Journal of Algebra 322 (2009) 3713–3732

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Induced orthogonal representations of Galois groups ☆

Ivo M. Michailov

Faculty of Mathematics and Informatics, Constantin Preslavski University, Universitetska str. 115, 9700 Shoumen, Bulgaria

ARTICLE INFO

Article history:
Received 9 January 2009
Available online 28 August 2009
Communicated by Eva Bayer-Fluckiger

Keywords:
Clifford algebra
Embedding problem
Galois
Kummer
Corestriction
Orthogonal representation
Spinor
Modular group
Dihedral group

ABSTRACT

We prove a result showing the connection between induced orthogonal representations and corestrictions of group extensions derived from their Clifford groups. By the means of the corestriction map we then obtain new obstructions to the μ_p-embedding problems given by the group extensions of the modular p-group, and to one μ_2-embedding problem given by a group extension of the dihedral group.

1. Introduction

In this paper we give new insights into the Galois cohomology structure of induced orthogonal representations of finite groups. These results are then extended to provide us with the ability to find new necessary and sufficient conditions for the realizability of certain series of finite groups as Galois groups.

The main tool in Galois realizability issues is the Galois embedding problem. Recall its definition. Let E/F be a Galois extension with Galois group H and let

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

☆ This work is partially supported by project No. RD-05-287/11.03.2009 of Shumen University.
E-mail address: ivo_michailov@yahoo.com.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.07.035

be a short exact sequence. The *embedding problem* related to E/F and (1.1) then consists in determining whether there exists a Galois extension (called also a *proper* solution) L, such that E is contained in L, G is isomorphic to $\mathrm{Gal}(L/F)$, and the homomorphism of restriction of L on E coincides with π. The group A we call the *kernel* of the embedding problem.

Throughout this work we assume that F is arbitrary field of characteristic not p, containing the full group of pth roots of unity $\mu_p = \langle\zeta\rangle$, where ζ is a fixed primitive pth root of unity. When $p = 2$, the 2nd root of unity -1 is, of course, always in F.

Especially important for our purposes are central embedding problems with kernel $C_p \cong \mu_p$ (called μ_p-embedding problems for short). In this way, the realizability of a given group is determined by the splitting of an element in the Brauer group $\mathrm{Br}_p(F)$, called *the obstruction*, which is the crossed product algebra related to the embedding problem with kernel μ_p. From the well-known Merkurjev–Suslin Theorem [MeS], follows that the obstruction is equal to a product of classes of p-cyclic algebras. The actual computation of these p-cyclic algebras for a given embedding problem, however, is not a trivial task.

We denote by $(a, b; \zeta)$ the equivalence class of the p-cyclic algebra which is generated by i_1 and i_2, such that $i_1^p = b$, $i_2^p = a$ and $i_1 i_2 = \zeta i_2 i_1$. For $p = 2$ we have the quaternion class $(a, b; -1)$, commonly denoted by (a, b).

Given a 2-cocycle $f \in Z^2(H, \mu_p)$ and a Galois extension L/F with Galois group H, we denote by $[L, H, f]$ the equivalence class of the crossed product algebra (L, H, f). Recall that (L, H, f) is a c.s. F-algebra, generated by L and elements u_σ for $\sigma \in H$, 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 $\sigma, \tau \in H$ and $x \in L$.

The following Theorem gives us a formula for the obstruction of an embedding problem related to a group extension of a group having a direct factor the cyclic group of order p.

Theorem 1.1. *(See [Mi1, Th. 2.1], [Mi2, Th. 4.1].) Let $\mathcal{H}$ be a p-group and let*

$$1 \to \mu_p \cong \langle\zeta\rangle \to \mathcal{G} \underset{\pi}{\to} \mathcal{H} \times C_p \to 1 \tag{1.2}$$

be a non-split central group extension with characteristic 2-coclass $\gamma \in H^2(\mathcal{H} \times C_p, \mu_p)$. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a minimal generating set for the maximal elementary abelian factor group of $\mathcal{H}$; and let τ be the generator of the direct factor C_p. Finally, let $s_1, s_2, \ldots, s_m, t \in \mathcal{G}$ 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 $i \in \{1, 2, \ldots, m\}$; $j, d_i \in \{0, 1, \ldots, p-1\}$.

Let K/F be a Galois extension with Galois group $\mathcal{H}$ and let $L/F = K(\sqrt[p]{b})/F$ be a Galois extension with Galois group $\mathcal{H} \times C_p$ ($b \in F^\times \setminus F^{\times p}$). Choose $a_1, a_2, \ldots, a_m \in F^\times$ 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

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

There are too many groups, however, which do not fit in the conditions of the latter result, so more criteria are needed.

Section 2 is devoted to the corestriction homomorphism (see [Br,Ri,Se1] for various definitions of this map), which appears to be one of the strongest tools in such situations. In [ST] and [Mi3] the reader can find applications of the quadratic corestriction for small 2-groups. The main result of our paper is Theorem 2.2, where we show explicitly the connection between the induced orthogonal representations and the corestriction maps.

In [Ri] is given an analogue of the corestriction homomorphism, acting on central simple algebras. Given a Galois extension K_1/F of degree p, we have the corestriction homomorhpism between the Brauer groups $\mathrm{cor}_{K_1/F} : \mathrm{Br}(K_1) \to \mathrm{Br}(F)$. Further, we denote by Ω_F the Galois group of the separable closure of F over the field F, and by Ω_{K_1} the subgroup of Ω_F, leaving K_1 fixed. Then we also have the corestriction $\mathrm{cor}_{\Omega_F/\Omega_{K_1}} : H^2(\Omega_{K_1}, \mu_p) \to H^2(\Omega_F, \mu_p)$. Riehm shows in [Ri, Th. 11] that the following commutative diagram holds:

$$\begin{array}{ccc} H^2(\Omega_{K_1}, \mu_p) & = & \mathrm{Br}_p(K_1) \\ \downarrow{\scriptstyle \mathrm{cor}_{\Omega_F/\Omega_{K_1}}} & & \downarrow{\scriptstyle \mathrm{cor}_{K_1/F}} \\ H^2(\Omega_F, \mu_p) & = & \mathrm{Br}_p(F) \end{array}$$

Tignol, in this context, gives in [Ti] a detailed proof of the so-called *projection formula*, which we will also need in our work: for $b \in F^\times \setminus F^{\times p}$ and $\delta \in K_1$ we have $\mathrm{cor}_{K_1/F}(\delta, b; \zeta)_{K_1} = (N_{K_1/F}(\delta), b; \zeta)_F$.

The remaining of this paper is organized as follows. In Section 3 we describe explicitly the modular p-extensions. We denote the modular p-group of order p^n by $M(p^n)$, for $n \geqslant 3$. It is generated by two elements α and β, such that $\alpha^{p^{n-1}} = \beta^p = 1$ and $\beta\alpha = \alpha^{1+p^{n-2}}\beta$, see for example [Ha, Th. 12.5.1]. Because of the frequent use of the prime power p^{n-2} in our work, we put $q = p^{n-2}$. The modular group $M(2^n)$ is one of the four non-abelian groups of order 2^n that have a cyclic subgroup of index 2, for $n \geqslant 4$. When p is odd, the modular group $M(p^n)$ is the only non-abelian group of order p^n that has a cyclic subgroup of index p, for $n \geqslant 3$. Note that the group $C_q \times C_p = \langle \alpha^p, \beta \rangle$ is an index p subgroup of the modular group $M(p^n)$. In Proposition 3.5 we obtain a group, which is generated by three elements σ_1, τ_1 and ρ_1, such that $|\sigma_1| = pq$, $\tau_1^p = \rho_1^p = 1$, $\tau_1\sigma_1 = \sigma_1^{q+1}\tau_1\rho_1$ and ρ_1 is central. We denote it by $\widetilde{M}(p^{n+1})$. Set $N_1 = \langle \sigma_1^p \rangle$, $N_2 = \langle \rho_1 \rangle$. Then N_1 and N_2 are normal in $\widetilde{M}(p^{n+1})$ and $N_1 \cap N_2 = \{1\}$. The quotient group $\widetilde{M}(p^{n+1})/N_1$ is isomorphic to the Heisenberg group H_{p^3}, for $p \neq 2$, and to the dihedral group D_8 of order 8, for $p = 2$. The quotient group $\widetilde{M}(p^{n+1})/N_2$ is isomorphic to the modular group $M(p^n)$. The group $\widetilde{M}(p^{n+1})$ then is isomorphic to the direct product of the groups $\widetilde{M}(p^{n+1})/N_1$ and $\widetilde{M}(p^{n+1})/N_2$ with amalgamated quotient group $\widetilde{M}(p^{n+1})/N_1N_2 \cong (C_p)^2$.

In Section 4 we begin with a description of the restriction $\mathrm{res} : H^2(S_d, \mu_2) \to H^2(G, \mu_2)$, for some 2-groups G which are embedded transitively into the symmetric group S_d of degree $d = 2^l \geqslant 4$. After, we describe the cohomology groups $H^2(C_q \times C_p, \mu_p)$, $H^2(M(p^n), \mu_p)$ and the corestriction map

$$\mathrm{cor}_{M(p^n)/C_q \times C_p} : H^2(C_q \times C_p, \mu_p) \to H^2\big(M\big(p^n\big), \mu_p\big).$$

Since Theorem 1.1 gives us the obstructions to the embedding problems related to the group extensions from $H^2(C_q \times C_p, \mu_p)$, we can apply the corestriction map so that we obtain the obstructions to the embedding problems related to the group extensions from $H^2(M(p^n), \mu_p)$.

In Section 5 we investigate one induced special orthogonal representation of the dihedral group of order $4n$ over a field F with $char(F) \neq 2$ and containing a primitive nth root of unity for n-even.

2. The corestriction homomorphism

Let G be a finite group, and let H be a proper subgroup of G. We decompose G into the cosets ρ with respect to H: $G = \bigcup_\rho \rho = \bigcup_\rho H\bar{\rho}$ with a given right transversal $R = \{\bar{\rho}\}$. Let A be a trivial H-module and choose a 2-cocycle $\bar{f} \in Z^2(H, A)$, corresponding to some exact sequence

$$1 \to A \to G_0 \underset{\varphi}{\to} H \to 1.$$

Tate gives in [Ta] an explicit formula for the corestriction homomorphism, which we display in the following

Theorem 2.1. *In the above notations, the corestriction homomorphism* $\mathrm{cor}_{G/H} : H^2(H, A) \to H^2(G, A)$ *is given by the following explicit formula*:

$$\mathrm{cor}_{G/H}\bar{f}(g_1, g_2) = \prod_{\bar{\rho} \in R} \bar{f}\big(r_0 g_1 r_1^{-1}, r_1 g_2 r_2^{-1}\big),$$

where r_0, r_1 *and* r_2 *are defined in this way*: $r_0 = \bar{\rho}$, $r_1 \in Hr_0g_1$ *and* $r_2 \in Hr_1g_2$.

We continue with some preliminaries about orthogonal representations. Let F be a field of characteristic $\neq 2$, let V be a finite-dimensional F-vector space, and let (V,q) be a quadratic space, q being a quadratic form. The isometries $(V,q)\mapsto(V,q)$ constitute a subgroup $O(q)$ of $\mathrm{GL}_F(V)$, called *the orthogonal group* of q. *An orthogonal representation* of a finite group G is then a homomorphism $\mu: G\to O(q)$ of G into the orthogonal group of some regular quadratic form q. From now on, by an orthogonal representation we will mean a *faithful* one, i.e., an embedding $\mu: G\hookrightarrow O(q)$.

Now, let L/F be a finite Galois extension with Galois group G, let H be a subgroup of G with fixed field $K=L^H$, and let $\mu: H\hookrightarrow O(q)$ be an orthogonal representation over F. Then, according to [Fr,FM], we can construct an *induced orthogonal representation* $\mathrm{ind}\mu: G\hookrightarrow O(q_{\mathrm{ind}\mu})$, where $\mathrm{ind}\mu$ has as underlying module the induced G-module of the H-module $V_q: V_{\mathrm{ind}\mu}=\bigoplus(V_q\otimes\sigma)=V_q\otimes_{FH}FG$, σ running over a given right transversal R of H in G. Note that $V_q\subset V_{\mathrm{ind}\mu}$ is a subspace which is H-invariant. It is not hard to show that, given an orthogonal representation $\mu: H\hookrightarrow O(q)$, such $V_{\mathrm{ind}\mu}$ exists and is unique up to an isomorphism (see e.g. [FH, §3.3]). Moreover, the action of G can be explicitly determined: Each element $v\in V_{\mathrm{ind}\mu}$ has a unique expression $v=\sum w_\sigma\otimes\sigma$ for elements w_σ in V_q. For a given $g\in G$, we must have

$$g\cdot(w_\sigma\otimes\sigma)=hw_\sigma\otimes\tau\quad\text{if } g\sigma=\tau h\ (\tau\in R). \tag{2.1}$$

We adopt the notations about Clifford algebras used in [Le, Ch. 5, §2]: $C(q)$ is the Clifford algebra of q; $C_0(q)$ is the even Clifford algebra; $C(q)=C_0(q)\oplus C_1(q)$; if $x\in C_i(q)$, we write $\partial x=i$; $C^\times(q)$ is the Clifford group, defined as the subgroup of $C(q)^\times$, consisting of those invertible elements x, for which $xVx^{-1}=V$. The anisotropic vectors of V are in $C^\times(q)$ and $vuv^{-1}=-T_v(u)$ for $u,v\in V$, where v is anisotropic and T_v is the reflection on the hyperplane $v^\perp$. There is an exact sequence

$$1\to F^\times\to C^\times(q)\xrightarrow{\ r\ } O(q)\to 1,$$

r being a map defined by $r_x: u\mapsto(-1)^{\partial x}xux^{-1}$, where $x\in C^\times(q)$ and $u\in V$. In particular, for $C_0^\times(q)=C^\times(q)\cap C_0(q)$ we get another exact sequence

$$1\to F^\times\to C_0^\times(q)\xrightarrow{\ r\ } SO(q)\to 1.$$

Denote by ι the principal involution on $C(q)$, which preserves the scalars, sums and vectors, and reverses products. Denote by $N: C^\times(q)\to F^\times$ the norm given by $N(x)=x\iota(x)$, and put $\mathrm{Pin}(q)=\ker(N)$, $\mathrm{Spin}(q)=\mathrm{Pin}(q)\cap C_0^\times(q)$.

Next, assume that we have a special orthogonal representation $\mu: H\hookrightarrow SO(q)$ over F. Denote by $\overline{F}_{sep}$ the separable closure of F, and by $\bar q$ the extension of q to $\overline{F}_{sep}$. Then we have a diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{H} & \longrightarrow & H & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Spin}(\bar q) & \longrightarrow & SO(\bar q) & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{F}_{sep}^\times & \longrightarrow & C_0^\times(\bar q) & \longrightarrow & SO(\bar q) & \longrightarrow & 1,
\end{array}$$

where as usual $\mu_2=\{\pm1\}$ and $1\to\mu_2\to\widetilde{H}\to H\to 1$ is the restriction of $1\to\mu_2\to\mathrm{Spin}(\bar q)\to SO(\bar q)\to 1$. The induced orthogonal representation $\mathrm{ind}\mu: G\hookrightarrow O(q_{\mathrm{ind}\mu})$, in its turn, gives us the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Pin}(\bar{q}_{\mathrm{ind}\mu}) & \longrightarrow & O(\bar{q}_{\mathrm{ind}\mu}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{F}^{\times}_{sep} & \longrightarrow & C^{\times}(\bar{q}_{\mathrm{ind}\mu}) & \longrightarrow & O(\bar{q}_{\mathrm{ind}\mu}) & \longrightarrow & 1.
\end{array}$$

Our main goal is to prove the following

Theorem 2.2. *Let G be a finite group, and let H be a subgroup of G, such that $|H| = 2^t m$, $(t, m \geqslant 1)$. Let also $\mu : H \hookrightarrow SO(q)$ be an orthogonal representation over F with an underlying module V_q, such that $n = \dim_F V_q \equiv 0 \pmod 4$. Denote by $\bar{f} \in Z^2(H, \mu_2)$ and by $f \in Z^2(G, \mu_2)$ the 2-cocycles given by the described above group extensions $1 \to \mu_2 \to \widetilde{H} \to H \to 1$ and $1 \to \mu_2 \to \widetilde{G} \to G \to 1$, respectively. Then $[f] = \mathrm{cor}_{G/H}([\bar{f}])$, where $\mathrm{cor}_{G/H} : H^2(H, \mu_2) \to H^2(G, \mu_2)$ is the corestriction map.*

We need first a cohomological

Lemma 2.3. *Let G be a pro-finite group, let H be a closed subgroup of index 2 in G, let $R = \{1, g\}$ be a right transversal of H in G, i.e., $G = H \cup Hg$, and set $h_0 = g^2$. Let $1 \to \mu_2 \to H_1 \to H \to 1$ be a group extension and choose a pre-image $\bar{u}_h \in H_1$ of each $h \in H$. The system $\{\bar{u}_h\}_{h\in H}$ then defines a 2-cocycle $\bar{f} \in Z^2(H, \mu_2)$ by $\bar{f}(s_1, s_2) = \bar{u}^{-1}_{s_1 s_2} \bar{u}_{s_1} \bar{u}_{s_2}$. Denote by $\delta : H \to \{0, 1\}$ the map, given by $\bar{u}_{h_0} \bar{u}_h \bar{u}^{-1}_{h_0} = (-1)^{\delta(h)} \bar{u}_{h_0 h h_0^{-1}}$. Let also $1 \to \mu_2 \to G_1 \to G \to 1$ be a group extension and choose a pre-image $u_{hg^i} \in G_1$ of each $hg^i \in G$, $i = 0, 1$. The system $\{u_{hg^i}\}$ then defines a 2-cocycle $f \in Z^2(G, \mu_2)$, and if the following three conditions*:

(i) $f(s_1, s_2) = u^{-1}_{s_1 s_2} u_{s_1} u_{s_2} = \bar{f}(s_1, s_2) \bar{f}(g s_1 g^{-1}, g s_2 g^{-1})$, $\forall s_1, s_2 \in H$;
(ii) $u_g u_h u_g^{-1} = (-1)^{\delta(h)} u_{ghg^{-1}}$, $\forall h \in H$; *and*
(iii) $u_g^2 = u_{h_0}$

are fulfilled, then $[f] = \mathrm{cor}_{G/H}([\bar{f}])$.

Proof. Theorem 2.1 implies

$$\big(\mathrm{cor}_{G/H}(\bar{f})\big)(s_1, s_2) = \begin{cases} \bar{f}(s_1, s_2) \bar{f}(g s_1 g^{-1}, g s_2 g^{-1}), & \text{if } (s_1, s_2) \in H \times H, \\ \bar{f}(s_1 g^{-1}, g s_2 g^{-1}) \bar{f}(g s_1, s_2), & \text{if } (s_1, s_2) \in Hg \times H, \\ \bar{f}(s_1, s_2 g^{-1}) \bar{f}(g s_1 g^{-1}, g s_2), & \text{if } (s_1, s_2) \in H \times Hg, \\ \bar{f}(s_1 g^{-1}, g s_2) \bar{f}(g s_1, s_2 g^{-1}), & \text{if } (s_1, s_2) \in Hg \times Hg. \end{cases}$$

Since the choice of u_{gh} for $h \neq 1$ does not impact the conditions (i)–(iii), we may assume that $u_{gh} = u_g u_h \bar{f}(h_0, h)$. Then $f(g, h) = u^{-1}_{gh} u_g u_h = \bar{f}(h_0, h)$, which satisfies the definition of the corestriction map.

Next,

$$u_{hg} = u_{g(g^{-1}hg)} = (-1)^{\delta(g^{-1}hg)} u_h u_g \bar{f}\big(h_0, g^{-1}hg\big),$$

since $u_g^{-1} u_h u_g = (-1)^{\delta(g^{-1}hg)} u_{g^{-1}hg}$. Therefore,

$$f(h, g) = u^{-1}_{hg} u_h u_g = (-1)^{\delta(g^{-1}hg)} \bar{f}\big(h_0, g^{-1}hg\big).$$

Now, from $\bar{u}_{h_0}\bar{u}_h\bar{u}_{h_0}^{-1} = (-1)^{\delta(h)}\bar{u}_{h_0hh_0^{-1}}$ follows that

$$\bar{u}_{h_0}\bar{u}_{g^{-1}hg}\bar{u}_{h_0}^{-1} = (-1)^{\delta(g^{-1}hg)}\bar{u}_{ghg^{-1}},$$

so

$$\bar{f}\big(ghg^{-1}, h_0\big) = \bar{u}_{ghg}^{-1}\bar{u}_{ghg^{-1}}\bar{u}_{h_0} = (-1)^{\delta(g^{-1}hg)}\bar{u}_{ghg}^{-1}\bar{u}_{h_0}\bar{u}_{g^{-1}hg} = (-1)^{\delta(g^{-1}hg)}\bar{f}\big(h_0, g^{-1}hg\big).$$

Therefore, $f(h,g) = \bar{f}(ghg^{-1}, h_0)$, which also satisfies the definition of the corestriction map.

Finally, from (iii) we get $f(g,g) = u_{h_0}^{-1}u_g^2 = 1$, so in order to obtain the remaining properties of the corestriction map, one have to apply only the standard cohomological identity. □

We can proceed now with the

Proof of Theorem 2.2. We will divide the proof into three steps.

(I) Assume that H is an index 2 subgroup of G. Let $R = \{1, g\}$ be a right transversal of H in G, i.e., $G = H \cup Hg$, and set $h_0 = g^2$. Define an F-module V by $V = V_{q_1} \oplus V_{q_2}$, where $q_1 = q_2 = q$ and $V_{q_1} = V_{q_2} = V_q$ as F-modules. Thus we get the quadratic space $(V, q_1 \perp q_2)$. According to (2.1), the induced action of G is given by:

$$h(v_1, v_2) = \big(hv_1, g^{-1}hgv_2\big) \quad \text{and} \quad hg(v_1, v_2) = \big(hh_0v_2, g^{-1}hgv_1\big),$$

for $h \in H$ and $v_i \in V_{q_i}$, $i = 1, 2$.

Next, we can extend the scalars to get a quadratic space $(V_{\bar{F}_{sep}}, \bar{q}_1 \perp \bar{q}_2)$, where $\bar{q}_i$ is the scalar extension of q_i. In this way, the orthogonal representation $\mu : H \hookrightarrow SO(q) \hookrightarrow SO(\bar{q})$ induces the orthogonal representation $\mathrm{ind}\mu : G \hookrightarrow O(q_1 \perp q_2) \hookrightarrow O(\bar{q}_1 \perp \bar{q}_2)$.

Let us now define isometries $h \oplus 1$ and $1 \oplus g^{-1}hg$ in $O(\bar{q}_1 \perp \bar{q}_2)$ by $(h \oplus 1)(v_1, v_2) = (hv_1, v_2)$ and $(1 \oplus g^{-1}hg)(v_1, v_2) = (v_1, g^{-1}hgv_2)$. Whence we get that $h = (h \oplus 1)(1 \oplus g^{-1}hg) \in O(\bar{q}_1 \perp \bar{q}_2)$ for all $h \in H$. Since h is in $SO(\bar{q})$, we can choose and fix a pre-image $u_h \in \mathrm{Spin}(\bar{q}_1) \subset C_0^\times(\bar{q}_1)$ of $h \oplus 1 \in O(\bar{q}_1 \perp \bar{q}_2)$. We may as well choose a pre-image $v_h \in C_0^\times(\bar{q}_2)$ of $1 \oplus g^{-1}hg \in O(\bar{q}_1 \perp \bar{q}_2)$ for all $h \in H$. However, we will fix the choice of v_h's a bit later.

From [Fr, p. 119] we know that for elements $x_i \in C^\times(q_i) \subset C^\times(q_1 \perp q_2)$, $i = 1, 2$, we have the commutation rule $x_1x_2 = (-1)^{\partial x_1 \partial x_2}x_2x_1$, and this determines the subgroup of $C^\times(q_1 \perp q_2)$ generated by $C^\times(q_i)$, $i = 1, 2$. Since in our case $\partial u_h = \partial v_h = 0$, we have that $u_{h_1}v_{h_2} = v_{h_2}u_{h_1}$, $\forall h_1, h_2 \in H$. Further, from the equations $g(h \oplus 1)(v_1, v_2) = (h_0v_2, hv_1) = (1 \oplus ghg^{-1})g(v_1, v_2)$, we get $g(h \oplus 1)g^{-1} = 1 \oplus ghg^{-1}$, so if we pick a pre-image $w_g \in \mathrm{Pin}(\bar{q}_1 \perp \bar{q}_2)$ of g, we obtain that $w_gu_hw_g^{-1} = \pm v_{ghg^{-1}}$. Clearly, we can assume that $u_{h_0}u_hu_{h_0}^{-1} = (-1)^{\delta(h)}u_{h_0hh_0^{-1}}$ for some map $\delta : H \to \{0, 1\}$. Now, set

$$v_{ghg^{-1}} = (-1)^{\delta(h)}w_gu_hw_g^{-1} \quad \text{and} \quad w_h = u_hv_h.$$

Then $w_g^2 = \pm u_{h_0}$ and $v_h = w_g^{-1}u_{ghg^{-1}}w_g$. Since the pre-images $\{u_h\}_{h\in H}$ determine the 2-cocycle $\bar{f} \in Z^2(H, \mu_2)$, given in the statement, we get

$$f(h_1, h_2) = w_{h_1h_2}^{-1}w_{h_1}w_{h_2} = \bar{f}(h_1, h_2)\bar{f}\big(gh_1g^{-1}, gh_2g^{-1}\big), \quad \forall h_1, h_2 \in H.$$

Thus the condition (i) from Lemma 2.3 is satisfied. The condition (ii) is also satisfied, as is seen from

$$w_gw_hw_g^{-1} = w_gu_hw_g^{-1}w_gv_hw_g^{-1} = (-1)^{\delta(h)}v_{ghg^{-1}}u_{ghg^{-1}} = (-1)^{\delta(h)}w_{ghg^{-1}}.$$

So, it remains only to verify that $w_g^2 = w_{h_0}$. Assume that $e_1, \ldots, e_n$ is an orthogonal basis of $V_{\bar{q}}$ over $\overline{F}_{sep}$, where $n = \dim_F V_q = \dim_{\overline{F}_{sep}} V_{\bar{q}}$. Clearly, the vectors $e'_1 = (e_1, 0)$, $\ldots$, $e'_n = (e_n, 0)$, $e'_{n+1} = (0, e_1)$, $\ldots$, $e'_{2n} = (0, e_n)$ form an orthogonal basis of $V_{\overline{F}_{sep}} = V_{\bar{q}_1} \oplus V_{\bar{q}_2}$ over $\overline{F}_{sep}$. Notice that $\bar{q}_1(e'_i) = \bar{q}_2(e'_{n+i}) = q(e_i) = a_i \in F^\times$ for $i = 1, \ldots, n$. It is not hard to check that the reflection $T_{(e'_i - e'_{n+i})/\sqrt{a_i}}$ interchanges e'_i and e'_{n+i}, leaving the other e'_k's invariant. As a pre-image of $T_{(e'_i - e'_{n+i})/\sqrt{a_i}}$ in $\mathrm{Pin}(\bar{q}_1 \perp \bar{q}_2)$ we can pick $x_i = (e'_i - e'_{n+i})/\sqrt{2a_i}$, $i = 1, \ldots, n$. Then $x_i^2 = 1$, $x_i x_j = -x_j x_i$ and $(x_i x_j)^2 = -1$, if $i \neq j$. Next, define an isometry $\varphi \in O(\bar{q}_1 \perp \bar{q}_2)$ by $\varphi(v_1, v_2) = (v_2, v_1)$ for $v_i \in V_{\bar{q}_i}$. φ can also be written as a product of reflections:

$$\varphi = T_{(e'_1 - e'_{n+1})/\sqrt{a_1}} T_{(e'_2 - e'_{n+2})/\sqrt{a_2}} \cdots T_{(e'_n - e'_{2n})/\sqrt{a_n}},$$

so we can pick a pre-image $x = x_1 x_2 \cdots x_n \in \mathrm{Pin}(\bar{q}_1 \perp \bar{q}_2)$ of φ. Since $n \equiv 0 \pmod 4$ and $(x_i x_j x_k x_l)^2 = 1$, for four different indices $i, j, k, l \leqslant n$, we get $x^2 = 1$. On the other hand, from the equation $(h_0^{-1} \oplus 1)g(v_1, v_2) = (v_2, v_1)$ follows that $\varphi = (h_0^{-1} \oplus 1)g$. Then $u_{h_0}^{-1} w_g$ is a pre-image of φ in $\mathrm{Pin}(\bar{q}_1 \perp \bar{q}_2)$, so $u_{h_0}^{-1} w_g = \pm x$ has order 2. Therefore, $w_g^2 = u_{h_0} w_g^{-1} u_{h_0} w_g = u_{h_0} v_{h_0} = w_{h_0}$, and we are done.

(II) Assume that G is a 2-group. This step follows from (I) and the transitivity of both the induced orthogonal representations and the corestriction homomorphism.

(III) The general case: $|H| = 2^t m$, $(t, m \geqslant 1)$. Let $\mathcal{H}$ be a Sylow 2-subgroup of H, and pick as well a Sylow 2-subgroup $\mathcal{G}$ of G. Then we have the group extensions:

$$\bar{f} : 1 \to \mu_2 \to \widetilde{H} \to H \to 1, \qquad \bar{f}_1 : 1 \to \mu_2 \to \widetilde{\mathcal{H}} \to \mathcal{H} \to 1,$$
$$f : 1 \to \mu_2 \to \widetilde{G} \to G \to 1, \qquad f_1 : 1 \to \mu_2 \to \widetilde{\mathcal{G}} \to \mathcal{G} \to 1,$$

where $[\bar{f}_1] = \mathrm{res}_{H/\mathcal{H}}([\bar{f}])$ and $[f_1] = \mathrm{res}_{G/\mathcal{G}}([f])$. According to the previous step, we also have $[f_1] = \mathrm{cor}_{\mathcal{G}/\mathcal{H}}([\bar{f}_1])$. The commutative diagram:

$$\begin{array}{ccc} H^2(H, \mu_2) & \xrightarrow{\mathrm{cor}} & H^2(G, \mu_2) \\ \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\ H^2(\mathcal{H}, \mu_2) & \xrightarrow{\mathrm{cor}} & H^2(\mathcal{G}, \mu_2) \end{array}$$

then yields $\mathrm{cor}_{\mathcal{G}/\mathcal{H}} \cdot \mathrm{res}_{H/\mathcal{H}}([\bar{f}]) = [f_1] = \mathrm{res}_{G/\mathcal{G}} \cdot \mathrm{cor}_{G/H}([\bar{f}]) = \mathrm{res}_{G/\mathcal{G}}([f])$, and taking into account that the vertical restriction maps are injective (see [Se1, §2.4]), we obtain what is desired. □

Now, assume again that L/F is a normal and separable extension with a finite Galois group G. We can always find a primitive element θ such that $L = F(\theta)$. Let $f(x) \in F[x]$ be the minimal polynomial of θ of degree $n = [L : F]$, and let $\theta = \theta_1, \theta_2, \ldots, \theta_n$ be the conjugates of θ. Then $G = G(f)$ embeds transitively into the symmetric group S_n.

For a given proper subgroup H of G, we set $m = |H|$ and $k = (G : H) = n/m$. Clearly, θ is a primitive element of the extension L/K as well, where $K = L^H$. Since the minimal polynomial of θ over K divides $f(x)$, we can assume that $\theta = \theta_1, \theta_2, \ldots, \theta_m$ for $1 < m = [L : K] < n$ are the conjugates of θ over K. H embeds transitively in S_m, so we can take the group extension

$$1 \to \mu_2 \to \widetilde{H} \to H \to 1, \tag{2.2}$$

which is the restriction of the group extension

$$1 \to \mu_2 \to \widetilde{S}_m \to S_m \to 1,$$

$\widetilde{S}_m$ being the positive double cover of S_m.

Next, recall that for the quadratic form $q_1 = \langle 1, \dots, 1\rangle$ on $V_1 = F^m$ we have that S_m embeds in $O_m(F) = O(q_1)$, so we get an orthogonal representation $H \hookrightarrow O_m(F)$. Set $q = q_1 \perp q_2 \perp \cdots \perp q_k$ and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, where $q_1 = q_2 = \cdots = q_k$ and $V_1 = V_2 = \cdots V_k$. In this way, we get the induced orthogonal representation $G \hookrightarrow O_n(F)$, which is identical to the transitive embedding of $G = G(f)$ in S_n. Now, take the group extension

$$1 \to \mu_2 \to \widetilde{G} \to G \to 1, \tag{2.3}$$

which is the restriction of the group extension

$$1 \to \mu_2 \to \widetilde{S}_n \to S_n \to 1.$$

Denote by $\bar{f} \in Z^2(H, \mu_2)$ the 2-cocycle representing (2.2) and by $f \in Z^2(G, \mu_2)$ the 2-cocycle representing (2.3), i.e., $\bar{f} = \mathrm{res}(s_m)$ and $f = \mathrm{res}(s_n)$. From Theorem 2.2 now follows that $[f] = \mathrm{cor}_{G/H}([\bar{f}])$, under the extra assumptions $H \hookrightarrow SO_m(F)$ and $m \equiv 0 \pmod 4$.

Remark. The type of transitive embedding we talk about is a special case of the embedding described in [Le, Ch. 6, §2] and [Se2, p. 653], where is taken an element θ which is not necessarily primitive. So, when θ is not primitive, i.e., $l = \deg\theta < n$, one can obtain a transitive embedding of G in S_l. In Example 4.1 we will illustrate the difference between the group extensions obtained by the two types of transitive embeddings of the modular 2-group.

3. $M(p^n)$ extensions

The description of Galois extensions is an essential part of the obstruction theory. On one hand, the precise calculation of an obstruction often leads to a set of solutions of an embedding problem. On the other hand, the knowledge of all Galois extensions that realize given group might enable us to go deeper into Galois cohomology issues and to calculate new obstructions, in particular.

In this Section, we are going to describe explicitly, to some extent, the modular p-extensions. The results presented here can be established in two ways: by basic Kummer theory following [Wa], or by 'higher' Kummer theory developed in the works [MS1,MS2,MSS1,MSS2]. We will sketch most of the proofs, using the results of Mináč, Schultz and Swallow.

Firstly, introduce some notation. Let $K_1 = F(\sqrt[p]{a_1})$ for $a_1 \in F^\times \setminus F^{\times p}$, and let K/F be a cyclic $C_q = \langle\sigma\rangle$ extension, such that $K_1 \subset K$.

For the group ring $\mathbb{F}_p[C_q]$ there exist precisely q non-zero ring quotients, namely $M_j = \mathbb{F}_p[C_q]/\langle(\sigma-1)^j\rangle$ for $j = 1, 2, \dots, q$. Each M_j is a C_q module, since the multiplication in $\mathbb{F}_p[C_q]$ induces an $\mathbb{F}_p[C_q]$-action on M_j. Further, let $J = K^\times/K^{\times p}$ be the $\mathbb{F}_p[C_q]$ module of pth-power classes. We write the elements of J as $[\gamma]$, $\gamma \in K^\times$. The socle series of J is defined by $J_1 = J^{C_q}$—the fixed submodule of J and $J_i/J_{i-1} = (J/J_{i-1})^{C_q}$ for $i > 1$. We have that $J_i = \ker(\sigma-1)^i$, where $(\sigma-1)^i$ is considered as an endomorphism of J. By [Wa] we have a Kummer correspondence over K of finite subspaces of J and finite abelian exponent p extensions of K.

Since α^q is central and $\alpha^{-1}\beta\alpha = \alpha^q\beta$, the subgroup generated by α^q and β is normal in $M(p^n)$. Thus we have the group extension:

$$1 \to C_p \times C_p \cong \langle\alpha^q, \beta\rangle \to M(p^n) \underset{\alpha\mapsto\sigma}{\longrightarrow} C_q \to 1. \tag{3.1}$$

Our initial objective is to describe the solutions to the embedding problem given by K/F and (3.1).

Proposition 3.1. *Let L/K be a Galois extension with Galois group isomorphic to $C_p \times C_p$. Then L/F is a non-abelian Galois extension if, and only if $L = K(b_0^{1/p}, b_1^{1/p})$, where $b_0 \in K^\times \setminus K^{\times p}$, $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$ and $b_2 = \sigma(b_1)/b_1 \in K^{\times p}$. In that case, $G = \mathrm{Gal}(L/F)$ is isomorphic either to $M(p^n)$, or to the semidirect product $C_q \rtimes (C_p)^2$.*

Proof. According to [MSS2], the non-abelian extensions L/F are in a bijective correspondence with the indecomposable dimension 2 submodules of J, and the Galois group $G = \mathrm{Gal}(L/F)$ is isomorphic either to the modular group, or to the semidirect product $C_q \rtimes (C_p)^2$. □

The description of all $M(p^n)$ extensions is now possible, and we make it in the following

Theorem 3.2. *L/F is an $M(p^n)$ Galois extension, solving the embedding problem given by* (3.1)*, if and only if, there exist $b_0 \in K^\times \setminus K^{\times p}$, $f \in F^\times \setminus F^\times \cap K^{\times p}$ and $x \in K^\times$ such that $\sigma(b_0)/b_0 = fx^p$, $L/F = K(\sqrt[p]{b_0}, \sqrt[p]{f})/F$ and $c = f^{q/p} N_{K/F}(x)$ is a pth root of unity, but $c \neq 1$*

Proof. 'Only-if part': Let $L/F = K(b_0^{1/p}, b_1^{1/p})/F$ be an $M(p^n)$ extension, such that $b_0 \in K^\times \setminus K^{\times p}$, $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$ and $\sigma(b_1)/b_1 = d^p$, where $d \in K^\times$. Let $\alpha \in \mathrm{Gal}(L/F)$ be a pre-image of σ. Now, put $\omega_0 = b_0^{1/p}$, $\omega_1 = \alpha(\omega_0)/\omega_0 = b_1^{1/p}$, $\omega_2 = \alpha(\omega_1)/\omega_1 = d$, …, $\omega_q = \alpha(\omega_{q-1})/\omega_{q-1}$. In exponential notation we have: $\omega_1 = \omega_0^{\alpha-1}$, $\omega_2 = \omega_0^{(\alpha-1)^2}$, …, $\omega_q = \omega_0^{(\alpha-1)^q}$. The binomial expression of $X^q = [(X-1)+1]^q$ then shows us that

$$\omega_0^{\alpha^q} = \omega_0^{\sum_{k=0}^{q}(\alpha-1)^k\binom{q}{k}} = \prod_{k=0}^{q} \omega_0^{(\alpha-1)^k\binom{q}{k}} = \prod_{k=0}^{q} \omega_k^{\binom{q}{k}}.$$

Put $c = \omega_0^{\alpha^q - 1} = \prod_{k=1}^{q} \omega_k^{\binom{q}{k}}$. From $\omega_0^p = b_0$ and $\alpha^q(b_0) = \sigma^q(b_0) = b_0$ follows that $c^p = 1$. Then we have $c = b_1^{q/p} d^\gamma$, where $\gamma = \binom{q}{2} + \binom{q}{3}(\sigma-1) + \cdots + \binom{q}{q}(\sigma-1)^{q-2}$. Let $\tau_0, \tau_1 \in \mathrm{Gal}(L/K)$ be such that $\tau_0(\omega_0) = \omega_0\zeta$, $\tau_0(\omega_1) = \omega_1$, $\tau_1(\omega_0) = \omega_0$ and $\tau_1(\omega_1) = \omega_1\zeta$. Note that $\alpha\tau_0\alpha^{-1} = \tau_0$ and $\alpha\tau_1\alpha^{-1} = \tau_1\tau_0^{-1}$, which is seen by comparing the actions on ω_0 and ω_1. The element α^q lies in $\mathrm{Gal}(L/K)$ and is fixed by the σ-action. Hence α^q has to be some power of τ_0, so it is trivial if and only if its action on ω_0 is trivial.

Now, taking into account that L/F is modular extension, we have that α^q is not trivial, therefore $c \neq 1$. Denote, as usual, by $N_{K/F} : K \to F$ the norm map. From $b_1 = \sigma(b_0)/b_0$ follows that $N_{K/F}(b_1) = 1$, so

$$N_{K/F}(b_1) = b_1\sigma(b_1)\cdots\sigma^{q-1}(b_1) = b_1^q\big(d^p\big)^{q-1}\sigma\big(d^p\big)^{q-2}\cdots\sigma^{q-2}\big(d^p\big) = 1.$$

Hence, the element $h = b_1^{q/p} d^{q-1}\sigma(d)^{q-2}\cdots\sigma^{q-2}(d)$ is in the cyclic group, generated by ζ. In particular, $\sigma(h)/h = N_{K/F}(d) = 1$. Now, from Hilbert's Theorem 90 follows that there exists $x \in K^\times$, such that $d = \sigma(x)/x$. Therefore, $\sigma(b_1)/b_1 = \sigma(x^p)/x^p$ and for some $f \in F^\times \setminus F^\times \cap K^{\times p}$ we get $b_1 = fx^p$. Furthermore, $c = (fx^p)^{q/p}(\sigma(x)/x)^\gamma = f^{q/p}x^\delta$, where $\delta = q + \binom{q}{2}(\sigma-1) + \cdots + \binom{q}{q}(\sigma-1)^{q-1} = \sum_{k=0}^{q-1}\sigma^k$, so $c = f^{q/p}N_{K/F}(x)$.

'If part': Let b_0, f and c be as in the statement. Put $b_1 = fx^p$ and $d = \sigma(x)/x$. From Proposition 3.1 follows that $L/F = K(b_0^{1/p}, b_1^{1/p})/F$ is either an $M(p^n)$, or a semidirect extension. With the same definitions of $\omega_0, \ldots, \omega_q$ as in the 'only-if part', we obtain that $c = (fx^p)^{q/p}(\sigma(x)/x)^\gamma = \omega_0^{\alpha^q - 1} \neq 1$, i.e., $\alpha^q \neq 1$, so L/F is exactly an $M(p^n)$ extension. □

Remark. In the latter Theorem we have that $b_1 = b_0^{\sigma-1} \notin K^{\times p}$, so $[b_0] \notin J_1$, and $b_2 = b_0^{(\sigma-1)^2} \in K^{\times p}$, so $[b_0] \in J_2$, i.e., $[b_0] \in J_2 \setminus J_1$. Thus the explicit look of the element b_0 is relevant to the structure

of the module J_2, which is not quite clear. However, the explicit nature of the element b_0 is of little importance for our goals.

Next, we will generalize Proposition 3.1 for non-abelian extensions of C_q with kernel $(C_p)^3$.

Proposition 3.3. *Let L/F be a non-abelian Galois extension, containing K/F and let* $\mathrm{Gal}(L/K)$ *be isomorphic to $(C_p)^3$. Then $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, where $b_0 \in K^\times \setminus K^{\times p}$, $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$, $b_2 = \sigma(b_1)/b_1$ and there are only two different possibilities:*

(i) $b_2 \in K^\times \setminus K^{\times p}$ *and* $\sigma(b_2)/b_2 \in K^{\times p}$;
(ii) $b_2 \in K^{\times p}$ *and* $\sigma(b_2)/b_2 \in K^{\times p}$.

Proof. The non-abelian Galois extensions L/F such that $\mathrm{Gal}(L/K)$ is isomorphic to $(C_p)^3$ are in a bijective correspondence with dimension 3 submodules of J not isomorphic to $\mathbb{F}_p^3$. From the theory of modules over a PID, there are only two isomorphism classes of such modules: $\mathbb{F}_p[C_q]/\langle(\sigma-1)^3\rangle$ and $\mathbb{F}_p \oplus \mathbb{F}_p[C_q]/\langle(\sigma-1)^2\rangle$, giving cases (i) and (ii), respectively. □

Let us consider now the two possibilities separately. The first one gives us a submodule $W \cong \mathbb{F}_p[C_q]/\langle(\sigma-1)^3\rangle$, so for $n > 3$ there are only two isomorphism classes possible for $\mathrm{Gal}(L/K)$, depending on whether the index of W is trivial or not.

Proposition 3.4. *Let $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, where $b_0 \in K^\times \setminus K^{\times p}$, $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$, $b_2 = \sigma(b_1)/b_1 \in K^\times \setminus K^{\times p}$ and $\sigma(b_2)/b_2 \in K^{\times p}$. Then L/F is Galois and the Galois group of L/F is isomorphic either to the semidirect product $C_q \rtimes (C_p)^3$, or to the group, generated by σ_1, τ_0, τ_1 and τ_2, such that $\sigma_1^q = \tau_0$, $\sigma_1\tau_1\sigma_1^{-1} = \tau_1\tau_0^{-1}$, $\sigma_1\tau_2\sigma_1^{-1} = \tau_2\tau_0\tau_1^{-1}$, where τ_0, τ_1 and τ_2 are the generators of* $\mathrm{Gal}(L/K)$, *given by $\tau_i(\sqrt[p]{b_j}) = \sqrt[p]{b_j}\,\xi^{\delta_{ij}}$.*

The second possibility gives us a submodule $W \cong \mathbb{F}_p \oplus \mathbb{F}_p[C_q]/\langle(\sigma-1)^2\rangle$, so there are three isomorphism classes possible for $\mathrm{Gal}(L/K)$, depending on the indexes of the two direct summands.

Proposition 3.5. *Let $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, where $b_0 \in K^\times \setminus K^{\times p}$, $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$, $\sigma(b_1)/b_1 \in K^{\times p}$, $b_2 \in K^\times \setminus K^{\times p}$ and $\sigma(b_2)/b_2 \in K^{\times p}$. Then L/F is a non-abelian Galois extension and the Galois group of L/F is isomorphic either to $(C_q \rtimes (C_p)^2) \times C_p$, or to $M(p^n) \times C_p$, or to $\widetilde{M}(p^{n+1})$.*

As an illustration of Theorem 3.2 and Proposition 3.5, we construct an $\widetilde{M}(2^{n+1})$ extension over the field of rationals in the following

Example 3.1. Let $p = 2$, $F = \mathbb{Q}$ and let ξ denote a primitive 2^{n+1}th root of unity for $n \geqslant 4$. It is well known that the Galois group of $\mathbb{Q}(\xi)/\mathbb{Q}$ is isomorphic to the multiplicative group $\mathbb{Z}_{2^{n+1}}^*$ which, in turn, is isomorphic to $C_{2^{n-1}} \times C_2 = \langle\bar{5}\rangle \times \langle-\bar{1}\rangle$. Set $\theta_k = \xi^k + \xi^{-k}$ for $k \geqslant 1$ and $\theta = \theta_1$. Then for odd k we have that θ_k are the conjugates of θ and $\mathbb{Q}(\xi) = \mathbb{Q}(\theta, i)$, where $i = \sqrt{-1} = \xi^{2^{n-1}}$. The actions of $\bar{5}$ and $-\bar{1}$ are:

$$\bar{5} : \theta \mapsto \theta_5 \quad i \mapsto i; \qquad -\bar{1} : \theta \mapsto \theta, \quad i \mapsto -i.$$

Therefore the Galois group of $K/F = \mathbb{Q}(\theta_2)/\mathbb{Q}$ is $\langle\bar{5}\rangle/\langle\bar{5}^{2^{n-2}}\rangle$, which is isomorphic to the cyclic group $C_{2^{n-2}}$.

Now, we can construct an $M(2^n)$ extension, applying Theorem 3.2. We have that $\theta^2 = \theta_2 + 2$ and $\sqrt{2}$ are in K, so we can put $b_0 = \sqrt{2}\theta^2$. Denote by σ the generator of $C_{2^{n-2}}$. Then $\sigma(b_0)/b_0 = -x^2$, where $x = \bar{5}(\theta)/\theta = \theta_5/\theta = \theta_2^2 - \theta_2 - 1 \in K^\times$. Next, we have to calculate the norm of x:

$$N_{K/F}(x) = \bar{5}^{2^{n-2}}(\theta)/\theta = \left(\xi^{1+2^n} + \xi^{-1-2^n}\right)/\theta = -1,$$

since $5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}$. Thus, for $f = -1$ we get $\sigma(b_0)/b_0 = fx^2$ and $c = f^{q/2}N_{K/F}(x) = -1$, whence $K(\sqrt[4]{2}\theta, i)/F = \mathbb{Q}(\theta_2, \sqrt[4]{2}\theta, i)/\mathbb{Q}$ is an $M(2^n)$ extension.

Next, put $b_1 = -x^2$ and $b_2 = \theta^2$ (here obviously b_1 and b_2 are in $K^\times \setminus K^{\times 2}$). Since $\sigma(\sqrt{2})/\sqrt{2} = -1$, we get $\sigma(b_2)/b_2 = x^2$, so $K(\sqrt[4]{2}\theta, i, \theta)/F = \mathbb{Q}(\sqrt[4]{2}, \xi)/\mathbb{Q}$ is an $\widetilde{M}(2^{n+1})$ extension.

The description of modular p-extensions can be made even more explicit in some particular cases, as we will show now.

Let $a_1, a_2 \in F^\times$ be independent mod $F^{\times p}$ and denote $K_i = F(\sqrt[p]{a_i})$, $i = 1, 2$. As before, let K/F be a $C_q = \langle\sigma\rangle$ extension, such that $K_1 \subset K$. Then $L/F = K(\sqrt[p]{a_2})/F$ is a $C_q \times C_p$ extension, generated by elements σ and τ, such that $\sigma^q = \tau^p = 1$. We have the group extension:

$$1 \to \mu_p \cong \langle\alpha^q\rangle \to M(p^n) \underset{\substack{\alpha\mapsto\sigma \\ \beta\mapsto\tau}}{\longrightarrow} C_q \times C_p \to 1. \tag{3.2}$$

By Theorem 1.1 the obstruction to solvability of the embedding problem given by L/F and (3.2) is

$$[K, C_q, \zeta](a_2, a_1; \zeta) \in \mathrm{Br}(F), \tag{3.3}$$

where $[K, C_q, \zeta]$ is the equivalence class of the crossed product cyclic algebra (K, σ, ζ), given by the restricted group extension

$$1 \to \mu_p \cong \langle\alpha^q\rangle \to C_{pq} \underset{\alpha\mapsto\sigma}{\longrightarrow} C_q \to 1.$$

Here are several examples showing specific modular extensions obtained by analyzing the obstruction (3.3).

Example 3.2. Assume that a primitive qth root of unity ζ_q is in F. According to [Pi, Corollary 15.1b], we have

$$(K, \sigma, \zeta) = \left(K, \sigma, \zeta_q^{q/p}\right) = (K_1, \sigma|_{K_1}, \zeta_q) = (a_1, \zeta_q; \zeta) \in \mathrm{Br}(F).$$

The obstruction then obtains this form:

$$[K, C_q, \zeta](a_2, a_1; \zeta) = (a_1, \zeta_q; \zeta)(a_2, a_1; \zeta) = \left(\zeta_q^{-1}a_2, a_1; \zeta\right) \in \mathrm{Br}(F).$$

Now, assume that $(\zeta_q^{-1}a_2, a_1; \zeta) = 1$, so there exists $y \in K_1$, such that $N_{K_1/F}(y) = \zeta_q^{-1}a_2$. We can also assume for simplicity that $K = F(\sqrt[q]{a_1})$. Set $\omega = \sqrt[q]{a_1}\, y^{p-1}\sigma(y)^{p-2}\cdots\sigma^{p-2}(y)$. Then we have $\sigma(\omega)/\omega = \zeta_q N_{K_1/F}(y)/y^p = a_2/y^p \in L^{\times p}$ and $\tau(\omega)/\omega = 1$. Therefore, $L(\sqrt[p]{\omega})/F$ is a Galois extension. Let g_1 and g_2 be the automorphisms from $\mathrm{Gal}(L(\sqrt[p]{\omega})/F)$, map respectively onto σ and τ. We can define their action thus: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\,\sqrt[p]{a_2}/y$ and $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$. Now, the relations: $g_1^{pq} = g_2^p = 1$ and $g_1^q = [g_2, g_1] = g_2^{-1}g_1^{-1}g_2g_1$ are easily verified, hence $L(\sqrt[p]{\omega})/F$ is exactly an $M(p^n)$ extension. □

Example 3.3. Assume that a primitive qth root of unity ζ_q is in $F^\times$, but not in $F^{\times p}$. Once again, we can assume that $K/F = F(\sqrt[q]{a_1})/F$ is a C_q extension. Now, put $b_0 = \sqrt[q]{a_1}$ and $b_1 = \zeta_q$. Then we have $b_1 = \sigma(b_0)/b_0 \in K^\times \setminus K^{\times p}$, $\sigma(b_1)/b_1 = 1$ and $c = b_1^{q/p} = \zeta_q^{q/p} = \zeta \neq 1$. Theorem 3.2 then implies that $K(\sqrt[pq]{a_1}, \sqrt[p]{\zeta_q})/F$ is an $M(p^n)$ extension. Exactly the same can be obtained if we put $a_2 = \zeta_q$, so $(\zeta_q^{-1}a_2, a_1; \zeta) = (1, a_1; \zeta) = 1$ and $\omega = \sqrt[q]{a_1}$.

Example 3.4. Let $n > 3$. Assume that $\zeta \in N_{K/F}(K^\times)$, i.e., there exists $\omega \in K^\times$, such that $\zeta = N_{K/F}(\omega)$. Now, let $\omega_1 \in K_1^\times \setminus F^\times$ be arbitrary. Then $N_{K/F}(\omega_1) = [N_{K_1/F}(\omega_1)]^{q/p} = f^{q/p}$ for $f = N_{K_1/F}(\omega_1)$, and the only restriction on the choice of ω_1 we need is $f \in F^\times \setminus K_1^{\times p} \cap F^\times$. If we put $x = \omega_1^{-1}\omega$ and $b_1 = fx^p$, we have $c = f^{q/p}N_{K/F}(x) = \zeta$. Then for any b_0, such that $\sigma(b_0)/b_0 = b_1$, we obtain an $M(p^n)$ extension $L/F = K(b_0^{1/p}, (N_{K_1/F}(\omega_1))^{1/p})/F$.

Note that the assumption $\zeta \in N_{K/F}(K^\times)$ means that the cyclic algebra $[K, C_q, \zeta]$ is split in $\mathrm{Br}(F)$, which leads to the obstruction $(a_2, a_1; \zeta) \in \mathrm{Br}(F)$. In our case the splitting of the obstruction is equivalent to $a_2 = f = N_{K_1/F}(\omega_1) \in F^\times \setminus K_1^{\times p} \cap F^\times$.

4. Restrictions, corestrictions and obstructions

We begin with a description of the restricted group extensions produced by transitive embeddings of some 2-groups into the symmetric group S_{2^l}.

Lemma 4.1. *Consider the restriction map*

$$\mathrm{res} : H^2(S_d, \mu_2) \to H^2(G, \mu_2),$$

where G is embedded transitively into the symmetric group S_d of degree $d = 2^l \geqslant 4$, according to the described in Section 2 method via a primitive element.

(1) *(See [DEK, Lemma 2].) Let $G = C_2 \times C_2$. Then* $\mathrm{res}(s_4)$ *corresponds to the quaternion group extension*

$$1 \to \mu_2 \to Q_8 \to C_2 \times C_2 \to 1.$$

(2) *Let $G = C_{2^{n-2}} \times C_2$ for $n \geqslant 4$. Then* $\mathrm{res}(s_{2^{n-1}})$ *corresponds to the group extension*

$$1 \to \mu_2 \to \widetilde{C_{2^{n-2}} \times C_2} \to C_{2^{n-2}} \times C_2 \to 1,$$

where $\widetilde{C_{2^{n-2}} \times C_2}$ has a presentation: $x^{2^{n-2}} = y^2 = 1$, $yx = -xy$.

(3) *Let $G = M(2^n)$. Then* $\mathrm{res}(s_{2^n})$ *corresponds to the group extension*

$$1 \to \mu_2 \to \widetilde{M(2^n)} \to M(2^n) \to 1,$$

where $\widetilde{M(2^n)} \cong \widetilde{M}(2^{n+1})$ is the group described in the Introduction for $p = 2$.

Proof. (1) Let $L/F = F(\sqrt{a}, \sqrt{b})/F$ be a $C_2 \times C_2$ extension. Then $\theta = \sqrt{a} + \sqrt{b}$ is a primitive element of L/F. The conjugates of θ are: $\theta = \theta_1 = \sqrt{a}+\sqrt{b}$, $\theta_2 = -\sqrt{a}+\sqrt{b}$, $\theta_3 = \sqrt{a}-\sqrt{b}$ and $\theta_4 = -\sqrt{a}-\sqrt{b}$. Then $\sigma = (1,2)(3,4)$ and $\tau = (1,3)(2,4)$ are the generators of $C_2 \times C_2 = \mathrm{Gal}(L/F)$. Since the product of two disjoint transpositions lifts to an element of order 4 in $\widetilde{S}_4$, we get $\widetilde{C_2 \times C_2} \cong Q_8$.

(2) Let $L/F = F(\alpha, \sqrt{b})/F$ be a $C_{2^{n-2}} \times C_2$ extension, and let σ and τ be the generators of the latter group: $\sigma^{2^{n-2}} = \tau^2 = 1, \sigma\tau = \tau\sigma$. Set $\alpha_1 = \alpha$, $\alpha_2 = \sigma(\alpha_1)$, …, $\alpha_{2^{n-2}} = \sigma^{2^{n-2}-1}(\alpha_1)$. Then $\theta = \alpha + \sqrt{b}$ is a primitive element of L/F and the conjugates of θ are

$$\theta_1 = \theta, \quad \theta_2 = \alpha_2 + \sqrt{b}, \quad \ldots, \quad \theta_{2^{n-2}} = \alpha_{2^{n-2}} + \sqrt{b},$$
$$\theta_{2^{n-2}+1} = \alpha_1 - \sqrt{b}, \quad \theta_{2^{n-2}+2} = \alpha_2 - \sqrt{b}, \quad \ldots, \quad \theta_{2^{n-1}} = \alpha_{2^{n-2}} - \sqrt{b}.$$

Whence

$$\sigma = \big(1, 2, \ldots, 2^{n-2}\big)\big(2^{n-2}+1, 2^{n-2}+2, \ldots, 2^{n-1}\big),$$
$$\tau = \big(1, 2^{n-2}+1\big)\big(2, 2^{n-2}+2\big)\cdots\big(2^{n-2}, 2^{n-1}\big).$$

Since $n \geqslant 4$ and the preimages $\widetilde{(i,j)}$ and $\widetilde{(k,l)}$ of two disjoint transpositions anticommute, we get $\tilde{\sigma}^{2^{n-2}} = \tilde{\tau}^2 = 1$.

Now, set $\sigma_1 = (1, 2, \ldots, 2^{n-2})$ and $\sigma_2 = (2^{n-2}+1, 2^{n-2}+2, \ldots, 2^{n-1})$. Calculations show that $\tau\sigma_1\tau = \sigma_2$. We can write down σ_1 and σ_2 as products of transpositions:

$$\sigma_1 = (1,2)(2,3)\cdots\big(2^{n-2}-1, 2^{n-2}\big),$$
$$\sigma_2 = \big(2^{n-2}+1, 2^{n-2}+2\big)\big(2^{n-2}+2, 2^{n-2}+3\big)\cdots\big(2^{n-1}-1, 2^{n-1}\big).$$

Clearly, all transpositions from the decomposition of σ_1 are disjoint with those from the decomposition of σ_2, so

$$\tilde{\sigma}_1\tilde{\sigma}_2 = (-1)^{(2^{n-2}-1)^2}\tilde{\sigma}_2\tilde{\sigma}_1 = -\tilde{\sigma}_2\tilde{\sigma}_1.$$

(3) Let $L/F = K(\sqrt{b_0}, \sqrt{f})/F$ be an $M(2^n)$ extension as in Theorem 3.2. Then $\theta = \sqrt{b_0} + \sqrt{f}$ is a primitive element of L/K. Denote by σ and τ the generators of $M(2^n) : \sigma^{2^{n-1}} = \tau^2 = 1$, $\tau\sigma = \sigma^{2^{n-2}+1}\tau$. By a similar argument as in (2), we obtain the decompositions of σ and τ in S_{2^n}:

$$\sigma = \big(1, 2, \ldots, 2^{n-1}\big)\big(2^{n-1}+1, 2^{n-1}+2, \ldots, 2^n\big),$$
$$\tau = \big(1, 2^{n-1}+1\big)\big(2, 2^{n-1}+2^{n-2}+2\big)\big(3, 2^{n-1}+3\big)\big(4, 2^{n-1}+2^{n-2}+4\big)\cdots\big(2^{n-1}, 2^{n-1}+2^{n-2}\big).$$

Whence $\tilde{\sigma}^{2^{n-1}} = \tilde{\tau}^2 = 1$. Set $\sigma_1 = (1, 2, \ldots, 2^{n-1})$ and $\sigma_2 = (2^{n-1}+1, 2^{n-1}+2, \ldots, 2^n)$. Calculations show that $\tau\sigma_1\tau = \sigma_2^{2^{n-2}+1}$ and $\tau\sigma_2\tau = \sigma_1^{2^{n-2}+1}$. Here again $\tilde{\sigma}_1\tilde{\sigma}_2 = -\tilde{\sigma}_2\tilde{\sigma}_1$, so

$$\tilde{\tau}\tilde{\sigma}\,\tilde{\tau} = \tilde{\sigma}_2^{2^{n-2}+1}\tilde{\sigma}_1^{2^{n-2}+1} = -\tilde{\sigma}^{2^{n-2}+1}.$$

We are done. □

We are now going to describe the corestriction homomorphism, keeping the notations for the groups that appear in the latter lemma.

Theorem 4.2. *Let G be a finite 2-group generated by two elements g and h_2 such that $g^2 = h_1$, $h_2^2 = 1$ and $h_1h_2 = h_2h_1$. Let H be the subgroup of G generated by h_1 and h_2.*

(2) *Let $G \cong C_4 \times C_2$, $H \cong C_2 \times C_2$ and let $\bar{f} \in Z^2(H, \mu_2)$ represent the exact sequence*

$$1 \to \mu_2 \to Q_8 \to H \to 1.$$

Then $f = \mathrm{cor}_{G/H}(\bar{f}) \in Z^2(G, \mu_2)$ represents the exact sequence

$$1 \to \mu_2 \to \widetilde{C_4 \times C_2} \cong D \curlywedge C \to G \to 1.$$

(2) *Let* $G \cong C_{2^{n-2}} \times C_2$, $H \cong C_{2^{n-3}} \times C_2$ *for* $n \geqslant 5$, *and let* $\bar{f} \in Z^2(H, \mu_2)$ *represent the exact sequence*

$$1 \to \mu_2 \to \widetilde{C_{2^{n-3}} \times C_2} \to H \to 1.$$

Then $f = \mathrm{cor}_{G/H}(\bar{f}) \in Z^2(G, \mu_2)$ *represents the exact sequence*

$$1 \to \mu_2 \to \widetilde{C_{2^{n-2}} \times C_2} \to G \to 1.$$

(3) *Let* $G \cong M(2^n)$, $H \cong C_{2^{n-2}} \times C_2$ *for* $n \geqslant 4$, *and let* $\bar{f} \in Z^2(H, \mu_2)$ *represent the exact sequence*

$$1 \to \mu_2 \to \widetilde{C_{2^{n-2}} \times C_2} \to H \to 1.$$

Then $f = \mathrm{cor}_{G/H}(\bar{f}) \in Z^2(G, \mu_2)$ *represents the exact sequence*

$$1 \to \mu_2 \to \widetilde{M\left(2^n\right)} \to G \to 1.$$

Proof. (1) Let $L/F = F(\alpha, \sqrt{b})/F$ be a $C_4 \times C_2$ extension, where $\alpha = \sqrt{r(a + \sqrt{a})}$ for $a = 1 + c^2$, $c, r \in F^\times$. Then $\theta = \alpha + \sqrt{b}$ is a primitive element for L/F. Denote by $K = F(\sqrt{a})$ the fixed subfield L^H of H, and by

$$\theta_1 = \alpha + \sqrt{b}, \qquad \theta_2 = -\alpha + \sqrt{b}, \qquad \theta_3 = \alpha - \sqrt{b}, \qquad \theta_4 = -\alpha - \sqrt{b},$$

the conjugates of θ over K. Then H embeds transitively in $A_4 \hookrightarrow SO_4(F)$:

$$h_1 = (1, 2)(3, 4), \qquad h_2 = (1, 3)(2, 4).$$

Next, set $\alpha' = g(\alpha)$ and

$$\theta_5 = \alpha' + \sqrt{b}, \qquad \theta_6 = -\alpha' + \sqrt{b}, \qquad \theta_7 = \alpha' - \sqrt{b}, \qquad \theta_8 = -\alpha' - \sqrt{b}$$

—the remaining conjugates of θ over F. The induced orthogonal representation then gives us a transitive embedding of G in S_8:

$$g = (1, 5, 2, 6)(3, 7, 4, 8),$$
$$h_2 = (1, 3)(2, 4)(5, 7)(6, 8).$$

Applying Lemma 4.1(1), (2) and Theorem 2.2 we obtain the group $D \curlywedge C$.

The proof of the remaining cases is similar, so we leave it to the reader. □

Remark. The latter Theorem can be proven also by applying the explicit formula from Theorem 2.1. For groups with more generators and relations, however, this is becoming an increasingly inefficient way of finding the corestricted group extensions.

We are now going to show that the two types of transitive embeddings into the symmetric group, described in Section 2, might lead to non-equivalent group extensions.

Example 4.1. Let F contain a primitive 2^{n-2}th root of unity ξ, but $\xi \notin F^2$. Let $a \in F^\times \setminus F^{\times 2}$ and let $M = F(\sqrt[2^{n-1}]{a}, \sqrt{\xi})$, i.e., M is the splitting field of the polynomial $f(x) = x^{2^{n-1}} - a$. From Example 3.3 we know that M/F is an $M(2^n)$ extension (see also [MR,KR]).

We are going to show now that $\theta = \sqrt[2^{n-1}]{a} + \sqrt{\xi}$ is a primitive element of M/F. Assume that $\sigma \in \mathrm{Gal}(M/F)$ leaves θ fixed. Since $\sigma(\sqrt[2^{n-1}]{a}) = \sqrt[2^{n-1}]{a}(\sqrt{\xi})^k$ and $\sigma(\sqrt{\xi}) = (-1)^l\sqrt{\xi}$ for some $k, l \geqslant 0$, we obtain that $\sqrt[2^{n-1}]{a} + \sqrt{\xi} = \sqrt[2^{n-1}]{a}(\sqrt{\xi})^k + (-1)^l\sqrt{\xi}$. Therefore $\sqrt[2^{n-1}]{a}(1 - (\sqrt{\xi})^k) = \sqrt{\xi}((-1)^l - 1)$, so $a(1 - (\sqrt{\xi})^k)^{2^{n-1}} = ((-1)^l - 1)^{2^{n-1}}$, which is possible if and only if $k = l = 0$, i.e. $\sigma = 1$.

Next, we can embed transitively $M(2^n)$ into the symmetric group S_{2^n} as described in Lemma 4.1(3). From [MR] we know that the trace form $\mathrm{tr}_{M/F}\langle 1\rangle$ of $M/F = F(\theta)/F$ is Witt-equivalent to the Pfister form $\langle\langle \xi, a\rangle\rangle$. Applying [Le, Th. 6.2.1] we can calculate that the obstruction (the second Stiefel–Whitney class) of the group extension

$$1 \to \mu_2 \to \widetilde{M(2^n)} \to M(2^n) \to 1$$

is (a, ξ).

Now, let $L = F(\sqrt[2^{n-1}]{a})$. Calculations show that the trace form $\mathrm{tr}_{L/F}\langle 1\rangle$ is Witt-equivalent to the quadratic form $\langle 2, 2a\rangle$. Then $M(2^n)$ embeds transitively in $S_{2^{n-1}}$ and the restriction $\mathrm{res}(s_{2^{n-1}})$ corresponds to a group extension

$$1 \to \mu_2 \to \widetilde{M(2^n)}' \to M(2^n) \to 1,$$

whose obstruction is split. Indeed, $2 \notin F^2$ for $n = 4$, so the obstruction is $(2, 2a)(2, a) = 1$. If $n > 4$ then $2 \in F^2$ and the obstruction is $(1, a) = 1$. All this shows that the two group extensions are non-equivalent.

Further, we will show that the group $H^2(C_q \times C_2, \mu_2)$ is isomorphic to μ_2^3 for $n \geqslant 4$, the group $H^2(M(2^n), \mu_2)$ is isomorphic to μ_2^2, and the corestriction homomorphism $\mathrm{cor} : H^2(C_q \times C_2, \mu_2) \to H^2(M(2^n), \mu_2)$ is surjective. Indeed, the elements $c_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \in H^2(C_q \times C_2, \mu_2)$ for $\varepsilon_i = \pm 1$ are determined by the non-equivalent exact sequences

$$1 \to \mu_2 \to G_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \underset{\substack{\tilde\sigma \mapsto \sigma \\ \tilde\tau \mapsto \tau}}{\longrightarrow} C_q \times C_2 \to 1,$$

where $\tilde\sigma^q = \varepsilon_1$, $\tilde\tau^2 = \varepsilon_2$, $[\tilde\tau, \tilde\sigma] = \varepsilon_3$.

Similarly, the elements $c_{\varepsilon_2,\varepsilon_3} \in H^2(M(2^n), \mu_2)$ for $\varepsilon_i = \pm 1$ are determined by the exact sequences

$$1 \to \mu_2 \to G_{\varepsilon_2,\varepsilon_3} \underset{\substack{\tilde\alpha \mapsto \alpha \\ \tilde\beta \mapsto \beta}}{\longrightarrow} M(2^n) \to 1,$$

where $\tilde\beta^2 = \varepsilon_2$, $\tilde\alpha^q[\tilde\beta, \tilde\alpha] = \varepsilon_3$ and $\tilde\alpha^{2q} = 1$, since there is no group of exponent 2^n which has a factor-group isomorphic to the modular group of order 2^n.

Recall that from Theorem 4.2 (3) we have that the corestriction of the 2-coclass $c_{1,1,-1}$ related to the exact sequence

$$1 \to \mu_2 \to \widetilde{C_{2^{n-2}} \times C_2} \to C_{2^{n-2}} \times C_2 \to 1$$

is the 2-coclass $c_{1,-1}$ which represents the exact sequence

$$1 \to \mu_2 \to \widetilde{M(2^n)} \to M(2^n) \to 1.$$

Similar arguments show also that $\operatorname{cor}(c_{-1,1,1}) = c_{-1,-1}$ and $\operatorname{cor}(c_{-1,1,-1}) = c_{-1,1}$.

With the aid of some cohomological computations one can show that all of the above groups have their 'twins' for p-odd, so the group $H^2(C_q \times C_p, \mu_p)$ is isomorphic to μ_p^3 for $n \geqslant 4$ and the group $H^2(M(p^n), \mu_p)$ is isomorphic to μ_p^2. Surprisingly enough, however, the corestriction homomorphism $\operatorname{cor} : H^2(C_q \times C_p, \mu_p) \to H^2(M(p^n), \mu_p)$ is not surjective, as we will see.

Let us describe first the cohomological groups. Take the group $M(p^n)$ with generators α and β as in the Introduction. The subgroup generated by $\sigma = \alpha^p$ and $\tau = \beta$ is isomorphic to $C_q \times C_p$, as we noted. The elements $c_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \in H^2(C_q \times C_p, \mu_p)$ for $\varepsilon_i = \zeta^k$ are determined by the exact sequences

$$1 \to \mu_p \to G_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \underset{\substack{\tilde{\sigma}\mapsto\sigma \\ \tilde{\tau}\mapsto\tau}}{\longrightarrow} C_q \times C_p \to 1,$$

where $\tilde{\sigma}^q = \varepsilon_1$, $\tilde{\tau}^p = \varepsilon_2$, $[\tilde{\tau}, \tilde{\sigma}] = \varepsilon_3$.

Similarly, the elements $c_{\varepsilon_2,\varepsilon_3} \in H^2(M(p^n), \mu_p)$ for $\varepsilon_i = \zeta^k$ are determined by the exact sequences

$$1 \to \mu_p \to G_{\varepsilon_2,\varepsilon_3} \underset{\substack{\tilde{\alpha}\mapsto\alpha \\ \tilde{\beta}\mapsto\beta}}{\longrightarrow} M\big(p^n\big) \to 1,$$

where $\tilde{\beta}^p = \varepsilon_2$, $\tilde{\alpha}^q[\tilde{\beta}, \tilde{\alpha}] = \varepsilon_3$ and $\tilde{\alpha}^{pq} = 1$.

Choose $\bar{f} = c_{\varepsilon_1,\varepsilon_2,\varepsilon_3}$ and let $f = \operatorname{cor}_{M(p^n)/C_q\times C_p}(\bar{f})$. We are going to find the order of $\tilde{\beta}$. Recall that $\alpha\beta\alpha^{-1} = \alpha^{-q}\beta = \sigma^{-q/p}\tau$. Then, according to Theorem 2.1 we obtain

$$f\big(\beta, \beta^{p-1}\big) = \prod_{k=0}^{p-1} \bar{f}\big(\alpha^k\beta\alpha^{-k}, \alpha^k\beta^{p-1}\alpha^{-k}\big) = \prod_{k=0}^{p-1} \bar{f}\big(\sigma^{-kq/p}\tau, \big(\sigma^{-kq/p}\tau\big)^{p-1}\big).$$

Since each multiplier in the latter product is equal to 1 for $\varepsilon_1 = \varepsilon_2 = 1$ and $\varepsilon_3 = \zeta$, we get $\tilde{\beta}^p = 1$. On the other hand, for $\varepsilon_1 = \zeta$, $\varepsilon_2 = 1$ and $\varepsilon_3 = 1$ we have $(\tilde{\sigma}^{-kq/p}\tau)^p = \zeta^{-k}$, so $f(\beta, \beta^{p-1}) = \zeta^{-1-2-\cdots-(p-1)} = \zeta^{-p(p-1)/2} = 1$, in contrast with the case $p = 2$, where the value of $\zeta^{-p(p-1)/2}$ is -1. This means that for p-odd the order of $\tilde{\beta}$ is p, while for $p = 2$ its order is 4.

Further, let p be arbitrary prime, set $\widetilde{C_q \times C_p} = G_{1,1,\zeta}$ and denote by $\bar{f} \in Z^2(C_q \times C_p, \mu_p)$ the 2-cocycle related to the group extension

$$1 \to \mu_p \cong \langle\zeta\rangle \to \widetilde{C_q \times C_p} \underset{\substack{\tilde{\sigma}\mapsto\sigma \\ \tilde{\tau}\mapsto\tau}}{\longrightarrow} C_q \times C_p \to 1. \tag{4.1}$$

Applying the explicit formula from Theorem 2.1 one can show that the 2-cocycle

$$f = \operatorname{cor}_{M(p^n)/C_q\times C_p}(\bar{f}) \in Z^2\big(M\big(p^n\big), \mu_p\big)$$

is related to the group extension:

$$1 \to \mu_p \cong \langle\zeta\rangle \to \widetilde{M}\big(p^{n+1}\big) \underset{\substack{\tilde{\alpha}\mapsto\alpha \\ \tilde{\beta}\mapsto\beta}}{\longrightarrow} M\big(p^n\big) \to 1. \tag{4.2}$$

Next, take arbitrary $M(p^n)$ extension L/F, according to the description given in Theorem 3.2: $L/F = K(\sqrt[p]{b_0}, \sqrt[p]{a_2})$, where $b_0 \in K^\times \setminus K^{\times p}$, $a_2 \in F^\times \setminus F^\times \cap K^{\times p}$ and $x \in K^\times$ are such that $\sigma(b_0)/b_0 = a_2x^p$, and $c = a_2^{q/p}N_{K/F}(x)$ is a pth root of unity, but $c \neq 1$. Furthermore, we have the inclusion $F(\sqrt[p]{a_1}, \sqrt[p]{a_2}) \subset L$, where $K_1 = F(\sqrt[p]{a_1}) = L^{C_q\times C_p}$. From Theorem 1.1 follows that the obstruction to

the embedding problem given by L/K and (4.1) is $(a_2, a_1'; \zeta) \in \mathrm{Br}_p(K_1)$, where $a_1' \in K_1^\times \setminus K_1^{\times p}$ is such that $N_{K_1/F}(a_1') = a_1$.

Proposition 4.3. *The obstruction to the embedding problem given by L/F and* (4.2) *is* $(a_2, a_1; \zeta) \in \mathrm{Br}_p(F)$.

Proof. In order to obtain the obstruction we only have to apply the projection formula:

$$\mathrm{cor}_{K_1/F}\big(a_2, a_1'; \zeta\big) = \big(a_2, N_{K_1/F}\big(a_1'\big); \zeta\big) = (a_2, a_1; \zeta). \qquad \square$$

The obstructions to the embedding problems given by the remaining two (generic) non-split group extensions now follow from the structure of the cohomology group $H^2(M(p^n), \mu_p)$. Note that the differences between the corestriction maps for $p = 2$ and p-odd do not impact our final results, since the projection formula is no longer needed.

Proposition 4.4. *The obstruction to the embedding problem given by L/F and the exact sequence*

$$1 \to \mu_p \to G_{\zeta,1} \to M\big(p^n\big) \to 1,$$

where $G_{\zeta,1} \cong \langle x, y \mid x^{p^{n-1}} = y^{p^2} = 1,\ y^p\text{–central},\ yx = x^{q+1}y\rangle$ *is* $(a_2, \zeta; \zeta) \in \mathrm{Br}_p(F)$.

Proposition 4.5. *The obstruction to the embedding problem given by L/F and the exact sequence*

$$1 \to \mu_p \to G_{\zeta,\zeta} \to M\big(p^n\big) \to 1,$$

where $G_{\zeta,\zeta} \cong \langle x, y \mid x^{p^{n-1}} = y^{p^2} = 1,\ y^p\text{–central},\ yx = x^{q+1}y^{p+1}\rangle$ *is* $(\zeta a_1, a_2; \zeta) \in \mathrm{Br}_p(F)$.

5. Special dihedral representations

Assume that $char(F) \neq 2$ and F contains a primitive nth root of unity η for n-even. Let $H \cong D_{2n}$ be the dihedral group of order $2n$ generated by elements h_0 and h_1 such that $h_0^n = h_1^2 = 1$, $h_1h_0 = h_0^{-1}h_1$

According to [Fr] we can construct a dihedral non-special orthogonal representation $H \hookrightarrow O(q_1)$, where (V_1, q_1) is a quadratic space such that the quadratic form q_1 is related to the bilinear form $b_1(x, y)$ given by $b_1(u, v) = 1$, $b_1(u, u) = b_1(v, v) = 0$ for a basis u, v of V_1. The action of H on V_1 is given by

$$h_0(u) = u\eta, \qquad h_0(v) = v\eta^{-1}, \quad h_1(u) = v, h_1(v) = u.$$

Let us change the basis of V_1. Set $u_1 = u + v$ and $u_2 = u - v$. Whence $b_1(u_1, u_1) = 2$, $b_1(u_2, u_2) = -2$, $b_1(u_1, u_2) = 0$, i.e., $q_1 \cong \langle 2, -2\rangle$. The action of H on u_1 and u_2 then is

$$h_0(u_1) = \frac{1}{2}\big(\big(\eta + \eta^{-1}\big)u_1 + \big(\eta - \eta^{-1}\big)u_2\big), \qquad h_1(u_1) = u_1,$$

$$h_0(u_2) = \frac{1}{2}\big(\big(\eta - \eta^{-1}\big)u_1 + \big(\eta + \eta^{-1}\big)u_2\big), \qquad h_1(u_2) = -u_2.$$

Next, assume that H is a subgroup of the dihedral group $G \cong D_{4n}$, i.e., G is generated by elements g and h_1 such that $g^2 = h_0$, $h_1g = g^{-1}h_1$. We can construct the induced orthogonal representation $G \hookrightarrow O(q)$, where $V = V_1 \oplus V_2$, $q = q_1 \perp q_2 = \langle 2, -2, 2, -2\rangle$, $V_1 \equiv V_2$, $q_1 \equiv q_2$. Recall the action of G:

$$h(v_1, v_2) = \big(hv_1, g^{-1}hgv_2\big) \quad \text{and} \quad hg(v_1, v_2) = \big(hh_0v_2, g^{-1}hgv_1\big),$$

for $h \in H$ and $v_i \in V_{q_i}$, $i = 1, 2$. Therefore, the action of G on the basis $w_1 = (u_1, 0)$, $w_2 = (u_2, 0)$, $w_3 = (0, u_1)$, $w_4 = (0, u_2) \in V$ is

$$g(w_1) = w_3, \qquad g(w_3) = (h_0 u_1, 0) = \frac{1}{2}\big((\eta + \eta^{-1})w_1 + (\eta - \eta^{-1})w_2\big),$$

$$g(w_2) = w_4, \qquad g(w_4) = (h_0 u_2, 0) = \frac{1}{2}\big((\eta - \eta^{-1})w_1 + (\eta + \eta^{-1})w_2\big),$$

$$h_1(w_1) = w_1, \qquad h_1(w_3) = \frac{1}{2}\big((\eta + \eta^{-1})w_3 - (\eta - \eta^{-1})w_4\big),$$

$$h_1(w_2) = -w_2, \qquad h_1(w_4) = \frac{1}{2}\big((\eta - \eta^{-1})w_3 - (\eta + \eta^{-1})w_4\big).$$

This representation is special, as is easily seen. Moreover, if (V_Q, Q) is a quadratic space over F and $\mathcal{H} \hookrightarrow O(Q)$ is an orthogonal representation of a subgroup $\mathcal{H}$ of a group $\mathcal{G}$ such that $\mathcal{G} = \mathcal{H} \cup g\mathcal{H}$ and $g^2 = h_0 \in SO(Q)$, then the induced orthogonal representation $\mathcal{G} \hookrightarrow O(Q \perp Q)$ is special if and only if $\dim(V_Q)$ is even. Indeed, the matrix of arbitrary $h \in \mathcal{H}$ as a linear mapping acting on $V_Q \oplus V_Q$ is

$$\mathbf{B}_h = \begin{pmatrix} \mathbf{A}_h & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{g^{-1}hg} \end{pmatrix},$$

where $\mathbf{A}_h$ is the matrix of h acting on V_Q. The matrix of g then is

$$\mathbf{B}_g = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{A}_{h_0} & \mathbf{0} \end{pmatrix},$$

where $\mathbf{I}$ is the identity matrix of size $\dim(V_Q)$. Therefore, $\det(\mathbf{B}_h) = 1$ and $\det(\mathbf{B}_g) = (-1)^{\dim(V_Q)}$.

Let us describe now the subgroup $\widetilde{G}$ of $\mathrm{Spin}(\bar{q})$. Calculations show that the transformation g is obtained by a conjugation with

$$z = \left(\frac{1}{2}(1 - \eta)w_1 w_2 + \eta + 1\right)(w_1 - w_3)(w_2 - w_4),$$

whence the spinor norm is $sp(g) = N(z) = -8^2\eta$. Then the preimage of g in $\widetilde{G}$ is $\tilde{g} = (i/8)\mu^{-1}z$, where $\mu^2 = \eta$, $i^2 = -1$. Further,

$$\tilde{g}^4 = \frac{\eta^{-2}}{2}\left(\frac{1}{2}(1 - \eta^4)w_1 w_2 + \eta^4 + 1\right),$$

whence

$$\tilde{g}^{2n} = \tilde{g}^{4\cdot n/2} = \frac{\eta^{-n}}{2^{n/2}}\left(\frac{1}{2}(1 - \eta^{2n})w_1 w_2 + \eta^{2n} + 1\right) \cdot 2^{n/2-1} = 1.$$

The transformation h_1, in turn, is obtained by a conjugation with

$$y = \left(\frac{1}{2}(1 - \eta)w_3 w_4 - (\eta + 1)\right)w_2 w_4,$$

whence $sp(h_1) = N(y) = 16\eta$. Then the preimage of h_1 in $\widetilde{G}$ is $\tilde{h}_1 = (\mu^{-1}/4)y$ and

$$\begin{aligned}\tilde{h}_1^2 &= \frac{\eta^{-1}}{16}\left(-\frac{1}{4}(1-\eta)^2(w_3w_4)^2 + (1+\eta)^2\right)(w_2w_4)^2\\ &= -\frac{\eta^{-1}}{4}\left(-(1-\eta)^2 + (1+\eta)^2\right) = -1.\end{aligned}$$

Finally, we have $(\tilde{h}_1\tilde{g})^2 = -1$, so $\widetilde{G}$ has a representation

$$\widetilde{G} \cong \left\langle \tilde{g}, \tilde{h}_1, \rho \mid \tilde{g}^{2n} = \rho^2 = 1,\ \tilde{h}_1^2 = \rho,\ \tilde{h}_1\tilde{g} = \tilde{g}^{-1}\tilde{h}_1,\ \rho\text{–central}\right\rangle.$$

In particular we see that the 2-coclass related to

$$1 \to \mu_2 \cong \langle\rho\rangle \to \widetilde{G} \to G \cong D_{4n} \to 1 \tag{5.1}$$

is non-trivial, while we know that the corestriction of the 2-coclass related to

$$1 \to \mu_2 \to \widetilde{H} \to H \cong D_{2n} \to 1 \tag{5.2}$$

is trivial.

Let M/F be a Galois extension with Galois group $G \cong D_{4n}$, let $K = M^H = F(\sqrt{a_1})$ be the fixed subfield of H, and let $L = M^{\langle g^4\rangle} = F(\sqrt{r(\alpha+\beta\sqrt{a_1})}, \sqrt{b})$ be the fixed subfield of the subgroup $\langle g^4\rangle$, where $\alpha^2 - a_1\beta^2 = a_1b$, $r, \beta \in F^\times$, $\alpha \in F$ and $\mathrm{Gal}(L/F) \cong D_8$.

Proposition 5.1. *The obstruction to the embedding problem given by M/F and* (5.1) *is* $(b,-1) \in \mathrm{Br}_2(F)$.

Proof. With the aid of [Fr, Th. 6(i)] and [KR, Lemma 2.3] we can find the twisted quadratic form q_t of the induced quadratic form q:

$$q_t = \left\langle 2\mathrm{tr}(a), 2\mathrm{tr}(a)N(a)a_1, -2\mathrm{tr}(a)b, -2\mathrm{tr}(a)bN(a)a_1\right\rangle,$$

where $a \in K$ is described in [Fr, Ex. 5]. The Hasse–Witt invariants of q and q_t are $(-1,-1)$ and $(-1,-1)(b,-N(a)a_1)$, respectively. According to [Fr, (7.10)], the obstruction to the embedding problem given by M/K and (5.2) is $(a,b)(\eta, r(\alpha+\beta\sqrt{a_1}))$. Note that we must have

$$\mathrm{cor}_{K/F}\left((a,b)\left(\eta, r(\alpha+\beta\sqrt{a_1})\right)\right) = \left(N(a),b\right)(\eta, a_1b) = 1,$$

since the corestriction of the 2-coclass related to (5.2) is trivial. Finally, from [Le, Th. 6.2.1] we get that the obstruction is

$$hw(q)hw(q_t)\left(a_1, sp(g)\right)\left(b, sp(h_1)\right) = (b,-a_1)(\eta, a_1b)(a_1,-\eta)(b,\eta) = (b,-1). \qquad \square$$

Acknowledgments

The author would like to thank an anonymous reviewer of an earlier version of this paper for suggesting the modified proofs in Section 3, based on the papers [MS1,MS2,MSS1,MSS2].

References

[Br] K. Brown, Cohomology of Groups, Springer-Verlag, New York, 1982.

[DEK] C. Drees, M. Epkenhans, M. Krüskemper, On the computation of the trace form of some Galois extensions, J. Algebra 192 (1) (1997) 209–234.

[Fr] A. Fröhlich, Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants, J. Reine Angew. Math. 360 (1985) 84–123.

[FM] A. Fröhlich, A.M. McEvett, The representations of groups by automorphisms of forms, J. Algebra 12 (1969) 114–133.

[FH] W. Fulton, J. Harris, Representation Theory. A First Course, Grad. Texts in Math., vol. 129, Springer-Verlag, New York, 1991.

[Ha] M. Hall, The Theory of Groups, Macmillan Company, New York, 1959.

[KR] D.-S. Kang, Z. Reichstein, Trace forms of Galois field extensions in the presence of roots of unity, J. Reine Angew. Math. 549 (2002) 79–89.

[Le] A. Ledet, Brauer Type Embedding Problems, Fields Inst. Monogr., vol. 21, Amer. Math. Soc., 2005.

[MeS] A.S. Merkurjev, A.A. Suslin, K-Cohomology of Severi–Brauer varieties and the norm residue homomorphism, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982) 1011–1046; English transl. in: Math. USSR Izv. 21 (1983) 307–340.

[Mi1] I. Michailov, Four non-abelian groups of order p^4 as Galois groups, J. Algebra 307 (2007) 287–299.

[Mi2] I. Michailov, Embedding obstructions for the cyclic and modular 2-groups, Math. Balkanica (N.S.) 21 (1–2) (2007) 31–50.

[Mi3] I. Michailov, On Galois cohomology and realizability of 2-groups as Galois groups, preprint.

[MR] J. Mináč, Z. Reichstein, Trace forms of Galois extensions in the presence of a fourth root of unity, Int. Math. Res. Not. (2004) 389–410.

[MS1] J. Mináč, J. Swallow, Galois module structure of pth-power classes of extensions of degree p, Israel J. Math. 138 (2003) 29–42.

[MS2] J. Mináč, J. Swallow, Galois embedding problems with cyclic quotient of order p, Israel J. Math. 145 (2005) 93–112.

[MSS1] J. Mináč, A. Schultz, J. Swallow, Galois module structure of pth-power classes of cyclic extensions of degree p^n, Proc. London Math. Soc. 92 (2006) 307–341.

[MSS2] J. Mináč, A. Schultz, J. Swallow, Automatic realizations of Galois groups with cyclic quotient of order p^n, J. Théor. Nombres Bordeaux 20 (2008) 419–430.

[Pi] R.S. Pierce, Associative Algebras, Springer-Verlag, New York, 1982.

[Ri] C. Riehm, The corestriction of algebraic structures, Invent. Math. 11 (1970) 73–98.

[Se1] J.-P. Serre, Galois Cohomology, Springer-Verlag, 1997.

[Se2] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984) 651–676.

[ST] J. Swallow, F. Thiem, Quadratic corestriction, C_2-embedding problems, and explicit construction, Comm. Algebra 30 (2002) 3227–3258.

[Ta] J. Tate, Relations between K_2 and Galois cohomology, Invent. Math. 36 (1976) 257–274.

[Ti] J.-P. Tignol, On the corestriction of central simple algebras, Math. Z. 194 (1987) 267–274.

[Wa] W.C. Waterhouse, The normal closures of certain Kummer extensions, Canad. Math. Bull. 37 (1) (1994) 133–139.