SOME GROUPS OF ORDERS 8 AND 16 AS GALOIS GROUPS OVER THE p-ADIC NUMBER FIELD

IVO M. MICHAILOV

Abstract. In this paper we analyze the isomorphism between the Brauer group $Br(k)$, over an arbitrary local field k, and the factor-group $\mathbb{Q}/\mathbb{Z}$. Then we find all solvable embedding problems with kernel of order 2 for some groups of orders 8 and 16 over the field $\mathbb{Q}_p$ of the p-adic numbers (p is a prime).

1. The embedding problem over an arbitrary field

We begin by giving the definition of the embedding problem over an arbitrary field k. Let K/k be a finite Galois extension with Galois group F and let

$$1 \to N \to G \underset{\psi}{\to} F \to 1 \tag{1.1}$$

is a finite group extension. The embedding problem given by (1.1) then consists in determining whether there exists a Galois extension L/k, containing K, such that $G \cong Gal(L/k)$ and for all automorphisms $\sigma \in G$ the restriction $\sigma|_K$ equals to $\psi(\sigma)$. The embedding problem is denoted by $(K/k, G, N)$. The group N is called *the kernel* of the embedding problem. If a Galois algebra is allowed as a solution to the embedding problem, we talk about "weak" solvability. Given that N is contained in the Frattini subgroup of G, i.e., $\mathrm{rank}(G) = \mathrm{rank}(F)$, the two terms for solvability are equivalent. A necessary condition to solvability is the so called *compatibility condition*. Since we are going to consider only embedding problem with an abelian kernel, we give the following form of the compatibility condition for the embedding problem with an abelian kernel N.

Assume that the Galois extension K/k contains a primitive root of unity of degree equal to the period of N and also that the characteristic of k is relatively prime to the period of N. Then is well defined the character group $\widehat{N} = Hom(N, K^{\times})$. The kernel N becomes an F-operator group by the rule $\chi^{\sigma}(a) = [\chi(\sigma a \sigma^{-1})]^{\sigma}$ for all $\sigma \in F$ and $a \in N$. Denote $F_{\chi} = \{\sigma \in F \mid \chi^{\sigma} = \chi\}$ and by χ^{*} the map, induced

Date: March 7, 2011.

1991 *Mathematics Subject Classification.* 12F12.

Key words and phrases. embedding problem, Galois extension, quaternion algebra, p-adic number, local field.

This work is partially supported by project of Shumen University.

by χ:

$$\chi^* : H^2(F, N) \to H^2(F_\chi, K^\times).$$

Let c be the 2-coclass in $H^2(F, N)$, related to the group extension (1.1). Then the compatibility condition is $\chi^*(c) = 1$ for all $\chi \in \widehat{N}$ (the cohomological groups are written multiplicatively). The embedding problem is called *Brauer* if $\chi^\sigma = \chi$ for all $\sigma \in F$ and $\chi \in \widehat{N}$. It is known that for the Brauer probem the compatibility condition is sufficient for solvability.

Let us recall now some facts about Brauer groups. Denote by $\mathcal{G}(k)$ the set of all finite dimensional central simple algebras over k. The equivalence classes of these algebras form the Brauer group $Br(k)$ with multiplication induced by the tensor product of algebras. For $A \in \mathcal{G}(k)$ we denote by $[A]$ the equivalence class of A in $Br(k)$. Let (K, F, f) be the crossed product of the field K and the group $F = Gal(K/k)$ with a factor system $f : F \times F \to K^\times$, satisfying the condition

$$f(\sigma, \tau\rho)f(\tau, \rho) = f(\sigma\tau, \rho)f(\sigma, \tau)^\rho,$$

for all $\sigma, \tau, \rho \in F$. It is known that the crossed product algebra (K, F, f) is in $\mathcal{G}(k)$. The subgroup generated by all such algebras is often denoted by $Br(K/k)$ and is called *the relative Brauer group*. Then f is in $Z^2(F, K^\times)$ and the map $[(K, F, f)] \mapsto [f]$ is an isomorphism between $Br(K/k)$ and $H^2(F, K^\times)$. We have that $Br(k) = \varinjlim Br(K/k)$, where K/k are all finite Galois extensions. In this way the solving of the Brauer problem is reduced to a computation of the related class of the crossed product in the Brauer group $Br(k)$.

The compatibility condition is also equivalent to the simultaneous solvability of a number of associated Brauer problems. As for local fields it is known that the compatibility condition is sufficient for solvability. For more information about embedding problem we refer our reader to [ILF] and for Brauer group to [He].

2. Brauer groups of local fields

At the beginning of this section we give without proofs some basic isomorphisms and commutative diagrams. The local class field theory is well developed in such monographs as [CF], [Se1], [Iv], [Pi]. Denote by Ω the maximal Galois extension of the local field k. Then the Brauer group $Br(k)$ is isomorhic to $H^2(\Omega/k) = \varinjlim H^2(K_i/k)$, where K_i/k are all finite Galois extensions. We will also use the notations $F_i = Gal(K_i/k)$ and $H^2(K_i/k) = H^2(F_i, k^\times)$. For all natural numbers

n there exists a unique unramified extension k_n of degree n over the local field k. The field k_n is the splitting field of the polynomial $x^{q^n-1}-1$, where q is the number of elements in the residue field $\bar{k}$ of k. Then for the maximal unramified extension k_{ur} we have that

$$k_{ur} = \bigcup_{n\geq 1} k_n.$$

We also have that k_{ur} is a subfield of Ω, since k_{ur} is abelian extension of k. Then we have the exact sequence

$$0 \to H^2(k_{ur}/k) \to Br(k) \to Br(k_{ur}).$$

If φ denotes the Frobenius automorphism for the extension k_{ur}/k, then $\varphi_n = \varphi|_{k_n}$ generates the group $F_n = Gal(k_n/k)$, which is cyclic of order n. Therefore

$$H^2(k_{ur}/k) = \varinjlim H^2(F_n, k_n^\times)$$

and

$$H^2(F_n, k_n^\times) \cong k^\times/N(k_n/k), \tag{2.1}$$

where $N : k_n \to k$ is the norm map of the extension k_n/k and $N(k_n/k)$ is the image of N in k. We use the standard notations: ν is the valuation, U is the group of units of k and π is the conforming element of the valuation ν. Since $NU(k_n/k) = U$ and $N(k_n/k) = \langle \pi^n \rangle \times U$, the regular valuation ν yields the isomorphisms $k^\times/U \cong \mathbb{Z}$ and $k^\times/N(k_n/k) \cong \mathbb{Z}/n\mathbb{Z}$. Therefore the map ν/n yields the isomorphism $k^\times/N(k_n/k) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Combining the latter isomorhpism with the isomorphism (2.1) we obtain the isomorphism

$$inv : H^2(F_n, k_n^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}. \tag{2.2}$$

More precisely, given an arbitrary $x \in k_n^\times$, we can put:

$$f(\varphi_n^i, \varphi_n^j) = \begin{cases} 1, & 0 \leq i, j, i+j < n \\ x, & 0 \leq i, j < n \leq i+j \end{cases} \tag{2.3}$$

The map $f : F_n \times F_n \to k_n^\times$ is a crossed homomorphism, i.e., f is in $Z^2(F_n, k_n)$. Denote by $[f]$ the 2-coclass generated by f in $H^2(F_n, k_n^\times)$. Then the isomorphism (2.2) is given by

$$inv : [f] \mapsto \frac{\nu(x)}{n} + \mathbb{Z}.$$

If $m|n$ then $k \subset k_m \subset k_n$ and the homomorphism inflation is defined:

$$inf : H^2(F_m, k_m^\times) \to H^2(F_n, k_n^\times).$$

We have the commutative diagram

$$\begin{array}{ccc} H^2(F_m, k_m^\times) & = & \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\ \downarrow inf & & \downarrow \\ H^2(F_n, k_n^\times) & = & \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \end{array}$$

where the right vertical map is an injection, since $\frac{1}{m}\mathbb{Z} \subset \frac{1}{n}\mathbb{Z}$. Therefore

$$H^2(k_{ur}/k) = \varinjlim H^2(F_n, k_n) \cong \varinjlim \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

Also, we have $Br(k_{ur}) = 0$ and the isomorphism

$$inf : H^2(k_{ur}/k) \cong H^2(\Omega/k) = Br(k),$$

whence $Br(k) \cong \mathbb{Q}/\mathbb{Z}$. The latter isomorphism we denote also by inv.

Now, let K/k be a finite Galois extension and $[K : k] = n$. Then $k \subset K \subset \Omega$ and the homomorphism restriction is defined:

$$res : Br(k) = H^2(\Omega/k) \to Br(K) = H^2(\Omega/K).$$

Then the diagram

$$\begin{array}{ccc} Br(k) & = & \mathbb{Q}/\mathbb{Z} \\ \downarrow res & & \downarrow n \\ Br(K) & = & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative. Therefore the group $H^2(K/k) = Br(K/k)$ is the kernel of the homomorphism $res : Br(k) \to Br(K)$. In this way we obtain the isomorphism

$$inv : H^2(K/k) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

We now proceed by considering cyclic and quaternion algebras. Let the algebra $A \in \mathcal{G}(k)$ be of degree n over k. Then $[A] = [(k_n, F_n, f)]$, where k_n, F_n and f are as before. Indeed, if K is the splitting field of A and $F = Gal(K/k)$ then

$$[A] \in Br(K/k) = H^2(F, K^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong H^2(F_n, k_n^\times).$$

The system of factors f is uniquely determined by some element $x \in k$, according to (2.3). Then

$$inv([A]) = \frac{\nu(x)}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Let $A, B \in \mathcal{G}(k)$. Here are some properties of the isomorphism inv:

- $A \sim B$ $(i.e. [A] = [B]) \iff inv(A) = inv(B)$;

- $A \sim k$ $(i.e.[A] = 1) \iff inv(A) = 0$;
- $inv(A \otimes B) = inv(A) + inv(B)$.

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

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

The system of factors f is defined by

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

It can be shown that f fulfils formula (2.3). We put $u_{\varphi_n} = u, u_{\varphi_n^i} = u^i, u_1 = u^n = x$.

Now, we consider the quaternion algebra Q_1, which is generated by the elements α and β, such that $\alpha^2 = a, \beta^2 = b$ and $\alpha\beta = -\beta\alpha$ $(a, b \in k^\times)$. We use the standard notation: by $(a, b/k)$ we denote the algebra Q_1 and by (a, b) the equivalence class of Q_1 in $Br(k)$. Since $\mathrm{Deg}(Q_1) = 2$, we have that $[Q_1] = [Q_2]$, where $Q_2 = (k_2, F_2, f)$ is the crossed product of the unramified extension $k_2 = k(\sqrt{c})$ with F_2, which is a cyclic group of order 2. Clearly, Q_2 is either quaternion division algebra or the matrix algebra $\mathrm{Mat}_2(k)$. In both cases we can put $Q_2 = (c, d/k)$. The elements γ and δ, such that $\gamma^2 = c, \delta^2 = d$ and $\gamma\delta = -\delta\gamma$ generate Q_2.

In fact, the unramified extension k_n is contained with exactness to a k-isomorphism in any algebra $A \in \mathcal{G}(k)$ of degree n over k. Of course, in A the unramified extension is not unique. However, every two of them are pairwise conjugate by the Noeter-Skoelem theorem. In our case we have that $Q_2 = k_2 \oplus \delta k_2$ and $inv([Q_1]) = inv([Q_2]) = \frac{\nu(d)}{2} + \mathbb{Z}$.

By the theory of quaternion algebras and quadratic forms is known that $(a, b) = (c, d)$ iff the quadratic forms $f_1(x, y, z) = ax^2 + by^2 - abz^2$ and $f_2(x, y, z) = cx^2 + dy^2 - cdz^2$ are equivalent. Then c and d are represented by $f_1(x, y, z) : c = ax_1^2 + by_1^2 - abz_1^2, d = ax_2^2 + by_2^2 - abz_2^2$, where $x_i, y_i, z_i \in k, i = 1, 2$. We can put $\gamma = x_1\alpha + y_1\beta + z_1\alpha\beta$, whence $\gamma^2 = c$. By Noeter-Skoelem theorem we can find an element $\delta \in Q_1$ such that $\delta\gamma\delta^{-1} = -\gamma$. If $\delta^2 = d \in k^\times$ then $Q_1 = (a, b/k) \cong Q_2 = (c, d/k)$. Thus we have shown how exactly the unramified extension $k_2 = k(\sqrt{c})$ is contained in Q_1.

We apply the local invariants to determine whether the embedding problem with cyclic kernel $\mu_2 = \{\pm 1\}$ of order 2 is solvable or not. Let $(K/k, G, \mu_2)$ be an embedding problem given by the group extension

$$1 \to \mu_2 \to G \underset{\psi}{\to} F = Gal(K/k) \to 1 \tag{2.4}$$

and let $c \in H^2(F, \mu_2)$ be the 2-coclass, related to (2.4). We have that $c^2 = 1$, so the image of c in $H^2(F, K^\times)$ is a product of classes of quaternion algebras, by the Merkurjev theorem (see [Me]). Consider the following example.

Example 2.1. *Let $K/k = k(\sqrt{a_1}, \sqrt{a_1}, \ldots, \sqrt{a_n})/k$ be a $(C_2)^n = \underbrace{C_2 \times \cdots \times C_2}_{n}$ extension. Let the generators $\rho_1, \ldots, \rho_n$ of the elementary abelian group $(C_2)^n$ be given by $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$, where δ_{ij} is the Kronecker delta. Let*

$$1 \to \mu_2 \to G \underset{\psi}{\to} (C_2)^n = Gal(K/k) \to 1 \tag{2.5}$$

is non-split group extension and let us choose pre-images $\sigma_1, \ldots, \sigma_n \in G$ of $\rho_1, \ldots, \rho_n$. We define $d_{ij}, i \leq j$ by $\sigma_i^2 = (-1)^{d_{ii}}$ and $\sigma_i\sigma_j = (-1)^{d_{ij}}\sigma_j\sigma_i, i < j$. Then the embedding problem $(K/k, G, \mu_2)$, given by (2.5) is solvable iff $\prod_{i\leq j}(a_i, a_j)^{d_{ij}} = 1$ in $Br(k)$ (see [Le]). If again $k_2 = k(\sqrt{c})$ is the unramified extension of degree 2 over k, then $(a_i, a_j) = (c, b_{ij})$ for some $b_{ij} \in k^\times$. Therefore $\prod_{i\leq j}(a_i, a_j)^{d_{ij}} = (c, b)$, where $b = \prod_{i\leq j} b_{ij}^{d_{ij}}$ and

$$inv(c, b) = \frac{\nu(b)}{2} + \mathbb{Z} \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

Next we will consider two special cases.

(1) Let p be an odd prime, $q = p^m$ be the number of elements in the residue field $\bar{k}$ of k and let $-1 \notin k^2$. Then the unramified extension k_2 is the splitting field of the polynomial

$$g(x) = x^{q^2-1} - 1 = x^{p^{2m}-1} - 1$$

over k. Since $4|p^{2m} - 1$, we have that $\sqrt{-1}$ is a root of $g(x)$, therefore $k_2 = k(\sqrt{-1})$.

Example 2.2. *Consider the embedding problem $(k(\sqrt{a})/k, C_4, \mu_2)$, given by the group extension*

$$1 \to \mu_2 \to C_4 \to C_2 = Gal(k(\sqrt{a})/k) \to 1.$$

The obstruction is $(a,a) \in Br(k)$ *(i.e.* $(a,a)=1$ *is necessary and sufficient for solvability of the embedding problem). From* $(a,a)=(-1,a)$ *follows that* $inv(a,a) = inv(-1,a) = \frac{\nu(a)}{2} + \mathbb{Z}$.

(2) Let $q = 2^m$ and $-3 \notin k^2$. Then $3|2^{2m}-1$, so $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ is a root of the polynomial

$$h(x) = x^{2^{2^m}-1} - 1,$$

therefore $k_2 = k(\sqrt{-3})$.

Now, let $k = \mathbb{Q}_p$ (p is a prime) be the p-adic number field. For $a, b \in k^\times$ the *Hilbert symbol* is defined by:

$$(a,b)_p = \begin{cases} 1, & (a,b) = 1 \\ -1, & (a,b) \neq 1, \end{cases}$$

where as usual (a,b) is the quaternion class in $Br(k)$. We are going to describe the solvable embedding problems $(K/k, G, \mu_2)$, where G is one of the following groups of order 8: D_8-*the dihedral* group (also denoted by many authors as D_4), Q_8-*the quaternion* group, C_8-*the cyclic* group; and the groups of order 16: M_{16}-*the modular* group, SD_{16}-*the semidihedral (quasidihedral)* group (also denoted as SD_8 and QD_8), D_{16}-*the dihedral* group (also denoted as D_8), Q_{16}-*the quaternion* group, $Q \curlywedge C$-*the pull-back* of the homomorphisms $Q_8 \mapsto C_2$ and $C_4 \mapsto C_2$, $D \curlywedge C$-the pull-back of the homomorphisms $D_8 \mapsto C_2$ and $C_4 \mapsto C_2$ and DC-*the central product* of D_8 and C_4. The groups of consideration have the following presentations by a set of generators:

$$\begin{aligned}
D_8 &\cong \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle, \\
Q_8 &\cong \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma = \sigma^3\tau \rangle, \\
M_{16} &\cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^5\tau \rangle, \\
SD_{16} &\cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle, \\
D_{16} &\cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle, \\
Q_{16} &\cong \langle \sigma, \tau \mid \sigma^8 = 1, \tau^2 = \sigma^4, \tau\sigma = \sigma^{-1}\tau \rangle, \\
Q \curlywedge C &\cong \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle, \\
D \curlywedge C &\cong \langle \sigma, \tau, \rho \mid \sigma^4 = \tau^2 = \rho^2 = 1, \tau\sigma = \sigma^3\tau\rho \rangle, \\
DC &\cong \langle \sigma, \tau, \rho \mid \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau, \sigma^2 = \rho^2, [\sigma,\rho] = [\tau,\rho] = 1 \rangle.
\end{aligned}$$

Some of the groups are considered in the works [Mi] and [MiZ]. The remaining non abelian groups of order 16 are $D_8 \times C_2$ and $Q_8 \times C_2$, which are of little interest:

for example, an embedding problem with the group $G = D_8 \times C_2$ is solvable iff an associated embedding problem with the group D_8 is solvable and there are at least 8 square classes in k.

3. Embedding problems over $\mathbb{Q}_p$, $(p \neq 2)$

We begin with some results from [Se2, II].

Theorem 3.1. *Let $x = p^n u \in \mathbb{Q}_p^\times, p \neq 2, n \in \mathbb{Z}, u \in U$ (i.e. u is a p-adic unit). Then $x \in (Q_p^\times)^2$ iff n is even and $(u|p) = 1$.*

Here $(u|p)$ is simpler notation of the Legendre symbol $(\bar{u}|p)$, where $\bar{u}$ is the image of u in the multiplicative group of the field having p elements: $F_p^\times = U/U_1$. Let us recall also that for $n \geq 1$ the groups $U_n = 1 + p^n\mathbb{Z}_p$ are defined, where $\mathbb{Z}_p$ is the ring of p-adic integers.

Corollary 1. *For $p \neq 2$ there is an isomorphism: $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \{1, p, u, pu\}$, where $(u|p) = -1$.*

Let us now consider the unramified extension k_2 over $\mathbb{Q}_p$. We have that $k_2 = \mathbb{Q}_p(\sqrt{a})$, where $a \in \{u, p, pu\}$. Than we have the isomorphism $k_2^\times \cong \langle p\rangle \times U(k_2)$, whence $\sqrt{a} = p^k v$ for some $v \in U(k_2)$. Then $a = p^{2k}v^2$, therefore we can assume that $a = u \in U$. Whence we get $inv(u, b) = \frac{\nu(b)}{2} + \mathbb{Z}$, i.e., $(u, v)_p = 1, (u, pv)_p = -1$ for all $v \in U$. If $(-1|p) = 1$, then $p \equiv 1 \pmod 4, -1 \in (\mathbb{Q}_p^\times)^2$ and $(p, p)_p = (-1, p)_p = 1$. If $(-1|p) = -1$, then $p \equiv 3 \pmod 4, -1 \notin (\mathbb{Q}_p^\times)^2$ and $(-1, p)_p = -1$, where we can assume that $u = -1$. In this way we have obtained the following

Theorem 3.2. *Let $a = p^i u_1, b = p^j u_2$, where $i, j = 0, 1$ and $u_1, u_2 \in U$. Then the Hilbert symbol can be described by the following properties:*

(i) $i = j = 0 : (u_1, u_2)_p = 1$;
(ii) $i = 1, j = 0 : (pu_1, u_2)_p = 1 \iff (u_2|p) = 1$;
(iii) $i = j = 1 : (pu_1, pu_2)_p = 1 \iff (-1)^{\frac{p-1}{2}}(u_1|p)(u_2|p) = 1$.

The class of the crossed product algebra related to an embedding problem with kernel of order 2 is called *the obstruction* to the embedding problem. We are going now to investigate the obstructions to realisability (i.e., to the related embedding problem) of the described before groups of orders 8 and 16. These obstructions are known from the works [Le] and [GSS], where they are presented as a product of quaternion classes over an arbitrary field of characteristic not 2. However, in this

general case it is not known when these obstructions disappear, i.e., are trivial. Our aim is to give the answer to this question over the p-adic number field. The results from this section can be generalized over the $\mathfrak{p}$-adic field k, where $\mathfrak{p}$ does not divide 2. The basic reason for this is that the number of square classes in k is 4, so there is an analog of theorem 3.2.

Proposition 3.1. *The embedding problem* $(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}, C_4, \mu_2)$ *related to the group extension*

$$1 \to \mu_2 \to C_4 \to C_2 = Gal(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p) \to 1$$

is solvable iff $a = u$ *and* p *is arbitrary; or* $a = pv, v \in \{1, u\}$ *and* $p \equiv 1\ (4)$.

Proof. The obstruction of the embedding problem is $(a, a) \in Br(\mathbb{Q}_p)$. Theorem 3.2 implies that $(a, a) = 1$ iff $a = u$ and p is arbitrary; or $a = pv, v \in \{1, u\}$ and $p \equiv 1\ (4)$. □

From now on we will assume the notation of u and v from the latter propositon.

Proposition 3.2. *Let* $(a, a) = 1 \in Br(\mathbb{Q}_p)$. *The embedding problem related to the group extension*

$$1 \to \mu_2 \to C_8 \to C_4 = Gal(\mathbb{Q}_p(\sqrt{r(a + \sqrt{a})})/\mathbb{Q}_p)) \to 1$$

is solvable iff

(1) $a = u$;
$r = u, \forall p$; *or*
$r = pv$ *for* $p \equiv 1\ (4)$;
or
(2) $a = pv, \forall r$ *and* $p \equiv 1\ (8)$.

Proof. The obstruction is $(a, 2)(r, -1) \in Br(\mathbb{Q}_p)$. Let us consider two cases:

(1) $a = u$. Then $(u, u) = (u, 2) = 1$. Therefore the embedding problem is solvable iff $(r, -1) = 1 \iff r = u, \forall p$ or $r = pv$ for $p \equiv 1\ (4)$;
(2) $a = pv, v \in \{1, u\}, p \equiv 1\ (4)$. Then $(r, r) = 1$ and $(pv, 2) = 1 \iff (2|p) = 1$, whence $p \equiv 1\ (8)$.

□

In the same way the remaining embedding problems are considered. We will formulate only the final results. Let $\mathbb{Q}_p(\sqrt{a},\sqrt{b})/\mathbb{Q}_p$ be a biquadratic extension with Galois group $C_2^2 = C_2 \times C_2$, which is generated by elements ρ_1 and ρ_2, such that:

$$\rho_1 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b}; \quad \rho_2 : \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b}.$$

Proposition 3.3. *The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1\mapsto\sigma^2}{\to} D_8 \underset{\substack{\sigma\mapsto\rho_1\\ \tau\mapsto\rho_2}}{\to} C_2^2 \to 1$$

is $(a, ab) \in Br(\mathbb{Q}_p)$. *The embedding problem is solvable iff* $p \equiv 3\ (4), a = pv, b = u$.

Proposition 3.4. *The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1\mapsto\sigma^2}{\to} Q_8 \underset{\substack{\sigma\mapsto\rho_1\\ \tau\mapsto\rho_2}}{\to} C_2^2 \to 1$$

is $(b, b)(a, ab) \in Br(\mathbb{Q}_p)$. *The embedding problem is solvable iff* $p \equiv 3\ (4)$, *for all quadratically independent* a *and* b.

Next, we will consider embedding problems for the non-abelian groups of order 16. Let $(a, a) = 1 \in Br(\mathbb{Q}_p)$. Then all $C_4 \times C_2$ extensions are described thus: $\mathbb{Q}_p(\sqrt{r(a+\sqrt{a})},\sqrt{b})/\mathbb{Q}_p$. Let the group $C_4 \times C_2$ be generated by ρ_1 and ρ_2, such that

$$\rho_1 : \sqrt{r(a+\sqrt{a})} \mapsto \sqrt{r(a-\sqrt{a})}, \sqrt{r(a-\sqrt{a})} \mapsto -\sqrt{r(a+\sqrt{a})}, \sqrt{b} \mapsto \sqrt{b};$$
$$\rho_2 : \sqrt{r(a+\sqrt{a})} \mapsto \sqrt{r(a+\sqrt{a})}, \sqrt{r(a-\sqrt{a})} \mapsto \sqrt{r(a-\sqrt{a})}, \sqrt{b} \mapsto -\sqrt{b}.$$

Proposition 3.5. *Let* $(a, a) = 1 \in Br(\mathbb{Q}_p)$. *The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1\mapsto\sigma^4}{\to} M_{16} \underset{\substack{\sigma\mapsto\rho_1\\ \tau\mapsto\rho_2}}{\to} C_4 \times C_2 \to 1$$

is $(a, 2b)(r, -1) \in Br(\mathbb{Q}_p)$. *The embedding problem is solvable iff*

(1) $p \equiv 5\ (8), a = pv, b \neq 1, a \bmod (\mathbb{Q}_p)^2$
or
(2) $p \equiv 3\ (4), a = u, r = pv, b \neq 1, a \bmod (\mathbb{Q}_p)^2$.

Now, let $(a, ab) = 1 \in Br(\mathbb{Q}_p)$, whence there exists $\alpha, \beta \in k$, such that $\alpha^2 - a\beta^2 = ab$. Then all D_8 extensions are described thus: $\mathbb{Q}_p(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b})/\mathbb{Q}_p$. Let the group D_8 be generated by ρ_1 and ρ_2, such that

$$\begin{aligned}
\rho_1 \quad &: \quad \sqrt{r(\alpha+\beta\sqrt{a})} \mapsto \sqrt{r(\alpha-\beta\sqrt{a})}, \sqrt{r(\alpha-\beta\sqrt{a})} \mapsto -\sqrt{r(\alpha+\beta\sqrt{a})}, \\
&\quad\ \sqrt{b} \mapsto \sqrt{b}; \\
\rho_2 \quad &: \quad \sqrt{r(\alpha+\beta\sqrt{a})} \mapsto \sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{r(\alpha-\beta\sqrt{a})} \mapsto -\sqrt{r(\alpha-\beta\sqrt{a})}, \\
&\quad\ \sqrt{b} \mapsto -\sqrt{b}.
\end{aligned}$$

Proposition 3.6. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_p)$. The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} SD_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is $(a, -2)(-b, 2r\alpha) \in Br(\mathbb{Q}_p)$. The embedding problem is solvable iff $p \equiv 3\ (8), a = pv, b = u, \forall r$.

Proposition 3.7. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_p)$. The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} D_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is $(a, 2)(-b, 2r\alpha) \in Br(\mathbb{Q}_p)$. The embedding problem is solvable iff $p \equiv 7\ (8), a = pv, b = u, \forall r$.

Proposition 3.8. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_p)$. The obstruction to the embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} Q_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is $(a, 2)(b, b)(-b, 2r\alpha) \in Br(\mathbb{Q}_p)$. The embedding problem is solvable iff $p \equiv 7\ (8), a = pv, b = u, \forall r$.

Since $|\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2| = 4$, the groups $Q_8 \times C_2$ and $D_8 \times C_2$ are not realisable over $\mathbb{Q}_p$.

Proposition 3.9. *The obstruction to realisability of the group DC over an arbitrary field is $(a, b)(c, -1)$, where a, b and c are quadratically independent. The group DC is not realisable over $\mathbb{Q}_p$.*

Proposition 3.10. *The obstruction to realisability of the group $Q \leftthreetimes C$ over an arbitrary field is (a,a) and $(-a,b)$, where a and b are quadratically independent. The group $Q \leftthreetimes C$ is realisable over $\mathbb{Q}_p$ for $p \equiv 3\ (4), a = u, b = pv$.*

Proposition 3.11. *The obstruction to realisability of the group $D \leftthreetimes C$ over an arbitrary field is (a,a) and (a,b), where a and b are quadratically independent. The group $D \leftthreetimes C$ is not realisable over $\mathbb{Q}_p$.*

4. Embedding problems over $\mathbb{Q}_2$

From [Se2, II] we have also the following:

Theorem 4.1. *Let $x = 2^n u \in \mathbb{Q}_2^\times, n \in \mathbb{Z}, u \in U$ (i.e. u is a 2-adic unit). Then $x \in (Q_2^\times)^2$ iff n is even and $u \equiv 1\ (8)$.*

Since the set $\{\pm 1, \pm 5\}$ is a system of representatives for the group U/U_3, we obtain:

Corollary 1. $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong C_2^3 \cong \{\pm 1, \pm 2, \pm 5, \pm 10\}$.

As we have shown at the end of section 2, the unramified extension of degree 2 is $k_2 = \mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\sqrt{-3})$, since $-3 \cdot 5 = -15 \equiv 1\ (8)$, whence $-15 \in (\mathbb{Q}_2^\times)^2$. Therefore $(5,1)_2 = (5,-1)_2 = (5,5)_2 = 1$ and $(5,\pm 2)_2 = (5,\pm 10)_2 = -1$. In this way we obtain:

Theorem 4.1. *Let $a = 2^i u_1, b = 2^j u_2; i,j = 0,1; u_1, u_2 \in \{\pm 1, \pm 5\}$. Then the Hilbert symbol has value 1 only in the following cases:*

(i) $i = j = 0 : (-1,5)_2 = (-5,5)_2 = (5,5)_2 = 1$;
(ii) $i = 1, j = 0 : (2,-1)_2 = (10,-1)_2 = (-2,-5)_2 = (-10,-5)_2 = 1$;
(iii) $i = j = 1 : (2,2)_2 = (2,-2)_2 = (-2,-10)_2 = (10,10)_2 = (10,-10)_2 = 1$.

The set of quaternion algebras is $\{1, (-1,-1)\} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

Proposition 4.1. *The embedding problem related to the group extension*

$$1 \to \mu_2 \to C_4 \to C_2 = Gal(\mathbb{Q}_2(\sqrt{a})/\mathbb{Q}_2) \to 1$$

is solvable iff $a = 2, 5, 10$.

Proposition 4.2. *Let $(a,a) = 1 \in Br(\mathbb{Q}_2)$. The embedding problem related to the group extension*

$$1 \to \mu_2 \to C_8 \to C_4 = Gal(\mathbb{Q}_2(\sqrt{r(a+\sqrt{a})})/\mathbb{Q}_2)) \to 1$$

is solvable iff

(1) $a = 2, r \in \{1, 2, 5, 10\}$;
(2) $a = 5, r \in \{-1, -2, -5, -10\}$;
(3) $a = 10, r \in \{-1, -2, -5, -10\}$.

Proposition 4.3. *The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^2}{\to} D_8 \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} C_2^2 \to 1$$

is solvable iff

(1) $a = -1, b \in \{-5, -2, -10\}$;
(2) $a = 5, b \in \{-1, -5\}$;
(3) $a = -5, b \in \{-1, 2, 10\}$;
(4) $a = 2, b \in \{-1, -2\}$;
(5) $a = -2, b \in \{-1, 5, 10\}$;
(6) $a = 10, b \in \{-1, -10\}$;
(7) $a = -10, b \in \{-1, 2, 5\}$.

Proposition 4.4. *The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^2}{\to} Q_8 \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} C_2^2 \to 1$$

is solvable iff

(1) $a = 2, b \in \{-5, -10\}$;
(2) $a = -2, b \in \{\pm 5, \pm 10\}$;
(3) $a = 5, b \in \{-2, -10\}$;
(4) $a = -5, b \in \{\pm 2, \pm 10\}$;
(5) $a = 10, b \in \{-2, -5\}$;
(6) $a = -10, b \in \{\pm 2 \pm 5\}$.

Proposition 4.5. *Let $(a, a) = 1 \in Br(\mathbb{Q}_2)$. The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} M_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} C_4 \times C_2 \to 1$$

is solvable iff

(1) $a = 2, b \in \{-1, -2\}, r \in \{1, 2, 5, 10\}$;
(2) $a = 2, b \in \{\pm 5, \pm 10\}, r \in \{-1, -2, -5, -10\}$;
(3) $a = 5, b \in \{-1, \pm 5\}, r \in \{-1, -2, -5, -10\}$;
(4) $a = 5, b \in \{\pm 2, \pm 10\}, r \in \{1, 2, 5, 10\}$;

(5) $a = 10, b \in \{-1, \pm 10\}, r \in \{-1, -2, -5, -10\}$;
(6) $a = 10, b \in \{\pm 2, \pm 5\}, r \in \{1, 2, 5, 10\}$.

Proposition 4.6. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_2)$. The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} SD_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is solvable iff

(1) $b = -1, a \in \{2, -5, -10\}, \forall r$;
(2) $b \neq -1$ *and all pairs a, b, such that $(a, -b) = 1 \in Br(\mathbb{Q}_2)$ (see proposition 4.3), for all r, α and β are properly chosen.*

Proposition 4.7. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_2)$. The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} D_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is solvable iff

(1) $b = -1, a = \pm 2, \forall r$;
(2) $b \neq -1$ *and the same conditions as in proposition 4.6.*

Proposition 4.8. *Let $(a, ab) = 1 \in Br(\mathbb{Q}_2)$. The embedding problem related to the group extension*

$$1 \to \mu_2 \underset{-1 \mapsto \sigma^4}{\to} Q_{16} \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} D_8 \to 1$$

is solvable iff

(1) $b = -1, a \in \{\pm 5, \pm 10\}, \forall r$;
(2) $b \neq -1$ *and the same conditions as in proposition 4.6.*

Since $|\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2| = 8$, the groups $Q_8 \times C_2$ and $D_8 \times C_2$ are realisable over $\mathbb{Q}_2$ given the same conditions as for the groups D_8 and respectively Q_8. It is easy to check that the groups $DC, Q \curlywedge C$ and $D \curlywedge C$ are always realisable over $\mathbb{Q}_2$. In the same way can be found the solvable embedding problems.

5. Embedding problems over the rational field $\mathbb{Q}$

We will formulate Albert-Hasse-Brauer-Noeter theorem over the field $\mathbb{Q}$. Let $A \in \mathcal{G}(\mathbb{Q})$ and p be a prime number or the symbol ∞. (If $p = \infty$, then $\mathbb{Q}_\infty = \mathbb{R}$.) The element $inv_p(A \otimes \mathbb{Q}_p)$ in the group $\mathbb{Q}/\mathbb{Z}$ is called *the local invariant* of the

algebra A, related to the p-adic valuation ν_p. The set of local invariants gives us *the global invariant* of the algebra A. The global invariant is in fact the map:

$$inv^{(\mathbb{Q})} : \mathcal{G}(\mathbb{Q}) \to \prod_p \mathbb{Q}/\mathbb{Z},$$

where the product is by all primes p and the symbol ∞, defined by:

$$inv^{(\mathbb{Q})}A = (\cdots inv_p(A \otimes \mathbb{Q}_p) \cdots).$$

Clearly, $inv^{(\mathbb{Q})}A = inv^{(\mathbb{Q})}B$ iff $A \sim B$. Therefore $inv^{(\mathbb{Q})}$ can be considered as a map from the group $Br(\mathbb{Q})$ into $\prod_p \mathbb{Q}/\mathbb{Z}$. Albert-Hasse-Brauer-Noeter theorem then says that $inv^{(\mathbb{Q})}$ is an injection. If we denote by $Br_2(\mathbb{Q})$ all elements in $Br(\mathbb{Q})$ of order 2, we will have the injective homomorphism

$$inv^{(\mathbb{Q})} : Br_2(\mathbb{Q}) \to \prod_p \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

The interpretation of this is that a given product of classes of quaternion algebras is 1 in $Br_2(\mathbb{Q})$ iff the same product is 1 in $Br_2(\mathbb{Q}_p)$ for all p, i.e., inv_p is 0 for all p.

Let us consider the embedding problem related to the group extension

$$1 \to \mu_2 \to C_4 \to C_2 = Gal(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \to 1.$$

The obstruction is $(a, a) \in Br_2(\mathbb{Q})$. Then $(a, a) = 1 \in Br_2(\mathbb{Q})$ iff $(a, a) = 1 \in Br_2(\mathbb{Q}_p)$ for all p. Whence $(a, a) = 1 \in Br_2(\mathbb{Q})$ iff $a > 0$ (i.e., $(a, a) = 1 \in Br(\mathbb{R})$) and every odd prime divisor p of a is $\equiv 1$ (4). (We assume that a is a square-free integer.)

Finally, we consider the embedding problem related to the group extension

$$1 \to \mu_2 \to C_8 \to C_4 = Gal(\mathbb{Q}(\sqrt{r(a + \sqrt{a})})/\mathbb{Q})) \to 1,$$

where $(a, a) = 1 \in Br(\mathbb{Q}), r \in \mathbb{Q}^\times$. The obstruction to this embedding problem is $(a, 2)(r, -1) \in Br(\mathbb{Q})$. Then $(a, 2)(r, -1) = 1 \in Br_2(\mathbb{Q})$ iff $(a, 2)(r, -1) = 1 \in Br_2(\mathbb{Q}_p)$ for all p. Whence by theorem 3.2 we obtain that $(a, 2)(r, -1) = 1 \in Br_2(\mathbb{Q}_p)$ for all p iff every odd prime divisor p of a is $\equiv 1$ (8) and every odd prime divisor q of r, which is not a divisor of a, is $\equiv 1$ (4).

The latter two examples are obtained in the work [Mi] by means of the elementary number theory. However, the most of the results in [Mi] can not be obtained by the means of this work, because of the great number of cases of the values of the prime numbers appearing in the obstructions.

References

[CF] J.W.S. Cassels, A. Fröhlich, "Algebraic number theory", Academic press, London and New York, 1967.

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

[He] I. N. Herstein, "Noncommutative rings", The Math. Soc. of Amer., New York, 1968.

[ILF] V. V. Ishanov, B. B. Lur'e and D. K. Faddeev, "The embedding problem in Galois theory", Amer. Math. Soc., Providence, 1997.

[Iv] K. Ivasava, "Local class field theory", Mir, Moscow, 1983. (in Russian)

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

[Me] A. Merkurjev, On the norm residue symbol of degree 2, *Soviet Math. Dokl.* **24** (1981), 546-551.

[Mi] I. Michailov, Some groups of orders 8 and 16 as Galois groups over $\mathbb{Q}$, *Math. Balk. New Series* **17** (2003), Fasc. 1-2, 155-170.

[MiZ] I. Michailov and N. Ziapkov, Embedding problems with Galois groups of order 16, *Math. Balk. New Series* **15** (2001), Fasc. 1-2, 99-108.

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

[Se1] J.-P. Serre, "Corps locaux", Paris, Hermann, 1962.

[Se2] J.-P. Serre, "A Course in Arithmetic", Springer-Verlag, New York, 1973.

Faculty of Mathematics and Informatics, Constantin Preslavski University, 9700 Shumen, Bulgaria

E-mail address: i.michailov@fmi.shu-bg.net