Serdica Math. J. **37** (2011), 173–210

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON REALIZABILITY OF p-GROUPS AS GALOIS GROUPS

Ivo M. Michailov, Nikola P. Ziapkov

Communicated by V. Drensky

Abstract. In this article we survey and examine the realizability of p-groups as Galois groups over arbitrary fields. In particular we consider various cohomological criteria that lead to necessary and sufficient conditions for the realizability of such a group as a Galois group, the embedding problem (i.e., realizability over a given subextension), descriptions of such extensions, automatic realizations among p-groups, and related topics.

1. Introduction: The inverse problem in Galois theory. The purpose of this article is to survey and examine the realizability of p-groups as Galois groups over arbitrary fields for any prime p. We discuss the inverse problem of Galois theory, its close relative – the embedding problem, and related topics.

Let G be a finite group, and let K be a field. The *inverse problem of Galois theory* consists of two parts:

2010 *Mathematics Subject Classification:* 12F12, 15A66.

Key words: Inverse problem, embedding problem, Galois group, p-group, Kummer extension, corestriction, orthogonal representation, Clifford algebra, spinor, modular group, dihedral group, quaternion group, Galois cohomology.

This work is partially supported by a project of Shumen University for year 2012.

1. **Existence.** Determine whether there exists a Galois extension M/K such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to G.

2. **Actual construction.** If G is realizable as a Galois group over K, construct explicitly either Galois extensions or polynomials over K having G as a Galois group.

The classical inverse problem of Galois theory is the existence problem for the field $K = \mathbb{Q}$ of rational numbers. The question whether all finite groups can be realized over $\mathbb{Q}$ is one of the most challenging problems in mathematics, and it is still unsolved.

Using the Dirichlet theorem on arithmetic progressions it is easy to construct explicitly for any positive integer n an extension of $\mathbb{Q}$ whose Galois group is cyclic of order n. This result can be extended to cover any finite abelian group. In the nineteenth century, the following deeper result was established:

Theorem 1.1 (Kronecker-Weber)**.** *Every algebraic number field whose Galois group over $\mathbb{Q}$ is abelian, is a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is an n-th root of unity for some natural number n.*

The latter theorem was first stated by Kronecker (1853) though his argument was not complete for extensions of degree a power of 2. Weber (1886) published a proof, but this had some gaps and errors that were pointed out and corrected by Neumann (1981). The first complete proof was given by Hilbert (1896). The proof can be found in most books on class field theory. In the early 20-th century Hilbert's 12-th problem on the generalization of the Kronecker-Weber Theorem gained popularity. The history of the 12-th problem is explained at lenght in [52].

The first systematic study of the inverse Galois problem started with Hilbert in 1892. Hilbert used his Irreducibility Theorem to establish the following result:

Theorem 1.2. *For any $n \geq 1$, the symmetric group S_n and the alternating group A_n occur as Galois groups over $\mathbb{Q}$.*

The first explicit examples of polynomials with the alternating group A_n as a Galois group were given by Schur [56] in 1930.

The next important step was taken in 1937 by A. Scholz and H. Reichard [54, 50] who proved the following existence result:

Theorem 1.3. *For an odd prime p, every finite p-group occurs as a Galois group over $\mathbb{Q}$.*

The final step concerning solvable groups was taken by Shafarevich [59], although with a mistake relative to the prime 2. In the notes appended to his Collected papers, p. 752, Shafarevich sketches a method to correct this. For a full correct proof, the reader is referred to the book by Neukirch, Schmidt and Wingberg [47, Chapter IX].

Theorem 1.4 (Shafarevich)**.** *Every solvable group occurs as a Galois group over* $\mathbb{Q}$.

Extensive surveys of recent developments regarding the classical inverse problem can be found in monographs such as [22, 30, 58, 68]. We will, however, concentrate on the inverse problem for p-groups over arbitrary fields.

Our paper is organized as follows. In Section 2 we discuss the cohomological approach to the embedding problem developed in such works as [18, 44, 42]. In Section 3 we present some more specific criteria concerning central embedding problems with cyclic p-kernel. In Sections 4 and 5 we discuss the quadratic corestriction homomorphism and orthogonal representations of Galois groups. There we also give proofs of some unpublished results of Michailov. In Section 6 we present some of the most significant results concerning the realizability of p-groups as Galois groups over arbitrary fields. Finally, in Section 7 we investigate automatic realizations among p-groups.

2. The embedding problem. Let k be arbitrary field and let G be a non simple group. Assume that A is a normal subgroup of G. Then the realizability of the quotient group $F = G/A$ as a Galois group over k is a necessary condition for the realizability of G over k. In this way arises the next generalization of the inverse problem in Galois theory – the embedding problem of fields.

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

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\alpha} F \longrightarrow 1, \tag{2.1}$$

be a group extension, i.e., a short exact sequence. Solving *the embedding problem* related to K/k and (2.1) consists of determining whether or not there exists a Galois algebra (called also a *weak* solution) or a Galois extension (called a *proper* solution) L, such that K is contained in L, G is isomorphic to $\mathrm{Gal}(L/k)$, and the homomorphism of restriction to K of the automorphisms from G coincides with α. We denote the so formulated embedding problem by $(K/k, G, A)$. We call the group A the *kernel* of the embedding problem.

A well known criterion for solvability is obtained by using the Galois group Ω_k of the algebraic separable closure $\bar{k}$ over k.

Theorem 2.1 [18, Theorem 1.15.1]**.** *The embedding problem $(K/k, G, A)$ is weakly solvable if and only if there exists a homomorphism $\delta : \Omega_k \to G$, such that $\alpha \cdot \delta = \varphi$, where $\varphi : \Omega_k \to F$ is the natural epimorphism. The embedding problem is properly solvable if and only if among the homomorphisms δ, there exists an epimorphism.*

Given that the kernel A of the embedding problem is abelian, another well known criterion holds. We can define an F-module structure on A by $a^\rho = \bar{\rho}^{-1} a \bar{\rho}$ ($\bar{\rho}$ is a pre-image of $\rho \in F$ in G).

Let us recall the definition of the inflation map $\inf_F^{\Omega_k} : H^2(F, A) \longrightarrow H^2(\Omega_k, A)$. Denote by $G \times_F \Omega_k$ the direct product with amalgamated quotient group F, i.e., the subgroup of the direct product $G \times \Omega_k$, containing only the elements (y, ω), such that $\alpha(y) = \varphi(\omega)$ for $y \in G$ and $\omega \in \Omega_k$. We have then the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & G \times_F \Omega_k & \xrightarrow{\beta} & \Omega_k & \longrightarrow & 1 \\ & & \| & & \psi \downarrow & & \varphi \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\alpha} & F & \longrightarrow & 1 \end{array}$$

where $\beta(y, \omega) = \omega$ and $\psi(y, \omega) = y$. The first row gives us the inflation of the second row.

Corollary 2.2 [18, Theorem 13.3.2]**.** *Let A be an abelian group and let c be the 2-coclass of the group extension (2.1) in $H^2(F, A)$. Then the embedding problem $(K/k, G,\ A)$ is weakly solvable if and only if $\inf_F^{\Omega_k}(c) = 0$*

Next, let K contain a primitive root of unity of order equal to the order of the kernel A. Then we can define the character group $\hat{A} = \mathrm{Hom}\,(A, K^*)$ and make it an F-module by ${}^\rho\chi(a) = \chi(a^\rho)^{\rho^{-1}}$, for $\chi \in \hat{A}$, $a \in A$, $\rho \in F$.

Let $\mathbb{Z}[\hat{A}]$ be the free abelian group with generators e_χ (for $\chi \in \hat{A}$). We make it an F-module by ${}^\rho e_\chi = e_{{}^\rho\chi}$. Then there exists an exact sequence of F-modules

$$0 \longrightarrow V \longrightarrow \mathbb{Z}[\hat{A}] \xrightarrow{\pi} \hat{A} \longrightarrow 0, \tag{2.2}$$

where π is defined by $\pi(\sum_i k_i e_{\chi_i}) = \prod_i \chi_i^{k_i}$ where $k_i \in \mathbb{Z}$.

We can clearly consider all F-modules as Ω_k-modules. The exact sequence (2.2) then implies the exact sequence

$$0 \longrightarrow A \cong \mathrm{Hom}(\hat{A}, \bar{k}^\times) \longrightarrow \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times) \longrightarrow \mathrm{Hom}(V, \bar{k}^\times) \longrightarrow 0.$$

Since $H^1(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times)) = 0$ (see [18, §3.13.3]), we obtain the following exact sequence

$$(2.3) \quad 0 \longrightarrow H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) \xrightarrow{\beta} H^2(\Omega_k, A) \xrightarrow{\gamma} H^2(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times)).$$

We call the element $\eta = \gamma\bar{c}$ *the (first) obstruction*. The condition $\eta = 0$ clearly is necessary for the solvability of the embedding problem $(K/k, G, A)$. This is the well-known *compatibility* condition found by Faddeev and Hasse. In general it is not a sufficient condition for solvability. Indeed if we assume that $\eta = 0$, then there appears a second obstruction, namely $\xi \in H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times))$ such that $\beta(\xi) = \bar{c}$. Thus, in order to obtain a necessary and sufficient condition we must have both $\eta = 0$ and $\xi = 0$. The second obstruction is very hard to calculate explicitly, though. That is why embedding problems for which $H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) = 0$ are of special interest. This condition turns out to be fulfilled in a number of cases.

Let us begin with the so called *Brauer problem*. The embedding problem $(K/k, G, A)$ is called *Brauer* if $\hat{A}$ is a trivial F-module. Then we have the well known.

Theorem 2.3 ([44, Theorem 3.1], [18, Theorem 3.1])**.** *The compatibility condition for the Brauer problem $(K/k, G, A)$ is necessary and sufficient for its weak solvability.*

Recently, Michailov generalized this result with the following.

Theorem 2.4 ([42, Theorem 3.2])**.** *Let A be an abelian group of order n, let the field K contain a primitive nth root of unity, and let m be an integer such that $m^2 \equiv 1 \pmod{n}$. Assume that $(K/k, G, A)$ is an embedding problem such that the action of $F = G/A$ on $\hat{A}$ satisfies the following: for any $\rho \in F$ we have either ${}^\rho\chi = \chi^m$ for all $\chi \in \hat{A}$, or ${}^\rho\chi = \chi$ for all $\chi \in \hat{A}$. Then the compatibility condition is necessary and sufficient for the weak solvability of the embedding problem $(K/k, G, A)$.*

We can easily obtain now some previously known results as corollaries from the latter theorem.

Corollary 2.5 ([44, Theorem 3.2])**.** *Let the kernel A be abelian and let ${}^\rho\chi = \chi^{\pm 1}$ for all $\chi \in \hat{A}, \rho \in F$. Then the compatibility condition is necessary and sufficient for the weak solvability of the embedding problem $(K/k, G, A)$.*

Corollary 2.6 ([18, §3.4.1],[44, Corollary 3.3])**.** *The embedding problem $(K/k, G, A)$ with a kernel A isomorphic to the cyclic group of order 4 is weakly solvable if and only if the compatibility condition is satisfied.*

Since one of the forms of the compatibility condition is that all associated Brauer problems are solvable, the above results reduce the considerations of the original embedding problem to certain associated Brauer problems. (For the definition of associated problems see [44], and for the reduction see [42]).

3. Cohomological criteria for solvability of embedding problems with cyclic kernel of order p. Let k be arbitrary field of characteristic not p, containing a primitive pth root of unity ζ, and put $\mu_p = \langle\zeta\rangle$. Let K be a Galois extension of k with Galois group F. Consider the group extension

$$1 \longrightarrow \langle\varepsilon\rangle \longrightarrow G \longrightarrow F \longrightarrow 1, \tag{3.1}$$

where ε is a central element of order p in G. We are going to identify the groups $\langle\varepsilon\rangle$ and μ_p, since they are isomorphic as F-modules.

Assume that $c \in H^2(F, \mu_p)$ is the 2-coclass corresponding to the group extension (3.1). *The obstruction* to the embedding problem $(K/k, G, \mu_p)$ we call the image of c under the inflation map $\inf_F^{\Omega_k} : H^2(F, \mu_p) \to H^2(\Omega_k, \mu_p)$.

Note that we have the standard isomorphism of $H^2(\Omega_k, \mu_p)$ with the p-torsion in the Brauer group of k induced by applying $H^*(\Omega_k, \cdot)$ to the p-th power exact sequence of Ω_k-modules $1 \longrightarrow \mu_p \longrightarrow \bar{k}^\times \longrightarrow \bar{k}^\times \longrightarrow 1$. In this way, the obstruction equals the equivalence class of the crossed product algebra $(F, K/k, \bar{c})$ for any $\bar{c} \in c$. Hence we may identify the obstruction with a Brauer class in $\mathrm{Br}_p(k)$.

Note that we have an injection $\mu_p \hookrightarrow K^\times$, which induces a homomorphism $\nu : H^2(F, \mu_p) \to H^2(F, K^\times)$. Then the obstruction is equal to $\nu(c)$, since there is an isomorphism between the relative Brauer group $\mathrm{Br}(K/k)$ and the group $H^2(F, K^\times)$.

Clearly, the problem $(K/k, G, \mu_p)$ is Brauer, so from the proof of Theorem 2.3 given in the paper [44] it follows that $H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) = 0$. Hence the homomorphism $\gamma : H^2(\Omega_k, A) \to H^2(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times))$ is an injection. Therefore, the problem is solvable if and only if the (first) obstruction is split.

More generally, the following result holds.

Theorem 3.1. *[25] Let c be the 2-coclass in $H^2(F, \mu_p)$, corresponding to the group extension* (3.1)*. Then the embedding problem $(K/k, G, \mu_p)$ is properly solvable if and only if $\nu(c) = 1$. If $K(\sqrt[p]{\beta})/k$ is a solution to the embedding problem for some $\beta \in K^\times$, then all solutions are of the kind $K(\sqrt[p]{f\beta})/k$, for $f \in k^\times$.*

Henceforth, embedding problems of the kind $(K/k, G, \mu_p)$ we will call for short μ_p-embedding problems. An abstract description of the solutions to the μ_p-embedding problems is given by Swallow in [63] and in a more concise form in [65, Theorem 4].

From the well-known Merkurjev-Suslin Theorem [34] it follows that the obstruction to any μ_p-embedding problem is equal to a product of classes of p-cyclic algebras. The explicit computation of these p-cyclic algebras, however, is not a trivial task. We are going to discuss the methods for achieving this goal.

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).

In 1987 Massy [32] obtained a formula for the decomposition of the obstruction in the case when $F = \mathrm{Gal}(K/k)$ is isomorphic to $(C_p)^n$, the elementary abelian p-group.

Theorem 3.2 ([32, Théorème 2])**.** *Let $K/k = k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \ldots, \sqrt[p]{a_n})/k$ be a $(C_p)^n$ extension, and let $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathrm{Gal}(K/k)$ be given by $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}$ (δ_{ij} is the Kronecker delta). Let*

$$1 \longrightarrow \mu_p \longrightarrow G \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$$

be a non split central extension, and choose pre-images $s_1, s_2, \ldots, s_n \in G$ of $\sigma_1, \sigma_2, \ldots, \sigma_n$. Define $d_{ij} (i \leq j)$ by $s_i^p = \zeta^{d_{ii}}$ and $s_i s_j = \zeta^{d_{ij}} s_j s_i (i < j)$. Then the obstruction to the embedding problem $(K/k, G, \mu_p)$ is

$$\prod_{i=1}^{n} (a_i, \zeta; \zeta)^{d_{ii}} \prod_{i<k} (a_i, a_k; \zeta)^{d_{ik}}.$$

In 1996 Swallow [64] described explicitly the solutions of μ_p-embedding problems with $F \cong (C_p)^n$.

In 2001 Quer [49] found necessary and sufficient conditions for solvability of the μ_p-embedding problem with an abelian quotient group F. The conditions are in terms of the existence of elements with certain norm properties. They appear in the theory of elliptic $\mathbb{Q}$-curves discussed in the same paper.

In 2007 Michailov [39] obtained a formula for the decomposition of the obstruction in the case when F has a direct factor C_p for an odd p. The same is done in [37] for $p = 2$. We are now going to formulate these results in a unified way.

Let H be a p-group and let

$$1 \longrightarrow \mu_p \longrightarrow G \xrightarrow{\pi} F \cong H \times C_p \longrightarrow 1 \tag{3.2}$$

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

$$1 \longrightarrow \mu_p \longrightarrow \pi^{-1}(H) \xrightarrow{\pi} H \longrightarrow 1.$$

Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a minimal generating set for the maximal elementary abelian quotient group 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 $i \in \{1, 2, \ldots, m\}; j, d_i \in \{0, 1, \ldots, p-1\}$.

Theorem 3.3 ([37, Theorem 4.1],[39, Theorem 2.1])**.** *Let K/k be a Galois extension with Galois group H and let $L/k = K(\sqrt[p]{b})/k$ be a Galois extension with Galois group $H \times C_p$ ($b \in k^\times \setminus k^{\times p}$). Choose $a_1, a_2, \ldots, a_m \in k^\times$, 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 $(L/k, G, \mu_p)$ is*

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

Ledet describes in his book [29] a more general formula for the decomposition of the obstruction of μ_p-embedding problems with finite group F isomorphic to a direct product of two groups.

Let G be arbitrary finite group, and let p be a prime divisor of $\mathrm{ord}(G)$. Define $\mathcal{O}^p(G)$ as the subgroup of G generated by all elements of order prime to p. It is clear that $\mathcal{O}^p(G)$ is the intersection of all normal subgroups in G of p-power index.

Theorem 3.4 ([29, Theorem 6.1.4]**.** *Let L/k be a $N \times H$ extension, where N and H are finite groups. Let*

$$1 \longrightarrow \mu_p \longrightarrow G \longrightarrow N \times H \longrightarrow 1$$

be a non split central group extension with cohomology class $\gamma \in H^2(N \times H, \mu_p)$. Let K'/k and K/k be the subextensions corresponding to the factors N and H. (I.e., $K' = L^H, K = L^N$.) Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ and $\tau_1, \tau_2, \ldots, \tau_n$ represent minimal generating sets for the groups $N/\mathcal{O}^p(N)$ and $H/\mathcal{O}^p(H)$, and choose $a_1, a_2, \ldots, a_m, b_1, \ldots b_n \in k^\times$, such that $\sqrt[p]{a_i} \in K^\times$, $\sqrt[p]{b_i} \in K'^\times, \sigma_\kappa \sqrt[p]{a_i} = \zeta^{\delta_{i\kappa}} \sqrt[p]{a_i}$

and $\tau_\ell \sqrt[p]{b_i} = \zeta^{\delta_{i\ell}} \sqrt[p]{b_i}$ *(δ is the Kronecker delta). Finally, let* $s_1, \dots, s_m; t_1, \dots, t_n \in G$ *be the pre-images of* $\sigma_1, \dots, \sigma_m; \tau_1, \dots, \tau_n$*, and let* $d_{ij} \in \{0, \dots, p-1\}$ *be given by* $t_j s_i = \zeta^{d_{ij}} s_i t_j$*.*

Then the obstruction to the embedding problem $(L/k, G, \mu_p)$ *given by* γ *is*

$$[K, N, \mathrm{res}_N \gamma] \cdot [K', H, \mathrm{res}_H \gamma] \cdot \prod_{i,j} (b_j, a_i; \zeta)^{d_{ij}}.$$

There are many groups, however, which do not fit in the conditions of the results listed above, so more criteria are needed. The corestriction homomorphism $\mathrm{cor}_{F/H} : H^*(H, \cdot) \to H^*(F, \cdot)$ appears to be one of the strongest tools in the case when F is not a direct product of smaller groups (H is a properly chosen subgroup of F). In [51] is given an analogue of the corestriction homomorphism, acting on central simple algebras. Given a Galois extension K_1/k of degree p, we have the corestriction homomorhpism between the Brauer groups $\mathrm{cor}_{K_1/k} : \mathrm{Br}(K_1) \longrightarrow \mathrm{Br}(k)$. Further, we denote by Ω_k the Galois group of the separable closure of k over the field k, and by Ω_{K_1} the subgroup of Ω_k, leaving K_1 fixed. Then we also have the corestriction $\mathrm{cor}_{\Omega_k/\Omega_{K_1}} : H^2(\Omega_{K_1}, \mu_p) \longrightarrow H^2(\Omega_k, \mu_p)$. Riehm shows in [51, Theorem 11] that the following commutative diagram holds:

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

In this way one can easily see that the obstruction to the corestricted embedding problem is equal to the corestriction of the obstruction to the original problem. In order to apply the corestriction homomorphism in the calculations, we need a formula for the corestriction of p-cyclic algebras. Tignol gave in [67] a detailed proof of the so-called *projection formula*: for $b \in k^\times \setminus k^{\times p}$ and $\delta \in K_1$ we have $\mathrm{cor}_{K_1/k}(\delta, b; \zeta)_{K_1} = (N_{K_1/k}(\delta), b; \zeta)_k$. There are some cases, however, when the projection formula is not enough. Swallow and Thiem found in [65] the following general formula for the quadratic corestriction homomorphism.

Proposition 3.5 ([65, Proposition 4]). *Let* $a \in k^\times, K = k(\sqrt{a}), \alpha_0 = a_0 + b_0\sqrt{a}$ *and* $\alpha_1 = a_1 + b_1\sqrt{a}$ *($a_i, b_i \in k$). Then*

(1) *If* $b_{1-i} = 0$*, then* $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0, \alpha_1)_K = (a_{1-i}, a_i^2 - ab_i^2)_k$*;*

(2) *If* $a_{1-i}b_i - a_i b_{1-i} = 0$*, then* $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0, \alpha_1)_K = (-a_i a_{1-i}, a_i^2 - ab_i^2)_k$*;*

(3) *Otherwise,*
$\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0,\alpha_1)_K = (a_0^2-ab_0^2, b_0(a_1b_0-a_0b_1))_k(a_1^2-ab_1^2, b_1(a_0b_1-a_1b_0))_k$.

Next, we are going to describe a situation which sometimes occurs, when a certain group extension can be constructed from other group extension by lowering or raising the order of one of its generators.

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 these 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

$$1 \longrightarrow \mu_p \longrightarrow G_1 \xrightarrow{\varphi} G \longrightarrow 1 \tag{3.3}$$

and

$$1 \longrightarrow \mu_p \longrightarrow G_2 \xrightarrow{\psi} G \longrightarrow 1. \tag{3.4}$$

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, $i = 1,\dots k$.

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 following theorem, proved by Michailov [41], gives us the connection between the obstructions of the two embedding problems related to (3.3) and (3.4).

Theorem 3.5 ([41, 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* (3.3) *and* (3.4) *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* $1 \longrightarrow \mu_p \longrightarrow C_{p^n} \longrightarrow G/H \cong C_{p^{n-1}} \longrightarrow 1$. *Then the relation between these obstructions is given by*

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

In the following two sections we will focus on some specific criteria related to the applications of the quadratic corestriction homomorphism for μ_2-embedding problems.

4. The quadratic corestriction homomorphism. Let G be a finite group and let H be an index 2 subgroup of G. Then we can define the quadratic corestriction homomorphism $\mathrm{cor}_{G/H} : H^*(H, \cdot) \to H^*(G, \cdot)$. One way of computing the quadratic corestriction is by applying the formula of Tate [66], which in our case takes the form displayed in the following

Lemma 4.1 ([66])**.** *Let* G *be a finite group, let* H *be a subgroup of index* 2 *in* G, *let* $g \in G \setminus H$ *and let* $\bar{f} \in Z^2(H, \mu_2)$ *be arbitrary* 2*-cocycle. Define a map* $f : G \times G \longrightarrow \mu_2$ *by:*

$$f(s_1, s_2) = \begin{cases} \bar{f}(s_1, s_2)\bar{f}(gs_1g^{-1}, gs_2g^{-1}), & if\ (s_1, s_2) \in H \times H \\ \bar{f}(s_1g^{-1}, gs_2g^{-1})\bar{f}(gs_1, s_2), & if\ (s_1, s_2) \in Hg \times H \\ \bar{f}(s_1, s_2g^{-1})\bar{f}(gs_1g^{-1}, gs_2), & if\ (s_1, s_2) \in H \times Hg \\ \bar{f}(s_1g^{-1}, gs_2)\bar{f}(gs_1, s_2g^{-1}), & if\ (s_1, s_2) \in Hg \times Hg. \end{cases}$$

Then $f \in Z^2(G, \mu_2)$ *and* $[f] = \mathrm{cor}_{G/H}([\bar{f}])$, *where* $[f] \in H^2(G, \mu_2)$ *and* $[\bar{f}] \in H^2(H, \mu_2)$ *are the* 2*-coclasses of* f *and* $\bar{f}$, *respectively.*

With the aid of Lemma 4.1 we can construct some corestricted group extensions and thus solve the related μ_2-embedding problems which can not be treated with the cohomological criteria given in Section 3. However, Lemma 4.1 does not provide us with the answer of the important question whether a given group extension is a corestricted group extension, i.e., lies in the image of $\mathrm{cor}_{G/H}$ for some subgroup H of G. In what follows, we will describe a construction which will help us relatively easy to recognize the corestricted group extensions.

Let $\mathcal{G}$ be a finite 2-group and let E_4 be a normal subgroup of $\mathcal{G}$, isomorphic to the elementary abelian group of order 4 with generators σ and τ. Assume, furthermore, that there exists a 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 $\tau^g = \sigma\tau$. In these notations, it holds

Theorem 4.2 ([41, Theorem 3.8])**.** *Let $c_1 \in H^2(G, \mu_2)$ be the 2-coclass, represented by the group extension $1 \longrightarrow E_4/\langle\sigma\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle\sigma\rangle \longrightarrow G \longrightarrow 1$, let $c_2 \in H^2(H, \mu_2)$ be the 2-coclass, represented by the group extension $1 \longrightarrow E_4/\langle\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\tau\rangle \longrightarrow H \longrightarrow 1$, and let $c_3 \in H^2(H, \mu_2)$ be the 2-coclass, represented by the group extension $1 \longrightarrow E_4/\langle\sigma\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\sigma\tau\rangle \longrightarrow H \longrightarrow 1$. Then $\mathrm{cor}_{G/H}(c_2) = \mathrm{cor}_{G/H}(c_3) = c_1$.*

In order to verify whether a given group extension is corestricted from some other group extension, we can try to construct the group $\mathcal{G}$, having the properties given above Theorem 4.2. If we obtain defining relations that are not contradictory, then we have reached our goal. This is done for instance in [41, Section 5]. On the other hand, if we are not able to do that, it is highly probable that the group extension is not a corestriction. In that case we can use Proposition 4.4, given below, in order to prove such a supposition.

In the statements of the following results we use the standard notations: $\mathrm{ord}(g)$ is the order of $g \in G$; $\exp(G)$ is the exponent of the group G, i.e., $\exp(G) = \mathrm{lcm}\{\mathrm{ord}(g) : g \in G\}$. Clearly, when G is a 2-group, the exponent is equal to the highest order of an element from G.

Lemma 4.3. *Let*

$$1 \longrightarrow \mu_2 = \{\pm 1\} \longrightarrow Y \xrightarrow{\ \alpha\ } Z \longrightarrow 1,$$

be a group extension of 2-groups, represented by the 2-cocycle $f \in Z^2(Z, \mu_2)$. Let $z \in Z, \mathrm{ord}(z) = k > 1$ and let $y \in Y$ be arbitrary preimage of z in Y. Then

$$f(z^{k/2}, z^{k/2}) = \begin{cases} 1, & if\ \mathrm{ord}(y) = k \\ -1, & if\ \mathrm{ord}(y) = 2k. \end{cases}$$

Proof. As we know, the 2-cocycle $f \in Z^2(Z, \mu_2)$ is defined by a set $\{u_x\}_{x\in Z} \subset Y$ in this way: $u_x u_y = u_{xy} f(x, y)$ with the natural condition $u_1 = 1, f(1, *) = f(*, 1) = 1$. Let y and z be such as in the statement. We may assume that $y = u_z$. Clearly $y^{k/2} = \pm u_{z^{k/2}}$, so $y^k = y^{k/2} y^{k/2} = u_{z^{k/2}} u_{z^{k/2}} = u_{z^k} f(z^{k/2}, z^{k/2}) = f(z^{k/2}, z^{k/2})$. Since $\alpha(y^k) = z^k = 1$, $y^k = \pm 1$ and we are done. □

Proposition 4.4. *Let G be a 2-group, let H be a subgroup of index 2 in G and let $g \in G \setminus H$. Further, let $\bar{f} \in Z^2(H, \mu_2)$ correspond to the group extension*

$$1 \longrightarrow \mu_2 = \{\pm 1\} \longrightarrow H_2 \xrightarrow{\beta} H \longrightarrow 1,$$

and let $f \in Z^2(G, \mu_2)$ correspond to the group extension

$$1 \longrightarrow \mu_2 = \{\pm 1\} \longrightarrow G_1 \xrightarrow{\alpha} G \longrightarrow 1,$$

such that $[f] = \mathrm{cor}_{G/H}([\bar{f}])$. Put $H_1 = \alpha^{-1}(H)$. Then the following conditions hold:

(1) $\exp(H_1) \leq \exp(H_2)$*;*

(2) *If for all $h \in H$ from $\mathrm{ord}(h) = \exp(H)$ follows that $ghg^{-1} \in \langle h \rangle$, then $\exp(H_1) = \exp(H)$.*

P r o o f. (1). If $\exp(H_1) = \exp(H)$, the inequality clearly holds. Now, let $\exp(H_1) > \exp(H)$. Denote $k_1 = \exp(H_1)$ and $k = \exp(H)$. Then $k_1 = 2k$ and there exists $h_1 \in H_1$ such that $\mathrm{ord}(h_1) = k_1$. Also, for $h = \alpha(h_1)$ we have $\mathrm{ord}(h) = k$. From Lemma 4.3 follows that $f(h^{k/2}, h^{k/2}) = -1$.

If $\exp(H_2) > \exp(H)$, then $\exp(H_2) = \exp(H_1) = k_1$. Now, suppose $\exp(H_2) = \exp(H) = k$. Then there exists $h_2 \in H_2$ such that $\beta(h_2) = h$ and $\mathrm{ord}(h_2) = k$. Therefore $\bar{f}(h^{k/2}, h^{k/2}) = 1$. Next, consider the element ghg^{-1}, which obviously has the same order k, and arbitrary preimage $h_2' = \beta^{-1}(ghg^{-1})$. Then $\mathrm{ord}(h_2') = k = \exp(H_2)$ and from Lemma 4.3 follows that $\bar{f}(gh^{k/2}g^{-1}, gh^{k/2}g^{-1}) = 1$. Finally, from Lemma 4.1 we obtain $f(h^{k/2}, h^{k/2}) = \bar{f}(h^{k/2}, h^{k/2})\bar{f}(gh^{k/2}g^{-1}, gh^{k/2}g^{-1}) = 1$, which is a contradiction.

(2). Let $h \in H$ be of order $k = \exp(H)$. Then $ghg^{-1} = h^l$ for some odd l. From Lemma 4.3 follows that

$$\bar{f}(h^{k/2}, h^{k/2}) = \bar{f}((h^l)^{k/2}, (h^l)^{k/2}) = \bar{f}(gh^{k/2}g^{-1}, gh^{k/2}g^{-1}),$$

so $f(h^{k/2}, h^{k/2}) = 1$. Therefore any preimage of h in H_1 will have order k. We are done. □

The non abelian 2-groups having a cyclic subgroup of index 2 are frequently discussed in various researches devoted to Galois theory. For $n > 3$, there are four such groups of order 2^n with exactness up to an isomorphism (see for example [17]): Q_{2^n} (the quaternion group), D_{2^n} (the dihedral group)[1], SD_{2^n}

[1]We prefer to denote by D_{2m} the dihedral group of order $2m$, rather than order m, to avoid any confusion with the notations for the remaining groups.

(the semidihedral or quasidihedral group) and M_{2^n} (the modular group). These groups are generated by two elements σ and τ. We list their presentations:

$$\begin{aligned} D_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle \\ SD_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{2^{n-2}-1}\tau \rangle \\ Q_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = 1, \tau^2 = \sigma^{2^{n-2}}, \tau\sigma = \sigma^{-1}\tau \rangle \\ M_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{2^{n-2}+1}\tau \rangle. \end{aligned}$$

If we suppose that the ground field contains enough roots of unity (e.g. 2^{n-2}-th roots of unity), the obstructions to the μ_2-embedding problems related to these groups are precisely calculated (see [7] for the dihedral and quaternion groups, and [40] for the modular group). On the other hand, if we relax the condition on the roots of unity even a little bit, the calculations become very difficult. Michailov calculated the obstructions to certain embedding problems with cyclic kernel in [35, 37] under some specific requirements for the roots of unity. If we have no requirements for the roots of unity it is not known how to decompose the obstructions as products of quaternion algebras for $n \geq 6$. That is why it is important to know whether these groups can be constructed via a corestriction. Unfortunately, as we will see, the answer is negative.

Note that the centre of $Q_{2^n}, D_{2^n}, SD_{2^n}$ is $\langle \sigma^{2^{n-2}} \rangle$, and the centre of M_{2^n} is $\langle \sigma^2 \rangle$. Observe that if $G_1 \cong Q_{2^n}, D_{2^n}$ or SD_{2^n} then $G \cong D_{2^{n-1}}$, and if $G_1 \cong M_{2^n}$, then $G \cong C_{2^{n-2}} \times C_2$. In particular we see that $\exp(G_1) = 2^{n-1}$ and $\exp(G) = 2^{n-2}$.

Proposition 4.5. *The non abelian groups of order 2^n ($n > 3$), having a cyclic subgroup of order 2^{n-1}, can not be constructed via a corestriction homomorphism.*

P r o o f. Assume that G_1 is one of these groups of order 2^n that can be construted via a corestriction. Namely, let

$$1 \longrightarrow \langle \sigma^{2^{n-2}} \rangle \cong \mu_2 \longrightarrow G_1 \xrightarrow{\alpha} G \longrightarrow 1,$$

be a group extension corresponding to a 2-cocylce $f \in H^2(G, \mu_2)$ such that $[f] = \mathrm{cor}_{G/H}([\bar{f}])$ for a subgroup $H < G$ of index 2. Write as usual $H_1 = \alpha^{-1}(H)$. There are several possibilities for H_1 and $H = \alpha(H_1)$: $H_1 = \langle \sigma \rangle \cong C_{2^{n-1}}$ and $H = H_1/\langle \sigma^{2^{n-2}} \rangle \cong C_{2^{n-2}}$; or $H_1 = \langle \sigma^2, \tau \rangle \cong D_{2^{n-1}}, Q_{2^{n-1}}, C_{2^{n-2}} \times C_2$ and $H = H_1/\langle \sigma^{2^{n-2}} \rangle \cong D_{2^{n-2}}, C_{2^{n-3}} \times C_2$. In all possibilities, however, the inequality $\exp(H_1) > \exp(H)$ holds.

Now, if $H \cong C_{2^{n-2}}$ or $D_{2^{n-2}}$ and $h \in H$ is an element of maximal order, then all elements of maximal orders are in $\langle h \rangle$. Indeed, in the dihedral groups

we have the relations $(\sigma^s\tau)^2 = 1$ for all s, so the elements of maximal orders are only of this kind: σ^l for an odd l. From Proposition 4.4 (2) follows then that $\exp(H_1) = \exp(H)$, a contradiction.

Finally, if $H \cong C_{2^{n-3}} \times C_2$ then $G \cong C_{2^{n-2}} \times C_2$ and all elements from G commute with the elements from H. Then form Proposition 4.4 (2) again follows that $\exp(H_1) = \exp(H)$, which again is a contradiction. □

5. Orthogonal representations of Galois groups. We begin with some preliminaries about orthogonal representations. Let k be a field of characteristic $\neq 2$, let V be a finite-dimensional k-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 $\mathrm{GL}_k(V)$, called *the orthogonal group* of q. *An orthogonal representation* of a finite group G is then a homomorphism $\mu : G \longrightarrow O(q)$ 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 $\mu : G \hookrightarrow O(q)$.

We adopt the notations about Clifford algebras used in [29, Ch. 5, S. 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

$$1 \longrightarrow k^\times \longrightarrow C^\times(q) \xrightarrow{r} O(q) \longrightarrow 1,$$

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

$$1 \longrightarrow k^\times \longrightarrow C_0^\times(q) \xrightarrow{r} SO(q) \longrightarrow 1.$$

Denote by ι the principal involution on $C(q)$, which preserves the scalars, sums and vectors, and reverses products. Denote by $N : C^\times(q) \longrightarrow k^\times$ the norm given by $N(x) = x\iota(x)$, and by $sp : O(q) \longrightarrow k^\times/2$ the spinor norm given by $sp(T_v) = \overline{q(v)}$. Put $\mathrm{Pin}(q) = \ker(N), \mathrm{Spin}(q) = \mathrm{Pin}(q) \cap C_0^\times(q)$.

Hence, we have the long exact sequences

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(q) \xrightarrow{r} O(q) \xrightarrow{sp} k^\times/2$$

and

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(q) \xrightarrow{r} SO(q) \xrightarrow{sp} k^\times/2.$$

If we take the separable closure $\bar{k}$ of k, we get the short exact sequences

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\bar{q}) \xrightarrow{r} O(\bar{q}) \longrightarrow 1 \tag{5.1}$$

and

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\bar{q}) \xrightarrow{r} SO(\bar{q}) \longrightarrow 1. \tag{5.2}$$

Proposition 5.1. *Let G and $H \leq G$ be as in the definitions above Theorem 3.5 for $p = 2$. Let $\varphi : G/H \longrightarrow \bar{k}^{\times}$ be the homomorphism induced by the isomorphism $G/H \cong \langle \zeta_{2^{n-1}} \rangle$ and the inclusion $\langle \zeta_{2^{n-1}} \rangle \hookrightarrow \bar{k}^{\times}$, where $\zeta_{2^{n-1}}$ is a primitive 2^{n-1}th root of unity. Assume that is given an orthogonal representation $G \hookrightarrow O(q)$, and take the restriction $1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$ of $1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\bar{q}) \longrightarrow O(\bar{q}) \longrightarrow 1$. Then there exists a subgroup $\bar{G}$ of $C^{\times}(\bar{q})$, such that*

(1) *The diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \bar{G} & \xrightarrow{r'} & G & \longrightarrow & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow \varphi & & \\ 1 & \longrightarrow & 1 & \longrightarrow & \bar{k}^{\times} & = & \bar{k}^{\times} & \longrightarrow & 1 \end{array}$$

is commutative with exact rows, where N is the norm and r' is the restriction of $r : C^{\times}(\bar{q}) \longrightarrow O(\bar{q})$ on $\bar{G}$;

(2) *Either $\bar{G} = \widetilde{G}^{(2^n,\sigma_1)}$, or $\widetilde{G} = \bar{G}^{(2^n,\sigma_1)}$.*

Proof. Choose and fix preimages $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_\kappa \in \widetilde{G}$ of the generators $\sigma_1, \ldots, \sigma_\kappa$ of G. Next, let $\bar{G}$ be the subgroup of $C^{\times}(\bar{q})$, generated by the elements $\bar{\sigma}_1 = \tilde{\sigma}_1\zeta_{2^n}, \bar{\sigma}_2 = \tilde{\sigma}_2, \ldots, \bar{\sigma}_\kappa = \tilde{\sigma}_\kappa$. We will show that $\bar{G}$ satisfies the conditions (1) and (2).

First, we will see that $\ker(r') \cong \mu_2$. Choose arbitrary x from $\ker(r')$, i.e., $x = \prod \bar{\sigma}_1^{i_1}\bar{\sigma}_2^{i_2}\cdots\bar{\sigma}_\kappa^{i_\kappa}$ and $r'(x) = \prod \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_\kappa^{i_\kappa} = 1$. Since $\sigma_1^{i_1} \notin H$ for $1 \leq i_1 < 2^{n-1}$, we get $i_1 \equiv 0 \pmod{2^{n-1}}$. Whence $x = \pm\bar{\sigma}_2^{i_2}\cdots\bar{\sigma}_\kappa^{i_\kappa} = \pm\tilde{\sigma}_2^{i_2}\cdots\tilde{\sigma}_\kappa^{i_\kappa} \in \ker(r) \cong \mu_2$, where by r we denote also the restriction of r on $\mathrm{Pin}(\bar{q})$.

Next, $N(\bar{\sigma}_1) = N(\tilde{\sigma}_1)\zeta_{2^n}^2 = \zeta_{2^{n-1}} = \varphi r'(\bar{\sigma}_1)$ and $N(\bar{\sigma}_i) = \varphi r'(\bar{\sigma}_i) = 1$ for $i = 2, \ldots, k$. Therefore, the diagram in the statement indeed is commutative and with exact rows.

Finally, we have either $|\tilde{\sigma}_1| = 2^{n-1}$, or $\tilde{\sigma}_1^{2^{n-1}} = -1$. If $|\tilde{\sigma}_1| = 2^{n-1}$, we have $\bar{\sigma}_1^{2^{n-1}} = \zeta_{2^n}^{2^{n-1}} = -1$, and since the remaining relations between the generators of

$\widetilde{G}$, respectively of $\bar{G}$, are identical, we see that $\bar{G} = \widetilde{G}^{(2^n,\sigma_1)}$. If $\tilde{\sigma}_1^{2^{n-1}} = -1$, we have $\bar{\sigma}_1^{2^{n-1}} = 1$, so $\widetilde{G} = \bar{G}^{(2^n,\sigma_1)}$. □

We will look now at the double covers of the symmetric group S_n. Let L/k be a Galois extension with Galois group G, and assume that L is the splitting field over k of an irreducible polynomial $f(x) \in k[x]$ of degree n. We can then embed G transitively into S_n by considering the elements of G as permutations of the roots of $f(x)$. Consider the 'positive' double cover

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n^+ \longrightarrow S_n \longrightarrow 1,$$

where transpositions lift to elements of order 2, and the 'negative' double cover

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n^- \longrightarrow S_n \longrightarrow 1,$$

where the transpositions lift to elements of order 4 (in both cases products of two disjoint transpositions lift to elements of order 4). Take now the restrictions

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G}^+ \longrightarrow G \longrightarrow 1,$$

and

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G}^- \longrightarrow G \longrightarrow 1,$$

of the 'positive' and, respectively, the 'negative' double covers of S_n.

Corollary 5.2. *Under the above notations, assume that G contains a transposition. Then $\widetilde{G}^- = \widetilde{G}^{+(4,\sigma_1)}$ and the relation between the obstructions of the related embedding problems is given by $O_{\widetilde{G}^-} = (-1, d_f)O_{\widetilde{G}^+}$, where d_f is the discriminant of $f(x)$.*

P r o o f. Denote by σ_1 any transposition from G, and by H the subgroup $G \cap A_n$ of G. Choose a set of generators $\sigma_2, \ldots, \sigma_\kappa$ for H, so $\sigma_1, \sigma_2, \ldots, \sigma_\kappa$ are generators for G. Then pick their preimages $\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_k$ in $\widetilde{G}^+$. Since $\widetilde{G}^+$ is in $\mathrm{Pin}_n(\bar{k})$ (see [29]) and $\sigma_1^2 = \tilde{\sigma}_1^2 = 1$, we can make use of Proposition 5.1. Whence we can define a subgroup $\bar{G} = \widetilde{G}^{+(4,\sigma_1)}$ of $C_n^\times(\bar{k})$, generated by $\bar{\sigma}_1 = \tilde{\sigma}_1 i, \bar{\sigma}_2 = \tilde{\sigma}_2, \ldots, \bar{\sigma}_\kappa = \tilde{\sigma}_\kappa$ (i is the imaginary unity). Now, from $\bar{\sigma}_1^2 = -1$ follows that each transposition from G lifts to an element of order 4 in $\bar{G}$. Indeed, if σ is another transposition in G, then $\sigma = \sigma_1\tau$ for $\tau \in H$, so we can choose preimage $\bar{\sigma} = \bar{\sigma}_1\bar{\tau} = i\tilde{\sigma}_1\bar{\tau} \in \bar{G}$, where $\bar{\tau}$ is also in $\widetilde{G}^+$, and $\mathrm{ord}(\tilde{\sigma}_1\bar{\tau}) = 2$. Therefore, $\bar{\sigma}^2 = -1$ and $\bar{G} \cong \widetilde{G}^-$.

Finally, from $\sigma_1(\sqrt{d_f}) = -\sqrt{d_f}$ we obtain the relation between the obstructions, given in the statement. □

Now, let us recall the definition of Galois twist, which involves the existence of the first cohomological group $H^1(G, \mathcal{G})$, where $\mathcal{G}$ is non abelian group with a G-action. Assume again that (V, q) is a quadratic space over k, and that K/k is a Galois extension with Galois group G. Then we can extend the scalars to get a quadratic space (V_K, q_K). The semi-linear action of G then gives us the equation $q_K(\sigma u) = \sigma q_K(u)$. Conversely, if (W, Q) is a quadratic space over K endowed with a semi-linear action such that $Q(\sigma u) = \sigma Q(u)$ is satisfied, we obtain a quadratic space (W^G, Q^G) over k by taking fixed points and restricting Q. These two operations (scalar extension and fixed points) preserve regularity and are each others inverses. Also, $O(Q)$ is a G-group by conjugation: $(\sigma\varphi)(u) = \sigma\varphi(\sigma^{-1}u)$.

Next, let $f : G \to O(q_K)$ be a crossed homomorphism. Then we can define a semi-linear action by ${}^{\sigma}u = f_\sigma(\sigma u)$ and get an induced quadratic space $(V_f, q_f) = ((V_K)^G, (q_K)^G)$ over k. Furthermore, if g is equivalent to f, i.e., $g_\sigma = \varphi f_\sigma \sigma \varphi^{-1}$ for some $\varphi \in O(q_K)$, then $V_g = \varphi(V_f)$, and consequently (V_f, q_f) and (V_g, q_g) are equivalent. Hence, to each element in $H^1(G, O(q))$ we can associate an equivalence class of quadratic spaces over k.

The quadratic space (V_f, q_f) is said to arise from (V, q) by taking the *Galois twist* with respect to f.

Define the element

$$\mathrm{hw}(q) = \prod_{i<j}(a_i, a_j) \in \mathrm{Br}(k),$$

where $a_i = q(u_i)$ for some canonical orthogonal basis $u_1, \ldots, u_n$ of q. Clearly, $\mathrm{hw}(q)$ depends only on the equivalence class of q. It is called the *Hasse-Witt invariant* or the *second Stiefel-Whitney class* of q.

The obstruction now can be calculated by the formula, displayed in the following.

Theorem 5.3 ([7, 29])**.** *Let L/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$ and assume $G \hookrightarrow O(q)$ for some regular quadratic form q over k. Let $e : \mathrm{Gal}(\overline{k}/k) \to O(q)$ be the induced crossed homomorphism, and let q_e be the Galois twist of q by e. Also, let*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

be the group extension induced by $G \hookrightarrow O(q)$ and the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\overline{q}) \xrightarrow{r} O(\overline{q}) \longrightarrow 1.$$

Let $K/k = k(\sqrt{a_1}, \ldots, \sqrt{a_r})/k$ be the maximal elementary abelian 2-subextension of L/k, and let $\rho_1, \ldots, \rho_r \in G$ be such that $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}} \cdot \sqrt{a_j}$. Then the

obstruction to the embedding problem $(L/k, \widetilde{G}, \mu_2)$ *is*

$$\mathrm{hw}(q)\mathrm{hw}(q_e)(d, -d_e)\prod_{i=1}^{r}(a_i, sp(\rho_i)) \in \mathrm{Br}(k),$$

where d *and* d_e *are discriminants of* q *and* q_e*, repectively.*

Now, let L/k 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 k. Then, according to [7, 8], 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 $V_q : V_{\mathrm{ind}\mu} = \oplus(V_q \otimes \sigma) = V_q \otimes_{kH} kG$, 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. [9, §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

$$g \cdot (w_\sigma \otimes \sigma) = hw_\sigma \otimes \tau \quad \text{if } g\sigma = \tau h \ (\tau \in R). \tag{5.3}$$

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

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

where as usual $\mu_2 = \{\pm 1\}$ and $1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$ is the restriction of $1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\bar{q}) \longrightarrow SO(\bar{q}) \longrightarrow 1$. The induced orthogonal representation

$\mathrm{ind}\mu : G \hookrightarrow O(q_{\mathrm{ind}\mu})$, in its turn, gives us the diagram

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

Recently, Michailov [40] proved the following.

Theorem 5.4 ([40, Theorem 2.2])**.** *Let G be a finite group, and let H be a subgroup of G, such that $|H| = 2^t m, (t, m \geq 1)$. Let also $\mu : H \hookrightarrow SO(q)$ be an orthogonal representation over k with an underlying module V_q, such that $n = \dim_k V_q \equiv 0 \pmod 4$. 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 $1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$ and $1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$, respectively. Then $[f] = \mathrm{cor}_{G/H}([\bar{f}])$, where $\mathrm{cor}_{G/H} : H^2(H, \mu_2) \longrightarrow H^2(G, \mu_2)$ is the corestriction map.*

Now, assume again that L/k is a normal and separable extension with a finite Galois group G. We can always find a primitive element θ such that $L = k(\theta)$. Let $f(x) \in k[x]$ be the minimal polynomial of θ of degree $n = [L : k]$, 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 $\kappa = (G : H) = n/m$. 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

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1, \tag{5.4}$$

which is the restriction of the group extension

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

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

Next, recall that for the quadratic form $q_1 = \langle 1, \ldots, 1 \rangle$ on $V_1 = k^m$ we have that S_m embeds in $O_m(k) = O(q_1)$, so we get an orthogonal representation $H \hookrightarrow O_m(k)$. Set $q = q_1 \perp q_2 \perp \cdots \perp q_\kappa$ and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_\kappa$,

where $q_1 = q_2 = \cdots = q_\kappa$ and $V_1 = V_2 = \ldots V_\kappa$. In this way, we get the induced orthogonal representation $G \hookrightarrow O_n(k)$, which is identical to the transitive embedding of $G = G(f)$ in S_n. Now, take the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1, \tag{5.5}$$

which is the restriction of the group extension

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

Denote by $\overline{f} \in Z^2(H, \mu_2)$ the 2-cocycle representing (5.4) and by $f \in Z^2(G, \mu_2)$ the 2-cocycle representing (5.5), i.e., $\overline{f} = \mathrm{res}(s_m)$ and $f = \mathrm{res}(s_n)$. From Theorem 5.4 now follows that $[f] = \mathrm{cor}_{G/H}([\overline{f}])$, under the extra assumptions $H \hookrightarrow SO_m(k)$ and $m \equiv 0 \pmod 4$.

6. Realizability of p-groups as Galois groups. The realizability of 2-groups as Galois groups is discussed in a great number of papers, but obstructions over arbitrary base field k are obtained in only a few of them. The precise calculation of the obstructions in general is a difficult and delicate task, but when done properly, it rewards the author with the opportunity to describe the Galois extensions realizing that group, and to discover new automatic realizations (see Section 7).

The condition for the realizability of the cyclic group C_4 over arbitrary fields with characteristic different from 2 has been known for a long time. Namely, if $k(\sqrt{a})/k$ is an arbitrary quadratic extension, then the group $C_2 = \mathrm{Gal}(k(\sqrt{a})/k)$ can be embedded into a C_4 extension if and only if a is a sum of two squares. Hence C_4 is realizable over k if and only if there exists $a \in k^\times \setminus k^{\times 2}$ such that $a = x^2 + y^2$ for some $x, y \in k$. It is easy to see that this condition descends from the obstruction to the embedding problem $(k(\sqrt{a})/k, C_4, \mu_2)$ which is exactly the quaternion algebra $(a, -1) \in \mathrm{Br}_2(k)$.

In 1886 Dedekind constructed for the first time Galois extensions over $\mathbb{Q}$ with Galois group Q_8, the quaternion group of order 8. This result was published in a posthumous article [6]. In 1936 Witt published a paper [71] where he obtained a general description of quaternion extensions over arbitrary fields with characteristic equal to or different from 2. Moreover, Witt found a necessary and sufficient condition for the realizability of p-groups over fields with characteristic p. In 1984 J.-P. Serre generalized Witt's construction of quaternion extensions [57, n. 3.2, Remarque]. A year later appeared a very significant paper by Fröhlich [7] where he developed the theory of orthogonal representations of Galois groups,

generalizing Serre's formula from [57]. In particular, Fröhlich calculated the obstructions to realizability of the dihedral and quaternion groups of order $4n$ over fields containing a primitive n-th root of unity for $n \geq 2$ (see [7, (7.10)]. An explicit description of the solutions to embedding problems associated to orthogonal Galois representations was done by Crespo in [5].

The first attempt at finding necessary and sufficient conditions for the realizability of a number of non abelian groups of order 16 was made by Kiming [25] in 1990. Five years later Ledet [26] found the decomposition of the obstructions as quaternion algebras of all groups of order 2^n for $n \leq 4$ with the exception of C_{16}, the cyclic group of order 16. For some of the groups Ledet applied Theorem 3.4, and for others (e.g. the dihedral, semi-dihedral and the quaternion groups) he applied 'brute force'. The latter approach exploits the well-known theorem for the centralizer of a c.s. subalgebra:

If A is a c.s. k-algebra and B is a c.s. k-subalgebra of A then $A \cong B \otimes_k C_A(B)$, where $C_A(B)$ is the centralizer of B in A.

Unfortunately, this method works exclusively for Brauer problems such that the obstruction can be decomposed as a product of at most three quaternion algebras (i.e., when the quotient group is of order ≤ 8, since the crossed product algebra then has dimension $\leq 64 = 4^3$ over the base field). Ledet made a parametrization of all Galois extensions realizing groups of order 16 in [28] in the case when the obstructions are decomposed as a product of two quaternion algebras. Such a description can be done for any 2-group if its obstruction is of this kind (see [38] concerning one group of order 32 and [36] for some particular cases concerning the quaternion group of order 16). In [22] the reader can find a good survey of explicit descriptions of generic polynomials and extensions realizing 2-groups as Galois groups.

Michailov [35, 37] applied brute force for specific Brauer problems with cyclic 2-kernel involving the four non abelian 2-groups having a cyclic subgroup of index 2.

The obstruction to the embedding of a C_8 extension into a C_{16} extension was found by Swallow [62] by applying brute force again. There are many more results concerning the realizability of cyclic and abelian 2-groups in articles such as [53, 31, 1, 23].

Grundman, Smith and Swallow wrote an extensive survey [15] of the results known until 1995 concerning the groups of order 2^n for $n \leq 4$.

Naturally, the next goal was the investigation of groups of order 32. There are 51 groups of order 32. With the aid of the corestriction homomorphism Swallow and Thiem calculated in [65] the obstructions to the realizability of

several non abelian groups of orders 32 and 64.

By applying a variation of Theorem 3.3, Grundman and Stewart [16] found the obstructions to the realizability of 13 groups of order 32 that have a quotient group isomorphic to a direct product of cyclic groups of order ≤ 4 and/or the dihedral group of order 8. T. Smith [61] investigated some realizability properties (e.g. obstructions, solutions and automatic realizations) of the two extra-special groups of order 32.

A systematic study of all non abelian groups of order 32 was done by Michailov [38] in 2007. Grundman and Smith further elaborated on the obstructions of some of these groups in [12, 13]. The latter two authors also determined in [14] the obstructions to the realizability of 134 non abelian groups of order 64. They used a variation of Theorem 3.4 to calculate the obstructions for 34 μ_2-embedding problems with quotient $(C_2)^r \times (C_4)^s \times (D_8)^t$. The remaining 100 obstructions were obtained for groups known as *pullbacks* by a method applied by Michailov in [38] for 18 groups of order 32.[2]

Namely, let $\varphi' : G' \to F$ and $\varphi'' : G'' \to F$ be homomorphisms with kernels N' and, respectively, N''. *The pullback* of the pair of homomorphisms φ' and φ'' is called the subgroup in $G' \times G''$ of all pairs (σ', σ''), such that $\varphi'(\sigma') = \varphi''(\sigma'')$. The pullback is denoted by $G' \curlywedge G''$. It is also called the direct product of the groups G' and G'' with amalgamated quotient group F and denoted by $G' *_F G''$.

Now, let $N_1 = N' \times \{1\}$ and $N_2 = \{1\} \times N''$. Then N_1 and N_2 are normal subgroups of $G' \curlywedge G''$, such that $N_1 \cap N_2 = \{1\}$. The converse is also true (see [18], I, §12):

Lemma 6.1. *Let N_1 and N_2 be two normal subgroups of the group G, such that $N_1 \cap N_2 = \{1\}$. Then G is isomorphic to the pullback $(G/N_1) \curlywedge (G/N_2)$.*

The application to embedding problems is given by:

Theorem 6.2 ([18, Theorem 1.12])**.** *Let K/k be a Galois extension with Galois group F. In the notations of the lemma, let $F \cong G/N_1N_2$ and $G \cong (G/N_1) \curlywedge (G/N_2)$. Then the embedding problem $(K/k, G, N_1 \times N_2)$ is solvable if and only if the embedding problems $(K/k, G/N_1, N_2)$ and $(K/k, G/N_2, N_1)$ are solvable.*

Next, according to a paper by Ninomia [48], there are 26 non isomorphic non abelian groups of order 2^n for $n \geq 4$ that have a cyclic subgroup of index 4.

[2] In fact, the first examples of the obstructions to the realizability of pullbacks were given by Ledet in [26].

Michailov determined in [41] the obstructions to the realizability of 14 groups by applying Theorems 3.3, 3.5 and 4.2. The obstructions to the remaining groups were obtained in [42] by taking embedding problems with cyclic kernel of order 2^{n-3} and applying Theorem 2.4. This is done with the assumption that the base field k contains a primitive 2^{n-3}th root of unity.

In what follows we will concentrate on results about p-groups for an odd prime p, although most of the groups have their twins for $p = 2$.

We begin with a μ_p-embedding problem, involving the cyclic group C_{p^2}. Let $K = k(\sqrt[p]{a})$, where $a \in k^\times \setminus k^{\times p}$. Now, consider the embedding problem given by K/k and the group extension:

$$1 \longrightarrow \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1. \tag{6.1}$$

Denote by Γ the crossed product algebra, corresponding to (6.1). As we know, Γ is generated by elements $\sqrt[p]{a}$ and u, such that $(\sqrt[p]{a})^p = a, u\sqrt[p]{a} = \zeta\sqrt[p]{a}u$ and $u^p = \zeta$. Therefore $[\Gamma] = (a, \zeta; \zeta)$, so $[\Gamma] = 1$ if and only if $\zeta \in N_{K/k}(K^\times)$.

Naturally, the two non abelian groups of order p^3 were the first non abelian p-groups investigated for realizability as Galois groups. The first one is the Heisenberg group of exponent p. We denote it by G_1 and its generators by g_1, g_2 and g_3, such that $g_1^p = g_2^p = g_3^p = 1, g_1g_2 = g_2g_1g_3$ and g_3 is central. The second group we denote it by G_2. It is generated by g_1 and g_2, such that $g_1^{p^2} = g_2^p = 1$ and $g_1g_2 = g_2g_1^{p+1}$.

Massy [32] investigated the realizability of G_1 and G_2 over arbitrary fields containing a primitive p-th root of unity.

Theorem 6.3 ([32],[39, Theorem 3.1]). *Let $K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ be a $C_p \times C_p$ extension of k and let $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Denote the generators of $C_p \times C_p$ by σ_1 and σ_2, such that $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}, i = 1, 2$. The embedding problem given by K/k and the group extension*

$$1 \longrightarrow \langle g_3 \rangle \cong \mu_p \longrightarrow G_1 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_p \times C_p \longrightarrow 1$$

is solvable if and only if $a_2 \in N_{K_1/k}(K_1^\times)$. In that case for $\omega \in K_1^\times$, such that $N(\omega) = a_2$ we put $\alpha = \omega^{p-1}\sigma_1(\omega)^{p-2} \cdots \sigma_1^{p-2}(\omega)$. Then the set $\{K(\sqrt[p]{f\alpha}) \mid f \in k^\times\}$ gives all solutions.

Theorem 6.4 ([32],[39, Theorem 3.2]). *Let $K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ be a $C_p \times C_p$ extension of k and let $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Denote the generators of*

$C_p \times C_p$ *by* σ_1 *and* σ_2, *such that* $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}, i = 1, 2$. *The embedding problem given by* K/k *and the group extension*

$$1 \longrightarrow \langle g_1^p \rangle \cong \mu_p \longrightarrow G_2 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_p \times C_p \longrightarrow 1$$

is solvable if and only if $a_2\zeta \in N_{K_1/k}(K_1^\times)$. *In that case for* $\omega \in K_1^\times$, *such that* $N(\omega) = a_2\zeta$ *we put* $\alpha = \omega^{p-1}\sigma_1(\omega)^{p-2} \cdots \sigma_1^{p-2}(\omega)$. *Then the set* $\{K(\sqrt[p]{f\sqrt[p]{a_1}^{-1}\alpha}) | f \in k^\times\}$ *gives all solutions.*

More results about the realizability of G_1 and G_2 over global fields were obtained in [33].

Michailov [39] investigated four non abelian groups of order p^4, that have a quotient group of the kind $H \times C_p$. Generally, there are 15 groups of order p^4 for any odd prime p. Of course, we do not need to bother about the groups of the type $G \times H$, since their realizability depends only on the realizability of G and H. From these four groups three have as a quotient group the group $C_{p^2} \times C_p$ and one has $(C_p)^3$ as a quotient group. The remaining non abelian groups of order p^4 do not have a quotient group that is a direct product of smaller groups.

Firstly, let us describe the non abelian groups, having $C_{p^2} \times C_p$ as a quotient group, which is generated by σ_1 and σ_2 such that $\sigma_1^{p^2} = \sigma_2^p = 1$ and $\sigma_1\sigma_2 = \sigma_2\sigma_1$. The presentations of these groups can be given by the relations between their generators g_1, g_2, g_3 and g_4. The symbol $[a, b]$ below stands for the commutator $a^{-1}b^{-1}ab$.

$$G_3 : g_1^p = g_4, g_2^p = g_3^p = g_4^p = 1, [g_2, g_1] = g_3,\ g_3 \text{ and } g_4 \text{ are central},$$
$$G_4 : g_1^p = g_4, g_2^p = g_3, g_3^p = g_4^p = 1, [g_2, g_1] = g_3,\ g_3 \text{ and } g_4 \text{ are central},$$
$$G_5 : g_1^p = g_3, g_3^p = g_4, g_2^p = g_4^p = 1, [g_2, g_1] = g_4,\ g_3 \text{ and } g_4 \text{ are central}.$$

The corresponding central group extensions are as follows:

$$1 \longrightarrow \langle g_3 \rangle \cong \mu_p \longrightarrow G_3 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1, \tag{6.2}$$

$$1 \longrightarrow \langle g_3 \rangle \cong \mu_p \longrightarrow G_4 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1, \tag{6.3}$$

$$1 \longrightarrow \langle g_4 \rangle \cong \mu_p \longrightarrow G_5 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1. \tag{6.4}$$

The last group is given by the presentation

$$G_6 : g_1^p = g_2^p = 1, g_3^p = g_4, g_4^p = 1, [g_2, g_1] = g_4,\ g_3 \text{ and } g_4 \text{ are central}.$$

Given that the group $(C_p)^3$ is generated by elements ρ_1, ρ_2 and ρ_3, we obtain the central group extension:

$$1 \longrightarrow \langle g_4 \rangle \cong \mu_p \longrightarrow G_6 \underset{g_i \mapsto \rho_i}{\longrightarrow} (C_p)^3 \longrightarrow 1. \tag{6.5}$$

Let k be a field with characteristic $\neq p$, let ζ be a primitive pth root of unity in k, and let $a_1, a_2 \in k^\times$ be linearly independent mod $k^{\times p}$. Denote $K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ and $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Now, assume that the embedding problem $(k(\sqrt[p]{a_1})/k, C_{p^2}, \mu_p)$ is solvable. Then $(a_1, \zeta; \zeta) = 1$, so there exists $\alpha \in K_1$, such that $\zeta = N_{K_1/k}(\alpha)$. Let $L_1/k = K_1(\sqrt[p]{f_1\beta})/k$ be arbitrary C_{p^2} extension, where $f_1 \in k^\times$ and $\beta = \sqrt[p]{a_1}(\alpha^{p-1}\sigma_1(\alpha)^{p-2} \cdots \sigma_1^{p-2}(\alpha))^{-1}$. Then we have a $C_{p^2} \times C_p$ extension $L = L_1(\sqrt[p]{a_2})$. We display the obstructions and the solutions to the μ_p-embedding problems in the following three theorems.

Theorem 6.5 ([39, Theorem 4.1])**.** *The obstruction to solvability of the embedding problem given by the Galois extension L/k and the group extension* (6.2) *is $(a_2, a_1; \zeta)$. If the embedding problem is solvable, i.e., $a_2 = N_{K_1/k}(\omega)$ for $\omega \in K_1^\times$, we may put $\gamma = \omega^{p-1}\sigma_1(\omega)^{p-2} \cdots \sigma_1^{p-2}(\omega)$. Then all Galois extensions realizing G_3 are $\{L(\sqrt[p]{f_2\gamma})/k : f_2 \in k^\times\}$.*

Theorem 6.6 ([39, Theorem 4.2])**.** *The obstruction to solvability of the embedding problem given by the Galois extension L/k and the group extension* (6.3) *is $(a_2, a_1\zeta; \zeta)$. If the embedding problem is solvable, i.e., $a_1\zeta = N_{K_2/k}(x)$ for $x \in K_2^\times$, we may put $\omega = \sqrt[p]{a_2}(x^{p-1}\sigma_2(x^{p-2})\sigma_2^2(x^{p-3}) \cdots \sigma_2^{p-2}(x))^{-1}$. Then all Galois extensions realizing G_4 are $\{L(\sqrt[p]{f_2\omega})/k : f_2 \in k^\times\}$.*

Theorem 6.7 ([39, Theorem 4.3])**.** *The obstruction to solvability of the embedding problem given by the Galois extension L/k and the group extension* (6.4) *is $[L_1, C_{p^2}, \zeta](a_2, a_1; \zeta)$. If a primitive p^2th root of unity $\zeta_{p^2} = \sqrt[p]{\zeta}$ is contained in k, then the obstruction is $(\zeta_{p^2}^{-1}a_2, a_1; \zeta)$. Given that the embedding problem is solvable, i.e., $\zeta_{p^2}^{-1}a_2 = N_{K_1/k}(y)$, for some $y \in K_1$, we may put $\omega = \sqrt[p^2]{a_1}y^{p-1}\sigma_1(y)^{p-2} \cdots \sigma_1^{p-2}(y)$. Then all Galois extensions realizing G_5 are $\{L(\sqrt[p]{f\omega})/k : f \in k^\times\}$.*

The groups of orders p^5 and p^6 that have abelian quotients obtained by factoring out μ_p or $(\mu_p)^2$ will be investigated in a future paper by Michailov [43].

In 2009 Michailov investigated in [40] the modular p-group $M(p^n)$ and the group extensions from $H^2(M(p^n)), \mu_2)$, for $n \geq 3$. The modular p-group $M(p^n)$ is generated by two elements α and β, such that $\alpha^{p^{n-1}} = \beta^p = 1$ and $\beta\alpha = \alpha^{1+p^{n-2}}\beta$, for $n \geq 3$. Put $q = p^{n-2}$.

Theorem 6.8 ([40, p. 3723])**.** *Let $a_1, a_2 \in k^\times$ be independent mod $k^{\times p}$ and denote $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Let K/k be a $C_q = \langle\sigma\rangle$ extension, such that $K_1 \subset K$. Then $L/k = K(\sqrt[p]{a_2})/k$ is a $C_q \times C_p$ extension, generated by elements σ and τ, such that $\sigma^q = \tau^p = 1$. Consider the group extension:*

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

The obstruction to solvability of the embedding problem $(L/k, M(p^n), \mu_p)$ is

$$[K, C_q, \zeta](a_2, a_1; \zeta) \in \mathrm{Br}(k), \tag{6.6}$$

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

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

According to [40, p. 3278], the cohomological group $H^2(M(p^n), \mu_p)$ is isomorphic to μ_p^2, and consists of the 2-coclasses related to the group extensions

$$1 \longrightarrow \mu_p \longrightarrow G_{\varepsilon_1,\varepsilon_2} \underset{\substack{\tilde\alpha\mapsto\alpha\\ \tilde\beta\mapsto\beta}}{\longrightarrow} M(p^n) \longrightarrow 1,$$

where $\varepsilon_i \in \mu_p, \tilde\beta^p = \varepsilon_1, \tilde\alpha^q[\tilde\beta, \tilde\alpha] = \varepsilon_2$ and $\tilde\alpha^{pq} = 1$. With the aid of the corestriction homomorphism, Michailov determined in [40] the obstructions to the μ_p-embedding problems, related to these group extensions.

Theorem 6.9 ([40, Proposition 4.3])**.** *Let L/k be a $M(p^n)$ extension containing the biquadratic extension $k(\sqrt[p]{a_1}, \sqrt[p]{a_2}) \subset L$, where $K_1 = k(\sqrt[p]{a_1}) = L^{C_q\times C_p}$. The obstruction to the embedding problem $(L/k, G_{1,\zeta}, \mu_p)$, where $G_{1,\zeta} \cong \langle x, y, z : x^{p^{n-1}} = y^p = z^p = 1, z - \text{ central}, yx = x^{q+1}yz\rangle$ is $(a_2, a_1; \zeta) \in \mathrm{Br}_p(k)$.*

Theorem 6.10 ([40, Proposition 4.4])**.** *Let L/k be a $M(p^n)$ extension containing the biquadratic extension $k(\sqrt[p]{a_1}, \sqrt[p]{a_2}) \subset L$, where $K_1 = k(\sqrt[p]{a_1}) = L^{C_q\times C_p}$. The obstruction to the embedding problem $(L/k, G_{\zeta,1}, \mu_p)$, where $G_{\zeta,1} \cong \langle x, y : x^{p^{n-1}} = y^{p^2} = 1, y^p - \text{ central}, yx = x^{q+1}y\rangle$ is $(a_2, \zeta; \zeta) \in \mathrm{Br}_p(k)$.*

Theorem 6.11 ([40, Proposition 4.5])**.** *Let L/k be a $M(p^n)$ extension containing the biquadratic extension $k(\sqrt[p]{a_1}, \sqrt[p]{a_2}) \subset L$, where $K_1 = k(\sqrt[p]{a_1}) = L^{C_q\times C_p}$. The obstruction to the embedding problem $(L/k, G_{\zeta,\zeta}, \mu_p)$, where $G_{\zeta,\zeta} \cong \langle x, y : x^{p^{n-1}} = y^{p^2} = 1, y^p - \text{ central}, yx = x^{q+1}y^{p+1}\rangle$ is $(\zeta a_1, a_2; \zeta) \in \mathrm{Br}_p(k)$.*

Michailov also made in [40] an explicit (to some extent) description of the modular p-extensions.

Theorem 6.12 ([40, Theorem 3.2]). *Let $K_1 = k(\sqrt[p]{a_1})$ for $a_1 \in k^\times \setminus k^{\times p}$, and let K/k be a cyclic $C_q = \langle\sigma\rangle$ extension, such that $K_1 \subset K$. L/k is an $M(p^n)$ Galois extension, solving the embedding problem $(K/k, M(p^n), C_p \times C_p)$, if and only if, there exist $b_0 \in K^\times \setminus K^{\times p}, f \in k^\times \setminus k^\times \cap K^{\times p}$ and $x \in K^\times$ such that $\sigma(b_0)/b_0 = fx^p, L/k = K(\sqrt[p]{b_0}, \sqrt[p]{f})/k$ and $c = f^{q/p}N_{K/k}(x)$ is a pth root of unity, but $c \neq 1$*

Waterhause's ideas from [69] were further developed in [40] with a number of propositions, e.g. the following.

Proposition 6.13 ([40, 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/k is Galois and the Galois group of L/k is isomorphic either to the semidirect product $(C_p)^3 \rtimes C_q$, 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 $\tau_i(\sqrt[p]{b_j}) = \sqrt[p]{b_j}\zeta^{\delta_{ij}}$.*

Note that for $q = p$, the group $(C_p)^3 \rtimes C_p$ from the latter proposition is a non abelian group of order p^4 that is not isomorphic to any of the groups $G_3, \ldots, G_6$ considered so far. Denote it by G_7. It is generated by elements σ, τ, λ and μ with the following relations:

$$G_7 \cong (C_p)^3 \rtimes C_p : \sigma^p = \tau^p = \lambda^p = \mu^p = 1, [\lambda, \tau] = 1, [\mu, \tau] = \sigma, [\mu, \lambda] = \tau,$$
$$\sigma \text{ is central.}$$

A necessary and sufficient condition for the embedding of a C_p-extension into a G_7-extension will be obtained in the example given at the end of this Section.

It turns out that the description of p-extensions given so far has an impact on certain realizability issues over the field of rational numbers $\mathbb{Q}$. By applying Michailov's methods from [39, 40], S. Checcoli [4] provided recently a characterization of infinite algebraic Galois extensions of the rationals with uniformly bounded local degrees.

Theorem 6.14 ([4, Theorem 1]). *Let $K/\mathbb{Q}$ be an infinite Galois extension. Then the following conditions are equivalent:*

(1) *K has uniformly bounded local degrees at every prime;*

(2) *K has uniformly bounded local degrees at almost every prime;*

(3) $\mathrm{Gal}(K/\mathbb{Q})$ *has finite exponent.*

Moreover, if $K/\mathbb{Q}$ *is abelian, then the three properties:*

(*a*) *K has uniformly bounded local degrees;*

(*b*) *K is contained in* $\mathbb{Q}^{(d)}$ *(the compositum of all number fields of degree at most d over* $\mathbb{Q}$*) for some positive integer d;*

(*c*) *every finite subextension of K can be generated by elements of bounded degree;*

are equivalent. However, in general, we have that (*c*) *implies* (*b*) *which implies* (*a*) *and none of the inverse implications holds.*

Waterhause's ideas [69] also inspired J. Mináč and J. Swallow, who considered in [46] certain embedding problems with a cyclic p-kernel. We are now going to state their main result.

Let k be an arbitrary field, and suppose that K/k is a cyclic extension with Galois group $G = \mathrm{Gal}(K/k) \cong \mathbb{Z}/p\mathbb{Z}$ [3], with generator σ. Let $A = \oplus_{j=0}^{p-1}\mathbb{F}_p\tau^j$ be a free $\mathbb{F}_p[G]$-module on the generator τ, where σ acts by multiplication by τ. Let A_i be the $\mathbb{F}_p[G]$-submodule generated by $(\tau-1)^i$. Finally, let $\mathcal{E}_i, 1 < i \leq p$, denote the Galois embedding problem related to the group extension:

$$\mathcal{E}_i: \quad 1 \to A_1/A_i \to (A/A_i) \rtimes G \to (A/A_1) \rtimes G = \mathrm{Gal}(L/k) \to 1.$$

Observe that $A/A_1 \cong \mathbb{F}_p$, a trivial $\mathbb{F}_p[G]$-module; hence $(A/A_1) \rtimes G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We also assume that the projection of $(A/A_1) \rtimes G = \mathrm{Gal}(L/k)$ onto G coincides with the restriction map $\mathrm{Gal}(L/k) \to G = \mathrm{Gal}(K/k)$. Assume that char $k \neq p$ and denote by ζ any primitive p-th root of unity. Then $\mathrm{Gal}(L/k)$ is naturally isomorphic to $\mathrm{Gal}(L(\zeta)/k(\zeta))$. After identifying these two Galois groups we set $k(\zeta, \sqrt[p]{b})$ to be the fixed field of $1 \rtimes G$ in $L(\zeta)$.

Theorem 6.15 ([46, Theorem 1])**.**
A) *Let k be an arbitrary field. Then the following are equivalent:*

(1) *Some* $\mathcal{E}_i$ *is solvable.*

(2) *Each* $\mathcal{E}_i$ *is solvable.*

[3] Henceforth we hold on to the additive notation $\mathbb{Z}/n\mathbb{Z}$ for the cyclic group of order n, which is used by Mináč, Schultz and other authors.

Consequently, if $(A/A_2) \rtimes G$ *occurs as a Galois group over* k*, then* $(A/A_i) \rtimes G$ *occurs as well, for all* $2 \leq i \leq p$.

B) *Now assume that* char $k \neq p$. *Then* (1) *and* (2) *are also equivalent to*

(3) $b \in N_{K(\zeta)/k(\zeta)}(K(\zeta)^\times)$.

C) *Now assume further that* $\zeta \in k$. *Suppose* (1)−(3) *hold, and let* $\omega \in K^\times$ *satisfy* $N(\omega) = b$. *Suppose* $i > 2$. *Then a solution to* $\mathcal{E}_i$ *is given by*

$$\tilde{L} = K(\sqrt[p]{f\omega^{(\sigma-1)^{p-i}}}, \sqrt[p]{\omega^{(\sigma-1)^{p-i+1}}}, \ldots, \sqrt[p]{\omega^{(\sigma-1)^{p-2}}}),$$

$f \in k^\times$. *If* $i = 2$ *then a solution to* $\mathcal{E}_2$ *is given by* $\tilde{L} = K(\sqrt[p]{\omega^{(\sigma-1)^{p-2}}})$. *Moreover, all solutions of* $\mathcal{E}_i$ *arise in this way.*

Schultz recently generalized in [55] these results by allowing $\mathrm{Gal}(K/k) \cong \mathbb{Z}/p^n\mathbb{Z}$ for any $n \in \mathbb{N}$, and removing the condition of cyclicity (as a module) for the kernel. Shirbisheh also considers non cyclic kernels in [60], where he studies embedding problems over the field $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}(\zeta_p)$. Schultz's approach differs in that he gives explicit descriptions for all possible extensions of $\mathbb{Z}/p^n\mathbb{Z}$ by a finite $\mathbb{F}_p[G]$-module A, and then he finds a parameterizing set for each such group within $J(K) = K^\times/K^{\times p}$. Note that the study of the $\mathbb{F}_p[\mathrm{Gal}(K/k)]$-structure of $J(K)$ was initiated by Waterhouse in [69], and Schultz's results from [55] can be thought of as a completion of the ideas that Waterhouse presents there.

We are going now to define three symbols that appear in the statement of the main result from [55]. For a field extension K/k with $\mathrm{Gal}(K/k) \cong \mathbb{Z}/p^n\mathbb{Z}$, let K_i denote the intermediate field of degree p^i over k. If the embedding problem $(K/k, \mathbb{Z}/p^{n+1}\mathbb{Z}, \mu_p)$ has a solution, then define $i(K/k) = -\infty$. Otherwise, let s be the minimum value such that the embedding problem $(K/K_s, \mathbb{Z}/p^{n-s+1}\mathbb{Z}, \mu_p)$ has a solution, and define $i(K/k) = s - 1$. Notice that we have $i(K/k) \in \{-\infty, 0, \cdots, n-1\}$ provided $K \neq k$.

Denote by $\binom{n}{m}_p$ the p-binomial coefficient, defined for $n \in \mathbb{N}$ and satisfying

$$\binom{n}{m}_p = \begin{cases} 0, & \text{if } m < 0 \text{ or } m > n \\ \frac{(p^n-1)\cdots(p^{n-m+1}-1)}{(p^m-1)\cdots(p-1)}, & \text{if } 0 \leq m \leq n. \end{cases}$$

Finally, denote by $\lceil x \rceil$ the standard ceiling function, i.e., the smallest integer not less than x.

Theorem 6.16 ([55, Theorem 1])**.** *Let* $G = \langle\sigma\rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$*, where* p *is a prime and* $n > 1$ *when* $p = 2$*, and suppose that* K/k *is an extension of fields so*

that $\mathrm{Gal}(K/k) \simeq G$ *and* $\zeta_p \in K$. *Suppose that* $A \simeq \bigoplus_{i=1}^{p^n} \oplus_{d_i} \mathbb{F}_p[G]/(\sigma-1)^i$ *as an* $\mathbb{F}_p[G]$*-module, and write* $\Delta(A_{\{i\}}) = \sum_{j\geq i} d_j$. *For* $1 \leq i \leq p^n$ *let*

$$\mathfrak{D}_{\{i\}} = \dim_{\mathbb{F}_p}\left(\frac{N_{K_{\lceil \log_p(i)\rceil}/k}(K^\times_{\lceil \log_p(i)\rceil})}{K^{\times p}}\right).$$

Then the embedding problem $(K/k, A \rtimes G, A)$ *has a solution over* K/k *if and only if* $\Delta(A_{\{i\}}) \leq \mathfrak{D}_{\{i\}}$.

If $k^\times/K^{\times p}$ *is infinite and the embedding problem* $(K/k, A \rtimes G, A)$ *is solvable, then there are infinitely many solutions to this embedding problem over* K/k. *If* $k^\times/K^{\times p}$ *is finite and the embedding problem* $(K/k, A \rtimes G, A)$ *is solvable, then the number of solutions to this embedding problem over* K/k *is*

$$\prod_{i=1}^{p^n} \binom{\mathfrak{D}_{\{i\}} - \Delta(A_{\{i+1\}}) - \mathbb{1}_{i=p^{i(K/k)}+1}}{\Delta(A_{\{i\}}) - \Delta(A_{\{i+1\}})}_p p^{d_i\left(\sum_{j<i}\mathfrak{D}_{\{j\}} - \Delta(A_{\{j\}}) - \mathbb{1}_{j=p^{i(K/k)}+1}\cdot\mathbb{1}_{i=p^n}\right)}.$$

Example. Let us consider the group $G_7 = (\mathbb{Z}/p\mathbb{Z})^3 \rtimes \mathbb{Z}/p\mathbb{Z}$ of order p^4 (see the definition of G_7 after Proposition 6.13). We may put $A = \mathbb{F}_p[G]/(\sigma-1)^3$, a cyclic module of dimension 3, and $G = \mathbb{Z}/p\mathbb{Z}$. Thus $G_7 \cong A \rtimes G$, and we can apply Theorem 6.16.

We have $d_3 = 1$ and $d_j = 0$ for $j \neq 3$, so $\Delta(A_{\{i\}}) = 0$ if $i \geq 4$ and $\Delta(A_{\{i\}}) = 1$ if $i \leq 3$. Therefore $(K/k, A \rtimes G, A)$ is solvable if and only if $\mathfrak{D}_{\{3\}} \geq 1$. As $\lceil \log_p(3)\rceil = 1$ for $p > 2$, one simply need to check that $N_{K_1/k}(K_1^\times)$ is not contained in $K^{\times p}$.

Schultz also investigates in [55] the case when K does not contain a primitive p-th root of unity. In [55, Section 6] $\mathfrak{D}_i$ is redefined in this case, and [55, Theorem 6.3] is the generalization of [55, Theorem 1] which drops the Kummer theory assumption. Thus the example given above can also be extended in the general case.

7. Automatic realizations. Let G and H be finite groups. If any field k admitting a G-extension also admits an H-extension, we will write $G \Longrightarrow H$. A statement $G \Longrightarrow H$ is called an *automatic realization*. For instance, it is well-known (see [70]) that $\mathbb{Z}/4\mathbb{Z} \Longrightarrow \mathbb{Z}/2^n\mathbb{Z}$ for all $n \in \mathbb{N}$. Of course, we always have the trivial automatic realization $G \Longrightarrow G/N$. Also, it is not hard to verify that a necessary condition for the automatic realization $G \Longrightarrow H$ to hold is

the minimum number of generators for H is less than or equal to the minimum number of generators for G (see [26, p. 1268]).

We keep the notations from Section 4 for the four non abelian 2-groups having a cyclic subgroup of index 2. Jensen and Yui determined in [24, Theorem III.3.6]) the automatic realization $Q_8 \Longrightarrow D_8$. Ledet proved in [26, Proposition 5.8, Proposition 5.10] the automatic realizations $Q_{16} \Longrightarrow D_{16}, SD_{16} \Longrightarrow M_{16}$ and many more. He also proved in [27] the automatic realization $Q_{32} \Longrightarrow D_{32}$. Other automatic realizations concerning groups of order 16 are found by Grundman and Smith in [11], where they consider fields with special properties (e.g. fields with a given level or a number of square classes). There are as well a number of non trivial automatic realizations among groups of order 32 considered in [38, 13, 61]. More automatic realizations among 2-groups can be found in three papers written by Jensen [19, 20, 21] and in a paper written by Gao, Leep, Minác and Smith [10].

We proceed with results about p-groups for an odd prime p. Whaples showed in [70] the automatic realization $\mathbb{Z}/p\mathbb{Z} \Longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ holds for all $n \in \mathbb{N}$. Brattström verified in [3, Theorem 2] the automatic realization $G_1 \Longrightarrow G_2$, where G_1 and G_2 are the two-non abelian groups of order p^3 defined in Section 6 (above Theorem 6.4). Michailov showed in [39, Theorem5.2] that the automatic realization $G_3 \Longrightarrow G_4$ holds, where G_3 and G_3 are non abelian groups of order p^4 defined in Section 6 (below Theorem 6.4). In [3, 39] is shown also that the reverse automatic realisations $G_2 \Longrightarrow G_1$ and $G_4 \Longrightarrow G_3$ are not valid.

Minác, Schultz and Swallow established in [45] automatic realizations among the semidirect products $M \rtimes G$, where $G = \langle\sigma\rangle$ is a cyclic group of order p^n, and M is a quotient of the group ring $\mathbb{F}_p[G]$. For the group ring $\mathbb{F}_p[G]$ there exist precisely p^n nonzero ring quotients, namely $M_j := \mathbb{F}_p[G]/\langle(\sigma - 1)^j\rangle$ for $j = 1, 2, \ldots, p^n$. Multiplication in $\mathbb{F}_p[G]$ induces an $\mathbb{F}_p[G]$-action on each M_j. In particular, each M_j is a G-module.

Theorem 7.1 ([45, Theorem 1])**.** *$M_{p^i+c} \rtimes G \Longrightarrow M_{p^{i+1}} \rtimes G$ for $0 \leq i < n, 1 \leq c < p^{i+1} - p^i$.*

There is a more general approach to the automatic realizations. We write $\nu(G, k)$ for the number of distinct G-extensions of k within a fixed algebraic closure of k. We then write $\mathfrak{K}(G)$ for the set of fields k such that $\nu(G, k) \geq 1$. Now it is clear that if $k \in \mathfrak{K}(G)$ implies $k \in \mathfrak{K}(H)$, then the automatic realization $G \Longrightarrow H$ holds.

Berg and Schultz recently considered in [2] a close cousin of automatic

realization results. The realization multiplicity of G, written $\nu(G)$, is defined as

$$\nu(G) = \min_{k \in \mathfrak{R}(G)} \{\nu(G,k)\}.$$

Theorem 7.2 ([2, Theorem 1.1])**.** *Suppose that p is prime and n is a positive integer, with $n \geq 2$ when $p = 2$. Let k be given. Then*

$$\nu\left(\mathbb{F}_p[\mathbb{Z}/p^n\mathbb{Z}]^k \rtimes \mathbb{Z}/p^n\mathbb{Z}\right) \geq p^k.$$

Schults generalized the latter result in [55].

Theorem 7.3 ([55, Theorem 1.3])**.** *Let $G = \langle\sigma\rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$, with $n > 1$ when $p = 2$. Suppose that A is an $\mathbb{F}_p[G]$-module which is not isomorphic to*

$$\mathbb{F}_p[G]/(\sigma-1)^{p^j+1} \bigoplus_{i=0}^{p^n} \oplus_{d_i} \mathbb{F}_p[G]/(\sigma-1)^{p^i}$$

for any choice of $j \in \{-\infty, 0, \cdots, n-1\}$ and $d_i \in \mathbb{Z}$. If $\hat{G}$ is any extension of G by A, and if A contains elements $a_1, \cdots, a_k$ which are $\mathbb{F}_p[G]$-independent, then $\nu(\hat{G}) \geq p^k$.

Acknowledgements. We are grateful to Prof. A. Schultz who read our manuscript, offered constructive comments and provided the example at the end of Section 6.

REFERENCES

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

[2] J. Berg, A. Schultz. p-groups have unbounded realization multiplicity. `arXiv:1109.4070v1 [math.NT]`.

[3] G. Brattström. On p-groups as Galois groups, *Math. Scand.* **65**, *2* (1989), 165–174.

[4] S. Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. `arXiv:1012.0984v2 [math.NT]`.

[5] T. Crespo. Explicit solutions to embedding problems associated to orthogonal Galois representations. *J. Reine Angew. Math.* **409** (1990), 180–189.

[6] R. Dedekind. Konstruktion von Quaternionkörpern. Gesammelte mathematische Werke. Herausgegeben von E. Fricke, E. Noether, Ö. Ore. Bd. II. (German) II + 442 S. Braunschweig, F. Vieweg & Sohn, 1931, 376–384.

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

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

[9] W. Fulton, J. Harris. Representation Theory. A First Course, Graduate Texts in Mathematics, vol. **129**, Springer-Verlag, New York, 1991.

[10] W. Gao, D. Leep, J. Mináč, T. Smith. Galois groups over nonrigid fields. In: Valuation Theory and Its Applications, Vol. II, Fields Institute Communications **33** (2003), 61–77.

[11] H. Grundman, T. Smith. Automatic realizability of Galois groups of order 16. *Proc. Amer. Math. Soc.* **124** (1996), 2631–2640.

[12] H. G. Grundman, T. L. Smith. Galois realisability of a central C_4-extension of D_8. *J. Algebra* **322** (2009), 3492–3498.

[13] H. Grundman, T. Smith. Realizability and automatic realizability of Galois groups of order 32. *Cent. Eur. J. Math.* **8**, *2* (2010), 244–260.

[14] H. Grundman, T. Smith. Galois realizability of groups of order 64. *Cent. Eur. J. Math.* **8**, *5* (2010), 846–854.

[15] H. G. Grundman, T. L. Smith, J. R. Swallow. Groups of order 16 as Galois groups. *Expo. Math.* **13** (1995), 289–319.

[16] H. G. Grundman, G. L. Stewart. Galois realizability of non-split group extensions of C_2 by $(C_2)^r \times (C_4)^s \times (D_4)^t$. *J. Algebra* **272** (2004), 425–434.

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

[18] V. V. Ishkhanov, B. B. Lur'e, D. K. Faddeev. The Embedding Problem in Galois Theory. Transl. from the Russian by N. B. Lebedinskaya. Translations of Mathematical Monographs vol. **165**. Providence, RI: American Mathematical Society, 1997.

[19] C. U. Jensen. On the representations of a group as a Galois group over an arbitrary field. In: The'orie des nombres, C. R. Conf. Int., Que'bec/Can. 1987, (1989) 441–458.

[20] C. U. Jensen. Finite groups as Galois groups over arbitrary fields. Proceedings of the International Conference on Algebra Memory A. I. Mal'cev, Novosibirsk/USSR 1989, *Contemp. Math.* **131**, Pt. 2 (1992) 435–448.

[21] C. U. Jensen. Elementary questions in Galois theory. In: Advances in algebra and model theory. Selected surveys presented at conferences in Essen 1994 and Dresden 1995, Gordon and Breach Science Publishers. *Algebra Log. Appl.* **9** (1997), 11-24.

[22] C. Jensen, A. Ledet, N. Yui. Generic Polynomials: Constructive Aspects of the Inverse Galois Problem. Cambridge University Press, 2002.

[23] C. U. Jensen, A. Prestel. Unique realizability of finite abelian 2-groups as Galois groups, *J. Number Theory* **40** (1992), 12–31.

[24] C. U. Jensen, N. Yui. Quaternion extensions, In: Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, Kinokuniya, Tokyo, 1987, 155–182.

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

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

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

[28] A. Ledet. Embedding problems and equivalence of quadratic forms. *Math. Scand.* **88** (2001), 279–302.

[29] A. Ledet. Brauer Type Embedding Problems. Fields Institute Monographs, vol. **21**, American Mathematical Society, 2005.

[30] G. Malle, B. H. Matzat. Inverse Galois Theory. Springer Monographs in Mathematics, Springer-Verlag, 1999.

[31] D. Martinais, L. Schneps. A complete parametrization of cyclic field extensions of 2-power degree. *Manuscripta Math.* **80** (1993), 181–197.

[32] R. Massy. Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p. *J. Algebra* **109** (1987), 508–535.

[33] R. Massy, T. Nguyen-Quang-Do. Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale. *J. Reine Angew. Math.* **291** (1977), 149–161.

[34] 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 (in Russian); English transl. in *Math. USSR Izvestiya* **21** (1983), 307–340.

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

[36] I. Michailov. Quaternion extensions of order 16. *Serdica Math. J.* **31**, *3* (2005), 217–228.

[37] I. Michailov. Embedding obstructions for the cyclic and modular 2-groups. *Math. Balk., New Series*, **21**, *1–2* (2007), 31–50.

[38] I. Michailov. Groups of order 32 as Galois groups. *Serdica Math. J.* **33**, *1* (2007), 1–34.

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

[40] I. Michailov. Induced orthogonal representations of Galois groups. *J. Algebra* **322** (2009), 3713–3732.

[41] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups, *Cent. Eur. J. Math.* **9**, *2* (2011), 403–419.

[42] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups II. *Cent. Eur. J. Math.* **9**, *6* (2011), 1333–1343.

[43] I. Michailov. Galois realizability of groups of orders p^5 and p^6, preprint.

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

[45] 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.

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

[47] J. Neukirch, A. Schmidt, K. Wingberg. Cohomology of Number Fields. Grundlehren der Mathematischen Wissenschaften, vol. **323**, Springer-Verlag, 2000.

[48] Y. Ninomiya. Finite p-groups with cyclic subgroups of index p^2. *Math. J. Okayama Univ.* **36** (1994), 1–21.

[49] J. Quer. Embedding Problems over Abelian Groups and an Application to Elliptic Curves. *J. Algebra* **237** (2001), 186–202.

[50] H. Reichardt. Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. Reine Angew. Math.* **177** (1937), 1–5.

[51] C. Riehm. The corestriction af algebraic structures. *Invent. Math.* **11** (1970), 73–98.

[52] N. Schappacher. On the History of Hilberts Twelfth Problem. Societe Mathematique de France, 1998.

[53] L. Schneps. On cyclic field extensions of degree 8. *Math. Scand.* **17** (1992), 24–30.

[54] A. Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I. *Math. Z.* **42** (1937), 161–188.

[55] A. Schultz. Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p-abelian kernel. `arXiv:1109.4071v2 [math.NT]`.

[56] I. Schur. Gleichungen ohne Affekt. Sitzungsberichte Akad. Berlin, 1930, 443–449.

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

[58] J.-P. Serre. Topics in Galois Theory. Research Notes in Mathematics, Jones & Barlett, 1992.

[59] I. R. Shafarevich. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Aksd. Nauk SSSR, Ser. Mat.* **18** (1954), 525–578 (in Russian).

[60] V. Shirbisheh. Galois Embedding Problems with Abelian Kernels of Exponent p. Saarbrücken: VDM Verlag Dr. Müller, 2009.

[61] T. Smith. Extra-special groups of order 32 as Galois groups. *Canad. J. Math.* **46**, *4* (1994), 886–896.

[62] J. Swallow. Embedding problems and the $C_{16} \to C_8$ obstruction. Proceedings of AMS summer conference Recent Developments in the Inverse Galois Problem. *Cont. Math.* **186** (1995), 75–90.

[63] J. Swallow. Solutions to central embedding problems are constructible. *J. Algebra* **184** (1996), 1041–1051.

[64] J. Swallow. Central p-extensions of $(p, p, \ldots, p)$-type galois groups. *J. Algebra* **186** (1996), 277–298.

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

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

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

[68] H. Völklein. Groups as Galois Groups, an Introduction. Cambridge Studies in Advanced Mathematics, vol. **53**, Cambridge University Press, 1996.

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

[70] G. Whaples. Algebraic extensions of arbitrary fields. *Duke Math. J.* **24** (1957), 201–204.

[71] E. Witt. Konstruktion von galoisschen Köpern der Characteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. Reine Angew. Math.* **174** (1936), 237–245.

Ivo M. Michailov, Nikola P. Ziapkov
Faculty of Mathematics and Informatics
"Episkop Konstantin Preslavski" University of Shumen
115, Universitetska Str.
9700 Shumen, Bulgaria
e-mail: ivo_michailov@yahoo.com
ziapkov2000@yahoo.co.uk

Received January 6, 2012