Cent. Eur. J. Math. • 9(2) • 2011 • 403-419
DOI: 10.2478/s11533-011-0004-4

Central European Journal of **Mathematics**

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

Research Article

Ivo M. Michailov[1]*

1 *Faculty of Mathematics and Informatics, Constantin Preslavski University, Shumen, Bulgaria*

Received 12 October 2010; accepted 17 December 2010

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

$$1 \longrightarrow X \longrightarrow Y \underset{\alpha}{\longrightarrow} Z \longrightarrow 1 \qquad (1)$$

* *E-mail: ivo_michailov@yahoo.com*

Springer

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 $\mathrm{Gal}\,(L/F)$, and the homomorphism of restriction of L on E coincides with α. 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 μ_p-embedding problem

Let p be a prime, let F be a field with characteristic not p, and let F contain all pth roots of unity. Denote by ζ a primitive pth root of unity and by μ_p the cyclic group of all pth roots of unity which is contained in $F^\times = F \setminus \{0\}$. For $b, c \in F^\times$ write $(b, c; \zeta)_F$ to denote the equivalence class in the Brauer group $\mathrm{Br}\,(F)$ 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 $(b, c)_F$, or simply (b, c) when there is no danger of confusion.

Let $1 \to X \to Y \to G \to 1$ 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 μ_p. We have the following well known

Theorem 2.1 ([7]).
Let L/F be a finite Galois extension with Galois group $G = \mathrm{Gal}\,(L/F)$ and let $1 \to \mu_p \to Y \to G \to 1$ be a non-split group extension with characteristic class $\gamma \in H^2(G, \mu_p)$. Also, let $i : H^2(G, \mu_p) \to H^2(G, L^\times)$ be a homomorphism induced by the inclusion $\mu_p \subset L^\times$. Then the embedding problem $(L/F, Y, \mu_p)$ is properly solvable iff $i(\gamma) = 1 \in H^2(G, L^\times)$.

Let $f \in Z^2(G, \mu_p)$ represent γ given in the statement of the latter theorem. Then from [6, Th. 8.11] it follows that $H^2(G, L^\times)$ is isomorphic to the relative Brauer group $\mathrm{Br}\,(L/F)$ by $[f] \mapsto [L, G, f]$, where $[f] \in H^2(G, L^\times)$ is the cohomological 2-coclass containing $f \in Z^2(G, L^\times)$, and $[L, G, f] \in \mathrm{Br}\,(L/F)$ 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_σ, $\sigma \in G$, 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 $\zeta^s u_\sigma$ in (L, G, f).

Definition 2.2.
We call the element $O_Y = i(\gamma) \in H^2(G, L^\times) \cong \mathrm{Br}\,(L/F)$ 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

$$1 \longrightarrow C_p \cong \langle \zeta \rangle \longrightarrow G \underset{\pi}{\longrightarrow} H \times C_p \longrightarrow 1 \tag{2}$$

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

$$1 \longrightarrow C_p \longrightarrow \pi^{-1}(H) \underset{\pi}{\longrightarrow} H \longrightarrow 1.$$

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 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 $t^p = \zeta^j$ and $ts_i = \zeta^{d_i} s_i t$, where $i \in \{1, 2, \ldots, m\}$, $j, d_i \in \{0, 1, \ldots, p-1\}$. 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 $L/F = K\left(\sqrt[p]{b}\right)/F$ be a Galois extension with Galois group $H \times C_p$, $b \in F^\times \setminus F^{\times p}$. Choose $a_1, a_2, \dots, a_m \in F^\times$ such that $\sigma_k \sqrt[p]{a_i} = \zeta^{\delta_{ik}} \sqrt[p]{a_i}$ (δ_{ik} is the Kronecker delta). Then the obstruction to the embedding problem given by L/F and the group extension (2) is

$$[K, H, \mathrm{res}_H \gamma]\left(b,\, b^j \zeta^i \prod_{i=1}^{m} a_i^{d_i};\, \zeta\right).$$

Now, let G be a finite group, and let $\{\sigma_1, \dots, \sigma_k\}$ be a fixed (not necessarily minimal) generating set of G with the following properties: $|\sigma_1| = p^{n-1}$ for $n > 1$, the subgroup H generated by $\sigma_2, \dots, \sigma_k$ is normal in G, and the quotient group G/H is isomorphic to the cyclic group $C_{p^{n-1}}$, i.e., $\sigma_1^i \notin H$, $1 \le i < p^{n-1}$. Take now two arbitrary group extensions

$$1 \longrightarrow \mu_p \longrightarrow G_1 \underset{\varphi}{\longrightarrow} G \longrightarrow 1 \tag{3}$$

and

$$1 \longrightarrow \mu_p \longrightarrow G_2 \underset{\psi}{\longrightarrow} G \longrightarrow 1. \tag{4}$$

Denote by $\widetilde{\sigma}_i = \varphi^{-1}(\sigma_i)$ any preimage of σ_i in G_1 and by $\bar{\sigma}_i = \psi^{-1}(\sigma_i)$ any preimage of σ_i in G_2, $i = 1, \dots, k$.

Definition 2.4.

We write $G_2 = G_1^{(p^n, \sigma_1)}$, if

(1) $|\widetilde{\sigma}_1| = p^{n-1}$;

(2) $\bar{\sigma}_1^{p^{n-1}} \in \mu_p$, $\bar{\sigma}_1^{p^{n-1}} \neq 1$; and

(3) all other relations between the generators of the groups G_1 and G_2 are identical, i.e., $\widetilde{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j\neq 1} \widetilde{\sigma}_j^{\beta_j} \iff \bar{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j\neq 1} \bar{\sigma}_j^{\beta_j}$ for $i = 2, 3, \dots, k$; $l, \alpha_i, \beta_j \in \mathbb{Z}$; and $[\widetilde{\sigma}_i, \widetilde{\sigma}_j] = \zeta^l \prod_{s\neq 1} \widetilde{\sigma}_s^{\varepsilon_s} \iff [\bar{\sigma}_i, \bar{\sigma}_j] = \zeta^l \prod_{s\neq 1} \bar{\sigma}_s^{\varepsilon_s}$ for $i, j = 1, 2, \dots, k$; $l, \varepsilon_s \in \mathbb{Z}$.

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 σ_1 and σ_2 such that $\sigma_1^2 = 1$, $\sigma_2^{2^{n-2}} = 1$ and $[\sigma_1, \sigma_2] = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 = \sigma_2^2$; $G_1 = D_{2^n}$, the dihedral group of order 2^n generated by $\widetilde{\sigma}_1$ and $\widetilde{\sigma}_2$ such that $\widetilde{\sigma}_1^2 = 1$, $\widetilde{\sigma}_2^{2^{n-2}} = -1$ and $[\widetilde{\sigma}_1, \widetilde{\sigma}_2] = \widetilde{\sigma}_2^2$; and $G_2 = Q_{2^n}$, the quaternion group of order 2^n generated by $\bar{\sigma}_1$ and $\bar{\sigma}_2$ such that $\bar{\sigma}_1^2 = \bar{\sigma}_2^{2^{n-2}} = -1$ and $[\bar{\sigma}_1, \bar{\sigma}_2] = \bar{\sigma}_2^2$. It is easy to see now that $Q_{2^n} = D_{2^n}^{(4,\sigma_1)}$.

Example 2.6.

Let p be an odd prime. Put $G = C_{p^2} \times C_p$, the direct product of the cyclic group $C_{p^2} = \langle\sigma_2\rangle$ with the cyclic group $C_p = \langle\sigma_1\rangle$; let G_1 be the group of order p^4 generated by $\widetilde{\sigma}_1$ and $\widetilde{\sigma}_2$ such that $\widetilde{\sigma}_1^p = 1$, $\widetilde{\sigma}_2^p$ is central, $|\widetilde{\sigma}_2| = p^2$ and $[\widetilde{\sigma}_2, \widetilde{\sigma}_1] = \zeta$ (this group is isomorphic to G_3 from [13]); and G_2 be the group of order p^4 generated by $\bar{\sigma}_1$ and $\bar{\sigma}_2$ such that $\bar{\sigma}_1^p = \zeta$, $\bar{\sigma}_2^p$ is central, $|\bar{\sigma}_2| = p^2$ and $[\bar{\sigma}_2, \widetilde{\sigma}_1] = \zeta$ (this group is isomorphic to G_4 from [13]). Similarly to the previous example, $G_4 = G_3^{(p^2,\sigma_1)}$.

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 $G = \mathrm{Gal}(L/F)$ 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 $G_2 = G_1^{(p^n,\sigma_1)}$. Denote by $O_{G_1} \in \mathrm{Br}_p(F)$ the obstruction of the embedding problem $(L/F, G_1, \mu_p)$, by $O_{G_2} \in \mathrm{Br}_p(F)$ the obstruction of the embedding problem $(L/F, G_2, \mu_p)$, and by $O_{C_{p^n}} \in \mathrm{Br}_p(F)$ the obstruction of the embedding problem $(K/F, C_{p^n}, \mu_p)$ given by the group extension $1 \to \mu_p \to C_{p^n} \to G/H \cong C_{p^{n-1}} \to 1$. Then the relation between these obstructions is given by

$$O_{G_2} = O_{G_1} O_{C_{p^n}} \in \mathrm{Br}_p(F).$$

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, Γ_1 is generated over F by the elements from L and $\{u_\sigma\}_{\sigma\in G}$, where $u_1 = f_1(1,1) = 1$, $u_\sigma x = \sigma x u_\sigma$ and $u_\sigma u_\tau = u_{\sigma\tau} f_1(\sigma,\tau)$. Note that the structure of G_1 impacts the structure of Γ_1, e.g., if $[\widetilde{\sigma}_i, \widetilde{\sigma}_j] = \zeta \widetilde{\sigma}_s$ then $[u_{\sigma_i}, u_{\sigma_j}] = \zeta u_{\sigma_s}$. The cyclic algebra A generated by the elements from K and the elements $u_{\sigma_1}^i = u_{\sigma_1^i}$, $i = 1, \dots, p^{n-1}$, is contained in Γ_1 and $u_{\sigma_1}^{p^{n-1}} = u_1 = 1$. Then $\Gamma_1 = A \otimes_F C_{\Gamma_1}(A)$. We will prove that u_{σ_1} 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 $\sigma_1^i \sigma$, where $\sigma \in H = \langle \sigma_2, \dots, \sigma_k\rangle$ and $i = 1, \dots, p^{n-1}$. Then $u_{\sigma_1^i\sigma} = u_{\sigma_1^i} u_\sigma f_1^{-1}(\sigma_1^i, \sigma)$, so for arbitrary $\alpha \in C_{\Gamma_1}(A)$ we can write

$$\alpha = \sum_{\sigma\in H, i} x_{\sigma,i}\, u_{\sigma_1^i\sigma} = \sum_{\sigma\in H,i} y_{\sigma,i}\, u_{\sigma_1}^i u_\sigma,$$

where $x_{\sigma,i} \in L^\times$ and $y_{\sigma,i} = x_{\sigma,i} f_1^{-1}(\sigma_1^i, \sigma) \in L^\times$. Suppose $y_{\sigma,i} \neq 0$ for some i relatively prime to p. Since K contains an element of the kind $\sqrt[p]{a}$ for $a \in F^\times \backslash F^{\times p}$ such that $\sigma_1 \sqrt[p]{a} = \sqrt[p]{a}\,\zeta$, we have the equations: $u_{\sigma_1}^i \sqrt[p]{a} = \sigma_1^i \sqrt[p]{a}\, u_{\sigma_1}^i = \sqrt[p]{a}\,\zeta^i u_{\sigma_1}^i$ and $u_{\sigma_1}^j \sqrt[p]{a} = \sqrt[p]{a}\, u_{\sigma_1}^j$ for all j such that p divides j. Taking into account that $\sigma \sqrt[p]{a} = \sqrt[p]{a}$ for all $\sigma \in H$, we get

$$\alpha \sqrt[p]{a} = \sqrt[p]{a} \left(\sum_{(i,p)=1} y_{\sigma,i}\, \zeta^i u_{\sigma_1}^i u_\sigma + \sum_{p|i} y_{\sigma,i}\, u_{\sigma_1}^i u_\sigma \right) = \sqrt[p]{a}\, \alpha,$$

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_{σ_1} is divisible by p, so we can assume that α is of the kind

$$\alpha = \sum_{j>0,\, \sigma\in H} y_{\sigma,j}\, u_{\sigma_1}^{p^j k_j} u_\sigma,$$

where $(p, k_j) = 1$. Let j_0 be the smallest number such that $y_{\sigma_0,j_0} \neq 0$ for some $\sigma_0 \in H$. The short exact sequences

$$1 \longrightarrow C_p \longrightarrow C_{p^j} \longrightarrow C_{p^{j-1}} \longrightarrow 1,$$

$j = 2, \dots, n-1$, yield the following property of the cyclic extensions which we apply to j_0: there exists $\sqrt[p]{\omega} \in K$ such that $\sigma_1^{p^{j_0}k_{j_0}} \sqrt[p]{\omega} = \sqrt[p]{\omega}\,\zeta$ and $\sigma_1^{p^j k_j} \sqrt[p]{\omega} = \sqrt[p]{\omega}$ for all $j > j_0$. For simplicity, we assume that the other y_{σ,j_0}'s in the sum are 0. Then from

$$\alpha \sqrt[p]{\omega} = \sqrt[p]{\omega} \left(y_{\sigma_0,j_0}\, \zeta u_{\sigma_1}^{p^{j_0}k_{j_0}} u_\sigma + \sum_{j>j_0,\, \sigma\in H} y_{\sigma,j}\, u_{\sigma_1}^{p^j k_j} u_\sigma \right) = \sqrt[p]{\omega}\, \alpha$$

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, Γ_2 is generated over F by the elements from L and $\{v_\sigma\}_{\sigma\in G}$, where $v_1 = f_2(1,1) = 1$, $v_\sigma x = \sigma x v_\sigma$ 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 $v_{\sigma_1}^i = v_{\sigma_1^i}$, $i = 1, \dots, p^{n-1}-1$, is contained in Γ_2. Here, however, $v_{\sigma_1}^{p^{n-1}} = \zeta^l$, where $\bar{\sigma}_1^{p^{n-1}} = \zeta^l$. Then similarly to Γ_1, we have $\Gamma_2 = B \otimes_F C_{\Gamma_2}(B)$, where v_{σ_1} and its powers do not participate in the products that generate the centralizer $C_{\Gamma_2}(B)$. Now, define a map $\theta : \Gamma_1 \to \Gamma_2$ by $x \mapsto x$ and $u_\sigma \mapsto v_\sigma$ for all $x \in L$ and $\sigma \in G$. From what we have already proved for the structure of the centralizers it follows that θ maps $C_{\Gamma_1}(A)$ onto $C_{\Gamma_2}(B)$ and that the restriction $\theta : C_{\Gamma_1}(A) \to C_{\Gamma_2}(B)$ is an isomorphism.

It remains to observe that the algebra A is split. Hence $O_{G_1} = [\Gamma_1] = [A]\big[C_{\Gamma_1}(A)\big] = \big[C_{\Gamma_1}(A)\big]$. Finally, $[B] = O_{C_{p^n}}$, so $O_{G_2} = [B]\big[C_{\Gamma_2}(B)\big] = O_{C_{p^n}} O_{G_1}$. We are done. □

Corollary 2.8.

Let $G = D_{2^{n-1}}$ be the dihedral group of order 2^{n-1} with generators σ and τ such that $\sigma^{2^{n-2}} = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$, and let $L = K\big(\sqrt{b}\big)/F$ be a $D_{2^{n-1}}$ 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 $\big(L/F, Q_{2^n}, \mu_2\big)$ with obstructions $O_{D_{2^n}}$ and $O_{Q_{2^n}}$, respectively, such that the relation between the obstructions is $O_{Q_{2^n}} = O_{D_{2^n}}(b, -1)$.

Proof. Put $\sigma_1 = \tau$ and $\sigma_2 = \sigma$. From Example 2.5 it follows that $Q_{2^n} = D_{2^n}^{(4,\tau)}$. The embedding problem $\big(F\big(\sqrt{b}\big)/F, C_4, \mu_2\big)$ has obstruction $(b, -1)$, as it is well known. From Theorem 2.7 we obtain what is desired. □

Corollary 2.9.

Let p be odd, let G_3 be the group of order p^4 generated by elements $g_1, \dots, g_4$ such that $g_1^p = g_4$, $g_2^p = g_3^p = g_4^p = 1$, $[g_2, g_1] = g_3$, g_3 and g_4 are central, and let G_4 be the group of order p^4 generated by elements $g_1, \dots, g_4$ such that $g_1^p = g_4$, $g_2^p = g_3$, $g_3^p = g_4^p = 1$, $[g_2, g_1] = g_3$, g_3 and g_4 are central; see [13]. Let $G = C_{p^2} \times C_p$ be the direct product with generators σ, τ such that $\sigma^{p^2} = \tau^p = 1$ and $\sigma\tau = \tau\sigma$. Let L/F be a $C_{p^2} \times C_p$ extension containing $F\big(\sqrt[p]{b}\big)$ such that $\tau\sqrt[p]{b} = \zeta\sqrt[p]{b}$ and $\sigma\sqrt[p]{b} = \sqrt[p]{b}$. Let $\big(L/F, G_3, \mu_p\big)$ and $\big(L/F, G_4, \mu_p\big)$ be the embedding problems given by the group extensions:

$$1 \longrightarrow \langle g_3 \rangle \cong C_p \longrightarrow G_3 \underset{\substack{g_1 \mapsto \sigma \\ g_2 \mapsto \tau}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1$$

and

$$1 \longrightarrow \langle g_3 \rangle \cong C_p \longrightarrow G_4 \underset{\substack{g_1 \mapsto \sigma \\ g_2 \mapsto \tau}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1.$$

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

Proof. Put $\sigma_1 = \tau$ and $\sigma_2 = \sigma$. The embedding problem $\big(F\big(\sqrt[p]{b}\big)/F, C_{p^2}, \mu_p\big)$ has obstruction $(b, \zeta; \zeta)$; see e.g. [13]. From Example 2.6 it follows that $G_4 = G_3^{(p^2,\tau)}$ and it remains to apply Theorem 2.7. □

Definition 2.10.

We write $X \Rightarrow Y$ and call this an *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 $n \le 5$ are proven in [8] and [9], and $G_3 \implies G_4$ 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]) $A^* = M_G^H(A)$ 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 μ_2^*: 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, μ_2^* is an elementary abelian group of order 4, which we will write multiplicatively. We can denote the elements of μ_2^* 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 H to -1 and Hg to 1; a_4^* sends G to -1. The action of G on μ_2^* is then given by $ha^* = a^*$ for all $h \in H$ and $a^* \in \mu_2^*$; $ga_1^* = a_1^*$, $ga_2^* = a_3^*$, $ga_3^* = a_2^*$ and $ga_4^* = a_4^*$.

Now, let us define a map $\varphi : \mu_2^* \to \mu_2$ by $\varphi(a^*) = a^*(1)$. Clearly, φ is an epimorphism, which is compatible with the natural inclusion of H in G. Furthermore, $\ker(\varphi) = \{a_1^*, a_2^*\}$ and φ 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

$$\pi(a^*) = \prod_{x \in G/H} xa^*(x^{-1}),$$

where it should be noted that by $xa^*(x^{-1})$ is meant the action of x on $a^*(x^{-1}) \in \mu_2$. Since μ_2 is a trivial G-module, we have that $\pi(a^*) = a^*(1)a^*(g)$. The map π is well defined and it is a G-epimorphism, which induces the homomorphism of *corestriction* (*transfer*):

$$\mathrm{cor}_{G/H} : H^q(H, \mu_2) \cong H^q(G, \mu_2^*) \longrightarrow H^q(G, \mu_2), \tag{5}$$

where the left map is the isomorphism (which, henceforth, we will call for short the *Shapiro isomorphism*) given in the proof of Shapiro's Lemma in [20]. Notice also that $\ker(\pi) = \{a_1^*, a_4^*\}$ is a trivial G-module.

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

Lemma 3.2.
Let $\varphi_1, \varphi_2 \in \mathrm{Hom}_H(E_4, \mu_2)$ be such that $\ker(\varphi_1) = \{1, \tau\}$ and $\ker(\varphi_2) = \{1, \sigma\tau\}$. Then φ_1 and φ_2 induce, respectively, homomorphisms $\varphi_1'', \varphi_2'' : H^2(H, E_4) \to H^2(H, \mu_2)$, such that the compositions

$$\psi_i : H^2(G, E_4) \xrightarrow{\ \mathrm{res}\ } H^2(H, E_4) \xrightarrow{\ \varphi_i''\ } H^2(H, \mu_2)$$

are isomorphisms for $i = 1, 2$.

Proof. We can define a G-isomorphism $E_4 \cong \mu_2^*$ by $\sigma \mapsto a_4^*$, $\tau \mapsto a_2^*$, $\sigma\tau \mapsto a_3^*$. Thus, we can assume that the homomorphisms φ_i, given in the statement, are in $\mathrm{Hom}_H(\mu_2^*, \mu_2)$, and have kernels $\ker(\varphi_1) = \{a_1^*, a_2^*\}$ and $\ker(\varphi_2) = \{a_1^*, a_3^*\}$. Then for arbitrary G-module B, the homomorphisms φ_i induce homomorphisms $\varphi_i' : \mathrm{Hom}_H(B, \mu_2^*) \to \mathrm{Hom}_H(B, \mu_2)$ for $i = 1, 2$. Now, the inclusion $H \hookrightarrow G$ gives us the composition

$$\theta_1 : \mathrm{Hom}_G(B, \mu_2^*) \xrightarrow{\ \mathrm{res}\ } \mathrm{Hom}_H(B, \mu_2^*) \xrightarrow{\ \varphi_1'\ } \mathrm{Hom}_H(B, \mu_2),$$

such that $\theta_1(f)(b) = f(b)(1)$ for $f \in \mathrm{Hom}_G(B, \mu_2^*)$ and $b \in B$. According to [20], θ_1 is an isomorphism, which induces the Shapiro isomorphism. Since two cohomological functors, identical in zero degree, must be identical elsewhere, we obtain that ψ_1 is an isomorphism.

Now, let us define a map $\xi : \mu_2^* \to \mu_2^*$ by $a_1^* \mapsto a_1^*$, $a_2^* \mapsto a_3^*$, $a_3^* \mapsto a_2^*$ and $a_4^* \mapsto a_4^*$. Clearly, ξ is a G-automorphism of μ_2^*, which induces an automorphism $\xi' : \mathrm{Hom}_G(B, \mu_2^*) \to \mathrm{Hom}_G(B, \mu_2^*)$. Then for the composition

$$\theta_2 : \mathrm{Hom}_G(B, \mu_2^*) \xrightarrow{\text{res}} \mathrm{Hom}_H(B, \mu_2^*) \xrightarrow{\varphi_2'} \mathrm{Hom}_H(B, \mu_2)$$

we have that $\theta_2 = \theta_1 \xi'$. Therefore θ_2 and ψ_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 $K = L^H$ be the fixed subfield of H. Then the embedding problem $(L/F, \mathcal{G}, E_4)$ is weakly solvable iff the embedding problem $\big(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle\big)$ is weakly solvable.

Proof. **'Only-if' part.** The embedding problem $\big(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle\big)$ can be reached by taking the associated embedding problem of the second kind $(L/K, \mathcal{H}, E_4)$ and after that the associated embedding problem of the first kind $\big(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle\big)$. From [16] or [5] it follows that the weak solvability of the base embedding problem $(L/F, \mathcal{G}, E_4)$ implies the weak solvability of the associated embedding problems.

'If' part. Let φ_i and ψ_i, $i = 1, 2$, be the defined homomorphisms in Lemma 3.2. If we consider the Galois groups Ω_F and Ω_K of the separable closures F_s over F and K, respectively, the homomorphisms φ_i induce also homomorphisms $\overline{\psi}_i : H^2(\Omega_F, E_4) \to H^2(\Omega_K, \mu_2)$. Since ψ_i and $\overline{\psi}_i$ respect inflation, we have the commutative diagrams ($i = 1, 2$):

$$\begin{array}{ccc} H^2(G, E_4) & \xrightarrow{\psi_i} & H^2(H, \mu_2) \\ \downarrow{\scriptstyle \inf_G^{\Omega_F}} & & \downarrow{\scriptstyle \inf_H^{\Omega_K}} \\ H^2(\Omega_F, E_4) & \xrightarrow{\overline{\psi}_i} & H^2(\Omega_K, \mu_2)\,. \end{array}$$

Now, assume that the embedding problem $\big(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle\big)$ is weakly solvable and denote by c the 2-coclass of the group extension

$$1 \longrightarrow E_4 \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$$

in $H^2(G, E_4)$. Since the 2-coclass $\psi_1(c)$ is represented by the group extension

$$1 \longrightarrow E_4/\langle\tau\rangle \longrightarrow \mathcal{H}/\langle\tau\rangle \longrightarrow H \longrightarrow 1,$$

we have that $\inf_H^{\Omega_K}(\psi_1(c)) = 0$. The commutative diagram for $i = 1$ then shows that $\overline{\psi}_1 \inf_G^{\Omega_F}(c) = 0$. Since $\overline{\psi}_1$ is an isomorphism, $\inf_G^{\Omega_F}(c) = 0$, whence the embedding problem $(L/F, \mathcal{G}, E_4)$ is weakly solvable. □

Whether we would choose τ 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. I, § 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 $X \le \Phi(Y)$. 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 $\mathcal{G}$ be a finite 2-group and let the group extensions $1 \to E_4/\langle\rho\rangle \to \mathcal{H}/\langle\rho\rangle \to H \to 1$ be non-split for all $\rho \in E_4$. Then $E_4 \leq \Phi(\mathcal{G})$.

Proof. Suppose E_4 is not contained in $\Phi(\mathcal{H})$. Then the group $E_0 = E_4 \cap \Phi(\mathcal{H})$ has an order ≤ 2, so the group extension $1 \to E_4/E_0 \to \mathcal{H}/E_0 \to H \to 1$ is split by Lemma 3.6, which is a contradiction. Hence $E_4 \leq \Phi(\mathcal{H}) \leq \Phi(\mathcal{G})$ 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 $1 \to E_4/\langle\sigma\rangle \cong \mu_2 \to \mathcal{G}/\langle\sigma\rangle \to G \to 1$, let $c_2 \in H^2(H, \mu_2)$ be the 2-coclass represented by the group extension $1 \to E_4/\langle\tau\rangle \cong \mu_2 \to \mathcal{H}/\langle\tau\rangle \to H \to 1$, and let $c_3 \in H^2(H, \mu_2)$ be the 2-coclass represented by the group extension $1 \to E_4/\langle\sigma\tau\rangle \cong \mu_2 \to \mathcal{H}/\langle\sigma\tau\rangle \to H \to 1$. Then $\mathrm{cor}_{G/H}(c_2) = \mathrm{cor}_{G/H}(c_3) = c_1$.

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

$$\mathrm{cor}_{G/H} : H^2(H, \mu_2) \longrightarrow H^2(G, \mu_2^*) \xrightarrow{\pi'} H^2(G, \mu_2),$$

where the left map is the Shapiro isomorphism and the right map is induced by π. Now, let $c \in H^2(G, E_4)$ be the 2-coclass represented by the group extension $1 \to E_4 \to \mathcal{G} \to G \to 1$, let $\xi_1 : E_4 \to \mu_2^*$ be the G-isomorphism defined by $\xi_1(\sigma) = a_4^*$, $\xi_1(\tau) = a_2^*$, $\xi_1(\sigma\tau) = a_3^*$, and let $\xi_1' : H^2(G, E_4) \to H^2(G, \mu_2^*)$ be the induced isomorphism. Similarly, let $\xi_2 : E_4 \to \mu_2^*$ be the G-isomorphism defined by $\xi_2(\sigma) = a_4^*$, $\xi_2(\tau) = a_3^*$, $\xi_2(\sigma\tau) = a_2^*$, and let $\xi_2' : H^2(G, E_4) \to H^2(G, \mu_2^*)$ be the induced isomorphism.

Now, from Lemma 3.2 it follows that $c_2 = \psi_1(c)$, where ψ_1 is an isomorphism. Furthermore, $c_1 = \pi'\xi_1'(c)$ and $c_1 = \pi'\xi_1'\psi_1^{-1}(c_2)$, where $\xi_1'\psi_1^{-1}$ is exactly the Shapiro isomorphism. Similarly, we have $c_3 = \psi_2(c)$ and $c_1 = \pi'\xi_2'(c)$, since $\pi(a_2^*) = \pi(a_3^*) = -1$. Therefore $c_1 = \pi'\xi_2'\psi_2^{-1}(c_3)$. The definitions of ψ_1 and ψ_2 in Lemma 3.2 show us that we have the commutative diagram:

$$\begin{array}{ccc} H^2(G, E_4) & \xrightarrow{\psi_1} & H^2(H, \mu_2) \\ \uparrow{\scriptstyle \xi_1'^{-1}} & & \uparrow{\scriptstyle \psi_2} \\ H^2(G, \mu_2^*) & \xrightarrow{\xi_2'^{-1}} & H^2(G, E_4) \end{array}$$

whence we obtain $\xi_1'\psi_1^{-1} = \xi_2'\psi_2^{-1}$, the Shapiro isomorphism. Therefore, $c_1 = \mathrm{cor}_{G/H}(c_2) = \mathrm{cor}_{G/H}(c_3)$. □

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 $\mathrm{Gal}(K/F) = \langle\sigma\rangle \cong C_2$. Since $\mathrm{Br}_2(F) \cong H^2(\Omega_F, \mu_2)$, we have the corestriction homomorphism $\mathrm{cor}_{\Omega_F/\Omega_K} : \mathrm{Br}_2(K) \to \mathrm{Br}_2(F)$. For $b \in F^\times$ and $\alpha \in K$, the projection formula states that $\mathrm{cor}_{\Omega_F/\Omega_K}(\alpha, b)_K = (N_{K/F}(\alpha), b)_F$, where $N_{K/F}$ is the norm map. This formula can be derived from the exercises in [21, XIV § 1, § 2].

With the aid of the projection formula we can prove directly the following lemma, which is an analog of [22, Pr. 4].

Lemma 4.1.

Let $a \in F^\times$, $K = F(\sqrt{a})$, $\alpha_0 = a_0 + b_0\sqrt{a}$ and $\alpha_1 = a_1 + b_1\sqrt{a}$, $a_i, b_i \in F$.

(1) *If $b_{1-i} = 0$, then $\operatorname{cor}_{\Omega_F/\Omega_K}(\alpha_0, \alpha_1)_K = \big(a_{1-i}, a_i^2 - ab_i^2\big)_F$.*

(2) *If $a_{1-i}b_i - a_ib_{1-i} = 0$, then $\operatorname{cor}_{\Omega_F/\Omega_K}(\alpha_0, \alpha_1)_K = \big(-a_ia_{1-i}, a_i^2 - ab_i^2\big)_F$.*

(3) *Otherwise,*

$$\operatorname{cor}_{\Omega_F/\Omega_K}(\alpha_0, \alpha_1)_K = \big(a_0^2 - ab_0^2, b_0(a_1b_0 - a_0b_1)\big)_F \big(a_1^2 - ab_1^2, b_1(a_0b_1 - a_1b_0)\big)_F.$$

Proof. (1) Follows from the projection formula.

(2) We have $a_1b_0 = a_0b_1$ and $a_i, b_i \neq 0$, so $a_1/a_0 = b_1/b_0 = x \in F^\times$. Therefore, $(\alpha_0, \alpha_1)_K = (\alpha_0, \alpha_0 x)_K = (\alpha_0, -x)_K = (\alpha_0, -a_0a_1)_K$ 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 $y = -\Delta b_0/b_1 \neq 0$. Then the following hold: $-\alpha_1 y = \Delta a_1b_0/b_1 + b_0\Delta\sqrt{a} = \Delta a_1b_0/b_1 - a_0\Delta + \alpha_0\Delta = -\Delta^2/b_1 + \alpha_0\Delta$, whence $b_1\alpha_1 y = \Delta^2 - \alpha_0 b_1\Delta$. Therefore $(\alpha_0b_1\Delta, -\alpha_1b_0\Delta)_K = 1 \in \operatorname{Br}_2(K)$, so $(\alpha_0b_1\Delta, -b_0\Delta)_K(\alpha_0b_1\Delta, \alpha_1)_K = 1$ or, equivalently, $(\alpha_0, \alpha_1)_K = (\alpha_0b_1\Delta, -b_0\Delta)_K(\alpha_1, b_1\Delta)_K = (\alpha_0, -b_0\Delta)_K(\alpha_1, b_1\Delta)_K(b_1\Delta, -b_0\Delta)_K$. Since $b_i\Delta \in F^\times$, we can apply again the projection formula to get the desired result. □

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

Definition 4.2 ([18, 19]).

The corestriction of R is the F-algebra of $\widetilde{\sigma}$-invariants: $\operatorname{cor}_{K/F}(R) = A^{\langle\widetilde{\sigma}\rangle}$.

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 $\psi : K \times \operatorname{cor}_{K/F}(R) \to A$ given by $(\alpha, x) \mapsto \alpha x$ is F-bilinear, multiplicative, and it induces a canonical K-algebra isomorphism $K \otimes_F \operatorname{cor}_{K/F}(R) \cong A$. From this we see that $\operatorname{cor}_{K/F}(R)$ is a c. s. F-algebra and $\dim_F \operatorname{cor}_{K/F}(R) = \dim_K A$. Notice that $\operatorname{cor}_{K/F}(R)$ does not contain K, which may cause difficulties in various situations. This, however, can be easily amended: Define $S = A \oplus Ae_\sigma$ as an F-vector space and turn S into an algebra by $e_\sigma^2 = 1$, $e_\sigma x = \widetilde{\sigma}(x)e_\sigma$ 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, $\dim_F S = 4\dim_K A = 4\dim_F \operatorname{cor}_{K/F}(R)$. The quaternion algebra S_1 generated by $\sqrt{a}$ and e_σ is contained in S, whence $S = S_1 \otimes_F C_S(S_1)$. Since S_1 is split and $C_S(S_1) \cong \operatorname{cor}_{K/F}(R)$, we obtain that S is similar to $\operatorname{cor}_{K/F}(R)$.

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

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, $H < G$, $(G : H) = 2$, $H = \operatorname{Gal}(L/K)$ and $\bar{f} \in Z^2(H, \mu_2)$ is a 2-cocycle representing a given group extension $1 \to \mu_2 \to H_2 \to H \to 1$. Denote $f = \operatorname{cor}(\bar{f})$, i.e., $[f] = \operatorname{cor}_{G/H}([\bar{f}]) \in H^2(G, \mu_2)$, and let the group extension $1 \to \mu_2 \to \mathcal{G} \to G \to 1$ be represented by f. In this way we have the embedding problems $(L/K, H, \mu_2)$ and $(L/F, G, \mu_2)$, which have obstructions $[L, H, \bar{f}] \in \operatorname{Br}_2(K)$ and $[L, G, f] \in \operatorname{Br}_2(F)$, respectively. Then we have the following

Proposition 4.3 ([22, Prop. 2]).

Under the above assumptions, we have $\operatorname{cor}_{K/F}([L, H, \bar{f}]) = [L, G, f]$.

In order to prove the proposition, it is enough to show that the following diagram is commutative:

$$\begin{array}{ccccc} H^2(H,\mu_2) & \xrightarrow{\inf_H^{\Omega_K}} & H^2(\Omega_K,\mu_2) & = & \mathrm{Br}_2(K) \\ \downarrow \mathrm{cor}_{G/H} & & \downarrow \mathrm{cor}_{\Omega_F/\Omega_K} & & \downarrow \mathrm{cor}_{K/F} \\ H^2(G,\mu_2) & \xrightarrow{\inf_G^{\Omega_F}} & H^2(\Omega_F,\mu_2) & = & \mathrm{Br}_2(F) \end{array}$$

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 $D \curlywedge C$

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 $a_1, \dots, a_5$ such that $a_1^2 a_4^{-1} = 1$, $a_2^2 = 1$, $[a_2, a_1] a_3^{-1} = 1$, $a_3^2 = 1$, $[a_3, a_1] a_5^{-1} = 1$, $[a_3, a_2] = 1$, $a_4^2 = 1$, $[a_4, a_1] = 1$, $[a_4, a_2] a_5^{-1} = 1$, $[a_4, a_3] = 1$, $a_5^2 = 1$. Put $E_4 = \langle a_3, a_5 \rangle$ and $G = \big\langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \sigma\tau = \tau\sigma \big\rangle \cong C_4 \times C_2$. Note that $a_1 a_3 a_1^{-1} = a_5 a_3$, $a_2 a_3 a_2^{-1} = a_3$ and $\langle a_5 \rangle$ is the centre of $G_{(32,6)}$. Consider the group extension

$$1 \longrightarrow E_4 \longrightarrow G_{(32,6)} \underset{\substack{a_1 \mapsto \sigma \\ a_2 \mapsto \tau}}{\longrightarrow} G \longrightarrow 1. \tag{6}$$

Further, put $H = \langle \sigma^2, \tau \rangle \cong C_2^2$ and let $\mathcal{H}$ be the preimage of H in $G_{(32,6)}$: $\mathcal{H} = \langle a_2, a_4, a_5 \rangle \times \langle a_3 \rangle \cong D_8 \times C_2$. Clearly, $\mathcal{H}$ lies in the centralizer of E_4 in $G_{(32,6)}$. We have the group extension $1 \to E_4 \to \mathcal{H} \to H \to 1$. Denote by c_1 the 2-coclass in $H^2(G,\mu_2)$, represented by the group extension

$$1 \longrightarrow E_4/\langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32,6)}/\langle a_5 \rangle \underset{\substack{a_1 \mapsto \sigma \\ a_2 \mapsto \tau}}{\longrightarrow} G \longrightarrow 1,$$

where $G_{(32,6)}/\langle a_5 \rangle$ is isomorphic to the pull-back $D \curlywedge C$ 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

$$1 \longrightarrow E_4/\langle a_3 \rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle a_3 \rangle \underset{\substack{a_4 \mapsto \sigma \\ a_2 \mapsto \tau}}{\longrightarrow} H \longrightarrow 1,$$

where $\mathcal{H}/\langle a_3 \rangle$ is isomorphic to the dihedral group D_8.

We move towards Galois extensions now. Let $a \in F^\times \setminus F^{\times 2}$, $a = 1 + c^2$, $c \in F^\times$, $L = F\big(\sqrt{r(a+\sqrt{a})}, \sqrt{b}\big)$. Hence $(a,a)_F = 1 \in \mathrm{Br}_2(F)$, $G = \mathrm{Gal}\,(L/F)$, and $K = F\big(\sqrt{a}\big)$ is the fixed subfield of H. From Theorem 3.3 it follows that the embedding problem $\big(L/F, G_{(32,6)}, E_4\big)$ 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 $\big(r\big(a+\sqrt{a}\big), -b\big)_K \in \mathrm{Br}_2(K)$. 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 $c_1 = \mathrm{cor}_{G/H}(c_2)$, so we obtain the confirmation of the fact which we already know that the obstruction to solvability of the embedding problem $(L/F, D \curlywedge C, \mu_2)$ is $(a,b) = (a,-b) = \mathrm{cor}_{K/F}\big(r\big(a+\sqrt{a}\big), -b\big)_K$.

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 $b_1, \dots, b_6$ such that $b_1^2 = b_4$, $b_2^2 = 1$, $[b_2, b_1] = b_3$, $b_3^2 = 1$, $[b_3, b_1] = b_5$, $[b_3, b_2] = 1$, $b_4^2 = 1$, $[b_4, b_2] = b_5$, $[b_4, b_3] = b_6$, $b_5^2 = 1$, $[b_5, b_1] = b_6$, $b_6^2 = 1$, $[b_5, b_2] = [b_5, b_3] = [b_5, b_4] = 1$ and $\langle b_6 \rangle$ is the centre of $G_{(64,32)}$. The pull-back $G = D \curlywedge C$ is generated by elements x and y such that $x^4 = y^2 = 1$, $[y, x] = z$, $z^2 = 1$ and z is central. Put $E_4 = \langle b_5, b_6 \rangle \cong C_2^2$. Observe that $b_1 b_5 b_1^{-1} = b_5 b_6$ and $b_i b_5 b_i^{-1} = b_5$ for $i = 2, \dots, 6$. Consider the group extension

$$1 \longrightarrow E_4 \longrightarrow G_{(64,32)} \underset{\substack{b_1 \mapsto x \\ b_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1. \tag{7}$$

Further, put $H = \langle x^2, y, z \rangle \cong C_2^3$ and let $\mathcal{H} = \left\langle b_2, \dots, b_6 \,|\, b_2^2 = \dots = b_6^2 = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6 \right\rangle$ be the preimage of H in $G_{(64,32)}$. Clearly, $\mathcal{H}$ lies in the centralizer of E_4 in $G_{(64,32)}$. We have the group extension $1 \to E_4 \to \mathcal{H} \to H \to 1$. Denote by c_1 the 2-coclass in $H^2(G, \mu_2)$ represented by the group extension

$$1 \longrightarrow E_4/\langle b_6 \rangle \cong \mu_2 \longrightarrow G_{(64,32)}/\langle b_6 \rangle \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1,$$

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 $H^2(H, \mu_2)$ represented by the group extension

$$1 \longrightarrow E_4/\langle b_5 \rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle b_5 \rangle \underset{\substack{a_4 \mapsto \sigma \\ a_2 \mapsto \tau}}{\longrightarrow} H \longrightarrow 1,$$

where $\mathcal{H}/\langle b_5 \rangle$ is isomorphic to the direct product $D_8 \times C_2$. According to [14], all $D \curlywedge C$-extensions L/F can be described in the following way:

$$L/F = F\left(\sqrt{s(\beta_1 + \beta_2 \sqrt{b})}, \sqrt{r(\alpha_1 + \alpha_2 \sqrt{a})} \right)/F,$$

where $\alpha_1^2 - a\alpha_2^2 = a$ and $a = \beta_1^2 - b\beta_2^2$ for some $\alpha_1, \alpha_2, \beta_1, \beta_2, r, s \in F$. We omit the details of the actions of the generators of $D \curlywedge C$, which can be found in [14]. We find that

$$\sqrt{s(\beta_1 + \beta_2 \sqrt{b})} = \frac{1}{2}\left(\sqrt{2s(\beta_1 + \sqrt{a})} \pm \sqrt{2s(\beta_1 - \sqrt{a})} \right) \qquad \text{and}$$
$$\sqrt{r(\alpha_1 + \alpha_2 \sqrt{a})} = \frac{1}{2}\left(\sqrt{2r(\alpha_1 + \sqrt{a})} \pm \sqrt{2r(\alpha_1 - \sqrt{a})} \right).$$

Hence L can be written in the form

$$L = K\left(\sqrt{b}, \sqrt{2r(\alpha_1 - \sqrt{a})}, \sqrt{2s(\beta_1 + \sqrt{a})} \right),$$

where $K = F(\sqrt{a})$ is the fixed subfield of $H \cong C_2^3$.

Applying a criterion from [8] we obtain that the obstruction of the embedding problem $(L/K, \mathcal{H}/\langle b_5 \rangle, \mu_2)$ given by c_2 is $\left(2r(\alpha_1 - \sqrt{a}), 2s(\beta_1 + \sqrt{a})\right)_K \in \mathrm{Br}_2(K)$. Further, from Theorem 3.3 and Proposition 3.7 it follows that the embedding problem $(L/F, G_{(64,32)}, E_4)$ given by (7) is properly solvable iff $\left(2r(\alpha_1 - \sqrt{a}), 2s(\beta_1 + \sqrt{a})\right)_K = 1 \in \mathrm{Br}_2(K)$.

Now, let $E = F(\sqrt{a}, \sqrt{b})$ and let $\gamma = \alpha_1 + \beta_1 + \alpha_2\sqrt{a} + \beta_2\sqrt{b}$. Then for the norm map N we obtain $N_{E/F(\sqrt{a})}(\gamma) = d\alpha$ and $N_{E/F(\sqrt{b})}(\gamma) = d\beta$, where $d = 2(\alpha_1 + \beta_1)$, $\alpha = \alpha_1 + \alpha_2\sqrt{a}$, $\beta = \beta_1 + \beta_2\sqrt{b}$. From Theorem 3.8 it follows that $c_1 = \mathrm{cor}_{G/H}(c_2)$, 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:

$$\begin{aligned}\mathrm{cor}_{K/F}\left(\left(2r(\alpha_1 - \sqrt{a}), 2s(\beta_1 + \sqrt{a})\right)_K\right) &= \left(4r^2(\alpha_1^2 - a), -2r(-2s\beta_1 2r - 2r\alpha_1 2s)\right)_F \left(4s^2(\beta_1^2 - a), 2s(4sr\beta_1 + 4rs\alpha_1)\right)_F \\ &= \left(4r^2 a\alpha_2^2, 2r4rs(\alpha_1 + \beta_1)\right)_F \left(4s^2 b\beta_2^2, 2s4rs(\alpha_1 + \beta_1)\right)_F = (a, sd)_F (b, rd)_F.\end{aligned}$$

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 $(L/F, G_{(32,6)}, \mu_2)$ is $(b, dr)(a, ds) \in \mathrm{Br}_2(F)$. If $(b, dr)(a, ds) = 1 \in \mathrm{Br}_2(F)$, then there exist elements $\delta_1, \delta_2, \delta_3 \in E$ and $v \in F^\times$, such that $drv = N_{E/F(\sqrt{a})}(\delta_1)$, $dsv = N_{E/F(\sqrt{b})}(\delta_2)$, $v = N_{E/F(\sqrt{a})}(\delta_3) = N_{E/F(\sqrt{b})}(\delta_3)$, and

$$M/F = E\left(\sqrt{r\alpha}, \sqrt{s\beta}, \sqrt{t\delta_1\delta_2\delta_3}\right)/F, \qquad t \in F^\times,$$

are all Galois extensions, solving the embedding problem $(L/F, G_{(32,6)}, \mu_2)$.

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 $a_1, \dots, a_5$. We begin with the groups $G_{(32,7)}$ and $G_{(32,8)}$ with presentations (of course, not minimal):

$$G_{(32,7)}: \quad a_1^2a_4^{-1} = a_2^2 = [a_2, a_1]a_3^{-1} = a_3^2 = [a_3, a_1]a_5^{-1} = [a_3, a_2] = a_4^2a_5^{-1} = [a_4, a_1] = [a_4, a_2]a_5^{-1} = [a_4, a_3] = a_5^2 = 1;$$
$$G_{(32,8)}: \quad a_1^2a_4^{-1} = a_2^2a_5^{-1} = [a_2, a_1]a_3^{-1} = a_3^2 = [a_3, a_1]a_5^{-1} = [a_3, a_2] = a_4^2a_5^{-1} = [a_4, a_1] = [a_4, a_2]a_5^{-1} = [a_4, a_3] = a_5^2 = 1.$$

Let L/F be the $D \curlywedge C$-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

$$1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32,7)} \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1$$

and

$$1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32,8)} \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1.$$

We can calculate the obstructions now.

Proposition 5.2.
$O_{G_{(32,7)}} = (b, dr)(a, 2ds)(-1, r) \in \mathrm{Br}_2(F)$.

Proof. Observe that $\{a_1, a_2\}$ is a minimal generating set for both groups $G_{(32,7)}$ and $G_{(32,6)}$, and also that $G_{(32,7)} = G_{(32,6)}^{(8,x)}$. Since the obstruction to the embedding problem given by the group extension $1 \to \mu_2 \to C_8 \to C_4 \to 1$ in our situation is $(a, 2)(-1, r) \in \mathrm{Br}_2(F)$, we obtain what is desired. □

Proposition 5.3.
$O_{G_{(32,8)}} = (b, -dr)(a, 2ds)(-1, r) \in \mathrm{Br}_2(F)$.

Proof. Here again $\{a_1, a_2\}$ is a minimal generating set for $G_{(32,8)}$. It is easy to see that $G_{(32,8)} = G_{(32,7)}^{(4,y)}$. 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 $G_{(32,8)} \implies G_{(32,7)}$ 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) $n \geq 4$

$$\begin{aligned}
G_1 &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1,\ \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}} \rangle,\\
G_2 &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \lambda^2 = 1,\ \sigma^{2^{n-3}} = \tau^2,\ \tau^{-1}\sigma\tau = \sigma^{-1},\ \sigma\lambda = \lambda\sigma,\ \tau\lambda = \lambda\tau \rangle,\\
G_3 &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1,\ \tau^{-1}\sigma\tau = \sigma^{-1}, \sigma\lambda = \lambda\sigma,\ \tau\lambda = \lambda\tau \rangle,\\
G_4 &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1,\ \sigma\tau = \tau\sigma,\ \sigma\lambda = \lambda\sigma,\ \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle,\\
G_5 &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1,\ \sigma\tau = \tau\sigma,\ \lambda^{-1}\sigma\lambda = \sigma\tau,\ \tau\lambda = \lambda\tau \rangle;
\end{aligned}$$

(II) $n \geq 5$

$$\begin{aligned}
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}}\tau \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}\tau,\ \tau\lambda = \lambda\tau \rangle,\\
G_{14} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = 1,\ \sigma^{2^{n-3}} = \lambda^2,\ \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}}\tau \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\tau,\ \tau\lambda = \lambda\tau \rangle,\\
G_{18} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = 1,\ \lambda^2 = \tau,\ \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}},\ \lambda^{-1}\sigma\lambda = \sigma^{-1}\tau \rangle;
\end{aligned}$$

(III) $n \geq 6$

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

(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 $\mathcal{G}$ generated by the elements $b_1, \dots, b_6$ such that $b_1^{2^{n-3}} = 1$, $b_1^2 = b_4$, $b_2^2 = 1$, $[b_2, b_1] = b_3$, $b_3^2 = 1$, $[b_3, b_1] = b_5$, $[b_3, b_2] = 1$, $b_4^{2^{n-4}} = 1$, $[b_4, b_2] = b_5$, $[b_4, b_3] = b_6$, $b_5^2 = 1$, $[b_5, b_1] = b_6$, $b_6^2 = 1$, $[b_5, b_2] = [b_5, b_3] = [b_5, b_4] = 1$ and b_6 is central. Put $E_4 = \langle b_5, b_6\rangle \cong C_2^2$. Observe that $b_1 b_5 b_1^{-1} = b_5 b_6$ and $b_i b_5 b_i^{-1} = b_5$ for $i = 2, \dots, 6$. Consider the group extension

$$1 \longrightarrow E_4 \longrightarrow \mathcal{G} \underset{\substack{b_1 \mapsto x \\ b_2 \mapsto y}}{\longrightarrow} G \longrightarrow 1,$$

where G is isomorphic to the group $\widetilde{C_{2^{n-3}} \times C_2}$ from [15], generated by elements x, y and z such that $x^{2^{n-3}} = y^2 = z^2 = 1$, $yx = xyz$, z is central. Further, put $H = \langle x^2, y, z\rangle \cong C_{2^{n-4}} \times C_2^2$ and let $\mathcal{H} = \langle b_2, \dots, b_6 : b_2^2 = b_3^2 = b_5^2 = b_6^2 = 1, b_4^{2^{n-4}} = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6\rangle$ be the preimage of H in $\mathcal{G}$. Clearly, $\mathcal{H}$ lies in the centralizer of E_4 in $\mathcal{G}$. We have the group extension $1 \to E_4 \to \mathcal{H} \to H \to 1$. Denote by c_1 the 2-coclass in $H^2(G, \mu_2)$ represented by the group extension

$$1 \longrightarrow E_4/\langle b_6\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle b_6\rangle \underset{\substack{\sigma \mapsto x \\ \tau \mapsto y}}{\longrightarrow} G \longrightarrow 1,$$

where $\mathcal{G}/\langle b_6\rangle$ is isomorphic to the group

$$G_{17}' \cong \left\langle \sigma, \tau, \lambda, \rho \,:\, \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = \rho^2 = 1,\ \tau^{-1}\sigma\tau = \sigma\rho,\ \lambda^{-1}\sigma\lambda = \sigma\tau,\ [\tau, \lambda] = [\rho, \sigma] = [\rho, \tau] = [\rho, \lambda] = 1 \right\rangle$$

for $\sigma = b_1$, $\tau = b_3$, $\lambda = b_2$, $\rho = b_5$. Denote by c_2 the 2-coclass in $H^2(H, \mu_2)$ represented by the group extension

$$1 \longrightarrow E_4/\langle b_5\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle b_5\rangle \underset{\substack{b_1 \mapsto x \\ b_2 \mapsto y}}{\longrightarrow} H \longrightarrow 1,$$

where $\mathcal{H}/\langle b_5\rangle \cong \widetilde{C_{2^{n-4}} \times C_2} \times C_2$. From Theorem 3.8 we have that $c_1 = \mathrm{cor}_{G/H}(c_2)$. Furthermore, any G-extension L'/F must contain a $D \curlywedge C$ extension L/F, since $G/\langle\sigma^4\rangle \cong D \curlywedge C$.

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

$$\left(L'/K,\, \mathcal{H}/\langle b_5\rangle \cong \widetilde{C_{2^{n-4}} \times C_2} \times C_2,\, \mu_2\right)$$

is equal to the obstruction to $(L/K, D_8 \times C_2, \mu_2)$, which we know is $\left(2r\left(\alpha_1 - \sqrt{a}\right), 2s\left(\beta_1 + \sqrt{a}\right)\right)_K \in \mathrm{Br}_2(K)$. Hence the obstruction to the embedding problem related to c_1 is exactly the same as for the embedding problem $\left(L/F, G_{(32,6)}, \mu_2\right)$.

Finally, note that we have $G_{17}'/\langle\rho\rangle \cong G_{17}/\left\langle \sigma^{2^{n-3}}\right\rangle$ and $G_{17} \cong G_{17}'^{(2^{n-2},\sigma)}$.

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

Observe first that $G_{14} = G_{13}^{(4,\lambda)}$. Therefore, we will focus on G_{13}.

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

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

$$1 \longrightarrow E_4/\langle\rho\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle\rho\rangle \cong G_{13} \underset{\substack{\sigma \mapsto \sigma \\ \tau \mapsto \tau}}{\longrightarrow} G \cong D_{2^{n-1}} \longrightarrow 1$$

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

$$1 \longrightarrow E_4/\langle\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\tau\rangle \underset{\substack{\lambda \mapsto \lambda \\ \rho \mapsto \rho}}{\longrightarrow} H \cong D_{2^{n-2}} \longrightarrow 1,$$

where $\mathcal{H}/\langle\tau\rangle$ is generated by elements σ^2, λ, ρ such that $(\sigma^2)^{2^{n-3}} = \lambda^2 = \rho^2 = 1$, $\lambda^{-1}\sigma^2\lambda = \sigma^{-2}\rho$, ρ is central. Therefore, $\mathcal{H}/\langle\tau\rangle$ is isomorphic to the group G_{13} of order 2^{n-1}. From Theorem 3.8 we have that $c_1 = \operatorname{cor}_{G/H}(c_2)$. Since the corestriction map is transitive, by induction we obtain that $c_1 = \operatorname{cor}_{G/H_0}(c_0)$, where c_0 is the 2-coclass in $H^2(D_8, \mu_2)$, represented by the group extension

$$1 \longrightarrow \mu_2 \longrightarrow D \curlywedge C \longrightarrow H_0 \cong D_8 \longrightarrow 1.$$

The obstruction to the embedding problem given by c_0 and a D_8 extension containing $K\big(\sqrt{a_1'}, \sqrt{a_2'}\big)/K$ is $(a_1', -1) \in \operatorname{Br}_2(K)$. Applying to each step the projection formula and [2, (2.22)] we obtain that $(a_1, -1)$ is the obstruction to the embedding problem given by c_1 and a $D_{2^{n-1}}$ extension, where $F\big(\sqrt{a_1}, \sqrt{a_2}\big)/F$ 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 four of the groups 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 $M_{2^{n-1}} \times C_2 \cong \big\langle \sigma, \tau, \rho : \sigma^{2^{n-2}} = \tau^2 = 1,\ \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}},\ \rho\sigma = \sigma\rho,\ \rho\tau = \tau\rho \big\rangle$. Then $\big(M_{2^{n-1}} \times C_2\big)/\langle\rho\rangle \cong G_1/\langle\tau^2\rangle \cong M_{2^{n-1}}$ and it is easy to see that $G_1 = \big(M_{2^{n-1}} \times C_2\big)^{(4,\tau)}$. Similarly, we have $G_6 = \big(D_{2^{n-1}} \times C_2\big)^{(4,\tau)}$, $G_7 = \big(SD_{2^{n-1}} \times C_2\big)^{(4,\tau)}$, $G_8 = \big(Q_{2^{n-1}} \times C_2\big)^{(4,\tau)}$.

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

$$\begin{aligned}
G_4/\big\langle\sigma^{2^{n-3}}\big\rangle &\cong C_{2^{n-3}} \times C_2^2 = \big\langle \sigma, \tau, \lambda : \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = 1,\ \sigma\tau = \tau\sigma,\ \sigma\lambda = \lambda\sigma,\ \tau\lambda = \lambda\tau \big\rangle;\\
G_5/\langle\tau\rangle &\cong C_{2^{n-2}} \times C_2 = \big\langle \sigma, \lambda : \sigma^{2^{n-2}} = \lambda^2 = 1,\ \sigma\lambda = \lambda\sigma \big\rangle;\\
G_9/\big\langle\tau^2\big\rangle &\cong C_{2^{n-2}} \times C_2 = \big\langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^2 = 1,\ \sigma\tau = \tau\sigma \big\rangle;\\
G_{12}/\big\langle\sigma^{2^{n-3}}\big\rangle &\cong G_{15}/\big\langle\sigma^{2^{n-3}}\big\rangle \cong G_{16}/\big\langle\sigma^{2^{n-3}}\big\rangle\\
&\cong D_{2^{n-2}} \times C_2 = \big\langle \sigma, \tau, \lambda : \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = 1,\ \sigma\tau = \tau\sigma,\ \lambda^{-1}\sigma\lambda = \sigma^{-1},\ \tau\lambda = \lambda\tau \big\rangle.
\end{aligned}$$

We will assume henceforth that the base field F contains a primitive 2^{n-3}th root of unity ζ. From [2, (7.10)] it follows that the obstruction to the embedding of a cyclic extension of degree 2^{n-3}, containing the quadratic extension $F(\sqrt{a_1})$, in a cyclic extension of degree 2^{n-2} is $(a_1, \zeta) \in \operatorname{Br}_2(F)$; the obstruction to the embedding of a dihedral extension of degree 2^{n-2}, containing the biquadratic extension $F\big(\sqrt{a_1}, \sqrt{a_2}\big)$, in a dihedral extension of degree 2^{n-1} is $(a, a_1)(a_2, \zeta) \in \operatorname{Br}_2(F)$ for some $a \in F$ described in [2, Example 5, (2.22)].

We can apply now Theorem 2.3 in order to obtain the obstructions to realisability 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 $1 \to \mu_2 \to G_i \to G \to 1$, 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 $\operatorname{Br}_2(F)$ for $n \geq 5$, since we assumed that $\zeta = \zeta_{2^{n-3}} \in F$. 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_{26} is isomorphic to $G_{(32,8)}$. Here C_4 is always realizable, so we must add only the obstruction to the realizability of $D \curlywedge C$.

Acknowledgements

This work is partially supported by project No RD-05-342/12.03.2010 of Shumen University.

Table 1. The obstructions when $\zeta = \zeta_{2^{n-3}} \in F$

Group	Obstructions
G_1	$(a_2,-1)$, $(\zeta^{-1}a_2,a_1)$
G_4	$(a_1,\zeta)(a_2,a_3)$
G_5	(a_1,a_2), (a_1,ζ)
G_6	$(a_2,-1)$, $(a,a_1)(a_2,\zeta)$
G_7	$(a_2,-1)$, $(a,a_1)(a_2,\zeta)$
G_8	$(a_2,-1)$, $(a,a_1)(a_2,\zeta)$
G_9	(a_1,a_2), (a_1,ζ)
G_{12}	$(a,a_1)(a_2,\zeta)(a_2,a_3)$
G_{13}	$(a_1,-1)$, $(a,a_1)(a_2,\zeta)$
G_{14}	$(a_1,-1)$, $(a,a_1)(a_2,\zeta)$
G_{15}	$(a,a_1)(a_2,\zeta)(a_1,a_3)$
G_{16}	$(a,a_1)(a_2,\zeta)(a_2a_1,a_3)$
G_{17}	$(a_1,ds\zeta)(a_2,dr)$
G_{26}	$(a_1,2ds)(a_2,dr)$, (a_1,a_2)

References

[1] Bechtell H., The Theory of Groups, Addison–Wesley, Reading–London–Don Mills, 1971
[2] Fröhlich A., Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants, J. Reine Angew. Math., 1985, 360, 84–123
[3] Grundman H.G., Smith T.L., Realizability and automatic realizability of Galois groups of order 32, Cent. Eur. J. Math., 2010, 8(2), 244–260
[4] Grundman H.G., Smith T.L., Galois realizability of groups of order 64, Cent. Eur. J. Math., 2010, 8(5), 846–854
[5] Ishkhanov V.V., Lur'e B.B., Faddeev D.K., The Embedding Problem in Galois Theory, Transl. Math. Monogr., 165, American Mathematical Society, Providence, 1997
[6] Jacobson N., Basic Algebra II, 2nd ed., W.H. Freeman and Company, New York, 1989
[7] Kiming I., Explicit classifications of some 2-extensions of a field of characteristic different from 2, Canad. J. Math., 1990, 42(5), 825–855
[8] Ledet A., On 2-groups as Galois groups, Canad. J. Math., 1995, 47(6), 1253–1273
[9] Ledet A., Embedding problems with cyclic kernel of order 4, Israel J. Math., 1998, 106(1), 109–131
[10] Ledet A., Brauer Type Embedding Problems, Fields Inst. Monogr., 21, American Mathematical Society, Providence, 2005
[11] Michailov I.M., Embedding obstructions for the dihedral, semidihedral, and quaternion 2-groups, J. Algebra, 2001, 245(1), 355–369
[12] Michailov I.M., Embedding obstructions for the cyclic and modular 2-groups, Math. Balkanica (N.S.), 2007, 21(1-2), 31–50
[13] Michailov I.M., Four non-abelian groups of order p^4 as Galois groups, J. Algebra, 2007, 307(1), 287–299
[14] Michailov I.M., Groups of order 32 as Galois groups, Serdica Math. J., 2007, 33(1), 1–34
[15] Michailov I.M., Induced orthogonal representations of Galois groups, J. Algebra, 2009, 322(10), 3713–3732
[16] Michailov I.M., Ziapkov N.P., Embedding obstructions for the generalized quaternion group, J. Algebra, 2000, 226(1), 375–389
[17] Ninomiya Y., Finite p-groups with cyclic subgroups of index p^2, Math. J. Okayama Univ., 1994, 36, 1–21
[18] Riehm C., The corestriction of algebraic structures, Invent. Math., 1970, 11(1), 73–98
[19] Scharlau W., Quadratic and Hermitian Forms, Grundlehren Math. Wiss., 270, Springer, Berlin, 1985
[20] Serre J.-P., Cohomologie Galoisienne, Lecture Notes in Math., 5, Springer, Berlin–Heidelberg–New York, 1964
[21] Serre J.-P., Corps Locaux, 2nd ed., Publications de l'Université de Nancago, 8, Hermann, Paris, 1968

[22] Swallow J.R., Thiem F.N., Quadratic corestriction, C_2-embedding problems, and explicit construction, Comm. Algebra, 2002, 30(7), 3227–3258
[23] Tignol J.-P., On the corestriction of central simple algebras, Math. Z., 1987, 194(2), 267–274
[24] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10, 2007, http://www.gap-system.org