Mathematica
Balkanica

New Series Vol. 21, 2007, Fasc. 1-2

Embedding Obstructions for the Cyclic and Modular 2-Groups [1]

Ivo M. Michailov

Presented by V. Kiryakova

In this paper, we consider certain embedding problems with kernel a cyclic 2-group. Our goal is to compute the obstructions in specific cases to realizability of the modular group $M_{2^{n+3}}$ and the group $C_{2^{n+2}} \times C_2$ ($n \geq 1$) over an arbitrary field with characteristic not 2. Also, we give a description of all Galois extensions realizing these groups over a quadratic extension, containing a primitive $(2^{n+2})^{\mathrm{th}}$ root of unity ζ.

AMS Subj. Classification: 12F12

1. Introduction

Let K/k be a Galois extension with Galois group H, and let

$$1 \to A \to G \underset{\pi}{\to} H \to 1 \tag{1.1}$$

be a finite group extension. The embedding problem given by K/k and (1.1) then consists of determining whether there exists a Galois extension L/k, such that $K \subset L$, $G \cong \mathrm{Gal}(L/k)$ and the homomorphism of restriction to K of the automorphisms from G coincides with π. The group A is called the *kernel* of the embedding problem. The problem we denote by $(K/k, G, A)$. The existence of a Galois algebra with the above properties is also known as *'weak' solvability*. When a Galois extension is available it is also called a *'proper' solution*.

Let k be of characteristic not 2, let ζ be a primitive 2^nth root of unity in K, and let μ_{2^n} be the cyclic group generated by ζ. If A is a cyclic group of order 2^n such that A and μ_{2^n} have the same H-module structure, we call the embedding problem *Brauer*. Assume that we have the Brauer problem given by K/k and the group extension

$$1 \to \mu_{2^n} \to G \underset{\pi}{\to} H \to 1. \tag{1.2}$$

Then we have the map $H^2(H, \mu_{2^n}) \to H^2(H, K^*) \cong \mathrm{Br}(K/k)$, induced by the inclusion map $\mu_{2^n} \hookrightarrow K^*$. Thus we can consider the 2-coclass c of the extension (1.2) as an element of the relative Brauer group $\mathrm{Br}(K/k)$. Let $\Gamma = (K, H, c)$ be the crossed product algebra, corresponding to the extension (1.2). Then the equivalence class $[\Gamma] = [K, H, c] \in \mathrm{Br}(K/k)$ is called the *obstruction*, and its splitting in the absolute Brauer group $\mathrm{Br}(k)$, i.e., $[\Gamma] = 1$, gives us the solvability condition of the Brauer problem. A necessary condition for solvability is the solvability of the associated embedding problem given by K/k and the group extension

$$1 \to \mu_{2^{n-1}} \to G/C_2 \underset{\pi}{\to} H \to 1,$$

which has as obstruction $[\Gamma]^2 \in \mathrm{Br}(k)$. If $[\Gamma]^2 = 1 \in \mathrm{Br}(k)$, then by the Merkuriev theorem [10] follows that Γ may be decomposed into quaternion and matrix algebras. We will use the standard notation (a, b) for the equivalence class of the quaternion algebra $(a, b/k)$ generated over k by the elements i and j, such that $i^2 = a, j^2 = b$ and $ij = -ji$. Information about Brauer groups and quaternion algebras can be found for example in [7].

We apply the following main results in order to investigate cyclic and modular embedding problems.

Theorem 1.1. *Let K/k be a finite Galois extension with Galois group H, and let $\zeta \in K$ be a primitive 2^nth root of unity $(n > 1)$, such that $\zeta + \zeta^{-1} \in k$ and $i(\zeta - \zeta^{-1}) \in k$. Let $N = \mathrm{Gal}(K/k(i))$ and H act trivially on C_{2^n}. Then the embedding problem $(K/k, G, C_{2^n})$ given by*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} H \to 1, \tag{1.3}$$

is solvable, if and only if the embedding problems $(K/k(i), \pi^{-1}(N), \mu_{2^n})$ and $(K/k, G/C_{2^{n-1}}, \mu_2)$, given by

$$1 \to \mu_{2^n} \to \pi^{-1}(N) \underset{\pi}{\to} N \to 1, \tag{1.4}$$

and

$$1 \to \mu_2 \to G/C_{2^{n-1}} \underset{\pi'}{\to} H \to 1, \tag{1.5}$$

are solvable.

P r o o f. Let $\bar{k}$ be the algebraic separable closure of k with profinite Galois group $\bar{H}$. Denote by $c \in H^2(H, C_{2^n}), c_1 \in H^2(N, \mu_{2^n})$ and $c_2 \in H^2(H, \mu_2)$ the cohomology classes respectively of (1.3), (1.4) and (1.5). Denote also by $\bar{c} \in H^2(\bar{H}, C_{2^n}), \bar{c}_1 \in H^2(\bar{N}, \mu_{2^n})$ and $\bar{c}_2 \in H^2(\bar{H}, \mu_2)$ the rise of c, c_1 and c_2, respectively, where $\bar{H} = \mathrm{Gal}(\bar{k}/k), \bar{N} = \mathrm{Gal}(\bar{k}/k(i))$.

Assume the embedding problems

$$(K/k(i), \pi^{-1}(N), \mu_{2^n}) \text{ and } (K/k, G/C_{2^{n-1}}, \mu_2)$$

are solvable. Then $\bar{c}_1 = 1$ and $\bar{c}_2 = 1$ by [4], Theorem 3.13.2. But from [12], §4,5, follows that $\bar{c}_1 = \mu\bar{c}$ and $\bar{c}_2 = \nu\bar{c}$, where the homomorphism $\mu : H^2(\bar{H}, C_{2^n}) \to H^2(\bar{N}, \mu_{2^n})$ is the restriction map and the homomorphism $\nu : H^2(\bar{H}, C_{2^n}) \to H^2(\bar{H}, \mu_2)$ is induced by the epimorphism $C_{2^n} \to C_2$. It remains to apply [1], Lemma 2 to obtain $\bar{c} = 1$, hence the embedding problem $(K/k, G, C_{2^n})$ is solvable. ∎

Corollary 1.2. *Let K/k be a finite Galois extension with Galois group H, and let ζ be a primitive 2^nth root of unity ($n > 1$), such that $\zeta + \zeta^{-1} \in k, i(\zeta - \zeta^{-1}) \in k$ and $i \notin K$. Let*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} H \to 1$$

be a group extension. The embedding problem $(K/k, G, C_{2^n})$ is solvable, if and only if the embedding problems $(K(i)/k(i), G, \mu_{2^n})$ and $(K/k, G/C_{2^{n-1}}, \mu_2)$ given by

$$1 \to \mu_{2^n} \to G \underset{\pi}{\to} H \to 1,$$

and

$$1 \to \mu_2 \to G/C_{2^{n-1}} \underset{\pi'}{\to} H \to 1,$$

are solvable.

Our intention at first was to compute the obstructions to several embedding problems in connection with the modular and cyclic 2-groups. This is done in Sections 2 and 3. The main reason to work with these groups is because, in our view, the modular group is often unregarded in the publications of the authors, who discuss 2-groups as Galois groups. The recent publication [5] gave us the idea to describe all $M_{2^{n+3}}$ and $C_{2^{n+2}} \times C_2$ ($n \geq 1$) extensions, containing a quadratic extension, which in turn, contains a primitive $(2^{n+2})^{\text{th}}$ root of unity ζ. This is done in Sections 6 and 7.

2. The cyclic group

We denote by C_{2^n} the cyclic group of order 2^n generated by the element σ. First consider the problem given by the quadratic extension $k(\sqrt{a})/k$ for $a \in k^* \setminus k^{*2}$ and the group extension

$$1 \to C_2 = \{\pm 1\} \hookrightarrow C_4 \to C_2 \to 1. \tag{2.1}$$

The obstruction is well known: $(a,a) \in \mathrm{Br}(k)$. Now let $(a,a) = 1 \in \mathrm{Br}(k)$. We can assume that $a = 1 + c^2, c \in k^*$. The full set of solutions of (2.1) is given by $\{k(\sqrt{r(a+\sqrt{a})}) \mid r \in k^*\}$. Indeed, if we set $\varphi = \sqrt{r(a+\sqrt{a})}, \psi = \sqrt{r(a-\sqrt{a})}$ and $K = k(\varphi)$ then $\mathrm{Gal}(K/k)$ is generated by the element $\sigma : \varphi \mapsto \psi, \psi \mapsto -\varphi$, where $\varphi\psi = rc\sqrt{a}$.

It is also known that the obstruction to the embedding problem $(K/k, C_8, C_2)$ given by the group extension

$$(2.2) \qquad 1 \to C_2 = \{\pm 1\} \hookrightarrow C_8 \to C_4 \to 1.$$

is $(a,2)(-1,r) \in \mathrm{Br}(k)$. In terms of norm maps the problem is solvable if and only if $-1 \in N_{K/k}(K^*)$. If $i \in k$ then the embedding problem given by $k(\sqrt{a})/k$ and (2.1) is always solvable and all solutions are described as $K/k = k(\sqrt[4]{a'})/k$, where $a' = [2r(1-ic)]^2 a$. In this case the obstruction to the embedding problem given by K/k and (2.2) is $(a,2)(-1,r) = (a,2) = (a,i) \in \mathrm{Br}(k)$.

Now, let $\zeta \in k$ be a primitive 2^nth root of unity $(n \geq 1)$, let $K/k = k(\sqrt[4]{a})/k$ be a C_4 extension, and let $\sigma \in C_4$ be given by $\sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$.

Lemma 2.1. *For the embedding problem $(K/k, C_{2^{n+2}}, \mu_{2^n})$ given by the group extension*

$$(2.3) \qquad 1 \to \mu_{2^n} \hookrightarrow C_{2^{n+2}} \to C_4 \to 1$$

to be solvable $(n \geq 1)$, it is necessary that there exist $\alpha, \beta \in k, \alpha \neq 0$, such that $\alpha^2 - a\beta^2 = \zeta$. In that case the obstruction is $(a,\alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$.

P r o o f. We proceed by induction. For $n = 1$ we have $i^2 = -1 = \zeta$ so we can let $\alpha = i, \beta = 0$ to get the obstruction $(a,i) \in \mathrm{Br}(k)$.

Now, assume that the embedding problem given by K/k and

$$1 \to \mu_{2^{n-1}} \hookrightarrow C_{2^{n+1}} \to C_4 \to 1$$

is solvable. Then we let $\alpha = \zeta, \beta = 0$, so the obstruction is $(a,\zeta)(\zeta^2, 0) = (a,\zeta) \in \mathrm{Br}(k)$. We note that when elements j and $k \neq 0$ with relations $j^2 = c^2, k^2 = 0$ and $jk = -kj$ show up in a centralizer, they demonstrate that it is split, even though they do not generate it. But the solvability of the associated problem $(K/k, C_4, \mu_{2^{n-1}})$ is necessary for the solvability of the embedding problem $(K/k, C_{2^{n+2}}, \mu_{2^n})$. Hence we must have $(a,\zeta) = 1 \in \mathrm{Br}(k)$, so there exist $\alpha, \beta \in k$, such that $\alpha^2 - a\beta^2 = \zeta$. We can always obtain $\alpha \neq 0$ in the following manner: Since $i \in k$, we have $\zeta = x^2 + y^2$, for some $x, y \in k, y \neq 0$. If $-a\beta^2 = \zeta$ then we let $\alpha' = y(1 + x^2/y^2) \neq 0$ and $\beta' = i\beta x/y$, and get $\alpha'^2 - a\beta'^2 = y^2(1 + x^2/y^2)^2 + a\beta^2 x^2/y^2 = \zeta(1 + x^2/y^2) - \zeta x^2/y^2 = \zeta$

Now consider the algebra $\Gamma = k[\sqrt[4]{a}, u], u^4 = \zeta, ux = \sigma(x)u, \forall x \in K$, representing the obstruction. We have the following two quaternion subalgebras in Γ:

$$Q_1 : i_1 = \sqrt{a}, \quad j_1 = (\alpha + \beta\sqrt{a} + iu^2)u,$$
$$Q_2 : i_2 = u^2, \quad j_2 = \sqrt[4]{a}(\alpha + i\beta\sqrt{a} + u^2).$$

We have $i_1 j_1 = -j_1 i_1, i_2 j_2 = -j_2 i_2, i_1^2 = a, j_1^2 = ((\alpha + iu^2)^2 - a\beta^2)u^2 = (\alpha^2 + 2\alpha i u^2 - u^4 - a\beta^2)u^2 = 2\alpha i\zeta, i_2^2 = \zeta, j_2^2 = \sqrt{a}((\alpha + i\beta\sqrt{a})^2 - u^4) = \sqrt{a}(\alpha^2 + 2\alpha\beta i\sqrt{a} - \beta^2 a - \zeta) = 2\alpha\beta i a$. Clearly i_1 commutes with Q_2 and i_2 commutes with Q_1. Finally, verify $j_2 j_1 = j_1 j_2$:

$$\begin{aligned} j_2 j_1 &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha i u^2 + \alpha\beta i\sqrt{a} + i\beta^2 a - \beta\sqrt{a}u^2 + \alpha u^2 + \beta\sqrt{a}u^2 + i\zeta)u \\ &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a}(1+i) + \alpha(1+i)u^2 + i(a\beta^2 + \zeta))u \\ &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha u^2)(1+i)u \end{aligned}$$

and

$$\begin{aligned} j_1 j_2 = &(\alpha + \beta\sqrt{a} + iu^2)\sqrt[4]{a} i(\alpha - i\beta\sqrt{a} + u^2)u = \sqrt[4]{a}(\alpha + \beta\sqrt{a} - iu^2)(\alpha - i\beta\sqrt{a} + \\ & u^2)iu = \sqrt[4]{a}(\alpha^2 - \alpha\beta i\sqrt{a} + \alpha u^2 + \alpha\beta\sqrt{a} - i\beta^2 a + \beta\sqrt{a}u^2 - \alpha i u^2 - \beta\sqrt{a}u^2 - \\ & i\zeta)iu = \sqrt[4]{a}(\alpha^2 - i\beta^2 a - i\zeta + \alpha\beta\sqrt{a}(1-i) + \alpha u^2(1-i))iu = \sqrt[4]{a}(\alpha^2 + \\ & \alpha\beta\sqrt{a} + \alpha u^2)(1-i)iu = \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha u^2)(1+i)u. \end{aligned}$$

Thus the quaternion algebras commute, so we get

$$[\Gamma] = [Q_1][Q_2] = (a, 2\alpha i\zeta)(\zeta, 2\alpha\beta i a) = (a, \alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k).$$

■

We now turn our attention to the case when ζ is a primitive 2^nth root of unity such that $\zeta + \zeta^{-1}$ and $i(\zeta - \zeta^{-1})$ are both in k. It turns out that the obstructions play an important role not only for the cyclic and modular groups, but as well for the dihedral, semidihedral and quaternion groups considered in [11]. We will investigate the three possible cases according to the location of i in $K(i)$:

1. $i \in k$. We can then write $K/k = k(\sqrt[4]{a})/k, a \in k^*$. As we saw in Lemma 2.1 the obstruction to the embedding problem $(K/k, C_{2^{n+2}}, \mu_{2^n})$ is $(a, \alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$, where the existence of $\alpha, \beta \in k, \alpha \neq 0$, such that $\alpha^2 - a\beta^2 = \zeta$ is necessary for solvability. In particular the quadratic extension $k(\sqrt{a})/k$ can be embedded in a $C_{2^{n+2}}$ extension, if and only if

$k(\sqrt[4]{r^2 a})/k$ can be embedded in a $C_{2^{n+2}}$ extension for some $r \in k^*$. Hence the embedding problem given by $k(\sqrt{a})/k$ and the group extension

$$1 \to C_{2^{n+1}} \hookrightarrow C_{2^{n+2}} \to C_2 \to 1$$

is solvable, if and only if $(a,\zeta) = 1 \in \mathrm{Br}(k)$ and $(a,\alpha)(\zeta, r\alpha\beta) = 1 \in \mathrm{Br}(k)$.

2. $a = -1$. We must have $-1 = u^2 + v^2$ for some $u, v \in k$ and $K = k(\sqrt{r(1-iu)})$, $r \in k^*$. By Theorem 1.1 for $a' = r(1-iu)$ the embedding problem
$(k(\sqrt{a'})/k, C_{2^{n+2}}, C_{2^n})$ related to the group extension

$$1 \to C_{2^n} \hookrightarrow C_{2^{n+2}} \to C_4 \to 1 \tag{2.4}$$

is solvable, if and only if the embedding problems $(k(\sqrt{a'})/k(i), C_{2^{n+1}}, C_{2^n})$ and $(K/k, C_8, C_2)$ related to

$$1 \to C_{2^n} \hookrightarrow C_{2^{n+1}} \to C_2 \to 1 \tag{2.5}$$

and (2.2) are solvable. But the embedding problem related to (2.5) is solvable, if and only if the embedding problem $(k(\sqrt[4]{r'^2 a'})/k, C_{2^{n+1}}, C_{2^{n-1}})$ is solvable for some $r' \in k^*$. Since ${\alpha'}^2 - a'{r'}^2{\beta'}^2 = \zeta^2$ is satisfied for $\alpha' = \zeta$, $\beta' = 0$, by Lemma 2.1 the obstruction is $(a',\alpha')(\zeta^2, \alpha'\beta') = (a',\alpha') = (a',\zeta) = (r(1-iu),\zeta) \in \mathrm{Br}(k(i))$. Respectively, the obstruction to the embbedding problem related to (2.2) is $(-1,r) \in \mathrm{Br}(k)$. Hence the embbedding problem $(k(\sqrt{a'})/k, C_{2^{n+2}}, C_{2^n})$ is solvable, if and only if $(-1,r) = 1 \in \mathrm{Br}(k)$ and $(r(1-iu),\zeta) = 1 \in \mathrm{Br}(k(i))$.

In particular $k(i)/k$ can be embedded in a $C_{2^{n+2}}$ extension, if and only if $(-1,-1) = 1 \in \mathrm{Br}(k)$, $(-1,r) = 1 \in \mathrm{Br}(k)$ and $(r(1-iu),\zeta) = 1 \in \mathrm{Br}(k(i))$ for some $r \in k^*$, where $u, v \in k^*$ are such that $-1 = u^2 + v^2$.

3. a and -1 are quadratically independent. Here $K = k(\sqrt{r(a+\sqrt{a})})$ and $K(i) = k(i, \sqrt[4]{a'})$ for $a' = [2r(1-ic)]^2 a$. By Corollary 1.2 the embed-ding problem $(K/k, C_{2^{n+2}}, C_{2^n})$ is solvable, if and only if the embedding problems $(K(i)/k(i), C_{2^{n+2}}, \mu_{2^n})$ and $(K/k, C_8, C_2)$ are solvable. Hence the embedding problem $(K/k, C_{2^{n+2}}, C_{2^n})$ is solvable, if and only if $(a,2)(-1,r) = 1 \in \mathrm{Br}(k)$ and $(a,\alpha')(\zeta,\alpha'\beta') = 1 \in \mathrm{Br}(k(i))$,where $\alpha' \in k(i)^*, \beta' \in k$, such that ${\alpha'}^2 - a'{\beta'}^2 = \zeta$.

In particular the quadratic extension $k(\sqrt{a})/k$ can be embedded in a $C_{2^{n+2}}$ extension, if and only if $(a,a) = 1$, $(a,2)(-1,r) = 1 \in \mathrm{Br}(k)$ and
$(a,\alpha')(\zeta,\alpha'\beta') = 1 \in \mathrm{Br}(k(i))$ for some $r \in k^*$, where $x, y \in k^*$, such that $a = x^2 + y^2$ and $\alpha' \in k(i)^*, \beta' \in k(i)$, such that ${\alpha'}^2 - [2r(x-iy)]^2 a{\beta'}^2 = \zeta$. Here $K(i) = k(i, \sqrt[4]{a''})$ for $a'' = [2r(x-iy)]^2 a$.

In this way we obtained the following theorem.

Theorem 2.2. *Let ζ be a primitive 2^nth root of unity, such that $\zeta+\zeta^{-1} \in k$ and $i(\zeta - \zeta^{-1}) \in k$. Let $K/k = k(\sqrt{r(a+\sqrt{a})})/k$ be a C_4 extension for $a = 1 + c^2$, $r \in k^*$. Then the embedding problem given by K/k and the group extension* (2.4) *has the following obstructions for $n \geq 2$:*

1. *$i \in k$ (i.e., $\zeta \in k$) : $(a, \alpha)(\zeta, r\alpha\beta) \in \mathrm{Br}(k)$, where we must have $\alpha \in k^*, \beta \in k$, such that $\alpha^2 - a\beta^2 = \zeta$.*
2. *$a = -1$: $(-1, r) \in \mathrm{Br}(k)$ and $(r(1 - iu), \zeta) \in \mathrm{Br}(k(i))$, where we must have $-1 = u^2 + v^2$ for some $u, v \in k$ and $K = k(\sqrt{r(1 - iu)})$.*
3. *a and -1 are quadratically independent : $(a, 2)(-1, r) \in \mathrm{Br}(k)$ and $(a, \alpha)(\zeta, r(1 - ic)\alpha\beta) \in \mathrm{Br}(k(i))$, where we must have $\alpha \in k(i)^*, \beta \in k(i)$, such that $\alpha^2 - a\beta^2 = \zeta$.*

Similarly to the case $n = 2$, considered in [9], one can show that the embedding problem related to (2.4) is solvable if and only if $-1 \in N_{K/k}(K^*)$ and $\zeta \in N_{K(i)/k(i)}(K(i)^*)$ – a particular case of [1], Theorem 3.

3. The modular group

The modular group of order 2^n, $n \geq 4$, is given by the presentation:

$$M_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, yx = x^{2^{n-2}+1}y\rangle.$$

Let $K = k(\varphi)$ and let $L/k = k(\varphi, \sqrt{b})/k$ be a $C_4 \times C_2$ extension, where $\varphi = \sqrt{r(a+\sqrt{a})}, \psi = \sqrt{r(a-\sqrt{a})}$ and $a = 1 + c^2$; $a, b, c, r \in k^*$. Let $\mathrm{Gal}(L/k)$ be generated by the elements σ and τ, such that $\sigma : \varphi \mapsto \psi, \sqrt{b} \mapsto \sqrt{b}$; $\tau : \varphi \mapsto \varphi, \sqrt{b} \mapsto -\sqrt{b}$.

Lemma 3.1. *The obstruction to the embedding problem $(L/k, M_{16}, C_2)$ related to the group extension*

$$1 \to C_2 = \langle x^4\rangle \hookrightarrow M_{16} \to C_4 \times C_2 \to 1 \tag{3.1}$$

is $(a, 2b)(-1, r) \in \mathrm{Br}(k)$.

P r o o f. The obstruction is represented by the cyclic algebra $\Gamma = (L, C_4 \times C_2, -1) = L[u, v]$, where $u^4 = -1, v^2 = 1, vu = -uv, ux = \sigma(x)u$ and $vx = \tau(x)v$, $x \in L$. We have the following three quaternion subalgebras in Γ:

$$\begin{aligned} Q_1 &: i_1 = \sqrt{a}, \quad j_1 = u + u^3, \\ Q_2 &: i_2 = u^2, \quad j_2 = (\varphi + \psi u^2)\sqrt{a}, \\ Q_3 &: i_3 = \sqrt{b}, \quad j_3 = \sqrt{a}v. \end{aligned}$$

It is not hard to see that Q_1, Q_2 and Q_3 centralize each other, so
$[\Gamma] = [Q_1][Q_2][Q_3] = (a, -2)(-1, 2ra^2)(b, a) = (a, 2b)(-1, r) \in \mathrm{Br}(k)$. ■

In terms of norm maps the embedding problem $(L/k, M_{16}, C_2)$ is solvable, if and only if $-1/b^2 \in N_{K/k}(K^*)$ (see [8], Example 3.3).

As we did before we will investigate embedding problems with cyclic 2-kernel. For the following theorem we introduce some notations : Let $\zeta \in k$ be a primitive 2^nth root of unity ($n \geq 2$), let $K = k(\sqrt[4]{a})$ and let $L/k = k(\sqrt[4]{a}, \sqrt{b})/k$ be a $C_4 \times C_2$ extension, where C_4 is generated by σ and C_2 is generated by τ, such that $\sigma\sqrt[4]{a} = i\sqrt[4]{a},\ \sigma\sqrt{b} = \sqrt{b};\ \tau\sqrt[4]{a} = \sqrt[4]{a},\ \tau\sqrt{b} = -\sqrt{b}$.

Lemma 3.2. *For the embedding problem $(L/k, M_{2^{n+3}}, \mu_{2^n})$ related to the group extension*

$$1 \to \mu_{2^n} = \langle x^4 \rangle \hookrightarrow M_{2^{n+3}} \to C_4 \times C_2 \to 1 \tag{3.2}$$

to be solvable, it is necessary that there exist $\alpha \in k^*, \beta \in k$, such that $\alpha^2 - a\beta^2 = \zeta$. In that case the obstruction is $(a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$.

Proof. If the embedding problem related to (3.2) is solvable then the associated problem given by L/k and

$$1 \to \mu_{2^{n-1}} \hookrightarrow C_{2^{n+1}} \times C_2 \to C_4 \times C_2 \to 1$$

is also solvable. Since ζ^2 is a primitive 2^{n-1}th root of unity, the obstruction is $(a, \zeta) \in \mathrm{Br}(k)$ by Lemma 2.1. Therefore we must have $\alpha^2 - a\beta^2 = \zeta$ for some $\alpha \in k^*$ and $\beta \in k$.

The obstruction to the initial problem is represented by the algebra $\Gamma = (L, C_4 \times C_2, \zeta) = k[\sqrt[4]{a}, \sqrt{b}, u, v]$, where $u^4 = \zeta, v^2 = 1, vu = -uv, ux = \sigma(x)u$ and $vx = \tau(x)v,\ \forall x \in L$. We have the following three quaternion subalgebras in Γ:

$$\begin{aligned} &Q_1 : i_1 = \sqrt{a}, \quad j_1 = (\alpha + \beta\sqrt{a} + iu^2)u, \\ &Q_2 : i_2 = u^2, \quad j_2 = \sqrt[4]{a}(\alpha + i\beta\sqrt{a} + u^2) \\ &Q_3 : i_3 = \sqrt{b}, \quad j_3 = \sqrt{a}v. \end{aligned}$$

Since Q_1, Q_2 and Q_3 centralize each other, we get

$$[\Gamma] = [Q_1][Q_2][Q_3] = (a, 2\alpha i\zeta)(\zeta, 2\alpha\beta ia)(b, a) = (a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k).$$

Note that the newly found obstruction agrees with Lemma 3.1 for $n = 1$: we let $i \in k, \alpha = i, \beta = 0, \zeta = -1$ and get $(a, \alpha b)(\zeta, \alpha\beta) = (a, ib) = (a, 2b) \in \mathrm{Br}(k)$. ■

Now, let $\zeta + \zeta^{-1}$ and $i(\zeta - \zeta^{-1})$ be in k. We will consider five cases according to the location of i in $L(i)$. The elements σ and τ act trivially on the generator of the kernel x^4, so we can apply Theorem 1.1.

1. $i \in k$. By Lemma 3.2 the obstruction to the embedding problem given by $L/k = k(\sqrt[4]{a}, \sqrt{b})/k$ and (3.2) is $(a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$, where $\alpha^2 - a\beta^2 = \zeta$ for some $\alpha \in k^*$ and $\beta \in k$.

2. $a = -1$. We must have $-1 = u^2 + v^2$ for some $u, v \in k^*$ and $L = k(\sqrt{a'}, \sqrt{b})$, where $a' = r(1 - iu)$, $r \in k^*$. Then the embedding problem $(L/k, M_{2^{n+3}}, C_{2^n})$ related to

$$(3.3) \qquad 1 \to C_{2^n} \hookrightarrow M_{2^{n+3}} \to C_4 \times C_2 \to 1$$

is solvable, if and only if the embedding problems $(L/k(i), C_{2^{n+1}} \times C_2, \mu_{2^n})$ and $(L/k, C_8 \times C_2, C_2)$ are solvable. The obstructions are: $(r(1-iu), \zeta) \in \mathrm{Br}(k(i))$ and $(-1, r) \in \mathrm{Br}(k)$.

3. $b = -1$. We can then write $L/k = k(\sqrt{r(a + \sqrt{a})}, i)/k$ and $L/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, where $a' = [2r(1 - ic)]^2 a$. Then the embedding problem given by L/k and (3.3) is solvable, if and only if the embedding problems $(L/k(i), C_{2^{n+2}}, \mu_{2^n})$ and $(L/k, C_8 \times C_2, C_2)$ are solvable. The obstructions are: $(a, \alpha')(\zeta, \alpha'\beta') \in \mathrm{Br}(k(i))$ and $(a, 2)(-1, r) \in \mathrm{Br}(k)$, where ${\alpha'}^2 - a'{\beta'}^2 = \zeta$ for some $\alpha' \in k(i)^*$ and $\beta' \in k(i)$.

4. $ab = -1$. We can again write $L/k = k(\sqrt{r(a + \sqrt{a})}, i)/k$ and $L/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, where $a' = [2r(1 - ic)]^2 a$. It is not hard to see that the obstructions are the same as in the previous case.

5. a, b and -1 are quadratically independent. By Corollary 1.2 the embedding problem given by L/k and (3.3) is solvable, if and only if the embedding problems $(L(i)/k(i), M_{2^{n+3}}, C_{2^n})$ and $(L/k, C_8 \times C_2, C_2)$ are solvable. The obstructions are: $(a, \alpha' b)(\zeta, \alpha'\beta') \in \mathrm{Br}(k(i))$ and $(a, 2)(-1, r) \in \mathrm{Br}(k)$, where ${\alpha'}^2 - a'{\beta'}^2 = \zeta$ for some $\alpha' \in k(i)^*$ and $\beta' \in k(i)$. Here denote $L(i)/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, where $a' = [2r(1 - ic)]^2 a$ and $K = k(\varphi)$.

We can summarize the obstructions to the embedding problem related to (3.3) in the following theorem.

Theorem 3.3. *Let ζ be a primitive 2^nth root of unity, such that $\zeta + \zeta^{-1} \in k$ and $(\zeta - \zeta^{-1})/i \in k$. Let $L/k = k(\sqrt{r(a + \sqrt{a})}, \sqrt{b})/k$ be a $C_4 \times C_2$ extension for $a = 1 + c^2$, $b, r \in k^*$. Then the embedding problem given by L/k and the group extension* (3.3) *has the following obstructions for $n \geq 2$:*

1. *$i \in k$ (i.e., $\zeta \in k$) : $(a, \alpha b)(\zeta, r\alpha\beta) \in \mathrm{Br}(k)$, where we must have $\alpha \in k^*, \beta \in k$, such that $\alpha^2 - a\beta^2 = \zeta$.*

2. $a = -1$ *:* $(-1, r) \in \mathrm{Br}(k)$ *and* $(r(1-iu), \zeta) \in \mathrm{Br}(k(i))$*, where we must have* $-1 = u^2 + v^2$ *for some* $u, v \in k$ *and* $L = k(\sqrt{r(1-iu)}, \sqrt{b})$*.*

3. $b = -1$ *or* $ab = -1$ *:* $(a, 2)(-1, r) \in \mathrm{Br}(k)$ *and* $(a, \alpha)(\zeta, r(1-ic)\alpha\beta) \in \mathrm{Br}(k(i))$*, where we must have* $\alpha \in k(i)^*, \beta \in k(i)$*, such that* $\alpha^2 - a\beta^2 = \zeta$*.*

4. a, b *and* -1 *are quadratically independent :* $(a, 2)(-1, r) \in \mathrm{Br}(k)$ *and* $(a, \alpha b)(\zeta, r(1-ic)\alpha\beta) \in \mathrm{Br}(k(i))$*, where we must have* $\alpha \in k(i)^*, \beta \in k(i)$*, such that* $\alpha^2 - a\beta^2 = \zeta$*.*

Example . . Let $\zeta \in k$ be a primitive $(2^{n+1})^{\text{th}}$ root of unity. Then we can set $\alpha = \zeta, \beta = 0 \ : \ \alpha^2 - a\beta^2 = \zeta^2$, so the obstruction to the embedding problem related to (3.3) is $(a, \alpha b)(\zeta^2, r\alpha\beta) = (a, \zeta b) \in \mathrm{Br}(k)$. If $b = \zeta \notin k^2$ then the embedding problem related to (3.3) is solvable and $k(\sqrt[2^{n+2}]{a}, \sqrt{\zeta})$ is a solution.

The special case $\sqrt{\zeta} \in k$ is discussed in the following proposition.

Proposition 3.4. *Let* $\zeta = \zeta_{2^{n+2}} \in k$ *be a primitive* $(2^{n+2})^{\text{th}}$ *root of unity. Then the obstruction to solvability of the embedding problem* $(K/k, M_{2^{n+3}}, \mu_{2^n})$ *is* $(a, b) \in Br(k)$*. Let* $(a, b) = 1 \in Br(k)$ *and assume* $\gamma, \delta \in k^*$ *are such that* $\gamma^2 - b\delta^2 = a$*. Let* $\omega = \gamma + \sqrt{b}\delta$ *and* $\theta = \sqrt[4]{a}/\omega^{2^{n-1}}$*. Then* $M/k = K(\sqrt[2^n]{\theta})/k$ *is a Galois extension and a solution to* $(K/k, M_{2^{n+3}}, \mu_{2^n})$*.*

Proof. From the example follows that the obstruction is $(a, b) \in Br(k)$, since the primitive $(2^{n+1})^{\text{th}}$ root of unity ζ^2 is in k^2. Now, let $(a, b) = 1 \in Br(k)$ and assume $\gamma, \delta \in k^*$ are such that $\gamma^2 - b\delta^2 = a$. Let $\omega = \gamma + \sqrt{b}\delta$ and $\theta = \sqrt[4]{a}/\omega^{2^{n-1}}$. We have

$$\sigma(\theta)/\theta = i = \zeta^{2^n}$$

and

$$\tau(\theta)/\theta = \frac{(\gamma^2 - b\delta^2)^{2^{n-1}}}{(\gamma + \sqrt{b}\delta)^{2^n}} = a_\tau^{2^n},$$

where $a_\tau = \sqrt{a}/(\gamma + \sqrt{b}\delta) \in K$. Now we can set for the generators x and y of $M_{2^{n+3}}$: $x(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}\zeta$ and $y(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau$, so that $x|_K = \sigma$ and $y|_K = \tau$. Then $x^{2^{n+2}}(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}$ and $y^2(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}$, whence $|x| = 2^{n+2}$ and $|y| = 2$. Furthermore, $yx(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau\zeta$ and $x^{2^{n+1}+1}(\sqrt[2^n]{\theta}) = x(-\sqrt[2^n]{\theta}) = -\sqrt[2^n]{\theta}\zeta$, whence $x^{2^{n+1}+1}y(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau\zeta$, so $yx = x^{2^{n+1}+1}y$. Therefore M/k is a Galois extension, that is a solution to the embedding problem $(K/k, M_{2^{n+3}}, \mu_{2^n})$. ■

In the latter proposition we gave one particular modular extension of degree 2^{n+3} over k, where a primitive $(2^{n+2})^{\text{th}}$ root of unity is contained in k. In Sections 6 and 7 we will describe all $M_{2^{n+3}}$ and $C_{2^{n+2}} \times C_2$ extensions that contain a quadratic extension L/F, such that a primitive $(2^{n+2})^{\text{th}}$ root of unity ζ is in L (F is an arbitrary field with characteristic not 2).

4. An embedding criterion

Let H be a 2-group and let

$$1 \to C_{2^n} \to G \underset{\pi}{\to} H \times C_2 \to 1 \tag{4.1}$$

be a non-split group extension with characteristic 2-coclass $\gamma \in H^2(H\times C_2, C_{2^n})$. By $res_H\gamma$ we denote the 2-coclass of the group extension

$$1 \to C_{2^n} \to \pi^{-1}(H) \underset{\pi}{\to} H \to 1. \tag{4.2}$$

Lemmas 2.1 and 3.2 inspired the following criterion, where we express the obstruction to the Brauer problem related to (4.1) as a product of the obstruction to the Brauer problem related to (4.2) with the equivalence class of a quaternion algebra.

First, we introduce some notation. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a minimal generating set for the maximal elementary abelian factorgroup of H; and let τ be the generator of C_2. Denote by -1 the element of order 2 in C_{2^n}. Finally, let $s_1, s_2, \ldots, s_m, t \in G$ be preimages of $\sigma_1, \sigma_2, \ldots, \sigma_m, \tau$ such that $t^2 = (-1)^j$ and $ts_i = (-1)^{d_i} s_i t$, where $i \in \{1, 2, \ldots, m\}; j, d_i \in \{0, 1\}$.

Theorem 4.1. *Let $L/k = K(\sqrt{b})/k$ be a Galois extension with Galois group $H \times C_2$. Let (4.1) be a non-split group extension with the properties given above. Choose $a_1, a_2, \ldots, a_m \in k^*$ such that $\sigma_k\sqrt{a_i} = (-1)^{\delta_{ik}}\sqrt{a_i}$ (δ_{ik} is the Kronecker delta). Then the obstruction to the Brauer problem $(L/k, G, C_{2^n})$ is*

$$[K, H, res_H\gamma] \cdot (b^j \prod_{i=1}^m a_i^{d_i}, b) \in \mathrm{Br}(k).$$

P r o o f. The crossed product algebra $B = (K, H, res_H\gamma)$ is included in $A = (L, H\times C_2, \gamma)$, therefore A is a tensor product of B with the centralizer of B in $A : A = B \otimes_k C_A(B)$. Now, consider the algebra $k[\sqrt{b}, \sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t] \subset A$. Since $t^2 = (-1)^j$, we have

$$(\sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t)^2 = (-1)^j b^j \prod_{i=1}^m a_i^{d_i} t^2 = b^j \prod_{i=1}^m a_i^{d_i}.$$

$t\sqrt{b} = -\sqrt{b}t$, hence $k[\sqrt{b}, \sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t]$ is a quaternion algebra isomorphic to $(b, b^j \prod_{i=1}^m a_i^{d_i}/k)$.

We will show that $C_A(B) = (b, b^j \prod_{i=1}^m a_i^{d_i}/k)$. Indeed, from $s_k\sqrt{b} = \sqrt{b}s_k$ follows that $\sqrt{b}$ is in $C_A(B)$. Finally,

$$\begin{aligned} s_k\sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t &= \sqrt{b}^j \prod_{i=1}^m ((-1)^{\delta_{ik}}\sqrt{a_i})^{d_i} s_k t \\ &= \sqrt{b}^j \prod_{i=1}^m ((-1)^{\delta_{ik}}\sqrt{a_i})^{d_i}(-1)^{d_k} t s_k = (-1)^{d_k}\prod_{i=1}^m (-1)^{\delta_{ik}d_i}\sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t s_k \\ &= (-1)^{d_k}(-1)^{\sum_{i=1}^m \delta_{ik}d_i}\sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t s_k = \sqrt{b}^j \prod_{i=1}^m \sqrt{a_i}^{d_i} t s_k, \end{aligned}$$

since $\sum_{i=1}^m \delta_{ik}d_i = d_k$. Since B is generated by K and $s_1, \ldots, s_m$, we have that B commutes with the quaternion algebra $(b, b^j \prod_{i=1}^m a_i^{d_i}/k)$. ■

Consider again the embedding problem $(L/k, M_{2^{n+3}}, \mu_{2^n})$. Since $\tau^2 = 1$ and $\tau\sigma = -\sigma\tau$ we once again obtain that the obstruction is $(a,\alpha)(\zeta,\alpha\beta)(a,b) = (a,\alpha b)(\zeta,\alpha\beta) \in \mathrm{Br}(k)$, where $\alpha \in k^*, \beta \in k$, are such that $\alpha^2 - a\beta^2 = \zeta$. Note that solvability of the cyclic and modular embedding problems is in terms of Galois extensions since the kernels are contained in the Frattini subgroup.

If $n = 1$ and H is the elementary abelian 2-group, we obtain as a corollary the well known criterion [8], Cor. 2.6.

5. Preliminaries for a description of Galois extensions

Let F be an arbitrary field with char $\neq 2$. Let $n \geq 1$ be an integer, let $m = 2^{n+2}$ and assume that ζ is a primitive m^{th} root of unity, contained in a quadratic extension $L = F(\sqrt{a})$ of F. Our goal is to describe all Galois extensions M, realizing the groups M_{2m} and $C_m \times C_2$ as Galois groups over F, such that $L \subset M$ and M is cyclic over L. We will make an extensive use of the notations and results from [5]. Let M be a cyclic extension of degree m over L. Then $M = L(\alpha^{1/m})$ for some $\alpha \in L^*$ by Kummer theory. If $\mathrm{Gal}(L/F) = \{1, \sigma\}$ then M is Galois over F just when $\sigma(\alpha) = \alpha^t\beta^m$, where $\beta \in L^*$ and $t^2 \equiv 1 \pmod{m}$. In order to construct explicitly all such Galois extensions M/F, we have to give a detailed description of all elements α, satisfying $\sigma(\alpha) = \alpha^t\beta^m$.

Now, let G be a group generated by elements σ and τ such that

$$\begin{aligned} &1)\ |\tau| = m,\ \sigma \notin \langle\tau\rangle; \\ &2)\ \sigma\tau\sigma^{-1} = \tau^j,\ \sigma^2 = \tau^l; \\ &3)\ j^2 \equiv 1 \pmod{m} \text{ and } l(j-1) \equiv 0 \pmod{m}. \end{aligned} \tag{5.1}$$

In fact, each group of order $2m$ that contain a cyclic subgroup of order m is defined in this way. For example, if $j \equiv m/2 + 1$ and $l \equiv 0$, we obtain the modular group M_{2m}; if $j \equiv 1$ and $l \equiv 0$, we obtain the group $C_m \times C_2$. It is well known that there are four such non abelian groups – the modular, the dihedral, the semidihedral and the quaternion groups, and two abelian groups – $C_m \times C_2$ and C_{2m}.

Let us denote by (G, j, l) the group described by (5.1). There is only one group with exactness to an isomorphism for $j \equiv m/2 + 1$ – the group M_{2m}, and two groups for $j \equiv 1$ – $C_m \times C_2$ and C_{2m}. The goup $C_m \times C_2$ occurs just when l is even and the group C_{2m} occurs just when l is odd.

Remark. Some of the statements mentioned in this section are not at all obvious, but are thoroughly discussed in [5]. A good monograph on group theory, for example [2], can be very useful to the reader.

When we write $\alpha^{1/m}$ or $\sqrt[m]{\alpha}$, for $\alpha \in L^*$, we will assume some specified m^{th} root of α has been selected and fixed. Since L contains a primitive m^{th} root of unity ζ, $M = L(\sqrt[m]{\alpha})$ is a splitting field of $x^m - \alpha$ over L and hence M/L is a Galois extension. If $[M : L] = m$, then $\mathrm{Gal}(M/L) \cong C_m$. Furthermore, $\sigma(\zeta) = \zeta^r$, where r is an integer, such that $\gcd(r, m) = 1$. This equation defines $r \pmod m$, such that $r^2 \equiv 1$, since $\zeta = \sigma^2(\zeta) = \zeta^{r^2}$.

If $L \subset M$, we will say that M/F realizes (G, j, l) if M/F is a Galois extension with Galois group $(G, j, l) = \langle \tau, \sigma \rangle$, where $\mathrm{Gal}(M/L) = \langle \tau \rangle, \sigma$ denotes an extension of $\sigma \in \mathrm{Gal}(L/F)$ to an authomorphism in $\mathrm{Gal}(M/F), \sigma\tau\sigma^{-1} = \tau^j$, and $\sigma^2 = \tau^l$.

Now, we give several lemmas, which are special cases of [5], Lemma 4.1, Theorem 3.4, Propositions 4.4, 4.5 and 4.8. We suggest to the reader to prove them directly.

Lemma 5.1. *If $\delta, \delta' \in L^*$ and $\sigma(\delta)/\delta = \sigma(\delta')/\delta'$, then $\delta' = b\delta$ with $b \in F$.*

Lemma 5.2. *Assume $\zeta \in L$. Let $M = L(\sqrt[m]{\alpha})$, where $\alpha \in L$, and assume $[M : L] = m$. Then the following statements are equivalent.*

1. *M/F realizes (G, j, l).*
2. *$\sigma(\alpha) = \alpha^t \beta^m$, with $t \equiv jr \pmod m$ and $\alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, where $l_1 \equiv l \pmod{\gcd(j+1, m)}$.*

Lemma 5.3. *If $a \notin -F^2$ (i.e., $L = F(\sqrt{a}) \neq F(\sqrt{-1})$), then $F \cap L^m = F^m \cup a^{m/2}F^m$.*

Lemma 5.4. *Let $L = F(\sqrt{-1})$, and assume $\zeta \in L$ is a primitive $(2^{n+2})^{th}$ root of unity, $n \geq 0$. Then $F \cap L^{2^{n+1}} = F^{2^{n+1}} \cup -F^{2^{n+1}}$.*

Lemma 5.5. *$L \neq F(\sqrt{-1})$ (i.e. $\sqrt{-1} \in F$) if and only if $r \equiv 1 \pmod{2^{n+1}}$. When this occurs, $\zeta^2 \in F$; furthermore, $\zeta \in F$ if and only if $r \equiv 1 \pmod{2^{n+2}}$.*

We can restrict the values of t, j and r on the set $\{1, -1, 2^{n+1}+1, 2^{n+1}-1\}$. The modular group M_{2m} then appears just when $j \equiv 2^{n+1}+1$ $(n \geq 1), t^2 \equiv 1$ and $t \equiv jr$. Namely, the values of t and r are:

1. $t = 1, r \equiv 2^{n+1}+1$;
2. $t = -1, r \equiv 2^{n+1}-1$;
3. $t = 2^{n+1}+1, r \equiv 1$;
4. $t = 2^{n+1}-1, r \equiv -1$.

The group $C_m \times C_2$ occurs just when $j \equiv 1$ (i.e., $t \equiv r$) and l is even.

6. $L \neq F(\sqrt{-1})$

Lemma 5.5 implies that $L \neq F(\sqrt{-1})$ if and only if $r \equiv 1 \pmod{2^{n+1}}$, so the modular group occurs just when $t = 1$ and $r \equiv 2^{n+1}+1$, or $t = 2^{n+1}+1$ and $r \equiv 1$.

As always, when working with Galois extensions, norm maps play a key role. The norm map $N = N_{L/F} : L \to F^*$ is defined by $N(x) = x\sigma(x), \forall x \in L^*$. The following theorem gives an explicit description of all M_{2m} extensions in the casse $a \neq_2 -1$.

Theorem 6.1. *Let $\alpha \in L^*$. Then $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension for $a \neq_2 -1$ if and only if*

$$\alpha = \begin{cases} c(1+\gamma^m), \text{ if } r \equiv 2^{n+1}+1; c \in F^*, \gamma \in L^*, N(\gamma)^m = 1, 1+\gamma^m = b\delta^2, \\ \qquad\qquad b \in F^*, \delta \in L^*, \text{ and } bc \notin F^2 \cup aF^2, \\ \dfrac{N(\delta)\eta^2}{\delta^{2^{n+1}}}, \qquad \text{if } r \equiv 1; \delta, \eta \in L^*, \eta \in F \cup \sqrt{a}F, \text{ and } N(\delta) \notin F^2 \cup aF^2. \end{cases}$$

P r o o f. Assume that α is given by the formula in the statement of this theorem. If $\alpha = c(1+\gamma^m)$, then $\sqrt{\alpha} = \pm\sqrt{bc}\delta$, so $L(\sqrt{\alpha}) = F(\sqrt{bc}, \sqrt{a})$ is a biquadratic extension over F. It is not hard now to verify that $[M : L] = m$. Furthermore, $\sigma(\alpha)/\alpha = 1/\gamma^m = \beta^m \neq -1$ for $\beta = 1/\gamma$. Therefore, $\sigma(\alpha) = \alpha\beta^m$, so $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension.

If $\alpha = \dfrac{N(\delta)\eta^2}{\delta^{2^{n+1}}}$, then $\sqrt{\alpha} = \pm\dfrac{\sqrt{N(\delta)}\eta}{\delta^{2^n}}$, so $L(\sqrt{\alpha}) = F(\sqrt{N(\delta)}, \sqrt{a})$ is a biquadratic extension over F. Here again $[M : L] = m$. Furthermore,

$$\sigma(\alpha)/\alpha^{2^{n+1}} = \alpha\delta^{2^{2n+2}}/\sigma(\delta^{2^{n+2}})\eta^{2^{n+2}} = \alpha\beta^m,$$

where $\beta = \delta^{2^n}/\sigma(\delta)\eta$. Therefore, $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^m$, so M/F is an M_{2m} extension.

Now, assume that $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension. If $r \equiv 2^{n+1}+1$ and $\sigma(\alpha) = -\alpha$, then $\sigma(\alpha) = -\alpha = \alpha\beta^m$ for $\beta \in L$. Therefore, $-1 = \beta^m \in L^m$ and since $\sigma(\sqrt{a}) = -\sqrt{a}$, Lemma 5.1 implies $\alpha = b\sqrt{a}, b \in F^*$. Then $L(\sqrt{\alpha}) = F(\sqrt{b\sqrt{a}}, \sqrt{a})$ is a cyclic extension over F. But $L(\sqrt{\alpha})$ is the fixed field of τ^2, which must be a biquadratic extension over F, a contradiction.

If $r \equiv 2^{n+1} + 1$ and $\sigma(\alpha) \neq -\alpha$, then $t = 1$ and $\sigma(\alpha) = \alpha\beta^m$, where $1 + \beta^m \neq 0$. Let $\gamma = \sigma(\beta)$, so $1 + \gamma^m \neq 0$. From $\beta^m = \sigma(\alpha)/\alpha$ follows that $\beta^m\sigma(\beta^m) = N(\beta^m) = N(\gamma^m) = 1$. Furthermore,

$$\sigma(\alpha)/\alpha = \beta^m = \frac{1+\beta^m}{1+\sigma(\beta^m)} = \frac{\sigma(1+\gamma^m)}{1+\gamma^m},$$

hence by Lemma 5.1, $\alpha = c(1 + \gamma^m)$, where $c \in F^*$.

If $r \equiv 1$, then $t = 2^{n+1} + 1$ and $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^{2^{n+2}}$ for $\beta \in L$. Let $k = 2^{n+1} (k \geq 4$, since $n \geq 1)$. Then $\sigma(\alpha) = \alpha^{k+1}\beta^{2k}$ and $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$. Let $\omega = N(\alpha\beta^2)$. Then $\omega^k = N(\sigma(\alpha)/\alpha) = 1$, so ω is a power of ζ^2. Since $\zeta \in F$ when $r \equiv 1$, we obtain in particular that $\omega \in F^2$. Let $\gamma = \alpha\beta^2$. Then

$$\sigma(\alpha\gamma^{k/2}) = \alpha\gamma^k\sigma(\gamma^{k/2}) = \alpha\gamma^{k/2}N(\gamma)^{k/2} = \alpha\gamma^{k/2}\omega^{k/2}.$$

From $\omega^k = 1$ follows that $\omega^{k/2} = \pm 1$. If $\omega^{k/2} = -1$, we get

$$\alpha\gamma^{k/2} \in \sqrt{a}F, N(\alpha\gamma^{k/2}) \in -aF^2, N(\alpha) \in -aF^2, N(\alpha\beta^2) \in -aF^2,$$

and $\omega \in -aF^2 = aF^2 \neq F^2$ (since $-1 = \zeta^k \in F^2$), a contradiction. Therefore, $\omega^{k/2} = 1$. Now, from $\sigma(\alpha\gamma^{k/2}) = \alpha\gamma^{k/2}$ follows that $\alpha\gamma^{k/2} = b \in F^*$ and $\alpha\beta^2 = b\beta^2\gamma^{-k/2} = b\delta^2$, where $\delta = \beta/\gamma^{k/4}$. Since $b^2N(\delta)^2 = N(b\delta^2) = N(\alpha\beta^2) = \omega$, we have that $b^kN(\delta^k) = \omega^{k/2} = 1$. Hence

$$\sigma(\alpha)/\alpha = (\alpha\beta^2)^k = \delta^{2k}/N(\delta)^k = \delta^k/\sigma(\delta)^k$$

and $\sigma(\alpha\delta^k) = \alpha\delta^k$, so $\alpha\delta^k = d \in F$. Now, from $\sigma(\alpha)/\alpha = (\delta/\sigma(\delta))^k$ follows that $\alpha\beta^2 = \omega'\delta/\sigma(\delta) = \omega'c/\sigma(\delta)^2$, where $(\omega')^k = 1$ and $c = N(\delta)$. Furthermore, $\alpha/d = \delta^{-k} \in L^2$ and $\alpha/c = \omega'/(\sigma(\delta)^2\beta^2) \in L^2$, hence $d/c \in L^2 \cap F$. Let $\eta^2 = d/c \in L^2 \cap F = F^2 \cup aF^2$, so $\eta \in F \cup \sqrt{a}F$, and $\alpha = c\eta^2/\delta^k$.

The remaining follows from the fact that the fixed field $F(\sqrt{\alpha},\sqrt{a})$ of τ^2 must be a biquadratic extension over F. ■

The following theorem gives us a description of all $C_m \times C_2$ extensions.

Theorem 6.2. *Let $\alpha \in L^*$. Then $M/F = L(\sqrt[m]{\alpha})/F$ is a $C_m \times C_2$ extension for $a \neq_2 -1$ if and only if*

$$\alpha = \begin{cases} b\gamma^m, & \text{if } r \equiv 1; b \in F^*, \gamma \in L^*, \text{ and } b \notin F^2 \cup aF^2, \\ N(\delta)\eta^2/\delta^{2^{n+1}}, & \text{if } r \equiv 2^{n+1}+1; \delta, \eta \in L^*, \eta \in F \cup \sqrt{a}F, \text{ and} \\ & N(\delta) \notin F^2 \cup aF^2. \end{cases}$$

Proof. Assume that α is given by the formula in the statement of this theorem. If $\alpha = b\gamma^m$, where $b \in F^*, \gamma \in L^*$ and $r \equiv 1$, then $\sqrt{\alpha} = \sqrt{b}\gamma^{m/2}$, so $L(\sqrt{\alpha})$ is biquadratic over F and $[M : L] = m$. Furthermore, $\sigma(\alpha)/\alpha = (\sigma(\gamma)/\gamma)^m$, i.e., $\sigma(\alpha) = \alpha\beta^m$, where $\beta = \sigma(\gamma)/\gamma$. Therefore, $M/F = L(\sqrt[m]{\alpha})/F$ is either a $C_m \times C_2$ or a C_{2m} extension. Lemma 5.2 implies that $\alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, where $l_1 \equiv l \pmod{\gcd(j+1,m)}$. In this case, $t = 1, \beta\sigma(\beta) = 1$ and $l \equiv 0 \pmod{\gcd(j+1,m)}$, therefore l is even, so M/F is a $C_m \times C_2$ extension.

If $\alpha = N(\delta)\eta^2/\delta^{2^{n+1}}, \delta \in L^*, \eta \in F \cup \sqrt{a}F$ and $r \equiv 2^{n+1}+1$, then we obtain by identical argument to Theorem 6.1 that M/F is Galois and $[M : L] = m$. Furthermore, $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^{2^{n+2}}$, where $\beta = \delta^{2^n}/\sigma(\delta)\eta$, therefore $t = 2^{n+1}+1$ and $j \equiv 1$. From $\zeta^{l_1} = \alpha^{2^n+1}\beta^{2^{n+1}+1}\sigma(\beta) = \eta/\sigma(\eta) = \pm 1 \in \langle\zeta^2\rangle$ follows that M/F is a $C_m \times C_2$ extension.

Now, assume that $M/F = L(\sqrt[m]{\alpha})/F$ is a $C_m \times C_2$ extension. If $r \equiv 1$, then $t = 1$, so $\sigma(\alpha) = \alpha\beta^m, \beta \in L^*$. Furthermore, $\zeta^{l_1} = \beta\sigma(\beta) = \zeta^{2s}$, for some $s \geq 1$. Then $\beta/\zeta^s\sigma(\beta/\zeta^s) = 1$ and from Hilbert Theorem 90 follows that $\beta/\zeta^s = \sigma(\gamma)/\gamma$, for some $\gamma \in L^*$. Therefore, $\beta^m = \sigma(\gamma^m)/\gamma^m = \sigma(\alpha)/\alpha$ and Lemma 5.1 implies that $\alpha = b\gamma^m$, for some $b \in F^*$.

If $r \equiv 2^{n+1}+1$, then $t = 2^{n+1}+1$. Let $k = 2^{n+1}$. Then $\sigma(\alpha) = \alpha^{k+1}\beta^{2k}$, for some $\beta \in L^*(k \geq 4)$, hence $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$. Let $\omega = N(\alpha\beta^2)$. Then $\omega^k = N(\sigma(\alpha)/\alpha) = 1$. Since ω is a power of ζ^2, we have $\omega \in L^2 \cap F = F^2 \cup aF^2$. Let $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, where $l_1 \equiv l \pmod{\gcd(j+1,m)}$. Since l is even, $\rho \in \langle\zeta^2\rangle$. Hence $\rho = \alpha^{k/2+1}\beta^{k+1}\sigma(\beta)$ and $N(\alpha) = \alpha^{k+2}\beta^{2k} = \rho^2/N(\beta^2) \in F^2$, since $\zeta^2 \in L^2 \cap F = F^2 \cup aF^2$ and $\zeta^4 \in F^2$. Now, $\omega^k = 1$ implies $\omega^{k/2} = \pm 1$. If $\omega^{m/2} = -1$, we obtain similarly to Theorem 6.1 that $N(\alpha) \in aF^2 \neq F^2$, a contradiction. Therefore, $\omega^{m/2} = 1$. The rest of the proof is again similar to Theorem 6.1.

■

7. $L = F(\sqrt{-1})$

Lemma 5.5 implies that $L = F(\sqrt{-1})$ just when $r \equiv -1 \pmod{2^{n+1}}$, i.e., $r \equiv -1 \pmod{m}$ or $r \equiv 2^{n+1} - 1 \pmod{m}$, so the modular group occurs just when $t = -1$ and $r \equiv 2^{n+1} - 1$, or $t = 2^{n+1} - 1$ and $r \equiv -1$.

Theorem 7.1. *Let $\alpha \in L^*$. Then $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension for $a =_2 -1$ if and only if*

$$\alpha = \begin{cases} \pm b^{m/2} N(\gamma)/\gamma^2, & \text{if } r \equiv 2^{n+1} - 1; b \in F^*, \gamma \in L^* \text{ and } N(\gamma) \notin F^2 \cup -F^2, \\ \\ c^{2^n+1}/\delta^2, & \text{if } r \equiv -1; c \in F^*, \delta \in L^*, N(\delta) = \pm c \text{ and } c \notin F^2 \cup -F^2. \end{cases}$$

P r o o f. Assume that α is given by the formula in the statement of this theorem. If $\alpha = \pm b^{m/2} N(\gamma)/\gamma^2, b \in F^*, \gamma \in L^*$ and $r \equiv 2^{n+1} - 1$, then $\sqrt{\alpha} = \pm b^{m/4}\sqrt{N(\gamma)}/\gamma$ or $\pm i b^{m/4}\sqrt{N(\gamma)}/\gamma$, so $L(\sqrt{\alpha})$ is biquadratic over F and $[M : L] = m$. Furthermore, $N(\alpha) = b^m$, i.e., $\sigma(\alpha) = \alpha^{-1} b^m$. Therefore, $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension.

If $\alpha = c^{2^n+1}/\delta^2, c \in F^*, N(\delta) = \pm c$ and $r \equiv -1$, then again $[M : L] = m$ and

$$\sigma(\alpha)/\alpha^{2^{n+1}} = \alpha^{-1}(\delta/c^{2^{n-1}})^{2^{n+2}}.$$

Let $\beta = \delta/c^{2^{n-1}}$. Then $\sigma(\alpha) = \alpha^{2^{n+1}-1}\beta^m$, hence $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension.

Now, assume that $M/F = L(\sqrt[m]{\alpha})/F$ is an M_{2m} extension. If $r \equiv 2^{n+1} - 1$, then $t = -1$, so $\sigma(\alpha) = \alpha^{-1}\beta^m$, for some $\beta \in L^*$. Then $N(\alpha) = \beta^m \in F$. From $N(\alpha) = \sigma(N(\alpha)) = [\sigma(\beta)]^m$ follows that $[\sigma(\beta)]^m = \beta^m$, so $\sigma(\beta) = \beta\omega$, where $\omega^m = 1$, i.e., $\omega \in \langle\zeta\rangle$. Furthermore, $\sigma^2(\beta) = \beta = \beta\omega\sigma(\omega)$, hence $\omega\sigma(\omega) = 1$. Now, from $\sigma(\zeta) = \zeta^r$ follows that $1 = \omega\sigma(\omega) = \omega^{r+1} = \omega^{m/2} = 1$, i.e., $\omega \in \langle\zeta^2\rangle$. We then have $\sigma(\beta^{m/2}) = \beta^{m/2}\omega^{m/2} = \beta^{m/2} \in F$, so $(\alpha/\beta^{m/2})\sigma(\alpha/\beta^{m/2}) = N(\alpha/\beta^{m/2}) = 1$. Hilbert Theorem 90 then implies that $\alpha/\beta^{m/2} = \sigma(\gamma)/\gamma$, for some $\gamma \in L^*$, hence $\alpha = \beta^{m/2}N(\gamma)/\gamma^2$. It remains to find the specific values of $\beta \in L^*$. We have that $\omega = \zeta^{2s}, s \geq 1$, and $\sigma(\beta) = \beta\omega = \beta\zeta^{2s}$. Then

$$\beta\sigma(\beta) = \beta^2\zeta^{2s} = (\beta\zeta^s)^2 \in L^2 \cap F = F^2 \cup -F^2,$$

hence $\beta^2\zeta^{2s} = \pm b^2, b \in F$. Therefore, $\beta^{m/2} = b^{m/2}(\zeta^s)^{m/2} = \pm b^{m/2}$.

Now, if $r \equiv -1$, then $t = 2^{n+1} - 1$. Let $k = 2^{n+1}$ $(n \geq 1)$. We then have $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$ and $N(\alpha) = (\alpha\beta^2)^k \in F \cap L^k = F^k \cup -F^k$, by Lemma 5.4. If $(\alpha\beta^2)^k \in F^k$, then $\alpha\beta^2 = c\omega$, where $\omega^k = 1, c \in F$, so $\omega \in \langle\zeta^2\rangle$. If we replace

β by $\beta\omega^{-1/2}$, the equation $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$ will not change, so we will assume that $\alpha\beta^2 = c \in F$. Let $\delta = c^{k/4}\beta$. Then

$$\alpha = c/\beta^2 = c^{k/2+1}/(c^{k/2}\beta^2) = c^{k/2+1}/\delta^2$$

and

$$N(\delta^2) = N(c^{k/2}\beta^2) = c^k N(c/\alpha) = c^2,$$

hence $N(\delta) = \pm c$. If $(\alpha\beta^2)^k \in -F^k$, then $\alpha\beta^2 = \zeta c\omega$, where $c \in F$ and $\omega^k = 1$. Again, we can replace β by $\beta\omega^{-1/2}$ and assume $\alpha\beta^2 = \zeta c$. Then $N(\alpha) = (\alpha\beta^2)^k = -c^k \in -F^2 \neq F^2$, therefore $N(\alpha\beta^2) \in -F^2$, but $N(\zeta c) = N(c) \in F^2$, a contradiction. Thus, if $r \equiv -1$ it remains that $\alpha = c^{k/2+1}/\delta^2, c \in F$ and $N(\delta) = \pm c$.

The remaining follows from the fact that the fixed field $F(\sqrt{\alpha}, \sqrt{-1})$ of τ^2 must be a biquadratic extension over F. This proves the theorem. ■

Finally, the following theorem gives us a description of all $C_m \times C_2$ extensions.

Theorem 7.2. *Let $\alpha \in L^*$. Then $M/F = L(\sqrt[m]{\alpha})/F$ is a $C_m \times C_2$ extension for $a =_2 -1$ if and only if*

$$\alpha = \begin{cases} \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2, & \text{if } r \equiv -1; b_1 \in F^*, \gamma_1 \in L^* \text{ and } N(\gamma_1) \notin F^2 \cup -F^2, \\ c^{2^n+1}/\gamma^2, & \text{if } r \equiv 2^{n+1} - 1; c \in F^*, \gamma \in L^*, N(\gamma) = \pm c \text{ and} \\ & \qquad c \notin F^2 \cup -F^2. \end{cases}$$

P r o o f. Assume that α is given by the formula in the statement of this theorem. If $\alpha = \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2$, where $b_1 \in F^*, \gamma_1 \in L^*$ and $r \equiv -1$, then $[M : L] = m$ as before and also $N(\alpha) = b_1^m = \beta^m$, where $\beta = b_1$. Therefore, $\sigma(\alpha) = \alpha^{-1}\beta^m$, so $M/F = L(\sqrt[m]{\alpha})/F$ is either a $C_m \times C_2$ or a C_{2m} extension. Let $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, where $l_1 \equiv l \pmod{\gcd(j+1, m)}$. We then have $\rho = \sigma(\beta)/\beta = 1$, hence l_1 is even and M/F is a $C_m \times C_2$ extension.

If $\alpha = c^{2^n+1}/\gamma^2$, where $c \in F^*, \gamma \in L^*, N(\gamma) = \pm c$ and $r \equiv 2^{n+1} - 1$, then $[M : L] = m$ and also $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$, where $k = 2^{n+1}$ and $\beta = \gamma/c^{k/4}$. Since $t = k - 1$, $M/F = L(\sqrt[m]{\alpha})/F$ is either a $C_m \times C_2$ or a C_{2m} extension. We then have $t^2 - 1 = k/2 - 1$ and

$$\rho = \alpha^{k/2-1}\beta^{k-1}\sigma(\beta) = (\alpha\beta^2)^{k/2}N(\beta)/(\alpha\beta^2) = \pm 1 \in \langle\zeta^2\rangle,$$

hence M/F is a $C_m \times C_2$ extension.

Now, assume that $M/F = L(\sqrt[m]{\alpha})/F$ is a $C_m \times C_2$ extension. If $r \equiv -1$, then $t = -1$ and $\sigma(\alpha) = \alpha^{-1}\beta^m$, where $\beta \in L^*$. Hence $N(\alpha) = \beta^m \in L^m \cap F$. Clearly, $\sigma(\beta^m) = [\sigma(\beta)]^m = \beta^m$, hence $\sigma(\beta) = \beta\omega$, where $\omega^m = 1$, i.e., $\omega \in \langle\zeta\rangle$. Since $\sigma(\zeta) = \zeta^r = \zeta^{-1}$, we get $N(\omega) = 1$. We then have $\omega^{m/2} = \pm 1$. If $\omega^{m/2} = 1$, we obtain similarly to Theorem 7.1 that $\alpha = \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2$, where $b_1 \in F^*$ and $\gamma_1 \in L^*$. If $\omega^{m/2} = -1$, then $\omega \notin \langle\zeta^2\rangle$ and $\sigma(\beta^{m/2}) = -\beta^{m/2}$, hence $\beta^{m/2} = b_3\sqrt{-1}$, for some $b_3 \in F^*$. Then $N(\alpha/\beta^{m/2}) = -1, N(\alpha^2/\beta^m) = 1$ and Hilbert Theorem 90 implies that $\alpha^2/\beta^m = \sigma(\gamma_2)/\gamma_2$, for some $\gamma_2 \in L^*$. Therefore, $\alpha^2 = \beta^m\sigma(\gamma_2)/\gamma_2 = \beta^m N(\gamma_2)/\gamma_2^2$, so $N(\gamma_2) \in L^2 \cap F = F^2 \cup -F^2$, i.e., $N(\gamma_2) = \pm\delta^2$, for some $\delta \in F^*$. Thus, $\alpha = \pm\beta^{m/2}\delta/\gamma_2$, where $\gamma_2 \in L^*$ and $N(\gamma_2) = \pm\delta^2$. Now, we must specify the values of β, such that $\beta^{m/2} = b_3\sqrt{-1}, b_3 \in F^*$ and $N(\alpha) \in L^m$. We have that $N(\alpha) = b_3^2\delta^2/N(\gamma_2)$, so we consider two cases. If $N(\gamma_2) = \delta^2$, then $N(\alpha) = b_3^2 = -\beta^m \in L^m$, hence $-1 \in L^m$. Therefore, $\sqrt{-1} \in L^{m/2}$ and $b_3\sqrt{-1} \in L^{m/2}$, so $b_3 \in L^{m/2} \cap F = F^{m/2} \cup -F^{m/2}$ by Lemma 5.4, i.e., $b_3 = \pm b_2^{m/2}$, for some $b_2 \in F^*$. Thus, $\alpha = \pm b_2^{m/2}\sqrt{-1}\delta/\gamma_2$. If $N(\gamma_2) = -\delta^2$, then $N(\alpha) = -b_3^2 = \beta^m \in L^m$. Furthermore, $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \sigma(\beta)/\beta = \zeta^{l_1}$, therefore $\rho^{m/2} = \sigma(\beta^{m/2})/\beta^{m/2} = -1 = (\zeta^{l_1})^{m/2}$, hence l_1 is odd, a contradiction. Now, from the fact that $L(\sqrt{\alpha})$ is biquadratic over F follows that α must look in the same way as in the case $\omega^{m/2} = 1$.

Finally, if $r \equiv 2^{n+1} - 1$, then $t = 2^{n+1} - 1$. Let $k = 2^{n+1}$. We then have $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$, so $N(\alpha) = (\alpha\beta^2)^k \in F \cap L^k = F^k \cup -F^k$. If $(\alpha\beta^2)^k \in F^k$, then we obtain identically to Theorem 7.1, that $\alpha = c^{k/2+1}/\gamma^2$ and $N(\gamma) = \pm c$. If $(\alpha\beta^2)^k \in -F^k$, then $\alpha\beta^2 = \zeta c\omega$, where $c \in F^*, \omega^k = 1$ and we can again replace β by $\beta\omega^{-1/2}$ and assume that $\alpha\beta^2 = \zeta c$. Furthermore, $\rho = \alpha^{k/2-1}\beta^{k-1}\sigma(\beta) = \zeta^{l_1}$. Let $\gamma = c^{k/4}\beta$. Then $\rho = (\alpha\beta^2)^{k/2}\sigma(\beta)/(\alpha\beta) = \zeta^{k/2-1}N(\gamma)/c$. From $N(\gamma^2) = c^2$ follows that $N(\gamma) = \pm c$. Therefore, $\rho = \pm\zeta^{k/2-1} = \zeta^{l_1}$, so l_1 is odd, a contradiction.

The remaining again follows from the fact that the fixed field $F(\sqrt{\alpha}, \sqrt{-1})$ of τ^2 must be a biquadratic extension over F. ■

References

[1] J. K. Arason, B. Fein, M. Schacher and J. Sonn, Cyclic extensions of $K(\sqrt{-1})/k$, *Trans. Amer. Math. Soc.* **313** (1989), 843-851.

[2] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

[3] K. Hoechsmann, Zum Einbettungsproblem, *J. Reine Angew. Math.* **229** (1968), 81-106.

[4] V. V. Ishanov, B. B. Lur'e and D. K. Faddeev, *The Embedding Problem in Galois Theory*, Amer. Math. Soc., Providence, 1997.

[5] Y.-S. Hwang, D. B. Leep, and A. R. Wadsworth, Galois groups of order $2n$ that contain a cyclic subgroup of order n, *available at* http://arxiv.org/find/math.

[6] I. Kiming, Explicit classifications of some 2-extensions of a field of characteristic different from 2, *Canad. J. Math.* **42** (1990), 825-855.

[7] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, MA, 1973.

[8] A. Ledet, On 2-groups as Galois groups, *Canad. J. Math.* **47** (1995), 1253-1273.

[9] A. Ledet, Embedding problems with cyclic kernel of order 4, *Israel J. Math.* **106** (1998), 109-131.

[10] A. Merkurjev, On the norm residue symbol of degree 2, *Soviet Math. Dokl.* **24** (1981), 546-551.

[11] I. Michailov, Embedding obstructions for the dihedral, semidihedral and quaternion 2-groups, *J. Algebra* **245** (2001), 355-369.

[12] I. Michailov and N. Ziapkov, Embedding obstructions for the generalized quaternion group, *J. Algebra* **226** (2000), 375-389.

Faculty of Mathematics,
Informatics and Economics,
Constantin Preslavski University,
9700 Shoumen, BULGARIA
E-mail: i.michailov@fmi.shu-bg.net

Received 30.07.2005