpha = (\gamma/\sigma(\gamma))^k(\sigma(\varphi)/\varphi) = ((\alpha\beta^2)^k/\varphi^k)(\sigma(\varphi)/\varphi) = (\alpha\beta^2)^k. \quad (1)$$

This implies that  $\alpha \in A$ . The case  $\varphi = 1$  shows that  $B \subseteq A$ . If  $r \equiv k+1 \pmod{2k}$ , then  $\zeta \in A$ , so  $B \cup \zeta B \subseteq A$ . We must show that  $A = B \cup \zeta B$  if  $r \equiv k+1 \pmod{2k}$  and  $A = B$  otherwise.

Take any  $\alpha \in A$ ; so  $\sigma(\alpha) = \alpha^{k+1}\beta^{2k}$ , i.e.,  $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$ . Let  $\omega = N_{L/F}(\alpha\beta^2)$ . Then,  $\omega^k = N_{L/F}(\sigma(\alpha)/\alpha) = 1$ , so, since  $\omega$  is a power of  $\zeta^2$ , we have  $\omega \in L^2 \cap F = F^2 \cup aF^2$ .

Let  $\epsilon = \omega^{k/2}$ . Then  $\epsilon^2 = \omega^k = 1$  and thus  $\epsilon = \pm 1$ . In either case,  $\epsilon = \omega^{k/2} \in F^2$ , since  $\omega \in F$  and  $k/2$  is even. Let  $\delta = \alpha\beta^2$ . Then,

$$\sigma(\alpha\delta^{k/2}) = \alpha\delta^k\sigma(\delta^{k/2}) = \alpha\delta^{k/2}(N_{L/F}(\delta))^{k/2} = \alpha\delta^{k/2}\omega^{k/2} = \alpha\delta^{k/2}\epsilon.$$

If  $\epsilon = 1$ , then  $\alpha\delta^{k/2} \in F$ . From this we conclude  $N_{L/F}(\alpha\delta^{k/2}) \in F^2$ ,  $N_{L/F}(\alpha) \in F^2$ ,  $N_{L/F}(\alpha\beta^2) \in F^2$ , and finally  $\omega \in F^2$ .

If  $\epsilon = -1$ , then  $\alpha\delta^{k/2} \in \sqrt{a}F$ . From this we conclude  $N_{L/F}(\alpha\delta^{k/2}) \in -aF^2$ ,  $N_{L/F}(\alpha) \in -aF^2$ ,  $N_{L/F}(\alpha\beta^2) \in -aF^2$ , and finally  $\omega \in -aF^2 = aF^2$ , since  $-1 = \epsilon \in F^2$ .

Case 1. Assume  $\epsilon = 1$ . Then  $N_{L/F}(\alpha\beta^2) = \omega \in F^2$ . Therefore  $\alpha\beta^2 = b\gamma^2$  for some  $b \in F^*$ ,  $\gamma \in L^*$ . Since,  $b^2 N_{L/F}(\gamma)^2 = N_{L/F}(b\gamma^2) = N_{L/F}(\alpha\beta^2) = \omega$ , we have  $b^k N_{L/F}(\gamma)^k = \omega^{k/2} = \epsilon = 1$ . This gives

$$\sigma(\alpha)/\alpha = (\alpha\beta^2)^k = (b\gamma^2)^k = \gamma^{2k}/N_{L/F}(\gamma)^k = \gamma^k/\sigma(\gamma)^k.$$

Thus,  $\sigma(\alpha\gamma^k) = \alpha\gamma^k$  and we have  $\alpha\gamma^k = d \in F$ .

Since  $(\alpha\beta^2)^k = (\gamma/\sigma(\gamma))^k$ , we have  $\alpha\beta^2 = \omega'\gamma/\sigma(\gamma) = \omega'c/\sigma(\gamma)^2$ , where  $(\omega')^k = 1$  and  $c = N_{L/F}(\gamma)$ . Note that  $\alpha/d = \gamma^{-k} \in L^2$  and  $\alpha/c = \omega'/(\sigma(\gamma)^2\beta^2) \in L^2$ ; so  $d/c \in L^2 \cap F$ . Let  $\eta^2 = d/c$ . Then,  $\alpha = c\eta^2/\gamma^k \in B$ .

Case 2. Now assume  $\epsilon = -1$ . Then  $\omega \in aF^2$  and  $-1 \in F^2$ . This implies  $r \equiv 1 \pmod{k}$  (see Proposition 4.8). Since  $\omega \notin F^2$ , it follows  $\zeta \notin F$  and  $r \not\equiv 1 \pmod{2k}$ . Hence,  $r \equiv k+1 \pmod{2k}$ . Because  $L = F(\zeta)$  and  $\zeta^2 \in F$  (see Proposition 4.8), we can take  $a = \zeta^2$ . The congruence condition on  $r$  says that  $\sigma(\zeta) = \zeta^{1+k}$ , showing that  $\zeta \in A$ . Since  $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$  and  $\sigma(\zeta)/\zeta = \zeta^k$ , we have  $\sigma(\alpha/\zeta)/(\alpha/\zeta) = ((\alpha/\zeta)\beta^2)^k$ . Also,  $N_{L/F}((\alpha/\zeta)\beta^2) = \omega(-\zeta^{-2}) = -a^{-1}\omega \in F^2$ . This shows that  $\alpha/\zeta \in A$ , and that Case 1 above applies to  $\alpha/\zeta$ . Hence,  $\alpha/\zeta \in B$ , so  $\alpha \in \zeta B$ . Since Case 2 occurs for  $\alpha$  only when  $r \equiv k+1 \pmod{2k}$ , the proof is complete.  $\square$

**Proposition 4.11.** *Assume  $t \equiv 2^{e-1} - 1 \pmod{2^e}$ ,  $e \geq 3$ , and let  $\alpha \in L$ ,  $\alpha \neq 0$ . Let  $\sigma(\zeta) = \zeta^r$ . Then  $\sigma(\alpha) = \alpha^{2^{e-1}-1}\beta^{2^e}$ ,  $\beta \in L$ , if and only if there exist  $c \in F$ ,  $\gamma \in L$ , with  $N_{L/F}(\gamma) = \pm c$ , such that  $\alpha = \theta c^{2^{e-2}+1}/\gamma^2$  where*

$$\theta = \begin{cases} 1, & \text{if } L \neq F(\sqrt{-1}), \\ 1, & \text{if } L = F(\sqrt{-1}), r \equiv -1 \pmod{2^e}, \\ 1 \text{ or } \zeta, & \text{if } L = F(\sqrt{-1}), r \equiv 2^{e-1} - 1 \pmod{2^e}. \end{cases}$$

*Proof.* First assume  $\alpha = \theta c^{2^{e-2}+1}/\gamma^2$  where  $N_{L/F}(\gamma) = \pm c$  and  $\theta = 1$  or  $\zeta$ , as above. We see that  $\theta^{2^{e-1}} = N_{L/F}(\theta)$  in all three cases since  $\zeta^{2^{e-1}} = \zeta \zeta^{2^{e-1}-1} = N_{L/F}(\zeta)$  in the third case. Let  $\beta = \gamma/c^{2^{e-3}}$ . Then  $\alpha\beta^2 = \theta c$  and

$$N_{L/F}(\alpha) = N_{L/F}(\theta)c^{2^{e-1}+2}/c^2 = N_{L/F}(\theta)c^{2^{e-1}} = \theta^{2^{e-1}}c^{2^{e-1}} = (\alpha\beta^2)^{2^{e-1}}.$$

Thus  $\sigma(\alpha) = \alpha^{2^{e-1}-1}\beta^{2^e}$ .

Now assume  $\sigma(\alpha) = \alpha^{2^{e-1}-1}\beta^{2^e}$ ,  $\beta \in L$ . Then  $N_{L/F}(\alpha) = (\alpha\beta^2)^{2^{e-1}}$ . Since

$$(\alpha\beta^2)^{2^{e-1}} \in F \cap L^{2^{e-1}} = \begin{cases} F^{2^{e-1}} \cup a^{2^{e-2}}F^{2^{e-1}}, & \text{if } L \neq F(\sqrt{-1}), \\ F^{2^{e-1}} \cup -F^{2^{e-1}}, & \text{if } L = F(\sqrt{-1}), \end{cases}$$

by Propositions 4.4 and 4.5, there exists  $c \in F$  such that  $\alpha\beta^2 \in \{c\omega, \sqrt{ac}\omega, \zeta c\omega\}$  where  $\omega^{2^{e-1}} = 1$ . Since  $\omega \in L^2$ , by replacing  $\beta$  by  $\beta\omega^{-1/2}$  we can assume

$$\alpha\beta^2 = \begin{cases} c \text{ or } \sqrt{ac}, & \text{if } L \neq F(\sqrt{-1}), \\ c \text{ or } \zeta c, & \text{if } L = F(\sqrt{-1}), \end{cases}$$

without affecting the equation  $\sigma(\alpha) = \alpha^{2^{e-1}-1}\beta^{2^e}$ .

If  $L \neq F(\sqrt{-1})$ , then  $-1 \in F^2$  (since  $-1 \in L^2$ ) and  $N_{L/F}(\alpha) \in F^{2^{e-1}} \cup a^{2^{e-2}}F^{2^{e-1}} \subseteq F^2$ , since  $e \geq 3$ . If  $\alpha\beta^2 = \sqrt{ac}$ , then  $N_{L/F}(\alpha) \in -aF^2 = aF^2 \neq F^2$ , a contradiction. Thus  $\alpha\beta^2 = c$ .

If  $L = F(\sqrt{-1})$  and  $\alpha\beta^2 = \zeta c$ , then

$$N_{L/F}(\alpha) = (\alpha\beta^2)^{2^{e-1}} = (\zeta c)^{2^{e-1}} = -c^{2^{e-1}} \in -F^2 \neq F^2.$$

Then the equation  $\alpha\beta^2 = \zeta c$  implies  $N_{L/F}(\zeta) \notin F^2$ , and thus  $N_{L/F}(\zeta) = -1$  and  $r \equiv 2^{e-1} - 1 \pmod{2^e}$  by Proposition 4.9.

We conclude  $\alpha\beta^2 = \theta c$ , where

$$\theta = \begin{cases} 1, & \text{if } L \neq F(\sqrt{-1}), \\ 1, & \text{if } L = F(\sqrt{-1}), r \equiv -1 \pmod{2^e}, \\ 1 \text{ or } \zeta, & \text{if } L = F(\sqrt{-1}), r \equiv 2^{e-1} - 1 \pmod{2^e}. \end{cases}$$

Let  $\gamma = c^{2^{e-3}}\beta$ . Then

$$\alpha = \theta c/\beta^2 = \theta c^{2^{e-2}+1}/(c^{2^{e-2}}\beta^2) = \theta c^{2^{e-2}+1}/\gamma^2.$$

Since  $N_{L/F}(\alpha) = (\alpha\beta^2)^{2^{e-1}} = \theta^{2^{e-1}} c^{2^{e-1}}$  and  $\theta^{2^{e-1}} = N_{L/F}(\theta)$  in all cases, we have

$$N_{L/F}(\gamma^2) = c^{2^{e-1}} N_{L/F}(\beta^2) = c^{2^{e-1}} N_{L/F}(\theta c/\alpha) = \frac{c^{2^{e-1}} \theta^{2^{e-1}} N_{L/F}(c)}{N_{L/F}(\alpha)} = c^2.$$

Thus  $N_{L/F}(\gamma) = \pm c$ . □

## 5. EXPLICIT CONSTRUCTIONS OF GALOIS EXTENSIONS $M/F$

Proposition 3.1 and Lemma 3.2 let us reduce the problem of describing explicit constructions of Galois extensions  $M/F$  as in Section 3 to the case  $n = p^e$ , where  $p$  is a prime number. In this section, we treat the case when  $p$  is an odd prime. The case  $p = 2$  will be handled in Section 6. Recall that  $r \bmod n$  is defined by  $\sigma(\zeta) = \zeta^r$ , where  $\zeta$  is a primitive  $n^{\text{th}}$  root of unity. Since  $j^2 \equiv r^2 \equiv 1 \pmod{p^e}$ , it follows that if  $p$  is odd, then  $j \equiv \pm 1 \pmod{p^e}$  and  $r \equiv \pm 1 \pmod{p^e}$ . Since it is no extra trouble, instead of considering only the case  $n = p^e$  with  $p$  odd, we will consider the more general case where  $n$  is arbitrary and  $j \equiv \pm 1 \pmod{n}$  and  $r \equiv \pm 1 \pmod{n}$ . Of course the case  $r \equiv 1 \pmod{n}$  occurs if and only if  $\zeta \in F$ . Recall from Proposition 2.5 that when  $j \equiv 1 \pmod{n}$ , either  $G \cong \mathbb{Z}/2n\mathbb{Z}$  or  $G \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , and when  $j \equiv -1 \pmod{n}$ , either  $G \cong D_n$  or  $G \cong Q_{2n}$ .

We saw in Theorem 3.4(3) that when  $M = L(\alpha^{1/n})$  realizes  $(G, j, l)$ , then  $\sigma(\alpha) = \alpha^t \beta^n$ , where  $t \equiv jr \pmod{n}$ . So,  $t \equiv \pm 1 \pmod{n}$ . By Theorem 3.4(1), we can assume that  $t = \pm 1$ . To be able to handle the two possible values of  $t$  at the same time, and to bring out the similarities in the two cases, we consider a modified group action. It will be convenient to use the language of group cohomology, though everything in this section can be derived easily without mentioning cohomology.

Let  $C = \text{Gal}(L/F) = \{1, \sigma\}$ . Let  $t = \pm 1$ . For any multiplicative group  $Q$  on which  $C$  acts, we have a “twisted”  $t$ -action of  $C$  on  $Q$  defined by

$$\sigma * q = (\sigma \cdot q)^t.$$

(Here  $\cdot$  denotes the original action and  $*$  denotes the  $t$ -action.) Of course, when  $t = 1$  the  $t$ -action coincides with the original action. Let  $\mu_n = \langle \zeta \rangle$  denote the group of  $n^{\text{th}}$  roots of unity in  $L$ . The short exact sequences

$$1 \rightarrow L^{*n} \rightarrow L^* \rightarrow L^*/L^{*n} \rightarrow 1 \quad \text{and} \quad 1 \rightarrow \mu_n \rightarrow L^* \rightarrow L^{*n} \rightarrow 1$$

are compatible with the usual Galois action of  $\text{Gal}(L/F)$ , but also with the  $t$ -action. They lead to connecting homomorphisms in cohomology (using the  $t$ -action):

$$f: H^0(C, L^*/L^{*n}) \rightarrow H^1(C, L^{*n}) \quad \text{and} \quad g: H^1(C, L^{*n}) \rightarrow H^2(C, \mu_n).$$

We describe the maps  $f$  and  $g$ : First,  $H^0(C, L^*/L^{*n})$  consists of the elements  $[\alpha] = \alpha L^{*n} \in L^*/L^{*n}$  stable under the  $t$ -action of  $C$ , i.e., those  $[\alpha]$  such that  $\sigma * [\alpha] = [\alpha]$ , i.e.,

$$\sigma * \alpha = \alpha \gamma^n \text{ for } \gamma \in L^*, \quad \text{i.e.,} \quad \sigma(\alpha) = \alpha^t \beta^n, \text{ where } \beta = \gamma^t.$$

The connecting map  $f$  takes the class of the 0-cocycle  $[\alpha]$  to the class of the 1-cocycle  $c_{\gamma^n}: C \rightarrow L^{*n}$  mapping  $1 \mapsto 1$  and  $\sigma \mapsto \gamma^n$ . Let  $N_t$  denote the “ $t$ -norm,” given by

$$N_t(x) = x \sigma * x = x \sigma(x)^t.$$

Note that by applying  $N_t$  to the equation  $\sigma * \alpha = \alpha \gamma^n$  we find that  $N_t(\gamma^n) = 1$ . Let

$$\omega = N_t(\gamma) = \gamma \sigma(\gamma)^t = \beta^t \sigma(\beta) \in \mu^n.$$

The map  $g$  takes the class of  $c_{\gamma^n}$  to the class of the 2-cocycle  $h_\omega: C \times C \rightarrow \mu_n$  given by  $h_\omega(\sigma, \sigma) = N_t(\gamma) = \omega$  and  $h_\omega(1, 1) = h_\omega(\sigma, 1) = h_\omega(1, \sigma) = 1$ . Thus,  $g \circ f[\alpha] = [h_\omega] \in H^2(C, \mu_n)$ .

Now, the  $t$ -action of  $C$  on  $\mu_n$  is determined by  $\sigma * \zeta = \sigma(\zeta)^t = \zeta^{rt} = \zeta^j$ , where  $j = rt$ . The group extension of  $C$  by  $\mu_n$  determined by the 2-cocycle  $h_\omega$  is the group  $\mathfrak{G} = \mu_n x_1 \cup \mu_n x_\sigma$ , with the multiplication given by (cf. [R], p. 154)  $(\zeta^i x_\rho)(\zeta^k x_\psi) = \zeta^i (\rho * \zeta^k) h_\omega(\rho, \psi) x_{\rho\psi}$ . If  $\omega = \zeta^l$ , then  $\mathfrak{G}$  is the group of order  $2n$  generated by  $\zeta, x_\sigma$  with the relations  $\zeta^n = 1, x_\sigma \zeta x_\sigma^{-1} = \sigma * \zeta = \zeta^j$ , and  $x_\sigma^2 = \zeta^l$ . That is,  $\mathfrak{G} \cong (G, j, l)$ . Observe also that for this  $j$  and  $l$ , we have  $(G, j, l) \cong \text{Gal}(L(\alpha^{1/n})/F)$ , by Theorem 3.4(3) (assuming  $[L(\alpha^{1/n}) : L] = n$ ). Now,  $\mathfrak{G}$  is the trivial group extension (i.e., a semidirect product, i.e.,  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  when  $j \equiv 1 \pmod n$  and  $D_n$  when  $j \equiv -1 \pmod n$ ) just when  $[h_\omega] = 0 \in H^2(C, \mu_n)$ . This occurs just when  $\omega$  is the  $t$ -norm of an element of  $\mu_n$  (cf. [R], Th. 10.35, p. 297), i.e., just when  $\omega = \zeta^l \in \langle N_t(\zeta) \rangle = \langle \zeta^{j+1} \rangle$ . Note in any case that since  $\omega = N_t(\gamma)$ ,  $\omega = \sigma * \omega = \omega^j$ . When  $j \equiv -1 \pmod n$  this says that  $\omega = \pm 1$ , and  $\mathfrak{G}$  is the trivial extension just when  $\omega = 1$ . When  $j \equiv 1 \pmod n$ ,  $\mathfrak{G}$  is the trivial extension just when  $\omega \in \langle \zeta^2 \rangle$ . When  $n$  is odd, we have  $H^2(C, \mu_n) = 0$  as  $\text{gcd}(|C|, |\mu_n|) = 1$ , so then  $\mathfrak{G}$  is always the trivial extension.

When  $t = 1$  we can say a little more. Then, the  $t$ -action is the usual  $C$ -action. Since  $H^1(C, L^*) = 0$  (Hilbert 90), the exact sequence  $H^1(C, L^*) \rightarrow H^1(C, L^{*n}) \xrightarrow{g} H^2(C, \mu_n)$  shows that the map  $g$  is injective. But, we also have the exact sequence  $H^0(C, L^*) \rightarrow H^1(C, L^*/L^{*n}) \xrightarrow{f} H^1(C, L^{*n})$ . Thus,  $[\alpha] \in H^0(C, L^*/L^{*n})$  determines the trivial group extension  $\Leftrightarrow g \circ f[\alpha] = 0$  in  $H^2(C, \mu_n) \Leftrightarrow f[\alpha] = 0 \Leftrightarrow [\alpha] \in \text{im}(H^0(C, L^*) \rightarrow H^0(C, L^*/L^{*n})) = F^* L^{*n}/L^{*n} \Leftrightarrow \alpha \in F^* L^{*n}$ . When  $n$  is odd, this always holds because then  $H^2(C, \mu_n) = 0$ .

The following propositions summarize what the preceding discussion has shown.

**Proposition 5.1.** *Assume that  $M/F$  is a Galois extension that realizes  $(G, j, l)$ . Thus  $\sigma(\alpha) = \alpha^t \beta^n$ , with  $\alpha, \beta \in L$ . Assume  $j \equiv 1 \pmod n$  and  $r \equiv \pm 1 \pmod n$ . Then,  $t \equiv r \pmod n$ . Assume  $t = \pm 1$  (and adjust  $\beta$  accordingly). Then,  $\beta^t \sigma(\beta)$  is an  $n^{\text{th}}$  root of unity. Furthermore,*

1. The following statements are equivalent.

- (a)  $\text{Gal}(M/F) \cong \mathbb{Z}/2n\mathbb{Z}$ .
- (b) The order of  $\beta^t\sigma(\beta)$  is divisible by  $2^{e_0}$ .
- (c)  $\beta^t\sigma(\beta) \in \zeta\langle\zeta^2\rangle$ .
- (d)  $n$  is odd or  $l$  is odd.

If  $n$  is odd, then (a)-(d) always hold. If  $n$  is even, then (a)-(d) are equivalent to the following statement.

- (e)  $(\beta^t\sigma(\beta))^{n/2} = -1$ .

2. The following statements are equivalent.

- (a)  $\text{Gal}(M/F) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- (b) If  $n$  is even, then the order of  $\beta^t\sigma(\beta)$  is not divisible by  $2^{e_0}$ .
- (c)  $\beta^t\sigma(\beta) \in \langle\zeta^2\rangle$ .
- (d)  $n$  is odd or  $l$  is even.

If  $r \equiv 1 \pmod{n}$  (i.e.,  $\zeta \in F$ ), so  $t = 1$ , then (a)-(d) are equivalent to the following statement.

- (e)  $\alpha \in F \cdot L^n$ .

If  $n$  is odd, then (a)-(e) always hold.

**Proposition 5.2.** *Assume  $M/F$  is a Galois extension that realizes  $(G, j, l)$  with  $j \equiv -1 \pmod{n}$  and  $r \equiv 1 \pmod{n}$ . Then,  $t \equiv -1 \pmod{n}$ , and we assume  $t = -1$ . Suppose  $\sigma(\alpha) = \alpha^t\beta^n$  with  $\beta \in L$ .*

1. The following statements are equivalent.

- (a)  $\text{Gal}(M/F) \cong D_n$ .
- (b)  $l \equiv 0 \pmod{n}$ .
- (c)  $N_{L/F}(\alpha) \in F^n$ .
- (d)  $\beta \in F$ .

If  $n$  is odd, then (a)-(d) always hold.

2. Assume  $n$  is even (and hence  $\text{char } F \neq 2$ ). Let  $L = F(\sqrt{a})$ . Then  $\beta \in F \cup \sqrt{a}F$  and  $N_{L/F}(\alpha) \in F^n \cup a^{n/2}F^n$ . In addition, the following statements are equivalent.

- (a)  $\text{Gal}(M/F) \cong Q_{2n}$ .
- (b)  $l \equiv n/2 \pmod{n}$ .
- (c)  $N_{L/F}(\alpha) \in a^{n/2}F^n$ .
- (d)  $\beta \in \sqrt{a}F$ .

*Proof.* In addition to the observations preceding Proposition 5.1, note the following: Because  $t = -1$ , we have  $\sigma(\alpha) = \alpha^{-1}\beta^n$ , so  $N_{L/F}(\alpha) = \beta^n$ . Since  $j \equiv -1 \pmod{n}$ ,  $\beta/\sigma(\beta) = N_t(\beta) \in \{\pm 1\} \cap \mu_n$ . So  $\sigma(\beta) = \pm\beta$ . The Galois group is  $D_n$  just when  $\sigma(\beta) = \beta$ , i.e.,  $\beta \in F$ ; then  $N_{L/F}(\alpha) = \beta^n \in F^n$ . We have  $\text{Gal}(M/F) \cong Q_{2n}$  just when  $\sigma(\beta) = -\beta$ , i.e.,  $\beta \in \sqrt{a}F$ ; then  $n$  is necessarily even since  $-1 \in \mu_n$ , and  $N_{L/F}(\alpha) \in a^{n/2}F^n \neq F^n$ .  $\square$

**Proposition 5.3.** *Assume  $M/F$  is a Galois extension that realizes  $(G, j, l)$  with  $j \equiv -1 \pmod n$  and  $r \equiv -1 \pmod n$ . Then, we may assume  $t = 1$ . Suppose  $\sigma(\alpha) = \alpha^t \beta^n$  with  $\beta \in L$ .*

1. *The following statements are equivalent.*
  - (a)  $\text{Gal}(M/F) \cong D_n$ .
  - (b)  $l \equiv 0 \pmod n$ .
  - (c)  $N_{L/F}(\beta) = 1$ .
  - (d)  $\alpha \in F \cdot L^n$ .*If  $n$  is odd, then (a)-(d) always hold.*
2. *The following statements are equivalent.*
  - (a)  $\text{Gal}(M/F) \cong Q_{2n}$ .
  - (b)  $l \equiv n/2 \pmod n$ .
  - (c)  $N_{L/F}(\beta) = -1$ .

## 6. THE CASE WHEN $n = 2^e$ WITH $e \geq 3$

We now study the problem of constructing Galois extensions  $M/F$ , which were considered in Section 3, when  $n = 2^e$  with  $e \geq 1$ . We have  $L = F(\sqrt{a})$ ,  $a \in F$ , since  $\text{char } F \neq 2$ . We continue to assume that  $\zeta \in L$  is a primitive  $(2^e)^{\text{th}}$  root of unity and that  $\sigma(\zeta) = \zeta^r$ . We shall assume  $e \geq 3$  since the cases when  $e \leq 2$  are covered in Propositions 5.1–5.3 when  $j \equiv \pm 1 \pmod n$  and  $r \equiv \pm 1 \pmod n$ . If  $M/F$  is a Galois extension that realizes  $(G, j, l)$  with  $n = 2^e$  and  $e \geq 3$ , then by Theorem 3.4(3),  $\sigma(\alpha) = \alpha^t \beta^n$  with  $\beta \in L$ ,  $t \equiv jr \pmod{2^e}$  and  $t, j, r \in \{1, -1, 2^{e-1} + 1, 2^{e-1} - 1\} \pmod{2^e}$ . By Theorem 3.4(1), we may assume that  $t \in \{1, -1, 2^{e-1} + 1, 2^{e-1} - 1\}$ . If  $j \equiv 2^{e-1} + 1$  or  $2^{e-1} - 1 \pmod{2^e}$ , then the group  $\text{Gal}(M/F)$  is uniquely determined up to isomorphism, by Lemma 2.4. Therefore, we shall focus only on values of  $t$  and  $r$  that give  $j \equiv 1$  or  $-1 \pmod{2^e}$ . So, if  $t \in \{1, -1\}$ , then  $r \equiv 1$  or  $-1 \pmod{2^e}$  since  $t \equiv jr \pmod{2^e}$ . These cases have already been discussed in §5. Thus, we can assume in this section that  $t \in \{2^{e-1} + 1, 2^{e-1} - 1\}$ . The interesting cases are when  $r \equiv 2^{e-1} + 1$  or  $2^{e-1} - 1 \pmod{2^e}$ .

**Proposition 6.1.** *Suppose  $M = L(\alpha^{1/2^e})$  is a Galois extension of  $F$  of degree  $2^{e+1}$  ( $e \geq 3$ ) which realizes  $(G, j, l)$  with  $t = 2^{e-1} + 1$ , i.e.,  $\sigma(\alpha) = \alpha^{2^{e-1}+1} \beta^{2^e}$  for some  $\beta \in L$ . So,  $\alpha = \varphi N_{L/F}(\gamma) \eta^2 / \gamma^{2^{e-1}}$ , where  $\gamma \in L^*$ ,  $\eta \in F \cup \sqrt{a}F$  and*

$$\varphi = \begin{cases} 1, & \text{if } r \equiv 1, -1, \text{ or } 2^{e-1} - 1 \pmod{2^e}, \\ 1 \text{ or } \zeta, & \text{if } r \equiv 2^{e-1} + 1 \pmod{2^e}. \end{cases}$$

1. *Suppose  $r \equiv 2^{e-1} + 1 \pmod{2^e}$  (so  $j \equiv 1 \pmod{2^e}$ ). Then,*
  - (a)  $\text{Gal}(M/F) \cong \mathbb{Z}/2^{e+1}\mathbb{Z}$  if and only if  $\varphi = \zeta$ , if and only if  $N_{L/F}(\alpha) \in aF^2$ .
  - (b)  $\text{Gal}(M/F) \cong \mathbb{Z}/2^e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  if and only if  $\varphi = 1$ , if and only if  $N_{L/F}(\alpha) \in F^2$ .

2. Suppose  $r \equiv 2^{e-1} - 1 \pmod{2^e}$  (so  $j \equiv -1 \pmod{2^e}$ ). Then,

- (a)  $\text{Gal}(M/F) \cong D_{2^e}$  if and only if  $\eta \in F$ .
- (b)  $\text{Gal}(M/F) \cong Q_{2^{e+1}}$  if and only if  $\eta \in \sqrt{a}F$ .

*Proof.* The description of  $\alpha$  is given in Proposition 4.10. We have  $(t^2 - 1)/2^e = 2^{e-2} + 1$  and  $\alpha = \varphi N_{L/F}(\gamma)\eta^2/\gamma^{2^{e-1}}$ . Equation (1) in the proof of Proposition 4.10 shows that  $\sigma(\alpha)/\alpha = (\alpha(\beta')^2)^{2^{e-1}}$ , where  $\beta' = \gamma^{2^{e-2}}/(\sigma(\gamma)\eta)$ . Thus, we may let  $\beta = \beta'$  here. Let  $\rho = \alpha^{(t^2-1)/2^e}\beta^t\sigma(\beta)$ . By Theorem 3.4(3),  $\rho = \zeta^{l_1}$ , where  $l_1 \equiv l \pmod{\text{gcd}(j+1, 2^e)}$ . Now,  $\alpha\beta^2 = \varphi\gamma/\sigma(\gamma)$ , which yields

$$\rho = (\alpha\beta^2)^{2^{e-2}} \alpha N_{L/F}(\beta) = \varphi^{2^{e-2}+1} \eta/\sigma(\eta).$$

Note that since  $\eta^2 \in F$ , we have  $\eta/\sigma(\eta) = \pm 1 \in \langle \zeta^2 \rangle$ . Also, the formula for  $\alpha$  shows that  $N_{L/F}(\alpha) \in N_{L/F}(\varphi)F^2$ .

For (1), suppose  $r \equiv 2^{e-1} + 1 \pmod{2^e}$ . Then, as  $t \equiv jr \pmod{2^e}$ , we have  $j \equiv 1 \pmod{2^e}$ . So,  $\rho = \varphi^{2^{e-2}+1} \eta/\sigma(\eta) \in \varphi \langle \zeta^2 \rangle$ . We have  $\text{Gal}(M/F) \cong \mathbb{Z}/2^e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  just when  $l$  is even, which (since  $\varphi = 1$  or  $\zeta$ ) occurs just when  $\varphi = 1$ . In this case,  $N_{L/F}(\alpha) \in F^2$ . The only other possibility is that  $\text{Gal}(M/F) \cong \mathbb{Z}/2^{e+1}\mathbb{Z}$ , which occurs just when  $l$  is odd, so just when  $\varphi = \zeta$ . Since  $\sigma(\zeta) = -\zeta$  and  $-1 \in F^2$  by Proposition 4.8, we have  $\zeta^2 F^2 = aF^2 = -aF^2$ . Thus, when  $\varphi = \zeta$  we have  $N_{L/F}(\alpha) \in N_{L/F}(\varphi)F^2 = -\zeta^2 F^2 = aF^2 \neq F^2$ .

For (2), suppose  $r \equiv 2^{e-1} - 1 \pmod{2^e}$ . Then,  $j \equiv -1 \pmod{2^e}$  and  $\varphi = 1$ , so  $\rho = \eta/\sigma(\eta) = \pm 1$ . We have  $\text{Gal}(M/F) \cong D_{2^e}$  just when  $l \equiv 0 \pmod{2^e}$ , which occurs just when  $\rho = 1$ ; this occurs just when  $\sigma(\eta) = \eta$ , i.e.,  $\eta \in F$ . The only other possibility is that  $\text{Gal}(M/F) \cong Q_{2^{e+1}}$ , which occurs just when  $l \equiv 2^{e-1} \pmod{2^e}$ . This holds just when  $\rho = -1$ , i.e.,  $\sigma(\eta) = -\eta$ , i.e.,  $\eta \in \sqrt{a}F$ .  $\square$

**Proposition 6.2.** *Suppose  $M = L(\alpha^{1/2^e})$  is a Galois extension of  $F$  of degree  $2^{e+1}$  ( $e \geq 3$ ) which realizes  $(G, j, l)$  with  $t = 2^{e-1} - 1$ , i.e.,  $\sigma(\alpha) = \alpha^{2^{e-1}-1}\beta^{2^e}$ . So,  $\alpha = \theta c^{2^{e-2}+1}/\gamma^2$  where  $\gamma \in L^*$ ,  $N_{L/F}(\gamma) = \pm c$ , and*

$$\theta = \begin{cases} 1, & \text{if } r \equiv 1, -1, \text{ or } 2^{e-1} + 1 \pmod{2^e}, \\ 1 \text{ or } \zeta, & \text{if } r \equiv 2^{e-1} - 1 \pmod{2^e}, \end{cases}$$

- 1. Suppose  $r \equiv 2^{e-1} - 1 \pmod{2^e}$  (so  $j \equiv 1 \pmod{2^e}$ ). Then,
  - (a)  $\text{Gal}(M/F) \cong \mathbb{Z}/2^{e+1}\mathbb{Z}$  if and only if  $\theta = \zeta$ , if and only if  $N_{L/F}(\alpha) \in -F^2$ .
  - (b)  $\text{Gal}(M/F) \cong \mathbb{Z}/2^e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  if and only if  $\theta = 1$ , if and only if  $N_{L/F}(\alpha) \in F^2$ .
- 2. Suppose  $r \equiv 2^{e-1} + 1 \pmod{2^e}$  (so  $j \equiv -1 \pmod{2^e}$ ). Then,
  - (a)  $\text{Gal}(M/F) \cong D_{2^e}$  if and only if  $N_{L/F}(\gamma) = c$ .
  - (b)  $\text{Gal}(M/F) \cong Q_{2^{e+1}}$  if and only if  $N_{L/F}(\gamma) = -c$ .

*Proof.* The proof is very similar to the proof of Proposition 6.1. The description of  $\alpha$  is given in Proposition 4.11. Since  $\alpha = \theta c^{2^{e-2}+1}/\gamma^2$ , the first paragraph of the proof of Proposition 4.11 shows that we can take  $\beta = \gamma/c^{2^{e-3}}$ . Let

$\rho = \alpha^{(t^2-1)/2^e} \beta^t \sigma(\beta) = \zeta^{l_1}$ , where  $l_1 \equiv l \pmod{\gcd(j+1, 2^e)}$ . Since  $(t^2 - 1)/2^e = 2^{e-2} - 1$  and  $\alpha\beta^2 = \theta c$ , we have

$$\rho = (\alpha\beta^2)^{2^{e-2}} \sigma(\beta)/(\alpha\beta) = \theta^{2^{e-2}-1} N_{L/F}(\gamma)/c.$$

The rest of the proof is left to the reader.  $\square$

In Propositions 6.1 and 6.2 it was assumed that  $[L(\alpha^{1/2^e}) : L] = 2^e$ . The next three results will allow us to identify when this occurs.

**Lemma 6.3.** *If  $r \equiv 2^{e-1} \pm 1 \pmod{2^e}$ ,  $e \geq 3$ , and  $c \in F^*$ , then  $\zeta c \notin L^2$ .*

*Proof.* First assume that  $r \equiv 2^{e-1} + 1 \pmod{2^e}$ . If  $\zeta c \in L^2$ , then  $N_{L/F}(\zeta) \in F^2$ , but we saw in the proof of Proposition 6.1 that  $N_{L/F}(\zeta) \in aF^2 \neq F^2$ . Hence,  $\zeta c \notin L^2$ .

Now assume that  $r \equiv 2^{e-1} - 1 \pmod{2^e}$ . Proposition 4.8 implies that  $L = F(\sqrt{-1})$ . Now Proposition 4.9(2) implies that  $\zeta \notin F \cdot L^2$  and thus  $\zeta c \notin L^2$ .  $\square$

**Corollary 6.4.** *Let  $\alpha = \varphi N_{L/F}(\gamma) \eta^2 / \gamma^{2^{e-1}}$  as in Propositions 4.10 and 6.1. Then  $[L(\alpha^{1/2^e}) : L] = 2^e$  if and only if  $\alpha \notin L^2$ , which holds if and only if  $\varphi = \zeta$  or  $N_{L/F}(\gamma) \notin F \cap L^2 = F^2 \cup aF^2$ .*

*Proof.* Since  $-1 \in L^2$ , it is standard that  $[L(\alpha^{1/2^e}) : L] = 2^e$  if and only if  $\alpha \notin L^2$ , see, e.g. [L], Theorem 9.1, p. 297. The formula for  $\alpha$  shows that this is equivalent to:  $\varphi N_{L/F}(\gamma) \notin L^2$ . This holds if  $\varphi = \zeta$  by Lemma 6.3, since then  $r \equiv 2^{e-1} + 1 \pmod{2^e}$ ; if  $\varphi = 1$ , this holds just when  $N_{L/F}(\gamma) \notin L^2 \cap F$ .  $\square$

**Corollary 6.5.** *Let  $\alpha = \theta c^{2^{e-2}+1} / \gamma^2$  as in Propositions 4.11 and 6.2. Then,  $[L(\alpha^{1/2^e}) : L] = 2^e$  if and only if  $\alpha \notin L^2$ , which holds if and only if  $\theta = \zeta$  or  $c \notin F \cap L^2 = F^2 \cup aF^2$ .*

*Proof.* The formula for  $\alpha$  shows that  $\alpha \notin L^2$  just when  $\theta c \notin L^2$ . The rest of the proof is analogous to the proof of Corollary 6.4.  $\square$

## REFERENCES

- [B] B. G. Basmaji, On the isomorphism of two metacyclic groups, *Proc. Amer. Math. Soc.*, **22** (1969), 175–182.
- [CR] C. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley-Interscience, New York, (1962).
- [D<sub>1</sub>] P. Damey, Sur certaines 2-extensions non abéliennes d'un corps de caractéristique différente de 2, cycliques sur une extension quadratique intermédiaire, *C. R. Acad. Sc. Paris*, **269** (1969), 503–506.
- [D<sub>2</sub>] P. Damey, Sur l'existence de certaines 2-extensions galoisiennes non abéliennes d'un corps  $\varkappa$  de caractéristique différente de 2, cycliques sur une extension quadratique de  $\varkappa$ , *C. R. Acad. Sc. Paris*, **274** (1972), 441–443.
- [DM] P. Damey and J. Martinet, Plongement d'une extension quadratique dans une extension quaternionienne, *J. Reine Angew. Math.*, **262/263** (1973), 323–338.

- [DP] P. Damey and J.-J. Payan, Existence et construction des extensions galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique différente de 2, *J. Reine Angew. Math.*, **244** (1970), 37–54.
- [G] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.
- [GSS] H. G. Grundman, T. L. Smith, and J. R. Swallow, Groups of order 16 as Galois groups, *Expo. Math.*, **13** (1995), 289–319.
- [J] C. U. Jensen, On the representations of a group as a Galois group over an arbitrary field, pp. 441 - 458 in *Théorie des nombres: comptes rendus de la Conférence internationale de théorie des nombres tenue à l'Université Laval, 5-18 juillet 1987*, eds. J.-M. de Koninck and C. Levesque, de Gruyter, Berlin, 1989.
- [K] I. Kiming, Explicit classifications of some 2-extensions of a field of characteristic different from 2, *Canad. J. Math.*, **42** (1990), 825–855.
- [L] S. Lang, *Algebra*, 3<sup>rd</sup> ed., Addison-Wesley, Reading Mass., (1993).
- [MM] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer, Berlin, 1999.
- [R] J. Rotman, *An introduction to homological algebra*, Academic Press, New York, (1979).
- [V] 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 address:* yhwang@semi.korea.ac.kr

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KENTUCKY, LEXINGTON, KY 40506-0027 U.S.A  
*E-mail address:* leep@ms.uky.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SAN DIEGO, CALIFORNIA 92093-0112, USA  
*E-mail address:* arwadsworth@ucsd.edu