On Galois cohomology and realizability of 2-groups as Galois groups

Ivo M. Michailov

Abstract: In this paper we develop some new theoretical criteria for the realizability of $p$-groups as Galois groups over arbitrary fields. We provide necessary and sufficient conditions for the realizability of 14 of the 22 non-abelian 2-groups having a cyclic subgroup of index 4 that are not direct products of groups.

MSC: 12F12

Keywords: Embedding problem • Galois extension • Quaternion algebra • Obstruction • Corestriction

1. Introduction

Let $F$ be a field and let $G$ be a finite group. The inverse problem of Galois theory consists of determining whether there exists a Galois extension $K/F$ with Galois group $G$. There are many recent papers devoted to the realizability of $p$-groups as Galois groups, especially for $p = 2$. For small 2-groups see e.g. [3, 4, 8, 14], and for $p$-groups see e.g. [13, 15]. One of the most challenging still open problems is to find necessary and sufficient conditions for the realizability over arbitrary fields of the non-abelian 2-groups having a cyclic subgroup of index 2. So far, such conditions are known over fields containing certain roots of unity, see [2, 11, 12]. The main goal of this paper is to find necessary and sufficient conditions for the realizability of 14 non-abelian groups of order $2^n$, $n \geq 4$, having a cyclic subgroup of order $2^{n-2}$, over fields containing a primitive $2^{n-3}$th root of unity. This is done in Section 5.

We recall now the definition of the Galois embedding problem, which is the main tool for finding necessary and sufficient conditions for the realizability of a given group.

Let $E/F$ be a Galois extension with Galois group $Z$ and let

$$1 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 1 \quad (1)$$

Received 12 October 2010; accepted 17 December 2010

© Versita Sp. z o.o.
be a group extension, i.e., a short exact sequence. The embedding problem related to \(E/F\) and (1) then consists of determining whether there exists a Galois algebra (called also a weak solution) or a Galois extension (called a proper solution) \(L\), such that \(E\) is contained in \(L\), \(Y\) is isomorphic to \(\text{Gal}(L/F)\), and the homomorphism of restriction of \(L\) on \(E\) coincides with \(a\). We denote the so formulated embedding problem by \((E/F, Y, X)\). We call the group \(X\) the kernel of the embedding problem. For more details concerning embedding problems and their associated problems we refer the reader to [5] and [16].

In Section 2 we give some criteria for solving embedding problems involving \(p\)-groups.

In Section 3 we develop a method applicable for \(2\)-groups, which is based on the corestriction map. The main result there is Theorem 3.8 which in conjunction with Theorems 2.3 and 2.7 will give us proper tools for the calculations in Section 5.

2. The \(\mu_p\)-embedding problem

Let \(p\) be a prime, let \(F\) be a field with characteristic not \(p\), and let \(F\) contain all \(p\)th roots of unity. Denote by \(\zeta\) a primitive \(p\)th root of unity and by \(\mu_p\) the cyclic group of all \(p\)th roots of unity which is contained in \(F^* = F \setminus \{0\}\).

For \(b, c \in F^*\) write \((b, c; \zeta)\) to denote the equivalence class in the Brauer group \(\text{Br}(F)\) of the \(p\)-cyclic algebra with generators \(i, j\) such that \(i^p = b, j^p = c\) and \(ji = \zeta ij\). For \(p = 2\) this is the quaternion algebra commonly denoted by \((b, c)\) or simply \((b, c)\) when there is no danger of confusion.

Let \(1 \rightarrow X \rightarrow Y \rightarrow G \rightarrow 1\) be a short exact sequence of finite groups, such that \(X\) is contained in the centre of \(Y\) and \(|X| = p\). Thus, we may identify \(X\) with \(\mu_p\). We have the following well known

\[ \text{Theorem 2.1 ([7]).} \]

Let \(L/F\) be a finite Galois extension with Galois group \(G = \text{Gal}(L/F)\) and let \(1 \rightarrow \mu_p \rightarrow Y \rightarrow G \rightarrow 1\) be a non-split group extension with characteristic class \(\gamma \in H^2(G, \mu_p)\). Also, let \(i : H^2(G, \mu_p) \rightarrow H^2(G, L^*)\) be a homomorphism induced by the inclusion \(\mu_p \subset L^*\). Then the embedding problem \((L/F, Y, \mu_p)\) is properly solvable iff \(i(\gamma) = 1\) in \(H^2(G, L^*)\).

Let \(f \in Z^2(G, \mu_p)\) represent \(\gamma\) given in the statement of the latter theorem. Then from [6, Th. 8.11] it follows that \(H^2(G, L^*)\) is isomorphic to the relative Brauer group \(\text{Br}(L/F)\) by \([f] \mapsto [L, G, f]\), where \([f] \in H^2(G, L^*)\) is the cohomological 2-coclass containing \(f \in Z^2(G, L^*)\), and \([L, G, f] \in \text{Br}(L/F)\) is the equivalence class of the crossed product algebra \((L, G, f)\). Assume in addition that \(f(1, 1) = 1\). We know that \((L, G, f)\) is an \(F\)-algebra, generated by \(L\) and elements \(u_\sigma, \sigma \in G\), with relations \(u_1 = f(1, 1) = 1, u_\sigma u_\tau = f(\sigma, \tau) u_{\sigma\tau}\) and \(u_\sigma x = \sigma x u_\sigma\) for all \(\sigma, \tau \in G\) and \(x \in L\). Notice that we have an isomorphism between \(Y\) and the subgroup generated by the elements \(\zeta^i u_\sigma\) in \((L, G, f)\).

\[ \text{Definition 2.2.} \]

We call the element \(O_\gamma = i(\gamma) \in H^2(G, L^*) \cong \text{Br}(L/F)\) the obstruction to solvability of the embedding problem \((L/F, Y, \mu_p)\).

We are going to recall now one criterion obtained in [13]. Let \(H\) be a \(p\)-group and let

\[ 1 \rightarrow C_p \cong \langle \zeta \rangle \xrightarrow{\pi} G \xrightarrow{\pi} H \times C_p \rightarrow 1 \]

be a non-split central group extension with characteristic 2-coclass \(\gamma \in H^2(H \times C_p, C_p)\). By \(\text{res}_H^G\gamma\) we denote the 2-coclass of the group extension

\[ 1 \rightarrow C_p \rightarrow H \times C_p \xrightarrow{\pi} H \rightarrow 1. \]

Let \(\sigma_1, \sigma_2, \ldots, \sigma_m\) be a minimal generating set for the maximal elementary abelian factor group of \(H\); and let \(\tau\) be the generator of the direct factor \(C_p\). Finally, let \(s_1, s_2, \ldots, s_m, t \in G\) be the pre-images of \(\sigma_1, \sigma_2, \ldots, \sigma_m, \tau\), such that \(t^p = \zeta i\) and \(ts_i = \zeta^is_it\), where \(i \in \{1, 2, \ldots, m\}, j, d, \in \{0, 1, \ldots, p - 1\}\). Then we have the following
Theorem 2.3 ([13, Theorem 2.1]).

Let \( K/F \) be a Galois extension with Galois group \( H \) and let \( L/F = K(\sqrt{\alpha})/F \) be a Galois extension with Galois group \( H \times C_2, \beta \in F^* \setminus \{1\} \). Choose \( a_1, a_2, \ldots, a_n \in F^* \) such that \( \alpha \zeta_i = \zeta \zeta_i \) and \( \delta_k ) \) is the Kronecker delta). Then the obstruction to the embedding problem given by \( L/F \) and the group extension (2) is

\[
[K, H, \text{res}_Y] \left( b, b^i \zeta \zeta \prod_{j=1}^m a_i^{\beta_j} ; \zeta \right).
\]

Now, let \( G \) be a finite group, and let \( \{a_1, \ldots, a_k\} \) be a fixed (not necessarily minimal) generating set of \( G \) with the following properties: \( |a_i| = p^{n-1} \) for \( n > 1 \), the subgroup \( H \) generated by \( a_2, \ldots, a_k \) is normal in \( G \), and the quotient group \( G/H \) is isomorphic to the cyclic group \( C_{p^{n-1}} \), i.e., \( a_i \notin H, 1 \leq i < p^{n-1} \). Take now two arbitrary group extensions

\[
1 \rightarrow \mu_p \rightarrow G_1 \rightarrow \varphi \rightarrow G \rightarrow 1
\]

and

\[
1 \rightarrow \mu_p \rightarrow G_2 \rightarrow \varphi \rightarrow G \rightarrow 1.
\]

Denote by \( \tilde{\alpha} = \varphi^{-1}(\alpha) \) any preimage of \( \alpha \) in \( G_1 \) and by \( \tilde{\alpha} = \psi^{-1}(\alpha) \) any preimage of \( \alpha \) in \( G_2, i = 1, \ldots, k \).

Definition 2.4.

We write \( G_2 = C_{p^{n-1}}^{a_i} \), if

1. \( \tilde{\alpha} = p^{n-1}; \)

2. \( \alpha_i^{p^{n-1}} \in \mu_p, \alpha_i^{p^{n-1}} \neq 1; \) and

3. all other relations between the generators of the groups \( G_1 \) and \( G_2 \) are identical, i.e., \( \tilde{\alpha} = \zeta \prod_{j=1}^m \alpha_j^{\beta_j} \iff \tilde{\alpha}^{a_i} = \zeta \prod_{j=1}^m \alpha_j^{\beta_j} \) for \( i = 2, 3, \ldots, k; l, o_i, \beta_i \in \mathbb{Z}; \) and \( [\tilde{\alpha}, \tilde{\alpha}] = \zeta \prod_{j=1}^m \alpha_j^{\gamma_j} \iff [\alpha_i, \alpha_j] = \zeta \prod_{j=1}^m \alpha_j^{\gamma_j} \) for \( i, j = 1, 2, \ldots, k; l, o_i, \beta_i \in \mathbb{Z} \).

The latter definition originated from the following two examples:

Example 2.5.

Put \( G = D_{2^{n-1}}, \) the dihedral group of order \( 2^{n-1} \) generated by two elements \( a_1 \) and \( a_2 \) such that \( a_1 = 1, a_2^{2^{n-2}} = 1 \) and \( [a_1, a_2] = a_1^{-1} a_2^{-1} a_1 a_2 = a_2^{2^{n-2}} \); \( G_1 = D_{2^n}, \) the dihedral group of order \( 2^n \) generated by \( a_1 \) and \( a_2 \) such that \( a_1 = 1, a_2^{2^{n-2}} = 1, [a_1, a_2] = a_2^{2^{n-2}} = 1 \) and \( [\tilde{\alpha}, \tilde{\alpha}] = \tilde{\alpha}^{2^{n-2}} \); and \( G_2 = Q_{2^n}, \) the quaternion group of order \( 2^n \) generated by \( a_1 \) and \( a_2 \) such that \( a_1 = a_2^{2^{n-2}} = 1 \) and \( [\tilde{\alpha}, \tilde{\alpha}] = \tilde{\alpha}^{2^{n-2}} \). It is easy to see now that \( Q_{2^n} = D_{2^{n+1}}^{a_1}. \)

Example 2.6.

Let \( p \) be an odd prime. Put \( G = C_{p^2} \times C_{p^2}, \) the direct product of the cyclic group \( C_{p^2} = \langle a \rangle \) with the cyclic group \( C_p = \langle a \rangle; \) let \( G_1 \) be the group of order \( p^4 \) generated by \( a_1 \) and \( a_2 \) such that \( a_1 = 1, a_2^{p^2} = 1, [a_1, a_2] = p^2 \) and \( [a_2, a_2] = \zeta \) (this group is isomorphic to \( G_1 \) from [13]); and \( G_2 \) be the group of order \( p^3 \) generated by \( a_1 \) and \( a_2 \) such that \( a_1 = 1, a_2 = 1, [a_2, a_2] = p^2 \) and \( [a_2, a_2] = \zeta \) (this group is isomorphic to \( G_4 \) from [13]). Similarly to the previous example, \( G_4 = C_{p^2}^{a_1, a_2} \).

Now, we will prove one of our main theorems, giving the connection between the obstructions of the two embedding problems related to (3) and (4).
Theorem 2.7.
Let $L/F$ be a finite Galois extension with Galois group $G = \text{Gal}(L/F)$ as described above, let $K = L^H$ be the fixed subfield of $H$, and let the groups $G_1$ and $G_2$ from (3) and (4) be such that $G_2 = G_1^{(p^i,\sigma)}$. Denote by $O_{G_1} \in Br_p(F)$ the obstruction of the embedding problem $(L/F, G_1, \mu_p)$, by $O_{G_2} \in Br_p(F)$ the obstruction of the embedding problem $(L/F, G_2, \mu_p)$, and by $O_{C_p^\infty} \in Br_p(F)$ the obstruction of the embedding problem $(K/F, C_p^\infty, \mu_p)$ given by the group extension $1 \to \mu_p \to C_p^\infty \to G/H \cong C_{p^{i-1}} \to 1$. Then the relation between these obstructions is given by

$$O_{G_2} = O_{G_1} O_{C_p^\infty} \in Br_p(F).$$

Proof. Denote by $\Gamma_1 = (L, G, f_1)$ the crossed product algebra representing the obstruction $O_{G_1}$, and by $\Gamma_2 = (L, G, f_2)$ the crossed product algebra representing the obstruction $O_{G_2}$. As we noted above, $\Gamma_1$ is generated over $F$ by the elements from $L$ and $\{u_\sigma\}_{\sigma \in G}$, where $u_1 = f_1(1,1) = 1$, $u_{\sigma} = \alpha \sigma u_\sigma$ and $u_{\sigma} u_\tau = u_{\sigma \tau}(\sigma, \tau)$. Note that the structure of $G_1$ impacts the structure of $\Gamma_1$, e.g., if $[\beta, \delta] = \zeta \delta_i$ then $[u_{\beta}, u_{\delta}] = \zeta u_{\beta \delta}$. The cyclic algebra $A$ generated by the elements from $K$ and the elements $u_\sigma^{(i)} = u_\sigma$, $i = 1, \ldots, p^{n-1}$, is contained in $\Gamma_1$ and $u_\sigma^{(p^{n-1})} = u_\sigma = 1$. Then $\Gamma_1 = A \otimes_F C_{\Gamma_1}(A)$. We will prove that each $u_\sigma$ and its powers do not participate in the products that generate the centralizer $C_{\Gamma_1}(A)$.

Observe first that each element from $G$ is uniquely written in the form $\sigma^i \sigma$, where $\sigma \in H = \langle \sigma_1, \ldots, \sigma_k \rangle$ and $i = 1, \ldots, p^{n-1}$. Then $u_{\sigma^i \sigma} = u_{\sigma^i} u_{\sigma} f_i^{-1}(\sigma, \sigma)$, so for arbitrary $\alpha \in C_{\Gamma_1}(A)$ we can write

$$\alpha = \sum_{\sigma \in H, i} x_{\sigma^i \sigma} u_{\sigma^i \sigma} = \sum_{\sigma \in H, i} y_{\sigma^i \sigma} u_{\sigma^i \sigma} u_\sigma,$$

where $x_{\sigma^i} \in L^\times$ and $y_{\sigma^i \sigma} = x_{\sigma^i} f_i^{-1}(\sigma, \sigma) \in L^\times$. Suppose $y_{\sigma^i \sigma} \neq 0$ for some $i$ relatively prime to $p$. Since $K$ contains an element of the kind $\sqrt[p]{} \alpha$ for $\alpha \in F \setminus F^{p^n}$ such that $\sigma \sqrt[p]{} \alpha = \sqrt[p]{} \alpha \zeta$, we have the equations: $u_\sigma^{(i)} \sqrt[p]{} \alpha = \alpha \sqrt[p]{} \alpha u_\sigma^{(i)} = \sqrt[p]{} \alpha \zeta u_\sigma^{(i)}$ and $u_\sigma^{(i)} \sqrt[p]{} \alpha = \sqrt[p]{} \alpha u_\sigma^{(i)}$ for all $j$ such that $p$ divides $j$. Taking into account that $\sigma \sqrt[p]{} \alpha = \sqrt[p]{} \alpha$ for all $\sigma \in H$, we get

$$\alpha \sqrt[p]{} \alpha = \sqrt[p]{} \alpha \left( \sum_{|j|=1} y_{\sigma^i \sigma} \zeta u_\sigma^{(j)} u_\sigma + \sum_{|j|=p} y_{\sigma^i \sigma} u_\sigma^{(j)} u_\sigma \right) = \sqrt[p]{} \alpha \alpha,$$

where $\zeta^i \neq 1$ for $i$ such that $(i, p) = 1$. Thus we arrive at a contradiction with the linear independence of the elements $\{u_\sigma\}_{\sigma \in G}$. Now, suppose each participating power of $u_\sigma$ is divisible by $p$, so we can assume that $\alpha$ is of the kind

$$\alpha = \sum_{(p, k) = 1, \sigma \in H} \left( \sum_{|j| = p^k} y_{\sigma^i \sigma} u_\sigma^{(j)} u_\sigma \right),$$

where $(p, k_j) = 1$. Let $j_0$ be the smallest number such that $y_{\sigma^i \sigma} \neq 0$ for some $\sigma \in H$. The short exact sequences

$$1 \longrightarrow C_p \longrightarrow C_p^{j_0} \longrightarrow C_p^{j_0-1} \longrightarrow 1,$$

$j = 2, \ldots, n-1$, yield the following property of the cyclic extensions which we apply to $j_0$: there exists $\sqrt[p]{} \omega = \sqrt[p]{} \alpha$ in $K$ such that $
abla_0^{(p^k_0)} \sqrt[p]{} \omega = \sqrt[p]{} \omega \zeta$ and $\nabla_0^{(p^k_j)} \sqrt[p]{} \omega = \sqrt[p]{} \omega$ for all $j > j_0$. For simplicity, we assume that the other $y_{\sigma^i \sigma}$'s in the sum are 0. Then from

$$\alpha \sqrt[p]{} \omega = \sqrt[p]{} \omega \left( y_{\sigma_0 \sigma_0} \zeta u_\sigma^{(p^k_0)} u_\sigma + \sum_{(p, k) = 1, \sigma \in H} \left( \sum_{|j| = p^k} y_{\sigma^i \sigma} u_\sigma^{(j)} u_\sigma \right) = \sqrt[p]{} \omega \alpha,$$

we again arrive at a contradiction. Therefore, each element $\alpha \in C_{\Gamma_1}(A)$ indeed is of the kind $\sum_{\sigma \in H} x_{\sigma} u_\sigma$, where $x_{\sigma} \in L$.

Further, $\Gamma_2$ is generated over $F$ by the elements from $L$ and $\{v_{\sigma} \}_{\sigma \in G}$, where $v_1 = f_2(1,1) = 1$, $v_\sigma x = \alpha \sigma v_\sigma$ and $v_\sigma v_\tau = v_{\sigma \tau} f_2(\sigma, \tau)$. The cyclic algebra $B$ generated by the elements from $K$ and the elements $v_\sigma^{(i)} = v_{\sigma^i}, i = 1, \ldots, p^{n-1}-1$, is contained in $\Gamma_2$. Here, however, $v_{\sigma^i}^{(p^i-1)} = \zeta^i$, where $\zeta^i = 1$. Then similarly to $\Gamma_1$, we have $\Gamma_2 = B \otimes_F C_{\Gamma_2}(B)$. 


where \( \nu_n \) and its powers do not participate in the products that generate the centralizer \( C_{G_2}(B) \). Now, define a map \( \theta : \Gamma_1 \to \Gamma_2 \) by \( x \mapsto x \) and \( u_\sigma \mapsto u_\sigma \) for all \( x \in L \) and \( \sigma \in G \). From what we have already proved for the structure of the centralizers it follows that \( \theta \) maps \( C_{G_1}(A) \) onto \( C_{G_2}(B) \) and that the restriction \( \theta : C_{G_1}(A) \to C_{G_2}(B) \) is an isomorphism.

It remains to observe that the algebra \( A \) is split. Hence \( O_{C_1} = \left[ \Gamma_1 \left\langle A \right] C_{G_1}(A) \right] = \left[ C_{G_1}(A) \right] \). Finally, \( [B] = O_{C_2} \), so \( O_{C_2} = [B][C_{G_2}(B)] = O_{C_2} \). We are done.

**Corollary 2.8.**

Let \( G = D_{2^n-1} \) be the dihedral group of order \( 2^{n-1} \) with generators \( a \) and \( \tau \) such that \( a^{2^{n-2}} = \tau^2 = 1 \), \( \tau a = a^{-1} \tau \), and let \( L = K(\sqrt{b})/F \) be a \( 2^{n-1} \) extension such that \( \sigma \sqrt{b} = \sqrt{b} \) and \( \tau \sqrt{b} = -\sqrt{b} \). Then there exist embedding problems \( (L/F, D_{2^n}, \mu_2) \) and \( (L/F, \sigma, \mu_3) \) with obstructions \( O_{D_{2^n}} \) and \( O_{\mu_2} \), respectively, such that the relation between the obstructions is \( O_{D_{2^n}} = O_{\mu_2} \).

**Proof.** Put \( \sigma_1 = \tau \) and \( \sigma_2 = \sigma \). From Example 2.5 it follows that \( Q_{2^n} = D_{2^{n-1}}^{(4,r)} \). The embedding problem \( (F(\sqrt{b})/F, C_4, \mu_3) \) has obstruction \( \left( b, \sigma, \zeta \right) \), as it is well known. From Theorem 2.7 we obtain what is desired.

**Corollary 2.9.**

Let \( p \) be odd, let \( G_2 \) be the group of order \( p^4 \) generated by elements \( g_1, \ldots, g_4 \) such that \( g_1^p = g_2, g_3^p = g_4, g_3 \) and \( g_4 \) are central, and let \( G_4 \) be the group of order \( p^4 \) generated by elements \( g_1, \ldots, g_4 \) such that \( g_1^p = g_2, g_3^p = g_4, g_3 \) and \( g_4 \) are central; see [13]. Let \( G = C_2 \times C_2 \) be the direct product with generators \( \sigma, \tau \) such that \( \sigma^2 = \tau^2 = 1 \) and \( \sigma \tau = \tau \sigma \). Let \( L/F \) be a \( C_2 \times C_2 \) extension containing \( F(\sqrt{b}) \) such that \( \sigma \sqrt{b} = \zeta \sqrt{b} \) and \( \sigma \sqrt{b} = \sqrt{b} \). Let \( (L/F, G_1, \mu_3) \) and \( (L/F, G_4, \mu_3) \) be the embedding problems given by the group extensions:

\[
1 \longrightarrow \langle g_1 \rangle \longrightarrow C_2 \longrightarrow C_2 \longrightarrow C_2 \times C_2 \longrightarrow 1
\]

and

\[
1 \longrightarrow \langle g_2 \rangle \longrightarrow C_2 \longrightarrow C_2 \longrightarrow C_2 \times C_2 \longrightarrow 1.
\]

Then the relation between the obstructions is given by \( O_{G_3} = O_{G_4}(b, \zeta, \zeta) \).

**Proof.** Put \( \sigma_1 = \tau \) and \( \sigma_2 = \sigma \). The embedding problem \( (F(\sqrt{b})/F, C_2, \mu_3) \) has obstruction \( \left( b, \sigma, \zeta \right) \); see e.g. [13]. From Example 2.6 it follows that \( G_3 = G_3^{(2,r)} \) and it remains to apply Theorem 2.7.

**Definition 2.10.**

We write \( X \Rightarrow Y \) and call this an \textit{automatic realization}, if from the realizability of the group \( X \) as a Galois group over any field \( F \) the realizability of \( Y \) over \( F \) follows.

The automatic realizations \( Q_{2^n} \Rightarrow D_{2^n} \) for \( n \leq 5 \) are proven in [8] and [9], and \( G_3 \Rightarrow G_4 \) is proven in [13]. Ledet states in [9] the conjecture that the automatic realizations \( Q_{2^n} \Rightarrow D_{2^n} \) for \( n > 5 \) also hold, which is still an open problem.

### 3. Shapiro’s Lemma. The quadratic corestriction homomorphism

In this section we will discuss Shapiro’s Lemma in the following specific situation: let \( G \) be a pro-finite 2-group, let \( H \) be a closed subgroup of index \( [G : H] = 2 \), and let \( \mu_2 = \{ \pm 1 \} \) be a trivial \( H \)-module. Our goal is to give a proper interpretation of Shapiro’s Lemma, which will aid our investigations.
Definition 3.1 ([20, Ch. I, § 2.5]).
Let \( A \) be an \( H \)-module. We define an induced module (coinduced in the terminology of [21]) \( A^* = M_H^n(A) \) as the set of all continuous maps \( a^* : G \to A \), such that \( a^*(hx) = ha^*(x) \), where \( h \in H \) and \( x \in G \). We can give \( A^* \) a \( G \)-module structure by \( (ga^*) (x) = a^*(xg) \) for all \( g \in G \).

In our situation we can easily describe the induced module \( \mu^* \): Choose an element \( g \in G \), such that \( g \notin H \), so \( H \) and \( Hg \) are the two right cosets of \( H \) in \( G \). The definition implies that \( a^* (h) = a^* (1) \) and \( a^* (hg) = a^* (g) \) for all \( h \in H \). Therefore, \( \mu^* \) is an elementary abelian group of order \( 4 \), which we will write multiplicatively. We can denote the elements of \( \mu^* \) in this way: \( a^*_1 = (1, 1) \), \( a^*_2 = (1, -1) \), \( a^*_3 = (-1, -1) \) and \( a^*_4 = (-1, 1) \), where \( a^*_1 \) sends \( G \) to \( 1 \); \( a^*_2 \) sends \( H \) to \( -1 \) and \( Hg \) to \( 1 \); \( a^*_3 \) sends \( G \) to \( -1 \). The action of \( G \) on \( \mu^* \) is then given by \( ha^* = a^* \) for all \( h \in H \) and \( a^* \in \mu^* \); \( ga^* = a^* \), \( ga^*_2 = a^*_3 \), \( ga^*_3 = a^*_2 \) and \( g a^*_4 = a^*_4 \).

Now, let us define a map \( \phi : \mu^*_2 \to \mu_2 \) by \( \phi (a^*) = a^* (1) \). Clearly, \( \phi \) is an epimorphism, which is compatible with the natural inclusion of \( H \) in \( G \). Furthermore, \( \ker (\phi) = \{ a^*_1, a^*_2 \} \) and \( \phi \) induces a homomorphism \( H^2 (G, \mu^*_2) \to H^2 (H, \mu_2) \). This homomorphism is an isomorphism by Shapiro’s Lemma [20, Ch. I, Prop. 10]. Following again [20], we define a map \( \pi : \mu^*_2 \to \mu_2 \) by

\[
\pi (a^*) = \prod_{x \in G \setminus H} x a^*(x^{-1}),
\]

where it should be noted that by \( x a^*(x^{-1}) \) is meant the action of \( x \) on \( a^*(x^{-1}) \) in \( \mu_2 \). Since \( \mu^*_2 \) is a trivial \( G \)-module, we have that \( \pi (a^*) = a^* (1) a^*(g) \). The map \( \pi \) is well defined and it is a \( G \)-epimorphism, which induces the homomorphism of corestriction (transfer):

\[
cor_{G/H} : H^2 (H, \mu_2) \cong H^2 (G, \mu^*_2) \to H^2 (G, \mu_2),
\]

where the left map is the isomorphism (which, henceforth, we will call short the Shapiro isomorphism) given in the proof of Shapiro’s Lemma in [20]. Notice also that \( \ker (\pi) = \{ a^*_1, a^*_2 \} \) is a trivial \( G \)-module.

Consider this specific situation: Let \( G \) be a pro-finite 2-group and let \( E_4 \) be a closed normal subgroup of \( G \), isomorphic to the elementary abelian group of order 4 with generators \( \sigma \) and \( \tau \). Assume further, that there exists a closed subgroup \( H \) in \( G \) such that \( E_4 \) is a normal subgroup in \( H \). \( H \) is contained in the centralizer \( C_G (E_4) \) of \( E_4 \) in \( G \), and the index of \( H \) in \( G \) is 2. Next, choose and fix \( g_1 \in G \setminus H \), and assume that \( g_1 g_1^{-1} \sigma = \sigma \) and \( g_1 \tau g_1^{-1} = \tau \). Then for \( H = H / E_4 \) and \( G = G / E_4 \) we have the isomorphism \( G / H \cong \hat{G} / \hat{H} \). Finally, choose and fix \( g \in G \setminus H \), so that we have a \( G \)-action on \( E_4 \), given by \( e^g = e \) for all \( e \in E_4 \) and \( h \in H \); \( \sigma^g = \sigma \) and \( \tau^g = \tau \). With these notations, we have

Lemma 3.2.
Let \( \varphi_1, \varphi_2 \in \text{Hom}_H (E_4, \mu_2) \) be such that \( \ker (\varphi_1) = \{ 1, \tau \} \) and \( \ker (\varphi_2) = \{ 1, \sigma \} \). Then \( \varphi_1 \) and \( \varphi_2 \) induce, respectively, homomorphisms \( \varphi^*_1, \varphi^*_2 : H^2 (H, E_4) \to H^2 (H, \mu_2) \), such that the compositions

\[
\psi_i : H^2 (G, E_4) \xrightarrow{\text{res}} H^2 (H, E_4) \xrightarrow{\varphi_i^*} H^2 (H, \mu_2)
\]

are isomorphisms for \( i = 1, 2 \).

Proof. We can define a \( G \)-isomorphism \( E_4 \cong \mu^*_2 \) by \( \sigma \mapsto a^*_1 \), \( \tau \mapsto a^*_2 \), \( \sigma \tau \mapsto a^*_3 \). Thus, we can assume that the homomorphisms \( \varphi_i \), given in the statement, are in \( \text{Hom}_H (\mu^*_2, \mu_2) \), and have kernels \( \ker (\varphi_1) = \{ a^*_1, a^*_2 \} \) and \( \ker (\varphi_2) = \{ a^*_1, a^*_2 \} \). Then for arbitrary \( G \)-module \( B \), the homomorphisms \( \varphi_i \) induce homomorphisms \( \varphi_i^* : \text{Hom}_H (B, \mu^*_2) \to \text{Hom}_H (B, \mu_2) \) for \( i = 1, 2 \). Now, the inclusion \( H \to G \) gives us the composition

\[
\theta_i : \text{Hom}_G (B, \mu^*_2) \xrightarrow{\text{res}} \text{Hom}_H (B, \mu^*_2) \xrightarrow{\varphi_i^*} \text{Hom}_H (B, \mu_2),
\]

such that \( \theta_i (f) (b) = f(b) (1) \) for \( f \in \text{Hom}_G (B, \mu^*_2) \) and \( b \in B \). According to [20], \( \theta_i \) is an isomorphism, which induces the Shapiro isomorphism. Since both cohomological functors, identical in zero degree, must be identical elsewhere, we obtain that \( \psi_i \) is an isomorphism.
Now, let us define a map \( \xi : \mu_2^* \to \mu_2^* \) by \( a_1^* \mapsto a_1^*, \ a_2^* \mapsto a_2^*, \ a_3^* \mapsto a_3^* \) and \( a_4^* \mapsto a_4^* \). Clearly, \( \xi \) is a \( G \)-automorphism of \( \mu_2^* \), which induces an automorphism \( \xi' : \text{Hom}_G(\mu_2^*) \to \text{Hom}_G(\mu_2^*) \). Then for the composition

\[
\vartheta_2 : \text{Hom}_G(\mu_2^*) \xrightarrow{\text{res}} \text{Hom}_\mu(\mu_2) \xrightarrow{\psi_2} \text{Hom}_\mu(\mu_2)
\]

we have that \( \vartheta_2 = \vartheta_1 \xi' \). Therefore \( \vartheta_2 \) and \( \psi_2 \) are also isomorphisms.

Keeping the notations from Lemma 3.2, we now prove the following

**Theorem 3.3.**

Let \( L/F \) be a finite Galois extension with Galois group \( G \) and let \( K = L^{\sigma} \) be the fixed subfield of \( H \). Then the embedding problem \( (L/F, G, E_i) \) is weakly solvable iff the embedding problem \( (L/K, H,(\tau), E_i(\tau)) \) is weakly solvable.

**Proof.** 'Only-if' part. The embedding problem \( (L/K, H,(\tau), E_i(\tau)) \) can be reached by taking the associated embedding problem of the second kind \( (L/K, H,E_i) \) and after that the associated embedding problem of the first kind \( (L/K, H,(\xi), E_i(\xi)) \). From [16] or [5] it follows that the weak solvability of the base embedding problem \( (L/F, G, E_i) \) implies the weak solvability of the associated embedding problems.

'If' part. Let \( \varphi_i \) and \( \psi_i, \ i = 1, 2 \), be the defined homomorphisms in Lemma 3.2. If we consider the Galois groups \( \Omega_F \) and \( \Omega_K \) of the separable closures \( F \) over \( F \) and \( K \), respectively, the homomorphisms \( \varphi_i \) induce also homomorphisms \( \overline{\varphi}_i : H^2(\Omega_F, E_i) \to H^2(\Omega_K, \mu_2) \). Since \( \psi_i \) and \( \overline{\psi}_i \) respect inflation, we have the commutative diagrams (\( i = 1, 2 \)) :

\[
\begin{array}{ccc}
H^2(G, E_i) & \xrightarrow{\psi_i} & H^2(H, \mu_2) \\
\downarrow \text{inf}^G_{\Omega_F} & & \downarrow \text{inf}^H_{\Omega_K} \\
H^2(\Omega_F, E_i) & \xrightarrow{\overline{\psi}_i} & H^2(\Omega_K, \mu_2) .
\end{array}
\]

Now, assume that the embedding problem \( (L/K, H,(\tau), E_i(\tau)) \) is weakly solvable and denote by \( c \) the 2-coclass of the group extension

\[ 1 \to E_i \to G \to G \to 1 \]

in \( H^2(G, E_i) \). Since the 2-coclass \( \psi_i(c) \) is represented by the group extension

\[ 1 \to E_i(\tau) \to H(\tau) \to H \to 1, \]

we have that \( \text{inf}^G_{\Omega_F}(\psi_i(c)) = 0 \). The commutative diagram for \( i = 1 \) then shows that \( \overline{\psi}_1 \text{inf}^G_{\Omega_F}(c) = 0 \). Since \( \overline{\psi}_1 \) is an isomorphism, \( \text{inf}^G_{\Omega_K}(c) = 0 \), whence the embedding problem \( (L/F, G, E_i) \) is weakly solvable. \( \Box \)

Whether we would choose \( \tau \) or \( \sigma \tau \) in the statement of Theorem 3.3 is of no importance, as Lemma 3.2 shows. In this connection, we do not need the verification of the well-known compatibility condition of Faddeev and Hasse; see [5, 16]. It is a necessary condition for solvability, which can be interpreted as the solvability of all associated Brauer embedding problems. In other words, we proved in Theorem 3.3 that the solvability of only one Brauer embedding problem (given in the statement) is necessary and sufficient for the solvability of the original embedding problem. More information on Brauer embedding problems can be found in [5] and [10].

For a weakly solvable embedding problem \( (E/F, Y, X) \) to be properly solvable, it is sufficient that the kernel \( X \) is contained in the Frattini subgroup \( \Phi(Y) \) of \( Y \) (see [5, Ch. 1, § 6, Cor. 5]). When dealing with smaller groups it is not hard to check whether this condition is fulfilled. With bigger groups, however, it may not be so obvious. The following properties of the Frattini subgroup are useful and lead to a sufficient condition for \( X \) to be in \( \Phi(Y) \).

**Lemma 3.4 ([1, Cor. 5.3.2]).**

Let \( X \) and \( Y \) be finite groups, let \( X \) be normal in \( Y \) and let \( X \leq \Phi(Y) \). Then \( \Phi(Y)/X = \Phi(Y/X) \).
Lemma 3.5 ([1, Ex. 5.3.8]).
Let X and Y be finite p-groups and $X \leq Y$. Then $\Phi(X) \leq \Phi(Y)$.

Lemma 3.6 ([5, Pr. 4.1.2]).
Let $1 \to X \to Y \to Z \to 1$ be a finite p-group extension and let $X_0 = X \cap \Phi(Y)$. Then the group extension $1 \to X/X_0 \to Y/Y_0 \to Z \to 1$ is split.

Proposition 3.7.
In the notations of Lemma 3.2, let $G$ be a finite 2-group and let the group extensions $1 \to E_4/\langle \rho \rangle \to H/\langle \rho \rangle \to H \to 1$ be non-split for all $\rho \in E_4$. Then $E_4 \leq \Phi(H)$.

Proof. Suppose $E_4$ is not contained in $\Phi(H)$. Then the group $E_0 = E_4 \cap \Phi(H)$ has an order $\leq 2$, so the group extension $1 \to E_4/E_0 \to H/E_0 \to H \to 1$ is split by Lemma 3.6, which is a contradiction. Hence $E_4 \leq \Phi(H) \leq \Phi(G)$ by Lemma 3.5.

Keeping the assumptions given above in Lemma 3.2, we are ready to prove the main theorem of this section. Applications of this result will be displayed in the last section.

Theorem 3.8.
Let $c_1 \in H^2(G, \mu_2)$ be the 2-coclass represented by the group extension $1 \to E_4/\langle \sigma \rangle \cong \mu_2 \to G/\langle \sigma \rangle \to G \to 1$, let $c_2 \in H^2(H, \mu_2)$ be the 2-coclass represented by the group extension $1 \to E_4/\langle \tau \rangle \cong \mu_2 \to H/\langle \tau \rangle \to H \to 1$, and let $c_3 \in H^2(H, \mu_2)$ be the 2-coclass represented by the group extension $1 \to E_4/\langle \sigma \tau \rangle \cong \mu_2 \to H/\langle \sigma \tau \rangle \to H \to 1$. Then $\text{cor}_{G/H}(c_2) = \text{cor}_{G/H}(c_3) = c_1$.

Proof. Recall that the homomorphism $\pi : \mu_2^2 \to \mu_2$ given by $\pi(a^*) = a^*(1)a^*(g)$ induces the homomorphism of corestriction (see (5)):

$$
cor_{G/H} : H^2(H, \mu_2) \longrightarrow H^2(G, \mu_2^2) \longrightarrow H^2(G, \mu_2),$$

where the left map is the Shapiro isomorphism and the right map is induced by $\pi$. Now, let $c \in H^2(G, E_4)$ be the 2-coclass represented by the group extension $1 \to E_4 \to G \to G \to 1$, let $\xi_1 : E_4 \to \mu_2$ be the $G$-isomorphism defined by $\xi_1(\sigma) = a_1^*$, $\xi_1(\tau) = a_2^*$, and let $\xi : H^2(G, E_4) \to H^2(G, \mu_2)$ be the induced isomorphism. Similarly, let $\xi_3 : H_3 \to \mu_2$ be the $G$-isomorphism defined by $\xi_3(\sigma) = a_3^*$, $\xi_3(\tau) = a_4^*$, and let $\xi : H^2(G, E_4) \to H^2(G, \mu_2)$ be the induced isomorphism.

Now, from Lemma 3.2 it follows that $c_1 = \psi_1(c)$, where $\psi_1$ is an isomorphism. Furthermore, $c_1 = \pi^*\xi_1^{-1}(c_2)$, where $\xi_1^{-1}$ is exactly the Shapiro isomorphism. Similarly, we have $c_3 = \psi_3(c)$ and $c_3 = \pi^*\xi_3^{-1}(c_3)$, since $\pi(c_3) = \pi(c_3) = -1$. Therefore $c_1 = \pi^*\xi_1^{-1}(c_2) = \pi^*\xi_3^{-1}(c_3)$. The definitions of $\psi_1$ and $\psi_3$ in Lemma 3.2 show us that we have the commutative diagram:

$$
\begin{array}{ccc}
H^2(G, E_4) & \overset{\phi_1}{\longrightarrow} & H^2(H, \mu_2) \\
\uparrow{\xi_1^{-1}} & & \uparrow{\phi_2} \\
H^2(G, \mu_2^2) & \overset{\xi_3^{-1}}{\longrightarrow} & H^2(G, E_4)
\end{array}
$$

whence we obtain $\xi_1^{-1}(c_2) = \xi_3^{-1}(c_3)$, the Shapiro isomorphism. Therefore, $c_1 = \text{cor}_{G/H}(c_2) = \text{cor}_{G/H}(c_3)$.

4. Corestriction of central simple algebras

We assume henceforth that $F$ is a field with characteristic not 2, $a \in F^\times \setminus F^{\times^2}$, $K = F(\sqrt{a})$ and $\text{Gal}(K/F) = \langle \sigma \rangle \cong C_2$. Since $Br(F) \cong H^2(Q_8, \mu_2)$, we have the corestriction homomorphism $\text{cor}_{F/K}(a, b_K) : Br_k(K) \to Br_k(F)$. For $b \in F^\times$ and $\sigma \in K$, the projection formula states that $\text{cor}_{F/K}(a, b)_K = (N_{K/F}(a), b)_F$, where $N_{K/F}$ is the norm map. This formula can be derived from the exercises in [21, XIV §1, §2].
Lemma 4.1.
Let \( a \in F^\times, K = F(\sqrt[3]{a}) \), \( a_0 = a_0 + b_0 \sqrt[3]{a} \) and \( a_1 = a_1 + b_1 \sqrt[3]{a}, a_0, b_0, b_1, a_1, b_1 \in F \).

(1) If \( b_{1-i} = 0 \), then \( \text{cor}_{K/F}(a_0, a_1) = (a_{1-i}, a_i^2 - ab_i^2)_F \).

(2) If \( a_1-b_1 = a_{1-i} = 0 \), then \( \text{cor}_{K/F}(a_0, a_1) = (a_i^2 - ab_i^2, a_1b_1(a_0b_1 - a_1b_0))_F \).

(3) Otherwise, \( \text{cor}_{K/F}(a_0, a_1) = (a_i^2 - ab_i^2, b_1(a_0b_1 - a_1b_0))_F \).

Proof. (1) Follows from the projection formula. (2) We have \( a_1b_0 = a_0b_1 \) and \( a_0, b_0 \neq 0 \), so \( a_1a_0 = b_1b_0 = x \in F^\times \). Therefore, \( (a_0, a_1)_K = (a_0, a_0x)_K = (a_0, -x)_K = a_0 - a_0a_1 \) and it remains to apply the projection formula. (3) Let \( b_1, b_2 \neq 0 \). Put \( \Delta = a_0b_1 - b_0a_1 \neq 0 \) and \( y = -\Delta b_1/b_2 \neq 0 \). Then the following hold: \( -a_1y = \Delta a_1b_2/b_1 + b_0\Delta \sqrt[3]{\Delta} = a_1b_0b_1 - a_0\Delta + a_0x = -\Delta^2/b_1 + a_0\Delta \), whence \( b_1a_1y = \Delta^2 - a_0b_1\Delta \). Therefore \( (a_0b_1\Delta, -a_0b_0\Delta)_K = 1 \) in \( Br_1(K) \), so \( (a_0b_1\Delta, -a_0b_0\Delta)_K (a_0b_1\Delta, a_0\Delta)_K = 1 \) or, equivalently, \( (a_0, a_1)_K = (a_0b_1\Delta, -a_0b_0\Delta)_K (a_0, a_1\Delta)_K = (a_0, -a_0\Delta)_K (a_0, -a_0\Delta)_K (a_0, b_1\Delta, -a_0\Delta)_K = 0, -a_0\Delta)_K \). Since \( b_1, b_2 \in F^\times \), we can apply again the projection formula to get the desired result. \( \square \)

Let \( R \) be a c. s. \( K \)-algebra, and let \( R^e \) be the ring \( R \) endowed with the twisted \( K \)-algebra structure given by \( \lambda \cdot a = \sigma(\lambda) a, a \in R^e, \lambda \in K \). Now, we can construct the tensor product algebra \( A = R \otimes_K R^e \) and define an action \( \bar{\sigma} : A \rightarrow A \) by \( \bar{\sigma}(a \otimes b) = b \otimes a \).

Definition 4.2 [(18, 19)].
The corestriction of \( R \) is the \( F \)-algebra of \( \bar{\sigma} \)-invariants: \( \text{cor}_{K/F}(R) = A(\bar{\sigma}) \).

We will not discuss the more complicated general definitions of the corestriction algebra, given in [18] or [23]. Even in our particular case, however, the structure of the corestriction algebra seems to be elusive. Scharlau proves in [19] that the canonical map \( \psi : K \times \text{cor}_{K/F}(R) \rightarrow A \) given by \( (a, x) \mapsto ax \) is \( F \)-bilinear, multiplicative, and it induces a canonical \( K \)-algebra isomorphism \( K \otimes_F \text{cor}_{K/F}(R) \cong A \). From this we see that \( \text{cor}_{K/F}(R) \) is a c. s. \( F \)-algebra and \( \text{dim}_K \text{cor}_{K/F}(R) = \text{dim}_F A \). Notice that \( \text{cor}_{K/F}(R) \) does not contain \( K \), which may cause difficulties in various situations. This, however, can be easily amended: Define \( S = A \otimes_A e_{\sigma} \) as an \( F \)-vector space and turn \( S \) into an algebra by \( e_{\sigma}^2 = 1, e_{\sigma}x = \bar{\sigma}(x)e_{\sigma} \) for all \( x \in A \). Then \( S \) is a c. s. \( F \)-algebra such that \( K \) is included in \( S \), say by \( \lambda \mapsto \lambda \otimes 1 \). Clearly, \( \text{dim}_F S = 4 \text{dim}_K A = 4 \text{dim}_F \text{cor}_{K/F}(R) \). The quaternion algebra \( S_1 \) generated by \( \sqrt{-1} \) and \( e_{\sigma} \) is contained in \( S \), whence \( S = S_1 \otimes_F C_S(S_1) \). Since \( S_1 \) is split and \( C_S(S_1) \cong \text{cor}_{F/K}(R) \), we obtain that \( S \) is similar to \( \text{cor}_{K/F}(R) \).

Another useful result that can be easily proved is that if \( R \) is the quaternion algebra \( (d, e/K) \), then \( R^e = (d(e), e(d)/K) \) if \( d \neq e). \)

It turns out that the projection formula is valid for the homomorphism of corestriction of algebras defined here. Tignol [23] proves this formula in maximal generality. Since in the proof of Lemma 4.1 we used only the projection formula, its analog holds for the corestriction of algebras.

Assume again that \( L/F \) is a Galois extension with a Galois group \( G, H \leq G, (G : H) = 2, H = \text{Gal}(L/K) \) and \( \tilde{I} \in Z^2(H, \mu_2) \) is a 2-cocycle representing a given group extension \( 1 \rightarrow \mu_2 \rightarrow H \rightarrow H \rightarrow 1 \). Denote \( I = \text{cor}(\tilde{I}) \), i.e., \( I = \text{cor}_{\tilde{I}}(\tilde{I}) \in H^2(G, \mu_2) \), and let the group extension \( 1 \rightarrow \mu_2 \rightarrow G \rightarrow G \rightarrow 1 \) be represented by \( I \). In this way we have the embedding problems \( (L/K, H, \mu_2) \) and \( (L/F, G, \mu_2) \), which have obstructions \( [L, H, \tilde{I}] \in \text{Br}_2(K) \) and \( [L, G, I] \in \text{Br}_2(F) \), respectively. Then we have the following

**Proposition 4.3 [(22, Prop. 2)].**
Under the above assumptions, we have \( \text{cor}_{K/F}(L, H, \tilde{I}) = [L, G, I] \).
In order to prove the proposition, it is enough to show that the following diagram is commutative:

\[
\begin{array}{ccc}
H^2(H, \mu_2) & \xrightarrow{\text{cor}_{G/H}} & H^2(\Omega_K, \mu_2) \\
\downarrow \text{cor}_{G/F} & & \downarrow \text{cor}_{G/F} \\
H^2(G, \mu_2) & \xrightarrow{\text{cor}_{G/F}} & H^2(\Omega_F, \mu_2) \\
\end{array}
\]

Br

We wish to emphasize that although the commutativity of the left square is obvious, the commutativity of the right square does not follow from the functorial properties of \( H^2 \). However, Riehm [18, Th.11] proves this result by applying non-abelian cohomology.

## 5. Some 2-groups as Galois groups

We begin with computations of the obstructions to the realizability of some small 2-groups which will be needed for our investigations on some of the 2-groups having a cyclic subgroup of index 4.

### 5.1. The group \( D \rtimes C \)

We denote by \( G_{(32,6)} \) the group of order 32 with number 6 in the 2-groups library of GAP [24]. It is of rank 2 and is generated by elements \( a_1, \ldots, a_5 \) such that \( a_1a_4^{-1} = 1, a_2^2 = 1, [a_2, a_1]a_3^{-1} = 1, a_5^2 = 1, [a_1, a_1]a_3^{-1} = 1, [a_1, a_2] = 1, a_4^2 = 1, [a_4, a_1] = 1, [a_4, a_2]a_5^{-1} = 1, [a_4, a_3] = 1, a_5^2 = 1 \). Put \( E_4 = \langle a_1, a_5 \rangle \) and \( G = \langle \sigma, \tau : \sigma^4 = r^2 = 1, \sigma \tau = \tau \sigma \rangle \cong C_4 \times C_2 \). Note that \( a_1a_2a_1^{-1} = a_2a_3, a_2a_2a_2^{-1} = a_3 \) and \( \langle a_5 \rangle \) is the centre of \( G_{(32,6)} \). Consider the group extension

\[
1 \longrightarrow E_4 \longrightarrow G_{(32,6)} \longrightarrow G \longrightarrow 1.
\]

Further, put \( H = \langle \sigma^2, \tau \rangle \cong C_2^2 \) and let \( \mathcal{H} \) be the preimage of \( H \) in \( G_{(32,6)} \): \( \mathcal{H} = \langle a_2, a_4, a_5 \rangle \cong D_8 \times C_2 \). Clearly, \( \mathcal{H} \) lies in the centralizer of \( E_4 \) in \( G_{(32,6)} \). We have the group extension \( 1 \rightarrow E_4 \rightarrow \mathcal{H} \rightarrow H \rightarrow 1 \). Denote by \( c_1 \) the 2-coclass in \( H^2(G, \mu_2) \), represented by the group extension

\[
1 \longrightarrow E_4/(a_5) \cong \mu_2 \longrightarrow G_{(32,6)}/(a_5) \longrightarrow G \longrightarrow 1,
\]

where \( G_{(32,6)}/(a_5) \) is isomorphic to the pull-back \( D \rtimes C \) of the groups \( D_8 \) and \( C_4 \). Denote by \( c_2 \) the 2-coclass in \( H^2(H, \mu_2) \), represented by the group extension

\[
1 \longrightarrow E_4/(a_3) \cong \mu_2 \longrightarrow \mathcal{H}/(a_3) \longrightarrow H \longrightarrow 1,
\]

where \( \mathcal{H}/(a_3) \) is isomorphic to the dihedral group \( D_8 \).

We move towards Galois extensions now. Let \( a \in F^* \setminus F^{*2}, a = 1 + c^2, c \in F^*, L = F(\sqrt{r(a + \sqrt{a})}, \sqrt{b}) \). Hence \( (a, a)_F = 1 \in Br_2(\mathcal{F}), G = \text{Gal}(L/F), \) and \( K = F(\sqrt{a}) \) is the fixed subfield of \( H \). From Theorem 3.3 it follows that the embedding problem \( \{ L/F, G_{(32,6)}, E_4 \} \) given by (6) is weakly solvable iff the embedding problem \( \{ L/K, D_8, \mu_2 \} \) given by \( c_2 \) is weakly solvable. As we know from [8] the obstruction to the latter embedding problem is \( \{ r(a + \sqrt{a}), -b \}_K \in Br_2(K) \).

Direct verification shows that \( E_4 \) lies in the Frattini subgroup of \( G_{(32,6)} \), so we have a proper solvability. Finally, from Theorem 3.8 we have that \( c_1 = \text{cor}_{G/F}(c_2) \), so we obtain the confirmation of the fact which we already know that the obstruction to solvability of the embedding problem \( \{ L/F, D \rtimes C, \mu_2 \} \) is \( (a, b) = (a, -b) = \text{cor}_{K/F}(r(a + \sqrt{a}), -b)_K \).
5.2. The group $G_{(32,6)}$

First, take the group of order 64 with number 32 in the 2-groups library of GAP [24], and denote it by $G_{(64,32)}$. It is of rank 2 and is generated by elements $b_1, \ldots, b_6$ such that $b_1^2 = \alpha$, $b_2^2 = 1, [b_2, b_1] = b_3$, $b_3^2 = 1, [b_3, b_1] = b_5$, $b_5^2 = 1, [b_5, b_2] = b_4$. Hence, put $G/H = \langle b_1, b_5 \rangle$. Further, put $E = \langle b_5, b_6 \rangle \cong C_2$. Further, put $H = \langle x^2, y, z \rangle \cong C_4$ and let $\mathcal{H} = \langle b_2, \ldots, b_6 | b_1^2 = \ldots = b_6^2 = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_5 \rangle$ be the preimage of $H$ in $G_{(64,32)}$. Clearly, $\mathcal{H}$ lies in the centralizer of $E$ in $G_{(64,32)}$. We have the group extension $1 \rightarrow E \rightarrow \mathcal{H} \rightarrow H \rightarrow 1$. Denote by $c_1$ the 2-coclass in $H^2(G, \mu_2)$ represented by the group extension

$$1 \rightarrow E \rightarrow \mathcal{H} \rightarrow \mu_2 \rightarrow 1,$$

where $G_{(64,32)}/\langle b_6 \rangle$ is isomorphic to the group $G_{(32,6)}$, described at the beginning of this section. Denote by $c_2$ the 2-coclass in $H^2(\mathcal{H}, \mu_2)$ represented by the group extension

$$1 \rightarrow E \langle b_6 \rangle \rightarrow \mathcal{H} \rightarrow H \rightarrow 1,$$

where $\mathcal{H}/\langle b_6 \rangle$ is isomorphic to the direct product $D_8 \times C_2$. According to [14], all $D \times C$-extensions $L/F$ can be described in the following way:

$$L/F = F \left( \sqrt{s(b_1 + b_2 \sqrt{a})}, \sqrt{r(a_1 + a_2 \sqrt{a})} \right)/F,$$

where $a_1^2 - aa_2^2 = a$ and $a = \beta_1^2 - b \beta_2^2$ for some $a_1, a_2, \beta_1, \beta_2, r, s \in F$. We omit the details of the actions of the generators of $D \times C$, which can be found in [14]. We find that

$$\sqrt{s(b_1 + b_2 \sqrt{a})} = \frac{1}{2} \left( \sqrt{2s(b_1 + \sqrt{a})} \pm \sqrt{2s(b_1 - \sqrt{a})} \right),$$

and

$$\sqrt{r(a_1 + a_2 \sqrt{a})} = \frac{1}{2} \left( \sqrt{2r(a_1 + \sqrt{a})} \pm \sqrt{2r(a_1 - \sqrt{a})} \right).$$

Hence $L$ can be written in the form

$$L = K \left( \sqrt{b}, \sqrt{2r(a_1 - \sqrt{a})}, \sqrt{2s(b_1 + \sqrt{a})} \right),$$

where $K = F(\sqrt{a})$ is the fixed subfield of $H \cong C_3^2$. Applying a criterion from [8] we obtain that the obstruction of the embedding problem $\{L/K, H/\langle b_6 \rangle, \mu_2 \}$ given by $c_2$ is $\{2r(a_1 - \sqrt{a}), 2s(b_1 + \sqrt{a}) \}_K \in Br_2(K)$. Further, from Theorem 3.3 and Proposition 3.7 it follows that the embedding problem $\{L/F, G_{(64,32)}, E \}$ given by (7) is properly solvable iff $\{2r(a_1 - \sqrt{a}), 2s(b_1 + \sqrt{a}) \}_K = 1 \in Br_2(K)$.

Now, let $E = F(\sqrt{a}, \sqrt{b})$ and let $y = a_1 + b_2 + a_2 \sqrt{a} + b_2 \sqrt{b}$. Then for the norm map $N$ we obtain $N_{E/F}(\sqrt{a}) = da$ and $N_{E/F}(\sqrt{b}) = db$, where $d = 2(a_1 + b_1), a = a_1 + a_2 \sqrt{a}, \beta = b_1 + b_2 \sqrt{b}$. From Theorem 3.8 it follows that $c_1 = cor_{G/\mathcal{H}}(c_2)$, so we can calculate the obstruction of the embedding problem $\{L/F, G_{(32,6)}, \mu_2 \}$ related to $c_1$, by applying Lemma 4.1:

$$cor_{G/F}(\{2r(a_1 - \sqrt{a}), 2s(b_1 + \sqrt{a}) \}_K) = \{4r^2(a_1^2 - a), -2r(-2s(a_1 + 2s)1s) \}_F \{4s^2(b_1^2 - a), 2s(4srb_1 + 4sr_1) \}_F = \{4r^2(a_1^2 - a), 2s(4sr(a_1 + b_1)) \}_F \{4s^2(b_1^2 - a), 2s(4sr(a_1 + b_1)) \}_F = (a, sd)(b, rd)_F.$$

Since the obstruction is a product of two quaternion algebras, we can describe all $G_{(32,6)}$ extensions:
Theorem 5.1 ([14, Th. 6.1]).
The obstruction to solvability of the embedding problem \( \{L/F, G_{(32, 0)}, \iota_2\} \) is \( (b, dr)(a, ds) \in Br_2(F) \). If \( (b, dr)(a, ds) = 1 \in Br_2(F) \), then there exist elements \( \delta_1, \delta_2, \delta_3 \in E \) and \( v \in F^\times \), such that \( drv = N_{E/F} \sigma_1(\delta), dsv = N_{E/F} \sigma_2(\delta) \), and

\[
\begin{align*}
M/F &= E(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma_1 \delta_3})/F, & t \in F^\times,
\end{align*}
\]

are all Galois extensions, solving the embedding problem \( \{L/F, G_{(32, 0)}, \mu_2\} \).

5.3. The groups \( G_{(32, 7)} \) and \( G_{(32, 8)} \)

Again, we exploit the 2-group library in GAP [24], where all groups of order 32 have five generators \( a_1, \ldots, a_5 \). We begin with the groups \( G_{(32, 7)} \) and \( G_{(32, 8)} \) with presentations (of course, not minimal):

\[
\begin{align*}
G_{(32, 7)} &:= \langle a_1^2a_4^{-1} = a_2^2 = [a_2, a_1]a_3^{-1} = a_3^2 = [a_3, a_1]a_4^{-1} = [a_4, a_1]a_5^{-1} = [a_4, a_2]a_5^{-1} = [a_4, a_3] = a_5^2 = 1 \rangle, \\
G_{(32, 8)} &:= \langle a_1^2a_4^{-1} = a_2^2a_5^{-1} = [a_2, a_1]a_3^{-1} = a_3^2 = [a_3, a_1]a_4^{-1} = [a_4, a_1]a_5^{-1} = [a_4, a_2]a_5^{-1} = [a_4, a_3] = a_5^2 = 1 \rangle.
\end{align*}
\]

Let \( L/F \) be the \( D \times C \)-extension described in the previous paragraph of this section. Denote by \( O_{G_{(32, 7)}} \) and \( O_{G_{(32, 8)}} \) the obstructions of the embedding problems given respectively by

\[
1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32, 7)} \xrightarrow{a_1 \mapsto x} G \cong D \times C \longrightarrow 1
\]

and

\[
1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32, 8)} \xrightarrow{a_1 \mapsto x} G \cong D \times C \longrightarrow 1.
\]

We can calculate the obstructions now.

Proposition 5.2.
\( O_{G_{(32, 7)}} = (b, dr)(a, 2ds)(-1, r) \in Br_2(F) \).

Proof. Observe that \( \{a_1, a_2\} \) is a minimal generating set for both groups \( G_{(32, 7)} \) and \( G_{(32, 0)} \), and also that \( G_{(32, 7)} = G_{(32, 0)}^{(0, 2)} \). Since the obstruction to the embedding problem given by the group extension \( 1 \rightarrow \mu_2 \rightarrow C_8 \rightarrow C_4 \rightarrow 1 \) in our situation is \( (a, 2)(-1, r) \in Br_2(F) \), we obtain what is desired.

Proposition 5.3.
\( O_{G_{(32, 8)}} = (b, -dr)(a, 2ds)(-1, r) \in Br_2(F) \).

Proof. Here again \( \{a_1, a_2\} \) is a minimal generating set for \( G_{(32, 8)} \). It is easy to see that \( G_{(32, 8)} = G_{(32, 7)}^{(1, 0)} \). Therefore, \( O_{G_{(32, 8)}} = O_{G_{(32, 7)}}(b, -1) \).

We leave as an exercise to the reader to prove that the automatic realization \( G_{(32, 8)} \Rightarrow G_{(32, 7)} \) is valid.
5.4. Non-abelian 2-groups having a cyclic subgroup of index 4

We begin with the list of all these groups given by Ninomiya in [17, Theorem 2]. Let $n \geq 4$. The finite non-abelian groups of order $2^n$ that have a cyclic subgroup of index 4, but not a cyclic subgroup of index 2, are of the following types:

(I) $n \geq 4$

\[
G_1 = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}} \rangle,
G_2 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \lambda^2 = 1, \sigma^{2^{n-3}} = \tau^2, \tau^{-1} \sigma \tau = \sigma^{-1}, \sigma \lambda = \lambda \sigma, \tau \lambda = \lambda \tau \rangle,
G_3 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{-1}, \sigma \lambda = \lambda \sigma, \tau \lambda = \lambda \tau \rangle,
G_4 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \sigma \lambda = \lambda \sigma, \lambda^{-1} \tau \lambda = \sigma^{2^{n-3}} \rangle,
G_5 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \lambda \sigma = \sigma \tau, \tau \lambda = \lambda \tau \rangle;
\]

(II) $n \geq 5$

\[
G_6 = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1} \sigma \tau = \sigma^{-1} \rangle,
G_7 = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}} \rangle,
G_8 = \langle \sigma, \tau : \sigma^{2^{n-2}} = 1, \sigma^{2^{n-3}} = \tau^4, \tau^{-1} \sigma \tau = \sigma^{-1} \rangle,
G_9 = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \sigma^{-1} \tau \sigma = \tau^{-1} \rangle,
G_{10} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \sigma \lambda = \lambda \sigma, \tau \lambda = \lambda \tau \rangle,
G_{11} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \sigma \lambda = \lambda \sigma, \tau \lambda = \lambda \tau \rangle,
G_{12} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \sigma \lambda = \sigma^{-1}, \lambda^{-1} \tau \lambda = \sigma^{2^{n-3}} \rangle,
G_{13} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \sigma \lambda = \sigma^{-1}, \lambda^{-1} \tau \lambda = \lambda \tau \rangle,
G_{14} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \sigma \lambda = \sigma^{-1} \tau, \tau \lambda = \lambda \tau \rangle,
G_{15} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1+2^{n-3}}, \tau \lambda = \lambda \tau \rangle,
G_{16} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1+2^{n-3}}, \lambda^{-1} \tau \lambda = \sigma^{2^{n-3}} \rangle,
G_{17} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1} \lambda \tau, \tau \lambda = \lambda \tau \rangle,
G_{18} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \lambda = \tau, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1} \tau \rangle;
\]

(III) $n \geq 6$

\[
G_{19} = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-4}} \rangle,
G_{20} = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-4}} \rangle,
G_{21} = \langle \sigma, \tau : \sigma^{2^{n-2}} = 1, \sigma^{2^{n-3}} = \tau^4, \sigma^{-1} \tau \sigma = \tau^{-1} \rangle,
G_{22} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \sigma \lambda = \sigma^{1+2^{n-4}}, \lambda^{-1} \tau \lambda = \sigma^{2^{n-3}} \rangle,
G_{23} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^{-1} \sigma \lambda = \sigma^{1+2^{n-4}}, \lambda^{-1} \tau \lambda = \sigma^{2^{n-3}} \rangle,
G_{24} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1+2^{n-4}}, \tau \lambda = \lambda \tau \rangle,
G_{25} = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1} \sigma \tau = \sigma^{1+2^{n-3}}, \lambda^{-1} \sigma \lambda = \sigma^{-1+2^{n-4}}, \tau \lambda = \lambda \tau \rangle;
\]

(IV) $n = 5$

\[
G_{26} = \langle \sigma, \tau, \lambda : \sigma^8 = \tau^2 = 1, \sigma^4 = \lambda^2, \tau^{-1} \sigma \tau = \sigma^5, \lambda^{-1} \sigma \lambda = \sigma \tau, \tau \lambda = \lambda \tau \rangle.
\]
5.4.1. The group $G_{17}$

Take the group $G$ generated by the elements $b_1, \ldots, b_6$ such that $b_1^{2^{n-1}} = b_1^4 = b_1, b_2^2 = b_2, b_3 = b_1, b_4 = 1, b_5 = b_6, b_6 = b_1, b_2 = b_3 = b_4 = 1, b_3 = b_1, b_4 = 1, [b_2, b_1] = [b_3, b_2] = 1, b_4^{2^{n-1}} = 1, [b_4, b_2] = b_1, [b_3, b_3] = b_1, b_2 = b_1, b_2 = b_1, b_3 = b_6, b_5 = b_1 = b_6, b_5 = 1$ and $b_6$ is central. Put $E_4 = \langle b_2, b_4 \rangle \cong C_2$. Observe that $b_1b_3b_1^{-1} = b_5b_4$ and $b_3b_3b_1^{-1} = b_5$ for $i = 2, \ldots, 6$. Consider the group extension

$$1 \rightarrow E_4 \rightarrow G \rightarrow \frac{G}{b_2} \rightarrow 1,$$

where $G$ is isomorphic to the group $C_{2^{n-1}} \times C_2$ from [15], generated by elements $x, y$ and $z$ such that $x^{2^{n-1}} = y^2 = z^2 = 1, yx = xy, z$ is central. Further, put $H = \langle x^2, y, z \rangle \cong C_{2^{n-1}} \times C_2$ and let $H = \langle b_2, \ldots, b_6 : b_2^2 = b_3^2 = b_4^2 = b_5^2 = b_6^2 = 1, [b_4, b_2] = b_1, [b_3, b_3] = b_6 \rangle$ be the preimage of $H$ in $G$. Clearly, $H$ lies in the centralizer of $E_4$ in $G$. We have the group extension $1 \rightarrow E_4 \rightarrow H \rightarrow H \rightarrow 1$. Denote by $c_1$ the $2$-coclass in $H^2(G, \mu_2)$ represented by the group extension

$$1 \rightarrow E_4 \langle b_6 \rangle \cong \mu_2 \rightarrow G \langle b_6 \rangle \rightarrow \frac{G}{b_6} \rightarrow 1,$$

where $G \langle b_6 \rangle$ is isomorphic to the group

$$G_1 \cong \left\langle \sigma, \tau, \lambda, \rho : \sigma^{2^{n-1}} = \lambda^2 = \rho^2 = 1, \tau^{-1} \sigma = \sigma \rho, \lambda^{-1} \sigma = \sigma \tau, [\tau, \lambda] = [\rho, \sigma] = [\rho, \tau] = [\rho, \lambda] = 1 \right\rangle$$

for $\sigma = b_1, \tau = b_2, \lambda = b_3, \rho = b_4$. Denote by $c_2$ the $2$-coclass in $H^2(H, \mu_2)$ represented by the group extension

$$1 \rightarrow E_4 \langle b_5 \rangle \cong \mu_2 \rightarrow H \langle b_5 \rangle \rightarrow H \rightarrow 1,$$

where $H \langle b_5 \rangle \cong C_{2^{n-1}} \times C_2 \times C_2$. From Theorem 3.8 we have that $c_1 = \text{cor}_{G_1}(c_2)$. Furthermore, any $G$-extension $L/F$ must contain a $D \times C$ extension $L/F$, since $G_1^{[\sigma^{2^{n-1}}]} \cong D \times C$.

From [15] we get that the obstruction to the embedding problem

$$(L/K, H \langle b_5 \rangle \cong C_{2^{n-1}} \times C_2 \times C_2, \mu_2)$$

is equal to the obstruction to $(L/K, D_4 \times C_2 \times \mu_2)$, which we know is \(\{2r(\sigma_1 - \sqrt{\sigma}), 2s(\beta_1 + \sqrt{\beta_1})\}_{\beta_1} \in B_{2^2}(K)\). Hence the obstruction to the embedding problem related to $c_1$ is exactly the same as for the embedding problem $(L/F, G_{13, b_6}, \mu_2)$.

Finally, note that we have $G_{17}/(\rho) \cong G_{17}/(\sigma^{2^{n-1}})$ and $G_{17} \cong G_{17}^{[\sigma^{2^{n-2}}]}$.

5.4.2. The groups $G_{13}$ and $G_{14}$

Observe first that $G_{14} \cong G_{13}^{[\sigma]}$. Therefore, we will focus on $G_{13}$.

Let the group $G$ be generated by elements $\sigma, \tau, \lambda, \rho$ such that $\sigma^{2^{n-2}} = \tau^2 = \lambda^2 = \rho^2 = 1, [\sigma, \rho] = \rho, \lambda^{-1} \sigma = \sigma^{-1} \tau, [\rho, \sigma] = [\rho, \tau] = 1, \rho$ is central. Define $E_4 = \langle \sigma, \rho \rangle \cong C_2^2, G = G/\langle \sigma, \rho \rangle \cong D_{2^{n-1}}, H = \langle \sigma^2, \tau, \lambda, \rho \rangle, H = H/\langle \sigma, \lambda, \rho \rangle \cong \langle \sigma^{-1}, \lambda, \rho \rangle \cong D_{2^{n-2}}$. We now have that $H$ lies in the centralizer of $E_4$ in $G$ and $\sigma \tau = \tau \rho$.

Denote by $c_1$ the $2$-coclass in $H^2(G, \mu_2)$ represented by the group extension

$$1 \rightarrow E_4 \langle \rho \rangle \cong \mu_2 \rightarrow G \langle \rho \rangle \cong G_{13} \rightarrow G \cong D_{2^{n-1}} \rightarrow 1$$

and by $c_2$ the $2$-coclass in $H^2(H, \mu_2)$, represented by the group extension

$$1 \rightarrow E_4 \langle \tau \rangle \cong \mu_2 \rightarrow H \langle \tau \rangle \cong H \cong D_{2^{n-2}} \rightarrow 1.$$
We will assume henceforth that the base field is a cyclic extension of degree $2^{n-1}$. From Theorem 3.8 we have that $c_1 = \text{cor}_{G/H}(c_0)$. Since the corestriction map is transitive, by induction we obtain that $c_1 = \text{cor}_{G/H}(c_0)$, where $c_0$ is the 2-cocycle in $H^2(D_8, \mu_2)$, represented by the group extension

$$1 \rightarrow \mu_2 \rightarrow D \times C \rightarrow H_0 \cong D_8 \rightarrow 1.$$ 

The obstruction to the embedding problem given by $c_0$ and a $D_8$ extension containing $K(\sqrt{\alpha}, \sqrt{\beta})/K$ is $(\alpha, \beta, -1) \in Br_2(K)$. Applying to each step the projection formula and (2.22) we obtain that $(\alpha_1, -1)$ is the obstruction to the embedding problem given by $c_1$ and a $D_{2^{n-1}}$ extension, where $F(\sqrt{\alpha_1}, \sqrt{\beta})/F$ is contained in the $D_{2^{n-1}}$ extension.

### 5.4.3. The groups $G_1$ to $G_{12}$ and $G_{15}$, $G_{16}$

Note first that there are direct products: $G_2 \cong Q_{2^{n-1}} \times C_2$, $G_3 \cong D_{2^{n-1}} \times C_2$, $G_{10} \cong M_{2^{n-1}} \times C_2$, $G_{11} \cong SD_{2^{n-1}} \times C_2$. Therefore, we will concentrate on the remaining 10 groups.

Let $M_{2^{n-1}} \times C_2 \cong \langle \sigma, \tau, \rho : \sigma^{2^{n-2}} = \tau^2 = 1, \tau^3 = 1, \tau^3 \sigma = \sigma^2 \tau \rangle$. Then $\langle M_{2^{n-1}} \times C_2 \rangle(\rho) \cong G_1(\tau^2) \cong M_{2^{n-1}}$ and it is easy to see that $G_1 = \langle M_{2^{n-1}} \times C_2 \rangle^{(4,\tau)}$. Similarly, we have $G_6 = \langle D_{2^{n-1}} \times C_2 \rangle^{(4,\tau)}$, $G_7 = \langle SD_{2^{n-1}} \times C_2 \rangle^{(4,\tau)}$, $G_8 = \langle M_{2^{n-1}} \times C_2 \rangle^{(4,\tau)}$.

The groups $G_i$ for $i = 4, 5, 9, 12, 15, 16$ have factor-groups which are direct products:

$$G_i/\langle \sigma^{2^{n-3}} \rangle \cong C_{2^{n-1}} \times C_2 \cong \langle \sigma, \tau, \lambda : \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \sigma \lambda = \lambda \sigma, \tau \lambda = \lambda \tau \rangle;$$

$$G_5/\langle \tau \rangle \cong C_{2^{n-1}} \times C_2 \cong \langle \sigma, \lambda : \sigma^{2^{n-2}} = \lambda^2 = 1, \sigma \lambda = \lambda \sigma \rangle;$$

$$G_9/\langle \tau^2 \rangle \cong C_{2^{n-1}} \times C_2 \cong \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^2 = 1, \sigma \tau = \tau \sigma \rangle;$$

$$G_{12}/\langle \sigma^{2^{n-3}} \rangle \cong G_{15}/\langle \sigma^{2^{n-3}} \rangle \cong G_{16}/\langle \sigma^{2^{n-3}} \rangle$$

$$\cong D_{2^{n-1}} \times C_2 \cong \langle \sigma, \tau, \lambda : \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = 1, \sigma \tau = \tau \sigma, \lambda^3 \sigma = \sigma^3, \tau \lambda = \lambda \tau \rangle.$$

We will assume henceforth that the base field $F$ contains a primitive $2^{n-3}$th root of unity $\zeta$. From (7.10) it follows that the obstruction to the embedding of a cyclic extension of degree $2^{n-3}$, containing the quadratic extension $F(\sqrt{\alpha_1}, \sqrt{\alpha_2})$, in a cyclic extension of degree $2^{n-2}$ is $\langle \alpha_1, \zeta \rangle \in Br_2(F)$; the obstruction to the embedding of a dihedral extension of degree $2^{n-2}$, containing the biquadratic extension $F(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_3})$, in a dihedral extension of degree $2^{n-1}$ is $\langle \alpha_1, \alpha_2, \zeta \rangle \in Br_2(F)$ for some $\alpha \in F$ described in [2, Example 5, (2.22)].

We can apply now Theorem 2.3 in order to obtain the obstructions to realizability of the groups $G_i$ for $i = 4, 5, 9, 12, 15, 16$ as Galois groups over $F$. The necessary and sufficient condition for any group $G_i$ to be realizable as Galois group over $F$ consists of two obstructions. The first obstruction is for the embedding problem given by $1 \rightarrow \mu_2 \rightarrow G_i \rightarrow G \rightarrow 1$, and the second is for the existence of $G$ extensions over $F$. We list these obstructions in Table 1. Note that the quaternion algebras of the kind $(+, -1)$ always split in $Br_2(F)$ for $n \geq 5$, since we assumed that $\zeta = \zeta_2 \in F$. Observe also that there always exist $C_{2^{n-3}}$ and $D_{2^{n-2}}$ extensions, according to [2].

The obstruction for the existence of an $M_{2^{n-1}}$ extension is taken from [15, Example 3.2]. The group $G_{28}$ is isomorphic to $G_{12,8}$. Here $C_i$ is always realizable, so we must add only the obstruction to the realizability of $D \times C$.

**Acknowledgements**

This work is partially supported by project No RD-05-342/12.03.2010 of Shumen University.
Table 1. The obstructions when $\zeta = \zeta_{p^{r-3}} \in F$

<table>
<thead>
<tr>
<th>Group</th>
<th>Obstructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>$(a_2, -1), (\zeta^{-1}a_2, a_1)$</td>
</tr>
<tr>
<td>$G_4$</td>
<td>$(a_1, \zeta)[a_2, a_3]$</td>
</tr>
<tr>
<td>$G_5$</td>
<td>$(a_1, a_2), (a_1, \zeta)$</td>
</tr>
<tr>
<td>$G_6$</td>
<td>$(a_2, -1), (a, a_1)(a_2, \zeta)$</td>
</tr>
<tr>
<td>$G_7$</td>
<td>$(a_2, -1), (a, a_1)(a_2, \zeta)$</td>
</tr>
<tr>
<td>$G_8$</td>
<td>$(a_2, -1), (a, a_1)(a_3, \zeta)$</td>
</tr>
<tr>
<td>$G_9$</td>
<td>$(a_1, a_2), (a_1, \zeta)$</td>
</tr>
<tr>
<td>$G_{12}$</td>
<td>$(a, a_1)(a_2, \zeta)(a_2, a_3)$</td>
</tr>
<tr>
<td>$G_{13}$</td>
<td>$(a_1, -1), (a, a_1)(a_2, \zeta)$</td>
</tr>
<tr>
<td>$G_{14}$</td>
<td>$(a_1, -1), (a, a_1)(a_2, \zeta)$</td>
</tr>
<tr>
<td>$G_{15}$</td>
<td>$(a, a_1)(a_2, \zeta)(a_1, a_3)$</td>
</tr>
<tr>
<td>$G_{16}$</td>
<td>$(a, a_1)(a_2, \zeta)(a_2a_1, a_3)$</td>
</tr>
<tr>
<td>$G_{17}$</td>
<td>$(a_1, ds\zeta)(a_2, dr)$</td>
</tr>
<tr>
<td>$G_{20}$</td>
<td>$(a_1, 2ds)(a_2, dr), (a_1, a_2)$</td>
</tr>
</tbody>
</table>

References

