Mathematatica Balkanica

Mathematical Society of South-Eastern Europe
A quarterly published by
the Bulgarian Academy of Sciences – National Committee for Mathematics

---

Mathematica
Balkanica

New Series Vol. 15, 2001, Fasc. 1-2

Embedding Problems with Galois Groups of Order 16

Ivo Michailov Michailov and Nikola Petkov Ziapkov

Presented by P. Kenderov

In this work, we consider certain embedding problems over fields of characteristic not 2. We make use of the well-known obstructions to realizing groups of order 16 in order to obtain conditions for solvability of embedding problems with non-abelian groups of order 16. Then we examine these conditions in concrete examples according to the properties of the base field. As a result we obtain numerous examples of solvable problems as well as realizability of these groups over fields of level 4. We conclude with the cyclic group of order 8.

AMS Subj. Classification: 11E57, 12F10

Key Words: Galois group, extension of field, emebedding problem

1. Introduction

Let K/k be a finite Galois extension of fields with Galois group F. The embedding problem associated to the extension of groups

$$1 \to A \to G \xrightarrow{\alpha} F = \mathrm{Gal}(K/k) \to 1$$

then consists of determining whether or not there exists Galois extension L/k, such that $G \cong \mathrm{Gal}(L/k)$, $K \subset L$ and $\sigma|_K = \alpha(\sigma)$, for all $\sigma \in G$.

In this work, we examine certain embedding problems for the following groups: D_{16}, the dihedral group of order 16; SD_{16}, the semidihedral group of order 16; M_{16}, the modular group of order 16; Q_{16}, the quaternion group of order 16; and C_8, the cyclic group of order 8.

If k has characteristic 2, then by a famous result of Witt [Wi] the realizability of a 2-group G over k depends only on the rank of G. Therefore, from now on let us assume k to be of characteristic other than 2.

A complete list with obstructions for the realizability of the groups of order 8 and 16 can be found in [GSS]. There also is given a full parametrization of all extensions realizing the groups C_8, D_{16}, and M_{16}, in some particular cases. It is derived from the full set of C_8 extensions over fields with a special property, given by Schneps [Sc]. Other questions concerning automatic realizability (when the realizability of one group implies the realizability of other group) can be found in [GS]. In [Ki] Kiming gives explicit constructions of all D_{16}, SD_{16}, and Q_{16} extensions. However, we will extensively use the results in [Le], obtained by decomposition of the obstructions as products of quaternion algebras. (Moreover, Ledet also proves a cohomological theorem [Le, Theorem 2.4], which admits computing of the obstructions for some groups of order 2^n, $n \geq 4$.)

Helping our consideration is the following salient theorem:

Theorem 1.1. *Let K/k be a Galois extension with Galois group $F = Gal(K/k)$ and let $B \subset A \subset G$ be groups such that A and B are normal in G and $F \cong G/A$. Then the field $L \supset K$ is a solution of the embedding problem*

$$1 \to A \to G \to F = Gal(K/k) \to 1$$

if and only if the problem

$$1 \to A/B \to G/B \to F = Gal(K/k) \to 1$$

has a solution $K_1 \supset K$ and the problem

$$1 \to B \to G \to G/B = Gal(K_1/k) \to 1$$

has a solution $L \supset K_1 \supset K$.

We will write (a, b) the equivalence class in the Brauer group $Br(k)$ of the quaternion algebra generated over k by two anti-commuting elements i and j such that $i^2 = a$, $j^2 = b$; $a, b \in k^*$. It is known that the realizability of groups of order a power of 2 over k is linked to the splitting of certain products of quaternion algebras in $Br(k)$. The following well-known facts about quaternion algebras are often useful.

Proposition 1.2. *Let $a, b, c, d \in k^*$. Then:*
1) $(a, b) = 1 \in Br(k) \iff \exists x, y \in k : a = x^2 - by^2$;
2) $(a, b)(c, d) = 1 \in Br(k) \iff \exists x \in k : (a, bx) = (c, dx) = (ac, x) = 1 \in Br(k)$.

Now, we give two definitions concerning the quadratic structure of the base field k.

Definition. The level $s(k)$ of the field k is the least positive integer n such that -1 can be expressed as a sum of n squares.

We show for example, that all these groups are always realizable over a field of level $s(k) = 4$.

Definition. An element $a \in k^* \setminus k^{*2}$ is rigid, if the set of elements in k represented by the quadratic form $\langle 1, a\rangle = x^2 + ay^2$, is precisely $k^{*2} \cup ak^{*2}$.

Obviously, b is not rigid if and only if there exists $a \in k^{*2} \setminus k^{*2}$ such that a and b are independent *mod* k^{*2} , and $(a, -b) = 1 \in Br(k)$.

Let $C_2^2 = C_2 \times C_2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k)$. We will assume without further mentioning that a and b are independent *mod* k^{*2}, and $C_2^2 \cong \langle \rho_1, \rho_2\rangle$, given by $\rho_1\sqrt{a} = -\sqrt{a}$, $\rho_1\sqrt{b} = -\sqrt{b}$; $\rho_2\sqrt{a} = \sqrt{a}$, $\rho_2\sqrt{b} = -\sqrt{b}$.

Our aim is to reduce the conditions for solvability of certain embedding problems to availability of special properties (e.g. the level and number of square classes of the base field; rigidity; presentation of given elements as a sum of squares).

We have to say that we consider only these four non-abelian groups of order 16 because their obstructions are most interesting. The obstructions for the rest five non-abelian groups of order 16 do not present enough material for studying of specific embedding problems. For more embedding problems with these groups over the rational field, see [Mi].

2. The dihedral group $D_{16} \cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^7\tau\rangle$

Consider the embedding problem

$$(1) \qquad 1 \to C_4 \cong \langle \sigma^2\rangle \to D_{16} \underset{\sigma \to \rho_1, \tau \to \rho_2}{\longrightarrow} C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1.$$

It is well-known that the associated problem

$$1 \to C_2 \cong \langle \sigma^2\rangle/\langle \sigma^4\rangle \to D_8 \cong D_{16}/\langle \sigma^4\rangle \to C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1$$

is solvable if and only if $(a, ab) = 1 \in Br(k)$. When $(a, ab) = 1$ there exists a D_8 (the dihedral group of order 8) extension L/k such that $L \supset k(\sqrt{a}, \sqrt{b})$. The problem

$$1 \to C_2 \cong \langle \sigma^4\rangle \to D_{16} \to D_8 = \mathrm{Gal}(L/k) \to 1$$

is solvable if and only if $(a, 2) = (-b, x) \in Br(k)$, for some $x \in k^*$. By Theorem 1.1 the problem (1) is solvable if and only if $(a, ab) = 1$ and $(a, 2) = (-b, x)$, for some $x \in k^*$.

Also, given the extensions

$$(2)\qquad 1 \to C_8 \cong \langle\sigma\rangle \to D_{16} \underset{\tau \to \rho}{\longrightarrow} C_2 = \langle\rho\rangle = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle\sigma\rangle/\langle\sigma^2\rangle \to C_2^2 \cong D_{16}/\langle\sigma^2\rangle \to C_2 = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$
$$1 \to C_4 \cong \langle\sigma^2\rangle \to D_{16} \to C_2^2 \to 1,$$

the problem (2) is solvable if and only if $\exists a \in k^* \setminus k^{*2}$: a and b are independent *mod* k^{*2}, $(a, ab) = 1$ and $(a, 2) = (-b, x)$, for some $x \in k^*$.

We note that when $(a, ab) = (a, 2) = 1$ in [Sw, GSS] is given a parametrization of all D_{16} extensions. In some of the examples below this situation is present, and the full set of solutions could be given.

Example 2.1. Let $b = -1$. Then $(a, ab) = (a, -a) = 1$ and $(-b, x) = (1, x) = 1$, whence the condition becomes $(a, 2) = 1$. Thus the problem (2) for $b = -1$ is solvable if and only if $\exists y, z \in k : y^2 - 2z^2 \notin \pm k^{*2}$.

Example 2.2. Let $2 \in k^{*2}$. By the previous example the problem (2), for $b = -1$ is solvable if and only if $\exists a \in k^* \setminus k^{*2}$: a and -1 are independent *mod* k^{*2} (i. e., $|k^*/k^{*2}| \geq 4$). Then $L = k(\sqrt[8]{a}, \sqrt{-1})$ is a solution to the problem (2), for $b = -1$.

Indeed, let $\zeta = \frac{\sqrt{2}}{2} + \sqrt{-1}\frac{\sqrt{2}}{2} \in k(\sqrt{-1})$ be a primitive 8th root of unity. Then we can define D_{16} - operation on L as follows:

$$\sigma(\sqrt[8]{a}) = \sqrt[8]{a}\zeta, \quad \sigma(\sqrt{-1}) = \sqrt{-1}; \quad \tau(\sqrt[8]{a}) = \sqrt[8]{a}, \quad \tau(\sqrt{-1}) = -\sqrt{-1}.$$

Whence $\sigma(\zeta) = \zeta$ and $\tau(\zeta) = \frac{\sqrt{2}}{2} - \sqrt{-1}\frac{\sqrt{2}}{2} = \zeta^{-1}$. Then we have

$$\tau(\sigma(\sqrt[8]{a})) = \tau(\sqrt[8]{a}\zeta) = \sqrt[8]{a}\zeta^{-1}, \qquad \text{and}$$
$$\sigma^{-1}(\tau(\sqrt[8]{a})) = \sigma^{-1}(\sqrt[8]{a}) = \sqrt[8]{a}\zeta^{-1}.$$

Therefore $\tau\sigma = \sigma^{-1}\tau$ and since the rest verification is trivial, we conclude that $D_{16} \cong \mathrm{Gal}(L/k)$.

Example 2.3. Let $b = -2$ and let $a = y^2 - 2z^2 \notin k^{*2} \cup (-2k^{*2})$; $y, z \in k$. Then a and b are independent *mod* k^{*2}, $(a, ab) = (a, 2) = 1$. Thus the problem (2) for $b = -2$ is solvable if and only if -2 is not rigid.

Example 2.4. Let $b = -a$. Then $(a, ab) = (a, a)$, and we set $x = 2$: $(-b, x) = (a, 2)$. Thus the problem (1) for $b = -a$ is solvable if and only if a is a sum of two squares.

Corollary 2.5. *Assume $s(k) = 4$. The group D_{16} is always realizable.*

Proof. $s(k) = 4 \Rightarrow \exists \alpha_i \in k^{*2}, i = 1 \div 5$ such that $\sum_{i=1}^{5} \alpha_i^2 = 0$. We set $a = \alpha_1^2 + \alpha_2^2$, then $-a = \alpha_3^2 + \alpha_4^2 + \alpha_5^2$, hence the problem (1) for $b = -a$ is solvable. Note that $a \notin \pm k^{*2}$ and a and $-a$ are independent *mod* k^{*2}, otherwise $s(k) \leq 2$. ■

3. The semidihedral group $SD_{16} \cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$

Similarly to the previous section, given the extensions

$$(3) \qquad 1 \to C_4 \cong \langle \sigma^2 \rangle \to SD_{16} \underset{\sigma \to \rho_1, \tau \to \rho_2}{\longrightarrow} C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma^2 \rangle / \langle \sigma^4 \rangle \to D_8 \cong SD_{16}/\langle \sigma^4 \rangle \to C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$
$$1 \to C_2 \cong \langle \sigma^4 \rangle \to SD_{16} \to D_8 \to 1,$$

by Theorem 1.1 the problem (3) is solvable if and only if $(a, ab) = 1$ and $(a, -2) = (-b, x) \in Br(k)$, for some $x \in k^*$.

Also, given the extensions

$$(4) \qquad 1 \to C_8 \cong \langle \sigma \rangle \to SD_{16} \underset{\tau \to \rho}{\longrightarrow} C_2 = \langle \rho \rangle = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma \rangle / \langle \sigma^2 \rangle \to C_2^2 \cong SD_{16}/\langle \sigma^2 \rangle \to C_2 = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$
$$1 \to C_4 \cong \langle \sigma^2 \rangle \to SD_{16} \to C_2^2 \to 1,$$

the problem (4) is solvable if and only if $\exists a \in k^* \setminus k^{*2}$: a and b are independent *mod* k^{*2}, $(a, ab) = 1$ and $(a, -2) = (-b, x)$, for some $x \in k^*$.

Example 3.1. Let $b = -2a$ and let $(a, -2) = 1$. Then $(a, ab) = (a, -2) = 1$ and we set $x = 1$. Thus the problem (3) for $b = -2a$ is solvable if and only if $(a, -2) = 1$.

Example 3.2. Let $b = 2$ and let $a = y^2 + 2z^2 \notin k^{*2} \cup 2k^{*2}$; $y, z \in k$. Then a and b are independent *mod* k^{*2}, $(a, ab) = (a, -b) = (a, -2) = 1$ and we set $x = 1$. Thus the problem (4) for $b = 2$ is solvable if and only if 2 is not rigid.

Example 3.3. Let $b = -1$ and let $a = y^2 + 2z^2 \notin \pm k^{*2}$; $y, z \in k$. Then a and b are independent *mod* k^{*2}, $(a, ab) = (a, -b) = (a, 1) = 1$ and $(a, -2) = 1$.

Thus the problem (4) for $b=-1$ is solvable if and only if $\exists y,z\in k: y^2+2z^2\not\in \pm k^{*2}$.

Example 3.4. Let -1 and 2 be independent *mod* k^{*2}. Then the problem (3) for $b=-1$ and $a=2$ is solvable, and $L=k(\sqrt[8]{2},\sqrt{-1})$ is a solution.

Indeed, let $\zeta=\frac{\sqrt{2}}{2}+\sqrt{-1}\frac{\sqrt{2}}{2}\in k(\sqrt{2},\sqrt{-1})$ be a primitive 8th root of unity. Then we can define SD_{16} - operation on L as follows:

$$\sigma(\sqrt[8]{2})=\sqrt[8]{2}\zeta,\quad \sigma(\sqrt{-1})=\sqrt{-1};\quad \tau(\sqrt[8]{2})=\sqrt[8]{2},\quad \tau(\sqrt{-1})=-\sqrt{-1}.$$

Whence $\sigma(\zeta)=-\zeta$ and $\tau(\zeta)=\frac{\sqrt{2}}{2}-\sqrt{-1}\frac{\sqrt{2}}{2}=\zeta^{-1}=\zeta^{-3}$. Then we have

$$\tau\sigma(\sqrt[8]{2}))=\tau(\sqrt[8]{2}\zeta)=\sqrt[8]{2}\zeta^{-1},\qquad \text{and}$$

$$\sigma^3(\tau(\sqrt[8]{2}))=\sigma^3(\sqrt[8]{2})=-\sqrt[8]{2}\zeta^3=\sqrt[8]{2}\zeta^{-1}.$$

Therefore $\tau\sigma=\sigma^3\tau$ and $SD_{16}\cong \mathrm{Gal}(L/k)$.

Example 3.5. Let $-2\in k^{*2}$, therefore -1 and 2 are dependent *mod* k^{*2}. Then the problem (4) for $b=-1$ is solvable if and only if $\exists a\in k^*\setminus k^{*2}$: a and $b=-1$ are independent *mod* k^{*2} (i. e., $|k^*/k^{*2}|\geq 4$). As before, we will show that $L=k(\sqrt[8]{a},\sqrt{-1})$ is a solution to the problem (4) for $b=-1$.

Indeed, let $\zeta=\frac{\sqrt{2}}{2}+\sqrt{-1}\frac{\sqrt{2}}{2}\in k(\sqrt{-1})$ be a primitive 8th root of unity. Again we can define SD_{16} - operation on L as follows:

$$\sigma(\sqrt[8]{a})=\sqrt[8]{a}\zeta,\quad \sigma(\sqrt{-1})=\sqrt{-1},\quad \tau(\sqrt[8]{a})=\sqrt[8]{a},\quad \tau(\sqrt{-1})=\sqrt{-1}.$$

Whence $\sigma(\zeta)=\zeta$ and $\tau(\zeta)=\frac{\sqrt{2}}{2}+\sqrt{-1}\frac{\sqrt{2}}{2}=-\zeta^{-1}$. Then we have

$$\tau\sigma(\sqrt[8]{a}))=\tau(\sqrt[8]{a}\zeta)=-\sqrt[8]{a}\zeta^{-1},\qquad \text{and}$$

$$\sigma^3(\tau(\sqrt[8]{a}))=\sigma^3(\sqrt[8]{a})=\sqrt[8]{a}\zeta^3=-\sqrt[8]{a}\zeta^{-1}.$$

Therefore $\tau\sigma=\sigma^3\tau$ and $SD_{16}\cong \mathrm{Gal}(L/k)$.

Example 3.6. Let $b=-a$. Then $(a,ab)=(a,-1)$ and we set $x=-2$ to get $(a,-2)=(-b,x)$. Thus the problem (3) for $b=-a$ is solvable if and only if a is a sum of two squares.

Whence we immediately get the following corollary as in the previous section.

Corollary 3.7. *Assume $s(k)=4$. The group SD_{16} is always realizable.*

4. The modular group $M_{16} \cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^5\tau \rangle$

As before, given the extensions

$$(5) \qquad 1 \to C_4 \cong \langle \sigma^2 \rangle \to M_{16} \underset{\sigma \to \rho_1, \tau \to \rho_2}{\longrightarrow} C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma^2 \rangle / \langle \sigma^4 \rangle \to C_4 \times C_2 \cong M_{16}/\langle \sigma^4 \rangle \to C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$
$$1 \to C_2 \cong \langle \sigma^4 \rangle \to M_{16} \to C_4 \times C_2 \to 1,$$

the problem (5) is solvable if and only if $(a, a) = 1$ and $(a, 2b) = (-1, x) \in Br(k)$, for some $x \in k^*$.

Also, given the extensions

$$(6) \qquad 1 \to C_4 \times C_2 \cong \langle \sigma^2, \tau \rangle \to M_{16} \underset{\tau \to \rho}{\longrightarrow} C_2 = \langle \rho \rangle = \mathrm{Gal}(k(\sqrt{a})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma^2, \tau \rangle / \langle \sigma^2 \rangle \to C_2^2 \cong M_{16}/\langle \sigma^2 \rangle \to C_2 = \mathrm{Gal}(k(\sqrt{a})/k) \to 1,$$
$$1 \to C_4 \cong \langle \sigma^2 \rangle \to M_{16} \to C_2^2 \to 1,$$

the problem (6) is solvable if and only if $(a, a) = 1$ and $\exists b \in k^* \setminus k^{*2}$: a and b are independent *mod* k^{*2}, and $(a, 2b) = (-1, x)$, for some $x \in k^*$.

Similarly to D_{16}, when $(a, a) = (a, 2b) = 1$ in [GSS] is given a parametrization of all M_{16} extensions.

Example 4.1. Let $a = -1$. Then $(a, a) = (-1, -1) = 1 \iff s(k) = 2$ and set $x = 2b$ to get $(a, 2b) = (-1, 2b)$. Thus the problem (6) for $a = -1$ is solvable if and only if $s(k) = 2$.

Example 4.2. Let $-1 \notin k^{*2}$ and let $a = 2$. If $-2 \in k^{*2}$ we choose $b \in k^* \setminus k^{*2}$: a and b are independent *mod* k^{*2}, and set $x = b$. Then $(a, a) = (2, 2) = 1$, $(a, 2b) = (2, 2b) = (2, b) = (-1, b) = (-1, x)$. If $-2 \notin k^{*2}$ we set $b = -2$ and $x = 1$. Thus the problem (6) for $-1 \notin k^{*2}$, $a = 2$, is solvable if and only if $|k^*/k^{*2}| \geq 4$.

Example 4.3. Let $-1 \in k^{*2}$. If $a = 2$ then $(a, 2b) = (2, b) = 1 \iff 2$ is not rigid. If $a \neq 2$ and $2 \in k^{*2}$ then $(a, 2b) = (a, b) = 1 \iff a$ is not rigid. If $a \neq 2$ and $2 \notin k^{*2}$ we choose $b = 2$ to get $(a, 2b) = (a, 1) = 1$. Thus the problem (6) for $-1 \in k^{*2}$ is solvable if and only if $|k^*/k^{*2}| \geq 4$, when $a \neq 2$, $2 \notin k^{*2}$ and is solvable if and only if a is not rigid otherwise.

In particular we obtain:

Corollary 4.4. *[GS, §3] Assume $2 \notin k^{*2}$. The group M_{16} is realizable if and only if $|k^*/k^{*2}| \geq 4$.*

Corollary 4.5. *Assume $s(k) = 4$. The group M_{16} is always realizable.*

Proof. As in corollary 2.5 $\exists a \notin \pm k^{*2}$: a and $-a$ are independent *mod* k^{*2}, whence $|k^*/k^{*2}| \geq 4$. If $2 \notin k^{*2}$ the group M_{16} is realizable by corollary 4.4. If $2 \in k^{*2}$ then $(a, 2b) = (a, b) = (a, -a) = 1$, hence M_{16} is realizable by a and $b = -a$. ■

5. The quaternion group $Q_{16} \cong \langle \sigma, \tau | \sigma^8 = 1, \tau^2 = \sigma^4, \tau\sigma = \sigma^7\tau \rangle$

As before, given the extensions

$$(7) \qquad 1 \to C_4 \cong \langle \sigma^2 \rangle \to Q_{16} \underset{\sigma \to \rho_1, \tau \to \rho_2}{\longrightarrow} C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma^2 \rangle / \langle \sigma^4 \rangle \to D_8 \cong Q_{16}/\langle \sigma^4 \rangle \to C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma^4 \rangle \to Q_{16} \to D_8 \to 1,$$

by Theorem 1.1 the problem (7) is solvable if and only if $(a, ab) = 1$ and $(a, 2)(b, b) = (-b, x)$, for some $x \in k^*$.

Also, given the extensions

$$(8) \qquad 1 \to C_8 \cong \langle \sigma \rangle \to Q_{16} \underset{\tau \to \rho}{\longrightarrow} C_2 = \langle \rho \rangle = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$

$$1 \to C_2 \cong \langle \sigma \rangle / \langle \sigma^2 \rangle \to C_2^2 \cong Q_{16}/\langle \sigma^2 \rangle \to C_2 = \mathrm{Gal}(k(\sqrt{b})/k) \to 1,$$

$$1 \to C_4 \cong \langle \sigma^2 \rangle \to Q_{16} \to C_2^2 \to 1,$$

the problem (8) is solvable if and only if $\exists a \in k^* \setminus k^{*2}$: a and b are independent *mod* k^{*2}, $(a, ab) = 1$ and $(a, 2)(b, b) = (-b, x)$, for some $x \in k^*$. By the remark after [Le, Example 4.4] b is a sum of nine squares and we can say when b is a sum of three squares (in fact two or three nonzero squares, since $b \in k^* \setminus k^{*2}$).

Lemma 5.1. *b is a sum of three squares in $k \iff \exists x \in k^* : (b, b) = (-b, x)$.*

Proof. We have $(b, b)(-b, x) = (b, -1)(-1, x)(b, x) = (-1, x)(b, -x) = 1 \iff \exists y \in k^* : (-1, xy) = (b, -xy) = (-b, y) = 1$, by Proposition 1.2. Then $xy = u^2 + v^2$, for some $u, v \in k$, and $b = w^2 + xyz^2 = w^2 + (u^2 + v^2)z^2$, for some $w, z \in k$. Conversely, let $b = u^2 + v^2 + w^2$. We set $x = u^2 + v^2$ and get $(-1, x) = (b, -x) = 1$. ■

With the help of the last lemma in [MZ] are proved the following examples.

Example 5.2. The problem (7) for $a = -2$, $b = 2$ is solvable if and only if $s(k) = 2$.

Example 5.3. The problem (7) for $a = 2, b = -2, s(k) = 2$ is solvable.

Example 5.4. The problem (7) for $b = -a$ is solvable if and only if a is a sum of two squares and $-a$ is a sum of three squares.

Corollary 5.5. *Assume $s(k) = 4$. The group Q_{16} is always realizable.*

Example 5.6. The problem (8) for $b = -1$ and $-2 \in k^{*2}$ is solvable if and only if $\exists y, z \in k : y^2 + z^2 \notin \pm k^{*2}$.

Example 5.7. The problem (8) for $b = -1$ and $2 \in k^{*2}$ is solvable if and only if $|k^*/k^{*2}| \geq 4$ and $s(k) = 2$.

Example 5.8. The problem (8) for $b = y^2 + 1/y^2$, $y \in k^*$, such that $b + (\alpha/\beta)^2 \notin k^{*2}$ and $1/b + (\beta/\alpha)^2 \notin k^{*2}$, where $\alpha^2 + 2\beta^2 = -2$, is solvable.

6. The cyclic group $C_8 \cong \langle\sigma|\sigma^8 = 1\rangle$

Finally, given the extensions

$$(9) \qquad 1 \to C_4 \cong \langle\sigma^2\rangle \to C_8 \to C_2 = \mathrm{Gal}(k(\sqrt{a})/k) \to 1,$$

$$1 \to C_2 \cong \langle\sigma^2\rangle/\langle\sigma^4\rangle \to C_4 \cong C_8/\langle\sigma^4\rangle \to C_2 = \mathrm{Gal}(k(\sqrt{a})/k) \to 1,$$

$$1 \to C_2 \cong \langle\sigma^4\rangle \to C_8 \to C_4 \to 1,$$

the problem (9) is solvable if and only if $(a, a) = 1$ and $\exists x \in k^* : (a, 2) = (-1, x)$.

When $(a, a) = (a, 2) = 1$ in [GSS] is given a parametrization of all C_8 extensions, derived from [Sc], where Schneps gives a number of fields (the rational field among others), for which this is always possible.

Example 6.1. Let $a = -1$. Then $(a, 2) = (-1, 2) = 1$, and $(a, a) = (-1, -1) = 1 \iff s(k) = 2$. Thus the problem (9) for $a = -1$ is solvable if and only if $s(k) = 2$.

Example 6.2. Let $a = y^2 + 1/y^2$, $y \in k^*$. Therefore $a = y^2 + 1/y^2 = (y + 1/y)^2 - 2$, hence $(a, 2) = 1$. Since $(a, a) = 1$, the problem (9) for $a = y^2 + 1/y^2$, $y \in k^*$, is solvable.

Example 6.3. Let $(a, a) = 1$. If $-2 \in k^{*2}$ then $(a, 2) = (a, -1) = 1$, hence the problem (9) is solvable. Therefore, we can assume $-2 \notin k^{*2}$. By

Proposition 1.2 $(a,2)=(-1,x) \iff \exists z \in k^*$: $(a,2z)=(-1,xz)=(-a,z)=1$, for some $x \in k^*$. Equivalently, there exist u_i , $v_i \in k$, $i=1,2$ such that $a=u_1^2-2zv_1^2$ and $-a=u_2^2-zv_2^2$ (we can always set $x=z$ to secure $(-1,xz)=1$). Then

$$u_1^2+u_2^2-z(v_2^2+2v_1^2)=0 \iff z=\frac{u_1^2+u_2^2}{v_2^2+2v_1^2},$$

where $v_2^2+2v_1^2 \neq 0$, since $-2 \notin k^{*2}$. Now, replace z in

$$a=u_1^2-2zv_1^2=u_1^2-2\frac{u_1^2+u_2^2}{v_2^2+2v_1^2}v_1^2=\frac{u_1^2v_2^2-2u_2^2v_1^2}{v_2^2+2v_1^2}=\frac{u^2-2v^2}{v_2^2+2v_1^2},$$

where $u^2=u_1^2v_2^2$, $v^2=u_2^2v_1^2$. Thus the problem (9) for $-2 \notin k^{*2}$ is solvable $\iff$ $(a,a)=1$ and $\exists u,v,u_1,v_1 \in k$ such that $a=\dfrac{u^2-2v^2}{v_2^2+2v_1^2}$.

References

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

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

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

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

[Mi] I. Michailov, Some groups of order 8 and 16 as Galois groups over Q, *J. Number Theory*, Submitted.

[MZ] I. Michail,ov, N. Ziapkov, Embedding obstructions for the generalized quaternion group, *J. Algebra* **226**, N 1 (2000), 375-389.

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

[Sw] J. Swallow, Embedding problems and the $C_{16} \to C_8$ obstruction, *Cont. Math.* **186** (1995), 75-90.

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

Faculty of Mathematics, Informatics and Economics
"Constantin Preslavski" University
9700 Shoumen, BULGARIA

Received: 07.04.2000

e-mail: i.michailov@fmi.shu-bg.net n.ziapkov@shu-bg.net