Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 307 (2007) 287–299
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Four non-abelian groups of order p^4 as Galois groups ☆

Ivo M. Michailov

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

Received 23 December 2005

Available online 15 June 2006

Communicated by Eva Bayer-Fluckiger

Abstract

Let p be an odd prime and let F be arbitrary field of characteristic not p, containing a primitive pth root of unity ζ. In this paper, we prove a criterion, giving the obstructions to realizability of p-groups as Galois groups over F, having a factor-group of the kind $H \times C_p$. We apply this to the non-abelian groups of orders p^3 and p^4. Where it is possible, we give a description of all Galois extensions realizing these groups. We discuss also automatic realizations and local fields.

Keywords: Galois; Embeding; Obstruction; Hilbert symbol

1. The central embedding problem for p-groups

Let F be arbitrary field of characteristic not p, containing a primitive pth root of unity ζ. We will assume the same conditions throughout the first four sections. Let K be a Galois extension of F with Galois p-group H. Consider the group extension

$$1 \to \langle \varepsilon \rangle \cong C_p \to G \to H \to 1, \tag{1.1}$$

where ε is a central element of order p in G and C_p is the cyclic group of order p. To solve the embedding problem given by K/F and the group extension (1.1) means to find a Galois extension L over F, such that $K \subset L$, $\mathrm{Gal}(L/F) \cong G$ and the restriction of an automorphism of G on K coincides with its image under the epimorphism $G \to H$. We can identify the groups $\langle \varepsilon \rangle$

☆ This work is partially supported by project of Shoumen University.
E-mail address: ivo_michailov@yahoo.com.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.05.021

and $\langle\zeta\rangle$, since they are isomorphic as H-modules. In this way we have an injection $\langle\varepsilon\rangle \to K^\times$, which induces a homomorphism $\mu : H^2(H, \langle\varepsilon\rangle) \to H^2(H, K^\times)$. From [Ki] we have

Theorem 1.1. *Let c be the 2-coclass in $H^2(H, \langle\varepsilon\rangle)$, corresponding to the group extension* (1.1). *Then the embedding problem given by K/F and* (1.1) *is solvable if and only if $\mu(c) = 1$. If $K(\sqrt[p]{\beta})/F$ is a solution to the embedding problem for some $\beta \in K^\times$, then all solutions are of the kind $K(\sqrt[p]{f\beta})/F$, for $f \in F^\times$.*

Since there is an isomorphism between the relative Brauer group $\mathrm{Br}(K/F)$ and the group $H^2(H, K^\times)$, we can identify c with the equivalence class in $\mathrm{Br}(K/F)$ of the crossed product algebra Γ, corresponding to (1.1). This class $[\Gamma]$ we call *the obstruction* to solvability of the embedding problem given by (1.1). We will also use the fact that if A is a central simple algebra over F and B is a subalgebra of A, then $A \cong B \otimes_F C_A(B)$, where $C_A(B)$ is the centralizer of B in A. The question whether a central simple algebra can be decomposed as a tensor product of generalized quaternion algebras is very important and difficult one. The *generalized quaternion algebra* of degree p is called a central simple algebra over F, generated by elements i and j, such that $i^p = a$, $j^p = b$ and $ji = \zeta ij$ $(a, b \in F^\times)$. We denote it by $(a, b; \zeta)$. We will not be too careful to distinguish between the quaternion algebra and its equivalence class in the Brauer group. We refer the reader for more information to [Pi, Chapter 15]. Here are some frequently used properties of the quaternion algebras:

- $(a, b; \zeta) = (b, a; \zeta^{-1})$;
- $(a, b; \zeta)^{-1} = (b, a; \zeta)$;
- $(a, bc; \zeta) = (a, b; \zeta)(a, c; \zeta)$;
- $(ab, c; \zeta) = (a, c; \zeta)(b, c; \zeta)$;
- $(a, b; \zeta) = 1 \in \mathrm{Br}(F) \Leftrightarrow a \in N_{F(\sqrt[p]{b})/F}(F(\sqrt[p]{b})^\times) \Leftrightarrow b \in N_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$, where as usual by $N_{K/F}$ we denote the norm map $N : K \to F$;
- $(a^m, a^n; \zeta) = 1$, $\forall m, n \in \mathbb{Z}$;
- $(a^p, b; \zeta) = 1$;
- If $a + b \in F^p$, then $(a, b; \zeta) = 1$. In particular $(a, -a; \zeta) = (a, 1 - a; \zeta) = 1$.

(For all $a, b, c \in F^\times$.)

Whenever the obstruction can be expressed as a tensor product of quaternion algebras, this can be used to construct the Galois extensions solving the embedding problem. At this point we can investigate one simple embedding problem, involving the cyclic group C_{p^2}. Let $H = C_p$ and let $K = F(\sqrt[p]{a})$, where $a \in F^\times \setminus F^{\times p}$. Denote by σ the generator of H such that $\sigma(\sqrt[p]{a})/\sqrt[p]{a} = \zeta$. Now, consider the embedding problem given by K/F and the group extension:

$$1 \to \langle\varepsilon\rangle \cong C_p \to C_{p^2} \to H \to 1. \tag{1.2}$$

Denote by Γ the crossed product algebra, corresponding to (1.2). 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 $\zeta \in N_{K/F}(K^\times)$. Now, we can easily describe the family of Galois extensions, realizing C_{p^2} as Galois group over F. Let the embedding problem be solvable, so there exists $\alpha \in K^\times$, such that $N_{K/F}(\alpha) = \zeta$. For $\beta = \sqrt[p]{a}(\alpha^{p-1}\sigma(\alpha)^{p-2}\cdots\sigma^{p-2}(\alpha))^{-1}$ we have $\sigma(\beta)/\beta = \alpha^p$, so $K(\sqrt[p]{\beta})/F$ is Galois. We can assume that the pre-image $\bar{\sigma}$ of σ in the

group $\mathrm{Gal}(K(\sqrt[p]{\beta})/F)$ acts in this way: $\bar{\sigma}(\sqrt[p]{\beta}) = \sqrt[p]{\beta}\alpha$. From $\bar{\sigma}^p(\sqrt[p]{\beta}) = \sqrt[p]{\beta}N_{K/F}(\alpha) = \sqrt[p]{\beta}\zeta$ follows that the order of $\bar{\sigma}$ is p^2.

Finally, let us consider a particular case, which we will use later. For $a = \zeta \notin F^{\times p}$ we have $(a, \zeta; \zeta) = 1$ and $\sigma(\sqrt[p]{\zeta})/\sqrt[p]{\zeta} = \zeta = (\sqrt[p]{\zeta})^p$. Thus we can put $\alpha = \sqrt[p]{\zeta} = \zeta_{p^2}$ and $\beta = \alpha$, whence $N_{K/F}(\alpha) = \alpha^p = \zeta$ and $\sigma(\beta)/\beta = \sigma(\alpha)/\alpha = \zeta = \alpha^p$. Therefore one solution is $K(\sqrt[p]{\beta})/F = F(\zeta_{p^3})/F$ and all solutions are $K(\sqrt[p]{f\zeta_{p^2}})/F$, $f \in F^\times$.

2. An embedding criterion

Let H be a p-group and let

$$1 \to C_p \cong \langle\zeta\rangle \to G \underset{\pi}{\to} H \times C_p \to 1 \tag{2.1}$$

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

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

Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a minimal generating set for the maximal elementary abelian factorgroup of H; and let τ be the generator of the direct factor C_p. Finally, let $s_1, s_2, \ldots, s_m, t \in G$ be the pre-images of $\sigma_1, \sigma_2, \ldots, \sigma_m, \tau$, such that $t^p = \zeta^j$ and $ts_i = \zeta^{d_i}s_it$, where $i \in \{1, 2, \ldots, m\}$; $j, d_i \in \{0, 1, \ldots, p-1\}$.

Theorem 2.1. *Let K/F be a Galois extension with Galois group H and let $L/F = K(\sqrt[p]{b})/F$ be a Galois extension with Galois group $H \times C_p$ ($b \in F^\times \setminus F^{\times p}$). Choose $a_1, a_2, \ldots, a_m \in F^\times$ such that $\sigma_k \sqrt[p]{a_i} = \zeta^{\delta_{ik}} \sqrt[p]{a_i}$ (δ_{ik} is the Kronecker delta). Then the obstruction to the embedding problem given by L/F and the group extension* (2.1) *is*

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

Proof. The crossed product algebra $B = (K, H, \zeta)$ is included in $A = (L, H \times C_p, \zeta)$, therefore A is a tensor product of B and the centralizer of B in A: $A = B \otimes_F C_A(B)$. Now, consider the subalgebra $F[\sqrt[p]{b}, \sqrt[p]{b^j}\prod_{i=1}^m \sqrt[p]{a_i}^{d_i}t]$ in A. Since $t^p = \zeta^j$ and $t\sqrt[p]{b} = \zeta\sqrt[p]{b}t$, we have

$$\left(\sqrt[p]{b^j}\prod_{i=1}^m \sqrt[p]{a_i}^{d_i}t\right)^p = b^j\zeta^j\zeta^{jp(p-1)/2}\prod_{i=1}^m a_i^{d_i} = b^j\zeta^j\prod_{i=1}^m a_i^{d_i}.$$

We will show that the quaternion subalgebra $F[\sqrt[p]{b}, \sqrt[p]{b^j}\prod_{i=1}^m \sqrt[p]{a_i}^{d_i}t]$ is in fact the centralizer $C_A(B)$. Indeed, the degree of $C_A(B)$ is p and from $s_k\sqrt[p]{b} = \sqrt[p]{b}s_k$ for all k, follows that $\sqrt[p]{b}$ is in $C_A(B)$. Finally,

$$s_k\left(\sqrt[p]{b^j}\prod_{i=1}^m \sqrt[p]{a_i}^{d_i}t\right) = \sqrt[p]{b^j}\prod_{i=1}^m\left(\zeta^{\delta_{ik}}\sqrt[p]{a_i}\right)^{d_i}s_kt = \sqrt[p]{b^j}\prod_{i=1}^m\left(\zeta^{\delta_{ik}}\sqrt[p]{a_i}\right)^{d_i}\zeta^{-d_k}ts_k$$

$$= \zeta^{-d_k} \prod_{i=1}^{m} \zeta^{\delta_{ik} d_i} \sqrt[p]{b}^{j} \prod_{i=1}^{m} \sqrt[p]{a_i}^{d_i} t s_k = \left(\sqrt[p]{b}^{j} \prod_{i=1}^{m} \sqrt[p]{a_i}^{d_i} t \right) s_k,$$

since $\sum_{i=1}^{m} \delta_{ik} d_i = d_k$. The theorem is done. □

One can easily obtain an analog of the latter theorem for $p = 2$. Here we get as an immediate corollary the criterion for $(p, p, \ldots, p)$ central extensions, which can be found also in [Sw].

Corollary 2.2. *Let* $L/F = F(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \ldots, \sqrt[p]{a_n})/F$ *be a* $(C_p)^n$ *extension, and let* $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathrm{Gal}(L/F)$ *be given by* $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}$ *(δ_{ij} is the Kronecker delta). Let*

$$1 \to C_p \to G \to \mathrm{Gal}(L/F) \to 1$$

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} $(i \leqslant j)$ *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 given by* L/F *is*

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

Proof. We apply induction by n. For $n = 1$ the group G is isomorphic to C_{p^2}, so the obstruction is $(a_1, \zeta; \zeta)$. Now, let for $n - 1$ the obstruction have the form as in the statement. Denote by H the Galois group of $K/F = F(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_{n-1}})/F$. By induction $[K, H, \mathrm{res}\,\gamma] = \prod_{i=1}^{n-1} (a_i, \zeta; \zeta)^{d_{ii}} \prod_{i<k} (a_i, a_k; \zeta)^{d_{ik}}$, where for the second product k runs through the set $\{1, 2, \ldots, n-1\}$. Then Theorem 2.1 implies that the obstruction to the original embedding problem is

$$[K, H, \mathrm{res}\,\gamma] \left(a_n, a_n^{d_{nn}} \zeta^{d_{nn}} \prod_{i=1}^{n-1} a_i^{-d_{in}}; \zeta \right).$$

Since $(a_n, a_n; \zeta) = 1$ and $(a_n, a_i^{-d_{in}}; \zeta) = (a_i, a_n; \zeta)^{d_{in}}$, finally we obtain the obstruction

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

3. The non-abelian groups of order p^3

In this section we will investigate the realizability of the two non-abelian groups of order p^3. 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 $g_1^p = g_2^p = g_3^p = 1$, $g_1 g_2 = g_2 g_1 g_3$ and g_3 is central. The Heisenberg group is discussed, for example, in [JLY,Ma,MS,Br], but not in terms of quaternion algebras. Let $K = F(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ be a $C_p \times C_p$ extension of F and let $K_i = F(\sqrt[p]{a_i})$, $i = 1, 2$. Denote by H the Galois group of K/F and the generators of H by σ_1 and σ_2, such that $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}$, $i = 1, 2$.

Theorem 3.1. *The embedding problem given by K/F and the group extension*

$$1 \to \langle g_3 \rangle \cong C_p \to G_1 \xrightarrow[\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}]{} H \to 1$$

is solvable if and only if $a_2 \in N_{K_1/F}(K_1^\times)$. 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 $\{K(\sqrt[p]{f\alpha}) \mid f \in F^\times\}$ gives all solutions.

Proof. From Corollary 2.2 follows that the obstruction is $(a_1, a_2; \zeta) \in \mathrm{Br}(F)$. Whence the embedding problem is solvable if and only if $a_2 \in N_{K_1/F}(K_1^\times)$.

Now, let $\omega \in K_1^\times$ be such that $N_{K_1/F}(\omega) = a_2$ and let α be given as in the statement of the theorem. Calculations show that $\sigma_2(\alpha) = \alpha$ and $\sigma_1(\alpha) = \alpha x^p$, where $x = \sqrt[p]{a_2}/\omega \in K^\times$. Therefore $L = K(\sqrt[p]{f\alpha})$ is Galois over F. Furthermore, $x\sigma_1(x) \cdots \sigma_1^{p-1}(x) = 1$, so the pre-image of σ_1 in $\mathrm{Gal}(L/F)$ has order p. The same holds for σ_2, whence $\mathrm{Gal}(L/F) \cong G_1$. □

Now, we consider the other non-abelian group of order p^3. We denote it by G_2 and its generators by g_1 and g_2, such that $g_1^{p^2} = g_2^p = 1$ and $g_1 g_2 = g_2 g_1^{p+1}$.

Theorem 3.2. *The embedding problem given by K/F and the group extension*

$$1 \to \langle g_1^p \rangle \cong C_p \to G_2 \xrightarrow[\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}]{} H \to 1$$

is solvable if and only if $a_2\zeta \in N_{K_1/F}(K_1^\times)$. 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 $\{K(\sqrt[p]{f\sqrt[p]{a_1}^{-1}\alpha}) \mid f \in F^\times\}$ gives all solutions.

Proof. From Corollary 2.2 follows that the obstruction is $(a_1, a_2\zeta; \zeta) \in \mathrm{Br}(F)$. Whence the embedding problem is solvable if and only if $a_2\zeta \in N_{K_1/F}(K_1^\times)$.

Now, let $\omega \in K_1^\times$ be such that $N_{K_1/F}(\omega) = a_2\zeta$, let α be given as in the statement of the theorem and denote $\alpha_1 = \sqrt[p]{a_1}^{-1}\alpha$. Calculations show that $\sigma_2(\alpha_1) = \alpha_1$ and $\sigma_1(\alpha_1) = \alpha_1\beta^p$, where $\beta = \sqrt[p]{a_2}/\omega \in K^\times$. Therefore, $L = K(\sqrt[p]{f\alpha_1})$ is Galois over F for all $f \in F^\times$. Furthermore, $\beta\sigma_1(\beta) \cdots \sigma_1^{p-1}(\beta) = \zeta^{-1}$, so the pre-image of σ_1 in $\mathrm{Gal}(L/F)$ has order p^2, whence $\mathrm{Gal}(L/F) \cong G_2$. □

4. Non-abelian groups of order p^4

In this section we will discuss the central embedding problems, involving the non-abelian groups of order p^4, that have a factor-group of the kind $H \times C_p$. Generally, there are 15 groups of order p^4 for any odd prime p. The description of these groups, by generators and relations between them, can be obtained by using the data base in the computer program GAP 4. In some cases, however, the descriptions depend on the prime number p, therefore we cannot consider realizability issues in general without a specification of p. Fortunately, the mentioned four non-abelian groups posses an easy description. Of course, we will not bother about the groups $G_1 \times C_p$ and $G_2 \times C_p$, since their realizability depends only on the realizability of G_1 and G_2. From

these four groups three have as a factor-group the group $C_{p^2} \times C_p$ and one has $(C_p)^3$ as a factor-group.

Firstly, let us describe the non-abelian groups, having $C_{p^2} \times C_p$ as a factor-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 presentations are not minimal, but are convenient for our goals. The symbol $[a, b]$ below stands for the commutator $a^{-1}b^{-1}ab$.

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

The corresponding central group extensions are as follows:

$$1 \to \langle g_3 \rangle \cong C_p \to G_3 \xrightarrow[\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}]{} C_{p^2} \times C_p \to 1, \tag{4.1}$$

$$1 \to \langle g_3 \rangle \cong C_p \to G_4 \xrightarrow[\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}]{} C_{p^2} \times C_p \to 1, \tag{4.2}$$

$$1 \to \langle g_4 \rangle \cong C_p \to G_5 \xrightarrow[\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}]{} C_{p^2} \times C_p \to 1. \tag{4.3}$$

The last group is given by the presentation

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

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

$$1 \to \langle g_4 \rangle \cong C_p \to G_6 \xrightarrow[g_i \mapsto \rho_i]{} (C_p)^3 \to 1. \tag{4.4}$$

Our first goal is to find the obstructions to realizability of these four groups as Galois groups by investigating the embedding problems associated to the corresponding central group extensions. Recall the notation from the previous section. Let F be a field with characteristic $\neq p$, let ζ be a primitive pth root of unity in F for an odd prime p and let a_1, a_2 be elements of $F^\times$, linearly independent modulo $F^{\times p}$. Denote $K = F(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ and $K_i = F(\sqrt[p]{a_i})$, $i = 1, 2$. Now, assume that the embedding problem $C_{p^2} \to C_p \cong \mathrm{Gal}(F(\sqrt[p]{a_1})/F)$ is solvable. Then $(a_1, \zeta; \zeta) = 1$, so there exists $\alpha \in K_1$, such that $\zeta = N_{K_1/F}(\alpha)$. Choose one C_{p^2} extension over F: $L_1 = K_1(\sqrt[p]{f_1\beta})$, where $f_1 \in F^\times$ 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 will find the obstructions and describe the extensions in the following three theorems.

Theorem 4.1. *The obstruction to solvability of the embedding problem given by the Galois extension L/F and the group extension* (4.1) *is $(a_2, a_1; \zeta)$. If the embedding problem is solvable, i.e., $a_2 = N_{K_1/F}(\omega)$ 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 $\{L(\sqrt[p]{f_2\gamma})/F \mid f_2 \in F^\times\}$.*

Proof. Since the pre-image of the group C_{p^2} in G_3 is isomorphic to $C_{p^2} \times C_p$, the crossed product algebra $[L_1, C_{p^2}, \zeta]$ is trivial in $\mathrm{Br}(F)$. From Theorem 2.1 then follows that the obstruction to the solvability of our problem is $(a_1, a_2; \zeta^{-1}) = (a_2, a_1; \zeta)$.

Now, let $(a_2, a_1; \zeta) = 1 \in \mathrm{Br}(F)$ and let γ be given as in the statement of the theorem. Then $\sigma_2(\gamma)/\gamma = 1$ and $\sigma_1(\gamma)/\gamma = N_{K_1/F}(\omega)/\omega^p = a_2/\omega^p$. Whence $\sigma_1(\gamma) = \gamma x^p$ for $x = \sqrt[p]{a_2}/\omega \in K^\times$. Therefore $M = L(\sqrt[p]{\gamma})$ is Galois over F.

We can put for the pre-images g_1 and g_2 of σ_1 and σ_2 in $\mathrm{Gal}(M/F)$, respectively, $g_1(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma} x$ and $g_2(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}$. Obviously $\operatorname{ord} g_2 = p$. From the equations $g_1^p(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma} a_2/N_{K_1/F}(\omega) = \sqrt[p]{\gamma}$ follows that $\operatorname{ord} g_1 = \operatorname{ord} \sigma_1 = p^2$. Furthermore, one can easily check the equations $g_3(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}\zeta$ and $[g_3, g_1](\sqrt[p]{\gamma}) = [g_3, g_2](\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}$, whence we obtain the relations $\operatorname{ord} g_3 = p$ and $[g_3, g_1] = [g_3, g_2] = 1$. Thus we have shown that M/F is exactly a G_3-extension. □

Theorem 4.2. *The obstruction to solvability of the embedding problem given by the Galois extension L/F and the group extension* (4.2) *is $(a_2, a_1\zeta; \zeta)$. If the embedding problem is solvable, i.e., $a_1\zeta = N_{K_2/F}(x)$ 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 $\{L(\sqrt[p]{f_2\omega})/F \mid f_2 \in F^\times\}$.*

Proof. Similarly to Theorem 4.1 we obtain the obstruction $(a_2, a_1\zeta; \zeta)$. Now, assume $(a_2, a_1\zeta; \zeta) = 1$ and ω is as in the statement. In that case $\sigma_1(\omega)/\omega = 1$ and $\sigma_2(\omega)/\omega = x^p/a_1 \in K^{\times p}$, so $M/F = L(\sqrt[p]{\omega})/F$ is Galois. We can put for the pre-images g_1 and g_2 of σ_1 and σ_2 in $\mathrm{Gal}(M/F)$: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$ and $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}x/\sqrt[p]{a_1}$. It is not hard to check that $g_3 = g_2^p$ is of order p and $g_3 = [g_2, g_1]$, which means that $\mathrm{Gal}(M/F) \cong G_4$. □

Theorem 4.3. *The obstruction to solvability of the embedding problem given by the Galois extension L/F and the group extension* (4.3) *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 F, then the obstruction is $(\zeta_{p^2}^{-1}a_2, a_1; \zeta)$. Given that the embedding problem is solvable, i.e., $\zeta_{p^2}^{-1}a_2 = N_{K_1/F}(y)$, 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 $\{L(\sqrt[p]{f\omega})/F \mid f \in F^\times\}$.*

Proof. Here the pre-image of C_{p^2} in G_5 is isomorphic to the cyclic group C_{p^3} and for this group is not clear how to express the crossed product algebra $[L_1, C_{p^2}, \zeta]$ as a product of quaternion algebras. That is why we leave the obstruction in this form: $[L_1, C_{p^2}, \zeta](a_2, a_1; \zeta)$. However, when ζ is in $F^{\times p}$, from [Pi, Chapter 15, §15.1, Corollary b], follows that $[L_1, C_{p^2}, \zeta] = [K_1, C_p, \zeta_{p^2}] = (a_1, \zeta_{p^2}; \zeta)$. In this case the obstruction accepts the form $(a_1, \zeta_{p^2}; \zeta)(a_2, a_1; \zeta) = (\zeta_{p^2}^{-1}a_2, a_1; \zeta)$.

Now, assume that $(\zeta_{p^2}^{-1}a_2, a_1; \zeta) = 1$, $L_1 = F(\sqrt[p^2]{a_1})$ and ω is as in the statement. In that case $\sigma_1(\omega)/\omega = a_2/y^p \in L^{\times p}$ and $\sigma_2(\omega)/\omega = 1$, so $M/F = L(\sqrt[p]{\omega})/F$ is Galois. We can put for the pre-images g_1 and g_2 of σ_1 and σ_2 in $\mathrm{Gal}(M/F)$: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\sqrt[p]{a_2}/y$ and $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$. Then $g_1^{p^2}(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$ and $[g_2, g_1](\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$, whence $g_1^{p^2} = [g_2, g_1]$ is of order p, so we have a G_5 extension. □

Now, we turn our attention to the group G_6. We need to introduce some new notation. Let $a_1, a_2, a_3 \in F^\times$, $K_i = F(\sqrt[p]{a_i})$ $(i = 1, 2, 3)$ and let $K/F = F(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \sqrt[p]{a_3})/F$ be a $(C_p)^3$

extension with generators ρ_1, ρ_2 and ρ_3, such that $\rho_j(\sqrt[p]{a_i})/\sqrt[p]{a_i} = \zeta^{\delta_{ij}}$ ($i, j = 1, 2, 3$ and δ_{ij} as usual is the Kronecker delta).

Theorem 4.4. *The obstruction to solvability of the embedding problem given by the Galois extension K/F and the group extension* (4.4) *is* $(a_3, \zeta; \zeta)(a_2, a_1; \zeta)$. *Given that* $(a_3, \zeta; \zeta) = (a_2, a_1; \zeta) = 1$, *i.e., there exists* $x \in K_3$, *such that* $\zeta = N_{K_3/F}(x)$ *and exists* $y \in K_2$, *such that* $a_1 = N_{K_2/F}(y)$, *we may put* $\omega = \sqrt[p]{a_3}(y^{p-1}\rho_2(y)^{p-2}\cdots\rho_2^{p-2}(y))^{-1}(x^{p-1}\rho_3(x)^{p-2}\cdots\rho_3^{p-2}(x))^{-1}$. *Then all Galois extensions realizing G_6 are* $\{K(\sqrt[p]{f\omega})/F \mid f \in F^\times\}$.

Proof. The obstruction follows directly from Corollary 2.2. Now, let ω be defined as in the statement. Then we have $\rho_1(\omega)/\omega = 1$, $\rho_2(\omega)/\omega = y^p/a_1 \in K^p$ and $\rho_3(\omega)/\omega = x^p \in K^p$. Therefore $K(\sqrt[p]{\omega})/F$ is Galois. Now we may put for the pre-images g_1, g_2 and g_3 of ρ_1, ρ_2 and ρ_3 in $\mathrm{Gal}(K(\sqrt[p]{\omega})/F)$: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$, $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}y/\sqrt[p]{a_1}$ and $g_3(\sqrt[p]{\omega}) = \sqrt[p]{\omega}x$. Then it is easy to verify that $g_1^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$, $g_2^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$, $g_3^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$ and $[g_2, g_1](\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$, whence we get exactly a G_6 extension. □

5. Automatic realizations

In this section we remove the condition that a primitive root of unity belongs to the ground field F. Our intentions follow that of [Br], which are both to describe Galois extensions and to discover automatic realizability. For example, in the latter work is discovered the automatic realizability $G_1 \Rightarrow G_2$, i.e., if the group G_1 is realizable over any field F, then G_2 is also realizable over the same field. We prove that the automatic realization $G_3 \Rightarrow G_4$ also holds. The converse realization $G_4 \Rightarrow G_3$ does not hold, as we will see in the following section.

Now, let F be arbitrary field with characteristic not p, which does not contain pth roots of unity. Choose arbitrary, but fixed primitive pth root of unity ζ. Then the extension $F(\zeta)/F$ is cyclic of degree d, so d must divide $p-1$. Let κ be a generator of the group $\mathrm{Gal}(F(\zeta)/F)$, which is isomorphic to the cyclic group C_d. Then there exists $e \in \mathbb{Z} \setminus p\mathbb{Z}$, such that $\kappa(\zeta) = \zeta^e$. Let K/F be a p-extension with Galois group $H = \mathrm{Gal}(K/F)$. Then $K(\zeta)/F(\zeta)$ is also a H-extension and we may identify the groups $\mathrm{Gal}(K/F)$ and $\mathrm{Gal}(K(\zeta)/F(\zeta))$. We may as well identify the groups $\mathrm{Gal}(K(\zeta)/K)$ and $\mathrm{Gal}(F(\zeta)/F)$. The following theorem is remarkable not only because of its statement, but also of the constructions which appear in the proof. It may be looked upon as a compilation of [Gi, Théorème 5], [Br, Theorem 4] and [JLY, Theorem 6.6.4].

Theorem 5.1. *Let*

$$1 \to C_p \to G \underset{\pi}{\to} H \to 1 \tag{5.1}$$

be a non-split group extension. Then the embedding problem given by (5.1) *and K/F is solvable $\Leftrightarrow$ the embedding problem given by* (5.1) *and $K(\zeta)/F(\zeta)$ is solvable.*

Proof. The forward implication is clear. For the reverse direction, let $K(\zeta, \sqrt[p]{\beta})/F(\zeta)$ be a solution to the embedding problem for some $\beta \in K(\zeta)^\times$. Then for all $\sigma \in H$ there exists $x_\sigma \in K(\zeta)^\times$, such that $\sigma(\beta)/\beta = x_\sigma^p$. We may extend σ to $K(\zeta, \sqrt[p]{\beta})$: $\bar{\sigma}(\sqrt[p]{\beta}) = x_\sigma \sqrt[p]{\beta}$. Then for all σ and τ in H we have $\bar{\sigma}\bar{\tau}\overline{\sigma\tau}^{-1}(\sqrt[p]{\beta})/\sqrt[p]{\beta} = x_\sigma \sigma(x_\tau) x_{\sigma\tau}^{-1} = \zeta^{X(\sigma,\tau)}$, where $X(\sigma, \tau)$ is the 2-cocycle from H to $\mathbb{F}_p$. (Note that we may identify the group $C_p = \mathrm{Gal}(K(\zeta, \sqrt[p]{\beta})/K(\zeta))$ with

$\mathbb{F}_p$ by the Kummer theorem.) Thus, to the epimorphism π (i.e., to the group extension (5.1)) corresponds the 2-coclass $[X] \in H^2(H, \mathbb{F}_p)$. Let the natural number m be such that $mde^{d-1} \equiv 1 \pmod{p}$. Define the map $\Phi : K(\zeta) \to K(\zeta)$ by

$$\Phi(x) = \left(x^{e^{d-1}} \kappa\left(x^{e^{d-2}}\right) \cdots \kappa^{d-1}(x)\right)^m,$$

for $x \in K(\zeta)$. Note that $\Phi(\zeta) = (\zeta^{de^{d-1}})^m = \zeta$. If we put $\omega = \Phi(\beta)$ and $y_\sigma = \Phi(x_\sigma)$, then $\sigma(\omega)/\omega = y_\sigma^p$. Furthermore, $\kappa(\omega)/\omega^e = (\beta^{-m(e^d-1)/p})^p$, so $K(\zeta, \sqrt[p]{\omega})/F$ is Galois. Then

$$y_\sigma \sigma(y_\tau) y_{\sigma\tau}^{-1} = \Phi\left(x_\sigma \sigma(x_\tau) x_{\sigma\tau}^{-1}\right) = \Phi\left(\zeta^{X(\sigma,\tau)}\right) = \zeta^{X(\sigma,\tau)}.$$

Therefore, we obtain the same 2-cocycle and in particular the isomorphism $\mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/F(\zeta)) \cong \mathrm{Gal}(K(\zeta, \sqrt[p]{\beta})/F(\zeta))$. Let us extend σ and κ to $K(\zeta, \sqrt[p]{\omega})$ by $\hat{\sigma}(\sqrt[p]{\omega}) = y_\sigma \sqrt[p]{\omega}$ and $\bar{\kappa}(\sqrt[p]{\omega}) = \beta^{-m(e^d-1)/p} \sqrt[p]{\omega}^e$, where $\bar{\kappa}$ is the only pre-image of order d. Then

$$\bar{\kappa}\hat{\sigma}(\sqrt[p]{\omega}) = \kappa(y_\sigma)\beta^{-m(e^d-1)/p} \sqrt[p]{\omega}^e$$

and

$$\hat{\sigma}\bar{\kappa}(\sqrt[p]{\omega}) = \beta^{-m(e^d-1)/p} x_\sigma^{-m(e^d-1)} y_\sigma^e \sqrt[p]{\omega}^e,$$

but $\kappa(y_\sigma) = x_\sigma^{-m(e^d-1)} y_\sigma^e$, so $\bar{\kappa}\hat{\sigma} = \hat{\sigma}\bar{\kappa}$. In this way we obtain the isomorphism $\mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/F) \cong G \times C_d$, where $G \cong \mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/F(\zeta))$, and C_d is generated by $\bar{\kappa}$. The fixed field $L = K(\zeta, \sqrt[p]{\omega})^{C_d}$ of C_d then gives us a solution to the embedding problem given by K/F and (5.1). The theorem is done. □

Now, we can prove the automatic realization $G_3 \Rightarrow G_4$.

Theorem 5.2. *Let F be arbitrary field. If G_3 is realizable over F, then so is G_4. If F has characteristic p or if $x^{p^2} - 1$ splits in $F(\zeta)$, then the converse also holds.*

Proof. If F has characteristic p, then the realizability of a p-group over F depends only on its rank (see [Wi, Satz, p. 237]), so G_3 and G_4 both having rank two, the theorem holds.

From now on, let us assume that F has characteristic not p. If $x^{p^2} - 1$ splits in F, then the obstructions which are calculated in Theorems 4.1 and 4.2 are equivalent, so the realizability of one of the two groups implies the realizability of the other. Note that the intermediate field L, described in the later theorems is the same for both groups. Now, suppose that $x^p - 1$ splits in F, but $x^{p^2} - 1$ does not. Suppose that M is a Galois extension of F with $\mathrm{Gal}(M/F)$ isomorphic to G_3, and let L be the intermediate (p^2, p) subextension, as described before Theorem 4.1. The images of a_1 and a_2 in $F^\times/F^{\times p}$ are linearly independent and therefore cannot both be contained in the line generated by the image of ζ. If ζ and a_2 are linearly independent, we can put $a_1 = \zeta^{-1}$, so $(a_1, \zeta; \zeta) = (a_2, \zeta a_1; \zeta) = 1$. In the other case, i.e., if a_1 and ζ are linearly independent, we can put $a_2 = \zeta$, so again $(a_1, \zeta; \zeta) = (a_2, \zeta a_1; \zeta) = 1$. Thus we conclude that G_4 is realizable over F.

Finally, let us drop the assumption that $x^p - 1$ splits in F. Suppose N/F is a Galois extension, such that $\mathrm{Gal}(N/F)$ is isomorphic to G_3. Then so is $\mathrm{Gal}(N(\zeta)/F(\zeta))$. Then from what we have

already proved follows that exists a G_4 extension $M/F(\zeta)$. Moreover, if $x^{p^2}-1$ splits in $F(\zeta)$, then we may choose M, such that its intermediate (p^2, p) subextension is the same as that of $N(\zeta)$; as before we call this field L. We know that $L = L'(\zeta)$, where L' is the intermediate (p^2, p) subextension of N/F. It now follows from Theorem 5.1 that L' is contained in a G_4 extension of F. The converse follows similarly. If $x^{p^2}-1$ does not split in $F(\zeta)$, let L_1 and L_2 be the intermediate (p^2, p) subextensions of $N(\zeta)/F(\zeta)$ and $M/F(\zeta)$, respectively. Let $K = F(\zeta)(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ be the intermediate (p, p) subextension of $L_1/F(\zeta)$ for some a_1 and a_2 in $F(\zeta)$. We have two cases.

First, if a_2 and ζ are linearly independent, we can take $F(\zeta)(\sqrt[p]{\zeta^{-1}}, \sqrt[p]{a_2})$ as an intermediate (p, p) extension; and put $L_2 = F(\zeta)(\sqrt[p^2]{\zeta^{-1}}, \sqrt[p]{a_2})$ as an intermediate (p^2, p) extension. Note that L_1, being the composite of $F(\zeta)$ and a (p^2, p) extension of F is abelian over F. In particular $F(\zeta)(\sqrt[p]{a_2})$ is abelian over F. So is $F(\zeta)(\sqrt[p^2]{\zeta^{-1}}) = F(\zeta_{p^3})$. Hence L_2 is also an abelian extension of F, and since p does not divide $[F(\zeta) : F]$, there has to exist a (p^2, p) extension L_2' of F, such that $L_2 = L_2'(\zeta)$. Thus we can use Theorem 5.1 again.

Second, if a_1 and ζ are linearly independent, we can take $F(\zeta)(\sqrt[p]{a_1}, \sqrt[p]{\zeta})$ as an intermediate (p, p) subextension of $L_2/F(\zeta)$. We have the (p^2, p) extension $L_1 = F(\zeta)(\sqrt[p]{f_1\beta}, \sqrt[p]{a_2})$ given above Theorem 4.1. (We note a slight inconformity between the descriptions of L and L_1, given before Theorem 4.1 and these given here, which at this point is hard to avoid.) Then L_1, being a composite of $F(\zeta)$ and a (p^2, p) extension of F, is abelian over F. In particular $F(\zeta)(\sqrt[p]{f_1\beta})$ is abelian over F and so is $F(\zeta)(\sqrt[p]{\zeta}) = F(\zeta_{p^2})$. Hence L_2 is also an abelian extension of F. Since p does not divide $[F(\zeta) : F]$, there exists a (p^2, p) extension L_2' of F, such that $L_2 = L_2'(\zeta)$. Thus we can use Theorem 5.1 again, and we are done. □

We will show in the following section that the converse realization need not hold in the case when $x^{p^2}-1$ does not split in $F(\zeta)$.

6. Local fields

Let F be a local field, i.e., locally compact with respect to a non-trivial valuation. Thus it is

(a) a finite extension of $\mathbb{Q}_p$ for some prime p;
(b) a finite extension of $\mathbb{F}_p((T))$, where $\mathbb{F}_p$ is the field with p elements; or
(c) $\mathbb{R}$ or $\mathbb{C}$.

We denote by v the regular valuation of F, by π the conforming element of v (also called uniformizing or prime element of F), and by U the group of units of F. Then every element of $F^\times$ can be written uniquely in the form $a = \pi^m u$ with $u \in U$ and $m = \operatorname{ord}_F(a)$. The residue field $\overline{F}$ of F has q elements, and its characteristic is p. For every natural number n there exists a unique unramified extension F_n of degree n over F. The field F_n is the splitting field of the polynomial $x^{q^n-1}-1$. Denote by H_n the Galois group of the extension F_n/F, which is cyclic of order n, generated by some element φ_n. Then we have the isomorphism

$$\text{INV}: \quad H^2\big(H_n, F_n^\times\big) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}. \tag{6.1}$$

Given an arbitrary $x \in F_n^\times$, we can define the crossed homomorphism $f \in Z^2(H_n, F_n)$ by

$$f\left(\varphi_n^i, \varphi_n^j\right) = \begin{cases} 1, & 0 \leqslant i, j, i+j < n, \\ x, & 0 \leqslant i, j < n \leqslant i+j. \end{cases} \tag{6.2}$$

Denote by $[f]$ the 2-coclass generated by f in $H^2(H_n, F_n^\times)$. Then the isomorphism (6.1) is given by

$$\mathrm{INV}: \quad [f] \mapsto \frac{v(x)}{n} + \mathbb{Z}.$$

Denote by $\mathcal{G}(F)$ the set of all finite dimensional central simple algebras over F. Let the algebra $A \in \mathcal{G}(F)$ be of degree n over F. Then $[A] = [(F_n, H_n, f)]$, where F_n, H_n and f are as before. Therefore, $\mathrm{INV}([A]) = \frac{v(x)}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Let $A, B \in \mathcal{G}(F)$. Here are some properties of the isomorphism INV:

- $A \sim B$ (i.e., $[A] = [B]$) $\Leftrightarrow \mathrm{INV}(A) = \mathrm{INV}(B)$;
- $A \sim F$ (i.e., $[A] = 1$) $\Leftrightarrow \mathrm{INV}(A) = 0$;
- $\mathrm{INV}(A \otimes B) = \mathrm{INV}(A) + \mathrm{INV}(B)$.

Next, consider the cyclic algebra $B = (F_n, H_n, f)$. The algebra B is fully described by the following properties:

- $B = \bigoplus_{0 \leqslant j < n} u^j F_n$;
- $u^{-1} d u = \varphi_n(d)$, $\forall d \in F_n$, where φ_n is the Frobenius automorphism of the extension F_n/F;
- $u^n = x \in F^\times$.

The system of factors f is defined by

$$u_{\varphi_n^i} u_{\varphi_n^j} = f\left(\varphi_n^i, \varphi_n^j\right) u_{\varphi_n^{i+j}}.$$

It can be shown that f fulfills formula (6.2). We put $u_{\varphi_n} = u$, $u_{\varphi_n^i} = u^i$, $u_1 = u^n = x$.

Let from now on F contain a primitive nth root of unity ζ. Denote by $\mathfrak{p}$ the prime ideal generated by the conforming element $\pi \in F$. Let $q = \mathbb{N}\mathfrak{p}$ be the number of elements in the residue field $\overline{F}$. Then $\mathbb{F}_q^\times$ is cyclic of order $q-1$, so $n \mid q-1$ and $u^{\frac{q-1}{n}} \in \langle \zeta \rangle = \mu_n \in \mathbb{F}_q^\times$. For $a \in F^\times$ define $(a \mid \mathfrak{p})$ to be the unique nth root of unity, such that $(a \mid \mathfrak{p}) \equiv a^{\frac{q-1}{n}} \pmod{\mathfrak{p}}$.

Theorem 6.1. *For $a \in F^\times$, such that $\mathrm{ord}_F\, a = 0$ the following statements are equivalent*:

(a) $(a \mid \mathfrak{p}) = 1$;
(b) *a becomes an nth power in $\overline{F}$*;
(c) *a becomes an nth power in F.*

Now, define the Hilbert Symbol $(a, b)_v$ for the local field F:

$$(a, b)_v = \zeta^{n\,\mathrm{INV}_v(a, b; \zeta)}.$$

Because the generalized quaternion algebra $(a, b; \zeta)$ is split by a field of degree n, its invariant is an element of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and hence $n\,\mathrm{INV}_v(a, b; \zeta)$ is an element of $\mathbb{Z}/n\mathbb{Z}$. Thus we have a bilinear pairing $F^\times/F^{\times n} \times F^\times/F^{\times n} \to \mu_n = \langle\zeta\rangle$. It can be easily proved that a product of quaternion classes in the Brauer group is split if and only if the product of corresponding Hilbert symbols is 1.

Now, assume $(a, b; \zeta)$ is a division algebra, generated by elements α and β, such that $\alpha^n = a$, $\beta^n = b$ and $\beta\alpha = \zeta\alpha\beta$. Recall that, to compute the invariant of a central division algebra D over a local field F, we:

(a) choose a maximal unramified field $L = F(i)$ in D, where $i^n = c \in F$;
(b) find an element $j \in D$, such that $x \mapsto jxj^{-1}$ is the Frobenius automorphism of L by the Noether–Skolem theorem;
(c) then we have $\mathrm{INV}_v([D]) = v(j) + \mathbb{Z}$.

We apply this with the unramified extension $L = F(\alpha) = F(\sqrt[n]{a})$. Let $(a \mid \mathfrak{p}) = \zeta^r$, so that $(\mathfrak{p}, L/F)(\alpha) = \zeta^r\alpha$, where $(\mathfrak{p}, L/F)$ is the Frobenius element at $\mathfrak{p}$, corresponding to the Frobenius automorphism in $\mathrm{Gal}(\overline{F(\alpha)}/\overline{F})$. Since $\beta\alpha\beta^{-1} = \zeta\alpha$, we see that we can take $j = \beta^r$. Then $j^n = b^r$, and so $v(j) = \frac{r}{n}v(b)$. Hence

$$(a, b)_v = \zeta^{n\,\mathrm{INV}_v(a,b;\zeta)} = \zeta^{r\,v(b)} = (a \mid \mathfrak{p})^{v(b)}.$$

Now, let $F = \mathbb{Q}_l$, where l is an odd prime, such that $l \equiv 1 \pmod p$, but $l \not\equiv 1 \pmod{p^2}$. Then $\zeta \in F$, but $\sqrt[p]{\zeta} = \zeta_{p^2} \notin F$. The unramified extension of F is the splitting field of the polynomial $g(x) = x^{l^p-1} - 1$ over F. Since p^2 divides $l^p - 1 = (l-1)(l^{p-1} + l^{p-2} + \cdots + l + 1)$, ζ_{p^2} is a root of $g(x)$, therefore $F(\zeta_{p^2})$ is the unramified extension. We have that $\dim_{\mathbb{F}_p} \mathbb{Q}_l^\times/\mathbb{Q}_l^{\times p} = 2$, i.e., $\mathbb{Q}_l^\times/\mathbb{Q}_l^{\times p}$ has p^2 elements. Therefore l and ζ generate $\mathbb{Q}_l^\times/\mathbb{Q}_l^{\times p}$ over $\mathbb{F}_p$. We now can fully describe the Hilbert symbol: $(\zeta, b)_l = (\zeta \mid l)^{v(b)} = \zeta^{\frac{l-1}{p}v(b)}$. In particular $(\zeta, b)_l = 1 \Leftrightarrow v(b) = 0$, i.e., $b \in U$. Hence there are only two embedding problems given by the group extension (1.2), and one of them is solvable, namely when a is contained in the line generated by ζ.

Let us consider now the groups G_1 and G_2. In order to have $(a_1, a_2)_l = 1$, the elements a_1 and a_2 must lie in the line generated by ζ, which is a contradiction to the assumption that they are linearly independent mod $(\mathbb{Q}_l)^p$. Therefore G_1 is not realizable over $\mathbb{Q}_l$. For $a_2 = \zeta^{-1}$, we get $(a_1, a_2\zeta)_l = 1$, so G_2 is realizable over $\mathbb{Q}_l$.

In order to construct embedding problems related to the group extensions (4.1) and (4.2), we must have $(a_1, \zeta)_l = 1$, i.e., a_1 and ζ must lie in one line. Then $(a_2, a_1) \neq 1$, since a_1 and a_2 cannot both lie in the line generated by ζ. Therefore G_3 is not realizable over $\mathbb{Q}_l$. For $a_1 = \zeta^{-1}$, we get $(a_2, a_1\zeta)_l = 1$, so the embedding problem given by (4.2) is solvable and the group G_4 is realizable over $\mathbb{Q}_l$. This shows that the automatic realization $G_4 \Rightarrow G_3$ does not hold.

In order to construct an embedding problem related to the group extensions (4.4), we must have $\dim_{\mathbb{F}_p} \mathbb{Q}_l^\times/\mathbb{Q}_l^{\times p} \geqslant 3$, which is impossible, so the group G_6 is not realizable over $\mathbb{Q}_l$.

Finally, let us consider the p-adic cyclotomic field $F = \mathbb{Q}_p(\zeta)$ for a primitive pth root of unity ζ. The Hilbert symbol can be fully described, as it is done, for example, in [Iw] and [CF]. We will now give some of the properties of the Hilbert symbol. The element $\pi = 1 - \zeta$ is conforming for the field F, which is totally ramified extension over $\mathbb{Q}_p$ of degree $p - 1$. Denote by U_i the subgroup of unities $\equiv 1 \pmod{\pi^i}$ in $F^\times$ for $i = 1, 2, \ldots$. Then the image of the element $\eta_i = 1 - \pi^i$ generates the group U_i/U_{i+1}, which is cyclic of order p. The elements

$\pi, \eta_1 = \zeta, \eta_2 = 1 - \pi^2, \ldots, \eta_p = 1 - \pi^p$ generate the group $F^\times / F^{\times p}$, which has order p^{p+1} and has dimension $p + 1$ over $\mathbb{F}_p$, so these generating elements can be chosen as a basis. Then the following lemmas hold.

Lemma 6.2. *For all i, j, such that $1 \leqslant i, j \leqslant p - 1$ we have $(\eta_j, \eta_i)_\pi = \prod_{r,s} \zeta^{i/s}$, where the product is taken for all $r, s \in \mathbb{N}$, such that $ri + sj = p$.*

Lemma 6.3. *The Hilbert pairing*

$$a, b \mapsto (a, b)_\pi : F^\times \times F^\times \to \mu_p$$

is the unique skew-symmetric pairing satisfying

(a) $(\eta_i, \eta_j)_\pi = (\eta_i, \eta_{i+j})_\pi (\eta_{i+j}, \eta_j)_\pi (\pi, \eta_{i+j})_\pi^j$, *for all* $i, j \geqslant 1$;

(b) $(\pi, \eta_i)_\pi = \begin{cases} 1, & 1 \leqslant i \leqslant p - 1, \\ \zeta, & i = p; \end{cases}$

(c) $(*, *)_\pi = 1$ *on* $U_i \times U_j$ *if* $i + j \geqslant p + 1$.

Consider the embedding problem involving the group C_{p^2}, given by the group extension (1.2). From Lemma 6.3 follows that $(a, \zeta)_\pi = 1$ for $a = \pi, \zeta$ and η_p, so the problem is solvable in these cases. Since $\dim_{\mathbb{F}_p} F^\times / F^{\times p} = p + 1$, we have $p + 1$ essentially different embedding problems given by (1.2). Here the question arises—which are the values of a, such that the embedding problem is solvable? We managed to prove, by applying Lemma 6.3, that if $\frac{p-1}{2} \leqslant j \leqslant p - 1$ the embedding problem for $a = \eta_j$ is not solvable. By applying Lemma 6.2 we obtained that if $p = 11$ the embedding problem is also solvable for $a = \eta_3$. It is not hard to show that for all a_1, such that we can construct the embedding problems given by (4.1) and (4.2), there exists a_2, such that these embedding problems are solvable. Finally, for $a_1 = \zeta$, $a_2 = \pi$ and $a_3 = \eta_p$ we have $(a_3, \zeta)_\pi = (a_2, a_1)_\pi = 1$, therefore the embedding problem given by (4.4) is solvable.

References

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

[CF] J.W.S. Cassels, A. Fröhlich, Algebraic Number Theory, Academic Press, 1967.

[Gi] R. Gillard, Plongement d'une extension d'ordre p ou p^2 dans une surextension non abelienne d'ordre p^3, J. Reine Angew. Math. 268–269 (1974) 418–426.

[Iw] K. Iwasawa, Local Class Field Theory, Oxford, 1986.

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

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

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

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

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

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

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