M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 17, 2003, Fasc. 1-2

Some Groups of Orders 8 and 16 as Galois Groups over $\mathbb{Q}$ [1]

Ivo M. Michailov

Presented by P. Kenderov

We consider some embedding problems relevant to the embedding of biquadratic extensions in M_{16}, SD_{16}, D_{16} and Q_{16} extensions over $\mathbb{Q}$. The existence of C_8 and Q_8 extensions over $\mathbb{Q}$ is studied as well. We find necessary and sufficient conditions in terms of congruencies and quadratic residues.

1. Introduction

Let a and b be distinct square-free integers. In this work, we consider the conditions for existence of G extensions over $\mathbb{Q}$ which are cyclic over $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, for some groups G of order 16. In other words, we consider the embedding problems related to the exact sequences of the type

$$1 \to C_4 \to G \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) \to 1,$$

where G is one of the following groups of order 16 : the modular group M_{16}; the semidihedral (or quasidihedral) group SD_{16} (also noted in the literature as QD_8); the dihedral group D_{16} (or D_8); and the quaternion group Q_{16}. Their presentations are as follows:

$$\begin{aligned} M_{16} &\cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^5\tau \rangle, \\ SD_{16} &\cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle, \\ D_{16} &\cong \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle, \\ Q_{16} &\cong \langle \sigma, \tau | \sigma^8 = 1, \tau^2 = \sigma^4, \tau\sigma = \sigma^{-1}\tau \rangle. \end{aligned}$$

[1]This work is partially supported by Project N^o15/14.03.2002 of Shoumen University

We also study the existence of C_8 (the cyclic group of order 8) extensions over $\mathbb{Q}$, containing $\mathbb{Q}(\sqrt{a})$; and Q_8 (the quaternion group of order 8) extensions over $\mathbb{Q}$, containing $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.

Our goal is to find necessary and sufficient conditions in terms of congruencies and quadratic residues. By the means of the elementary number theory we find these conditions when a or b is a prime.

Of course, many other similar problems could be treated in this manner, thus obtaining analogous results.

In Section 3 we investigate the existence of Q_8 extensions over $\mathbb{Q}$, containing given $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Part of the results there are known and can also be obtained by applying the methods of the works [Re] (by solving a set of three quadratic equations), or [Va] (by the norms of algebraic integers in quadratic subfields of $\mathbb{Q}(\sqrt{a}, \sqrt{b})$). Such a fact is that $\mathbb{Q}(\sqrt{3}, \sqrt{b})$ admits a Q_8 extension if and only if $b = 2n$, where every prime divisor p of $n \in \mathbb{N}$ satisfies $p \equiv 1$ (6).

In Sections 4-7 we consider the mentioned groups of order 16. An essential part is given to the existence of extensions containing $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are distinct primes. We must say that we investigate only a part of the ways of embedding such extensions. If one similarly considers all non-equivalent embedding problems with kernels of order 4, this will give the answer of the question whether the biquadratic extension of that kind is contained (whatever the embedding might be) in the extensions realizing these groups.

We will write (a, b) the equivalence class in the Brauer group $\mathrm{Br}(\mathbb{Q})$ of the quaternion algebra generated over $\mathbb{Q}$ by two anti-commuting elements i and j such that $i^2 = a, j^2 = b$. It is known that the realizability of groups of order a power of 2 is linked to the splitting of certain products of quaternion algebras in the Brauer group. The obstructions for the realizability of the groups of order 16 over arbitrary fields of characteristic not 2 are well-known and can be found in [GSS, GS, Ki, Le]. Very helpful in our consideration is the following lemma.

Lemma 1 *Let $a, b, c,$ and $d \in \mathbb{Z}^*$. Then*

(1). $(a, b) = 1 \in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow \exists x, y, z \in \mathbb{Z} : ax^2 + by^2 = z^2$;

(2).*(the common slot property)* $(a, b)(c, d) = 1 \in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow \exists x \in \mathbb{Z} : (a, bx) = (c, dx) = (ac, x) = 1 \in \mathrm{Br}(\mathbb{Q})$.

Now let a and b be square-free relatively prime natural numbers. By the lemma $(a, b) = 1 \in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow \exists x, y, z \in \mathbb{Z} : ax^2 + by^2 = z^2$. This equation is solvable if and only if $a \equiv \alpha^2 \pmod{b}$ and $b \equiv \beta^2 \pmod{a}$, for some $\alpha, \beta \in \mathbb{N}$. In other words, a must be a quadratic residue mod q, for every prime divisor q of b, and b must be a quadratic residue mod p, for every prime divisor p of a. The other situation which we will encounter is $(a, -b) = 1 \in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow \exists x, y, z \in$

$\mathbb{Z} : ax^2 - by^2 = z^2$. This equation is solvable if and only if $a \equiv \alpha^2 \pmod{b}$ and $b \equiv -\beta^2 \pmod{a}$, for some $\alpha, \beta \in \mathbb{N}$. Of course these two situations are special cases of the diophantine equation $ax^2 + by^2 = cz^2$, where a, b and c are square-free natural numbers, which is solved by Legendre (cf. [Na, VI, Theorem 113]).

Given an odd prime p and an integer n relatively prime to p, Legendre introduces the symbol $(n|p)$ defined as follows : $(n|p) = 1$, if n is a quadratic residue mod p and $(n|p) = -1$, if n is a non-residue mod p. We have the relations $(-1|p) = (-1)^{\frac{p-1}{2}}, (nm|p) = (n|p)(m|p)$, and if $n \equiv m \pmod{p}$ then $(n|p) = (m|p)$. Moreover, the quadratic reciprocity law holds : if p and q are distinct odd primes then $(p|q)(q|p) = (-1)^h$, where $h = \frac{1}{4}(p-1)(q-1)$.

Then $(p, q) = 1 \in \mathrm{Br}(\mathbb{Q})$ if and only if $(p|q) = (q|p) = 1$. In particular p or q is of the form $4s + 1$. Also $(p, pq) = (p, -1)(p, q) = (p, -q) = 1 \in \mathrm{Br}(\mathbb{Q})$ if and only if $(p|q) = (-q|p) = 1$. If $p \equiv 1\ (4)$ then $p = x^2 + y^2$, for some $x, y \in \mathbb{Z}$ (see for example [Sa, V, §5.6]), and $(p, -1) = 1 \in \mathrm{Br}(\mathbb{Q})$. Whence $(p, pq) = (p, q) = 1 \in \mathrm{Br}(\mathbb{Q})$ if and only if $(p|q) = 1$ by the reciprocity law. If $p \equiv 3\ (4)$ then $(-1|p) = -1$, and $(p, -q) = 1 \in \mathrm{Br}(\mathbb{Q})$ if and only if $(p|q) = 1$ and $(q|p) = -1$. Again, by the reciprocity law this is equivalent to $(p|q) = 1$ and $q \equiv 3\ (4)$.

We will also make extensive use of the following facts (for p odd prime):

$$\begin{aligned} (2, p) = 1 \quad &\in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow (2|p) = 1 \quad \Leftrightarrow p \equiv 1, 7\ (8); \\ (-2, p) = 1 \quad &\in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow (-2|p) = 1 \quad \Leftrightarrow p \equiv 1, 3\ (8). \end{aligned}$$

By the Davenport- Cassels result [Se, IV, Lemma B] is known that if a natural number is a sum of two (three) rational squares then it is also a sum of two (three) integer squares. Therefore $(p, p) = 1 \in \mathrm{Br}(\mathbb{Q})$ if and only if $p = x^2 + y^2$, for some $x, y \in \mathbb{Z}$, which is equivalent to $p \equiv 1\ (4)$. For a natural number to be a sum of two squares it is necessary and sufficient that, for every prime divisor of the form $4s + 3$, its exponent in the prime factorization be even [Sa, V, §5.6, Theorem 1]. For a natural number to be a sum of three squares it is necessary and sufficient that it can not be represented in the form $4^k(8s + 7)$ [Se, IV, Theorem(Gauss)]. The necessary and sufficient conditions for solvability of the embedding problems which we shall consider are taken from [MZ2]. Finally, I would like to thank N. Ziapkov for his support and suggestions during the preparation of this paper.

2. The cyclic group of order 8

The necessary and sufficient condition for the solvability of the embedding

problem related to the exact sequence

$$1 \to C_4 \hookrightarrow C_8 \to C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \to 1 \tag{2.1}$$

is $(a,a) = 1$ and $(a,2) = (-1,x)$, for some $x \in \mathbb{Z}^*$. If the condition is satisfied we will also say that $\mathbb{Q}(\sqrt{a})$ admits a C_8 extension.

Proposition 2.1 *Let a be a square-free natural number. Then $\mathbb{Q}(\sqrt{a})$ admits a C_8 extension if and only if every odd prime divisor p of a satisfies $p \equiv 1$ (8).*

P r o o f. Let $(a,a) = 1$; i.e., a does not have prime divisors of the form $4s+3$. Then the condition $(a,2) = (-1,x), x \in \mathbb{Z}$, is equivalent to $(a,2y) = (-a,y) = 1$, for some $y \in \mathbb{N}$ (we can always set $x = y$ to ensure $(-1,xy) = 1$).

Since $(a,a) = (a,-a) = 1$, we can assume that a does not divide y. If p is a prime divisor of a such that $p \equiv 1$ (8) or $p = 2$ we have $(p,2) = 1$.

Now let $p \equiv 5$ (8) be a prime divisor of a such that p and y are relatively prime. If 2 does not divide y then from $(a,2y) = 1$ and $(2|p) = -1$ follows that $(2y|p) = (2|p)(y|p) = -(y|p) = 1$ but $(-a,y) = 1$ implies $(y|p) = 1$, an impossibility. If $y = 2z, z \in \mathbb{N}$, then from $(a,2y) = (a,z) = 1$ follows that $(z|p) = 1$ but $(-a,y) = (-a,2z) = 1$ implies $(2z|p) = (2|p)(z|p) = -(z|p) = 1$, an impossibility.

Thus, we have proved that every odd prime divisor p of a must be of the form $8s+1$. ∎

In particular, for all $a \in \mathbb{Q}$ such that $(a,a) = 1$ and $(a,2) = (-1,x)$, we have $(a,2) = 1$. In [Sc] Schneps gives the complete set of C_8 extensions over fields with that property.

3. The quaternion group of order 8

The realizability of Q_8 over fields of characteristic not 2 is extensively studied in the literature (see the works [Wa, Wi, Ki, Re] among others). In [MZ1] are given some examples of solvable embedding problems both with Q_8 and Q_{16}. In [JY] Jensen and Yui give an explicit construction (when -1 is a sum of two squares), and a survey of known results. Some of the following cases are investigated in [Va] as well.

The necessary and sufficient condition for the solvability of the embedding problem related to the exact sequence

$$1 \to C_2 \hookrightarrow Q_8 \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a},\sqrt{b})/\mathbb{Q}) \to 1 \tag{3.1}$$

is $(a,ab)(b,b) = 1$ (or, equivalently, $(a,a)(b,ba) = 1$). Since the condition is symmetrical regarding a and b, we will just say that $\mathbb{Q}(\sqrt{a},\sqrt{b})$ admits a Q_8 extension.

For $b = 2$ the condition becomes $(a, 2a)(2, 2) = (a, -2) = 1$. Let p be an odd prime divisor of a. From $(a, -2) = 1$ follows that $(-2|p) = 1$; i.e., $p \equiv 1, 3\ (8)$. (The case $a = p \equiv 1, 3\ (8)$ is studied in details in [Co].) Therefore $\mathbb{Q}(\sqrt{a}, \sqrt{2})$ admits a Q_8 extension if and only if every odd prime divisor p of a satisfies $p \equiv 1, 3\ (8)$.

Proposition 3.1 *For $\mathbb{Q}(\sqrt{3}, \sqrt{b})$ to admit a Q_8 extension it is necessary that b be even.*

Proof. We have $(a, ab)(b, b) = (3, 3b)(b, b) = (3, -b)(-1, b)$. By lemma 1 the condition $(3, -b)(-1, b) = 1$ is equivalent to $(3, -bk) = (-3, k) = (-1, bk) = 1$, for some $k \in \mathbb{Z}$. Obviously, k and b must be natural.

Let us assume $b = mn$, where $m \in \mathbb{N}$ is a product of primes of the form $4s+1$, and $n \in \mathbb{N}$ is a product of primes of the form $4s+3$. Further, $(-1, bk) = 1$ implies $k = nm_1$, where m_1 does not have prime divisors of the form $4s + 3$. Then the condition becomes $(3, -mm_1) = (-3, nm_1) = 1$.

Then for every prime divisor q of n we have $(-3|q) = -(3|q) = 1$ and $(q|3) = 1$, since $q \equiv 3\ (4)$. Therefore $(-3, q) = 1$, and also $(-3, n) = 1$. Since $(-1, m_1) = 1$, we obtain $(3, m_1) = 1$. Finally, the condition $(3, -m) = 1$ implies that for every prime divisor p of m we have $(3|p) = (p|3) = 1$, since $p \equiv 1\ (4)$. Therefore $(3, p) = 1$, and also $(3, -m) = (3, -1)(3, m) = (3, -1) = 1$, an impossibility. In that way, if the condition is satisfied then b must be even. ■

Proposition 3.2 *For $\mathbb{Q}(\sqrt{3}, \sqrt{b})$ to admit a Q_8 extension it is necessary and sufficient that $b = 2n$, where every prime divisor p of $n \in \mathbb{N}$ satisfies $p \equiv 1\ (6)$.*

Proof. We have already proved that $b = 2n, n \in \mathbb{N}$, is a necessary condition. Then the solvability condition becomes $(a, ab)(b, b) = (3, 6n)(-1, 2n) = (3, n)(-1, n) = (-3, n) = 1$.

Let p be an arbitrary divisor of n. From $(-3, n) = 1$ follows that $(-3|p) = 1$; i.e., $p \equiv 1\ (6)$. Conversely, let $p \equiv 1\ (6)$. Then $(-3|p) = (p|3) = 1$, consequently $(-3, p) = 1$, respectively, $(-3, n) = 1$. ■

Proposition 3.3 *For $a = p, b = q$- distinct odd primes, the problem (3.1) is solvable $\Leftrightarrow p \equiv 1\ (4), q \equiv 1\ (4)$, and $(p|q) = 1$.*

Proof. Indeed, $p \equiv 1\ (4)$ implies $(p, p) = 1, q \equiv 1\ (4)$ implies $(q, q) = 1$, and $(p|q) = 1$ implies $(p, q) = 1$. Whence $(p, pq)(q, q) = (p, p)(p, q)(q, q) = 1$.

Conversely, let the problem (3.1) be solvable. If $p \equiv 1\ (4)$ then $(p, pq)(q, q) = (p, q)(q, q) = (-p, q) = 1$ implies $(q|p) = 1$ and $(-p|q) = (p|q) = 1$. Therefore we must have $q \equiv 1\ (4)$.

By the symmetry the case $p \equiv 3\ (4), q \equiv 1\ (4)$ is impossible.

Now let $p \equiv 3\ (4), q \equiv 3\ (4)$. If $(p|q) = 1$ then $(p, -q) = 1$. But $(p, -q)(q, q) = (q, q) = 1$ implies $q \equiv 1\ (4)$, an impossibility. Finally, if $(p|q) = -1$ then $(-p|q) = 1$ and $(q|p) = 1$, therefore $(-p, q) = 1$. But $(p, pq)(q, q) = (p, p)(-p, q) = (p, p) = 1$ implies $p \equiv 1\ (4)$, an impossibility.

Thus, we must have $p \equiv 1\ (4), q \equiv 1\ (4)$, and $(p, q) = 1$ (i.e., $(p|q) = 1$).

■

Now, let p and q be distinct odd primes, and let $a = p, b = 2q$. Then the condition is $(p, 2pq)(2q, 2q) = (p, p)(p, 2q)(q, q) = 1$, and we have four cases.

1. $p \equiv 1\ (4), q \equiv 1\ (4)$. The condition becomes $(p, p)(p, 2q)(q, q) = (p, 2q) = 1$. Then $(p|q) = (q|p) = 1$; i.e., $(p, q) = 1$. Therefore $(p, 2) = 1$, which can occur if and only if $p \equiv 1\ (8)$. Thus, in this case the problem (3.1) is solvable $\Leftrightarrow p \equiv 1\ (8)$ and $(p|q) = 1$.

2. $p \equiv 1\ (4), q \equiv 3\ (4)$. We have $(p, p)(p, 2q)(-1, 2q) = (-p, 2q) = 1 \Leftrightarrow (-p|q) = 1$ and $(2q|p) = 1$. By the reciprocity law this is equivalent to $(p|q) = (q|p) = -1$ and $(2q|p) = (2|p)(q|p) = -(2|p) = 1$, which can occur if and only if $p \equiv 5\ (8)$. Thus, in this case the problem (3.1) is solvable $\Leftrightarrow p \equiv 5\ (8)$ and $(p|q) = -1$.

3. $p \equiv 3\ (4), q \equiv 1\ (4)$. We have $(p, 2pq)(2q, 2q) = (p, -2q) = 1 \Leftrightarrow (p|q) = 1$ and $(-2q|p) = 1$. Again by the reciprocity law this is equivalent to $(p|q) = (q|p) = 1$ and $(-2q|p) = (-2|p)(q|p) = (-2|p) = 1$, which can occur if and only if $p \equiv 3\ (8)$. Thus, in this case the problem (3.1) is solvable $\Leftrightarrow p \equiv 3\ (8)$ and $(p|q) = 1$.

4. $p \equiv 3\ (4), q \equiv 3\ (4)$. If $p \equiv 3\ (8)$ then $(p, -2) = 1$ and the condition becomes $(p, 2pq)(-1, 2q) = (p, -2)(p, q)(-1, q) = (-p, q) = 1$. This is equivalent to $(-p|q) = (q|p) = 1$. This is possible since $(-p|q) = -(p|q)$. If $p \equiv 7\ (8)$ then $(p, 2) = 1$ and the condition becomes $(p, 2pq)(-1, 2q) = (p, -q)(-1, q) = 1$, which is impossible as we have seen in proposition 3.3.

Thus, we have shown that for $a = p$ and $b = 2q$, the problem (3.1) is solvable in either of the following cases :

1. $p \equiv 1\ (8), q \equiv 1\ (4), (p|q) = 1$;
2. $p \equiv 5\ (8), q \equiv 3\ (4), (p|q) = -1$;
3. $p \equiv 3\ (8), q \equiv 1\ (4), (p|q) = 1$;
4. $p \equiv 3\ (8), q \equiv 3\ (4), (p|q) = -1$.

4. The modular group of order 16

The necessary and sufficient condition for the solvability of the embedding problem related to the exact sequence

$$1 \to C_4 \cong \langle \sigma^2 \rangle \hookrightarrow M_{16} \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) \to 1 \tag{4.1}$$

is $(a, a) = 1$ and $(a, 2b) = (-1, x)$, for some $x \in \mathbb{Z}^*$.

Proposition 4.1 *For $a = 2$, the problem (4.1) is solvable if and only if every odd prime divisor p of b satisfies $p \equiv 1, 3, 7$ (8).*

Proof. Since $(2, 2) = 1$, the condition becomes $(b, 2) = (-1, x)$. Of course, if b does not have odd prime divisors, the problem (4.1) is solvable since then b must be equal to -2 or -1, therefore $(b, 2) = 1$.

Now let p be an odd prime divisor of b. If $p \equiv 7$ (8) then $(p, 2) = 1$. If $p \equiv 3$ (8) then $(p, 2) = (-1, p)$. Therefore, we can suppose that b does not have prime divisors of the form $4s + 3$. Since $(-1, 2) = 1$ we can also assume that b is natural. But then $(b, b) = 1$ and by proposition 2.1 the condition is satisfied if and only if every odd prime divisor p of b satisfies $p \equiv 1$ (8). ∎

If $b = 2$, the problem (4.1) obviously is solvable if and only if $a \neq 2$ is a natural number, which does not have prime divisors of the form $4s + 3$.

Let $a = p$ and $b = q$ be distinct odd primes. Then $p \equiv 1$ (4) $\Leftrightarrow (p, p) = 1$, and the condition becomes $(p, 2q) = (-1, x)$. This is equivalent to $(p, 2qy) = (-p, y) = 1$, for some $y \in \mathbb{N}$ (since $(p, p) = (p, -p) = 1$, we can again assume that p does not divide y). Then $(y|p) = 1$ and $(2qy|p) = (2q|p)(y|p) = (2q|p) = 1$.

Further, if q divides y then $(-p, y) = 1$ implies $(-p|q) = 1$; otherwise $(p, 2qy) = 1$ implies $(p|q) = 1$. Therefore, we have either $(-p, 2q) = 1$ (and we can put $x = 2q$) or $(p, 2q) = 1$ (and we can put $x = 1$).

Thus, for $a = p$ and $b = q$, the problem (4.1) is solvable in either of the following cases:

1. $p \equiv 1$ (4), $(2q|p) = 1$ and $(p|q) = 1$
2. $p \equiv 1$ (4), $(2q|p) = 1$ and $(-p|q) = 1$.

Now, let p and q be distinct odd primes, and let $a = p, b = 2q$. Then we must have $p \equiv 1$ (4), and the condition becomes $(p, q) = (-1, x)$. If $(p|q) = 1$ then $(p, q) = 1$. If $(p|q) = -1$ then $(q|p) = -1$. The condition is equivalent to $(p, qy) = (-p, y) = 1$, for some $y \in \mathbb{N}$. Therefore $(y|p) = 1$ and $(qy|p) = (q|p)(y|p) = (q|p) = 1$, an impossibility.

Thus, for $a = p, b = 2q$, the problem (4.1) is solvable $\Leftrightarrow p \equiv 1\ (4)$ and $(p|q) = 1$.

5. The semidihedral group of order 16

The necessary and sufficient condition for the solvability of the embedding problem related to the exact sequence

$$(5.1) \qquad 1 \to C_4 \cong \langle \sigma^2 \rangle \hookrightarrow SD_{16} \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) \to 1$$

is $(a, ab) = 1$ and $(a, -2) = (-b, x)$, for some $x \in \mathbb{Z}^*$.

First of all we will prove two lemmas which will also be used for the groups D_{16} and Q_{16}.

Lemma 5.1 *Let p be an odd prime, let n be an integer, and let p and n be relatively prime such that $(p, pn) = (p, -n) = 1$. Then :*

1. $\exists x \in \mathbb{Z} : (p, -1) = (-n, x) \Leftrightarrow p \equiv 1\ (4)$;
2. $\exists x \in \mathbb{Z} : (p, 2) = (-n, x) \Leftrightarrow p \equiv 1, 7\ (8)$;
3. $\exists x \in \mathbb{Z} : (p, -2) = (-n, x) \Leftrightarrow p \equiv 1, 3\ (8)$.

Proof. We need only establish necessity ($\Rightarrow$) in each case.

1. Let us assume that $p \equiv 3\ (4)$ and $(p, -1) = (-n, x)$. Then by lemma 1 $(-1, py) = (n, y) = 1$, for some $y \in \mathbb{N}$. But $(-1, py) = 1$ can occur if and only if $y = pz$, where z is a square-free natural number which does not have prime divisors of the form $4s + 3$.

   Then $(n, pz) = 1$ implies $(n|p) = 1$, but $(p, -n) = 1$ implies $(-n|p) = -(n|p) = 1$, an impossibility.

2. Let $p \equiv 3\ (8)$. Then $(p, -2) = 1$ and $(p, 2) = (p, -1) = (-n, x)$ can not occur as we have just shown.

   Now let $p \equiv 5\ (8)$ and $(p, 2) = (-n, x)$. Then $(p, 2y) = (-pn, y) = 1$, for some $y \in \mathbb{N}$. If $y = pz, z \in \mathbb{N}$, then $(p, 2pz) = (p, p)(p, 2z) = (p, 2z)$, since $p \equiv 1\ (4)$. Also, $(-pn, pz) = (-pn, p)(-pn, z) = (-pn, z)$, since $(p, -n) = 1$. Therefore, we can assume that p and y are relatively prime. Then $(-pn, y) = 1$ implies $(y|p) = 1$, but $(p, 2y) = 1$ implies $(2y|p) = (2|p)(y|p) = -(y|p) = 1$, an impossibility.

3. Let $p \equiv 5\ (8)$. Then $(p,-1) = 1$ and $(p,-2) = (p,2) = (-n,x)$ can not occur as we saw in 2.

   Let $p \equiv 7\ (8)$. Then $(p,2) = 1$ and $(p,-2) = (p,-1) = (-n,x)$ also can not occur as we saw in 1. This proves our lemma.

■

Lemma 5.2 *Let p and q be distinct odd primes, m be a product of primes of the form $4s+1$, and let t be an integer such that p, q, m and t be pairwise relatively prime. If $(pq, tm) = 1$ then $(t|p)(t|q) = 1$.*

Proof. Let $(pq, tm) = 1$. In particular $(tm|p) = (tm|q) = 1$. We have that $m = \prod_{i=1}^{k} r_i$, where $r_i \equiv 1\ (4)$ are distinct primes (if $k = 1$, i.e., $m = 1$ then obviously, $(pq, t) = 1$ implies $(t|p) = (t|q) = 1$).

If $(p|r_i) = (q|r_i) = 1$ then $(r_i|p) = (r_i|q) = 1$, and also $(pq, r_i) = 1$. Therefore, we can assume that m does not have such divisors. Then $(pq, tm) = 1$ implies $(pq|r_i) = 1; i = 1, \ldots, k$. Whence $(p|r_i) = (q|r_i) = -1$ and $(r_i|p) = (r_i|q) = -1$. Finally, from

$$(tm|p) = (t|p) \prod_{i=1}^{k} (r_i|p) = (t|p)(-1)^k$$

and

$$(tm|q) = (t|q) \prod_{i=1}^{k} (r_i|q) = (t|q)(-1)^k.$$

follows that $(tm|p)(tm|q) = (t|p)(t|q) = 1$. ■

For $a = 2$: $(a,-2) = (2,-2) = 1$, so the condition becomes $(a, ab) = (2, b) = 1$. Therefore the problem (5.1) is solvable if and only if every odd prime divisor p of b satisfies $p \equiv 1, 7\ (8)$.

For $b = 2$ the condition becomes $(a, ab) = (a, 2a) = (a,-2) = 1$, therefore the problem (5.1) is solvable if and only if every odd prime divisor p of a satisfies $p \equiv 1, 3\ (8)$.

By lemma 5.1 we immediately get

Proposition 5.3 *For $a = p$- an odd prime which is relatively prime to b, the problem (5.1) is solvable if and only if $p \equiv 1, 3\ (8)$ and $(p,-b) = 1$.*

Corollary 5.4 *For $a = p$ and $b = q$- distinct odd primes, the problem (5.1) is solvable if and only if*

1. $p \equiv 1\ (8)$ *and* $(p|q) = 1$*;*
2. $p \equiv 3\ (8), q \equiv 3\ (4)$ *and* $(p|q) = 1$*.*

We proceed with two examples where we can not use lemma 5.1 since b is a multiple of a.

Proposition 5.5 *For $a = p$- an odd prime, $b = 2p$, the problem (5.1) is solvable $\Leftrightarrow p \equiv 1, 7\ (8)$.*

P r o o f. Indeed, we have that $(a, ab) = (p, 2) = 1 \Leftrightarrow p \equiv 1, 7\ (8)$. If $p \equiv 1\ (8)$ then $(a, -2) = (p, -2) = 1$.

Now let $p \equiv 7\ (8)$. By the Chinese theorem we can choose a prime q such that $q \equiv 5\ (8)$ and $q \equiv -1\ (p)$. (In fact, they are infinitely many by Dirichlet theorem.) Then $(q|p) = (p|q) = -1$, and $(2|q) = -1$. From $(2p|q) = 1$ and $(-q|p) = 1$ follows that $(2p, -q) = 1$. Put $x = 2q : (-b, x) = (-2p, 2q) = (-1, 2q)(2p, 2q) = (2p, -2)(2p, -q) = (2p, -2) = (p, -2)$. Therefore, for $p \equiv 7\ (8)$, the condition also holds. ∎

Now, let p and q be distinct odd primes, and let $a = p, b = pq$. Then we must have $(a, ab) = (p, q) = 1$ which means that $(p|q) = 1$, and either p or q is $\equiv 1\ (4)$. The condition becomes $(p, -2) = (-pq, x)$. We consider the following cases:

1. $p \equiv 1, 3\ (8)$. Obviously $(p, -2) = 1$.
2. $p \equiv 5\ (8)$. We have the following subcases.
   (a) $q \equiv 1, 7\ (8)$. Put $x = 2 : (-pq, 2) = (-p, 2)(q, 2) = (-p, 2) = (p, 2) = (p, -2)$.
   (b) $q \equiv 3\ (8)$. Then $(q, 2) = (q, -1) \neq 1$. The condition is equivalent to $(p, -2y) = (-q, y) = 1$, for some $y \in \mathbb{N}$. (Since $(p, p) = (p, q) = 1$ we can again assume that p and q do not divide y.) If y is odd then for every prime divisor r of y we have $(p|r) = (r|p) = 1$ and $(p, r) = 1$. Therefore $(p, y) = 1$ and $(p, -2y) = (p, -2)(p, y) = (p, -2) = 1$, an impossibility.
   Now let $y = 2mn$, where m is a product of primes $\equiv 1\ (4)$, n is a product of primes $\equiv 3\ (4)$. Then, for every odd prime divisor r of y we have the following. If r divides m, i.e., $r \equiv 1\ (4)$ then $(-q, 2mn) = 1$ implies $(-q|r) = (q|r) = (r|q) = 1$. Therefore $(-q, r) = 1$, also $(-q, m) = 1$. If r divides n, i.e., $r \equiv 3\ (4)$ then $(-q, 2n) = 1$ implies $(-q|r) = -(q|r) = (r|q) = 1$. Therefore $(-q, r) = 1$, also $(-q, n) = 1$. Thus $(-q, 2) = (q, 2) = 1$, an impossibility.

(c) $q \equiv 5\ (8)$. As before, we can choose a prime $r \equiv 3\ (4)$ such that $(r|p) = 1$ and $(r|q) = -1$. Then we have $(p, r) = 1$ and $(-q|r) = -(q|r) = 1$. Therefore $(2r|q) = 1$, also $(-q, 2r) = 1$. Put $x = 2r$: $(-pq, 2r) = (p, 2r)(-q, 2r) = (p, 2r) = (p, 2) = (p, -2)$.

Finally,

3. $p \equiv 7\ (8)$. We have two subcases.

(a) $q \equiv 1\ (8)$. The condition $(p, -2) = (p, -1) = (-pq, x)$ is equivalent to $(-1, py) = (pq, y) = 1$, for some $y \in \mathbb{N}$. This can occur only if $y = pz$, z- a natural number which does not have prime divisors of the form $4s + 3$. Then $z = m$ or $z = 2m$, where m is a product of primes $\equiv 1\ (4)$. Since $(pq, q) = (p, q)(q, q) = 1$, the condition becomes $(pq, pz) = (pq, q)(pq, pz) = (pq, pqz) = (pq, -z) = 1$.
If $z = m$ then we can put $t = -1$. Since $(-1|p) = -1$ and $(-1|q) = 1$, by lemma 5.2 we have $(pq, -m) \neq 1$, an impossibility. If $z = 2m$ then we can put $t = -2$. Since $(-2|p) = -1$ and $(-2|q) = 1$, by lemma 5.2 we have $(pq, -2m) \neq 1$, an impossibility.

(b) $q \equiv 5\ (8)$. Again, by the Chinese theorem we can choose a prime $r \equiv 1\ (4)$ such that $(r|p) = (r|q) = -1$. Then we have $(p|r) = (q|r) = -1$, and $(pq|r) = 1$. From $(-2|p) = (-2|q) = -1$ we obtain $(-2r|p) = (-2r|q) = 1$, therefore $(pq, -2r) = 1$. Put $x = 2r$: $(-pq, 2r) = (pq, 2r) = (pq, -1)(pq, -2r) = (p, -1)(q, -1) = (p, -1) = (p, -2)$.

Thus, we have obtained that for $a = p, b = pq$, the problem (5.1) is solvable only in the following cases :

1. $p \equiv 1\ (8)$ and $(p|q) = 1$;
2. $p \equiv 3\ (8), q \equiv 1, 5\ (8)$ and $(p|q) = 1$;
3. $p \equiv 5\ (8), q \equiv 1, 5, 7\ (8)$ and $(p|q) = 1$;
4. $p \equiv 7\ (8), q \equiv 5\ (8)$ and $(p|q) = 1$.

Note that the last two examples also show that when a and b are not relatively prime the lemma 5.1 is not true.

6. The dihedral group of order 16

The necessary and sufficient condition for the solvability of the embedding problem related to the exact sequence

$$1 \to C_4 \cong \langle \sigma^2 \rangle \hookrightarrow D_{16} \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) \to 1 \tag{6.1}$$

is $(a, ab) = 1$ and $(a, 2) = (-b, x)$ (or, equivalently, $(ab, 2) = (-b, x)$), for some $x \in \mathbb{Z}^*$.

For $a = 2$, the condition becomes $(a, ab) = (2, b) = 1$. Therefore the problem (6.1) is solvable if and only if every odd prime divisor p of b satisfies $p \equiv 1, 7\ (8)$.

Proposition 6.1 *For $b = 2$, the problem (6.1) is solvable if and only if every odd prime divisor p of a satisfies $p \equiv 1\ (8)$.*

P r o o f. We have that $(a, ab) = (a, 2a) = (a, -2) = 1$ if and only if every odd prime divisor p of a satisfies p$\equiv 1, 3\ (8)$. Then the condition $(a, 2) = (-2, x)$ is equivalent to $(ay, 2) = (-1, y) = 1$, for some $y \in \mathbb{N}$. Equivalently, $\exists u, v, w$, and $z \in \mathbb{N}$ such that $2z^2 + a(u^2 + v^2) = w^2$. Let $p \equiv 3\ (8)$ be an arbitrary prime divisor of a. If p divides both z and w then an even power of p divides $a(u^2 + v^2)$, i.e., an odd power of p divides $u^2 + v^2$, an impossibility. But when p does not divide z or w the congruence $2z^2 \equiv w^2 \pmod{p}$ can not occur, since 2 is a quadratic non- residue mod p.

Thus, we have obtained that every odd prime divisor of a must be $\equiv 1\ (8)$. Since then $(a, 2) = 1$, the condition holds. ∎

Again, by lemma 5.1 we immediately get

Proposition 6.2 *For $a = p$- an odd prime which is relatively prime to b, the problem (6.1) is solvable if and only if $p \equiv 1, 7\ (8)$ and $(p, -b) = 1$.*

Corollary 6.3 *For $a = p$ and $b = q$- distinct odd primes, the problem (6.1) is solvable if and only if*

1. *$p \equiv 1\ (8)$ and $(p|q) = 1$;*
2. *$p \equiv 7\ (8), q \equiv 3\ (4)$, and $(p|q) = 1$.*

Now, let p and q be distinct odd primes, and let $a = p, b = pq$. Similarly to Section we must have $(a, ab) = (p, q) = 1$, which means that $(p|q) = 1$, and either p or q is $\equiv 1\ (4)$. Then, the condition becomes $(p, 2) = (-pq, x)$ (equivalently $(q, 2) = (-pq, x)$). Obviously, this is satisfied if $p \equiv 1, 7\ (8)$ or $q \equiv 1, 7\ (8)$.

If $p \equiv 5\ (8)$ then $(p, 2) = (p, -2)$, therefore we can use the results from Section . Namely, the condition holds if and only if $q \equiv 1, 5, 7\ (8)$.

If $p \equiv 3\ (8)$ then the condition holds if and only if $q \equiv\ 1(8)$, since the case $p \equiv 3\ (8), q \equiv 5\ (8)$ is symmetrical to the case $p \equiv 5\ (8), q \equiv 3\ (8)$.

Thus, finally, we have obtained that for $a = p, b = pq$, the problem (6.1) is solvable in either of the following cases :

1. $p \equiv 1\ (8)$ and $(p|q) = 1$;
2. $p \equiv 3\ (8), q \equiv 1\ (8)$ and $(p|q) = 1$;
3. $p \equiv 5\ (8), q \equiv 1, 5, 7\ (8)$ and $(p|q) = 1$;
4. $p \equiv 7\ (8), q \equiv 1, 5\ (8)$ and $(p|q) = 1$.

7. The quaternion group of order 16

The necessary and sufficient condition for the solvability of the embedding problem related to the exact sequence

$$1 \to C_4 \cong \langle \sigma^2 \rangle \hookrightarrow Q_{16} \to C_2 \times C_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) \to 1 \tag{7.1}$$

is $(a, ab) = 1$ and $(a, 2)(b, b) = (-b, x)$ (or, equivalently, $(ab, 2)(b, b) = (-b, x)$), for some $x \in \mathbb{Z}^*$.

The following lemma is derived from [MZ1, Lemma 7.1].

Lemma 7.1 *A natural number b is a sum of three integer squares if and only if $(b, b) = (-b, x)$, for some $x \in \mathbb{Z}^*$.*

Let us recall that a square-free natural number b is a sum of three integer squares if and only if b is not of the form $8s + 7$.

Proposition 7.2 *For $a = 2$, the problem (7.1) is solvable if and only if b is a natural number such that every odd prime divisor p of b satisfies $p \equiv 1, 7\ (8)$, and if b is odd then also the number of the prime divisors $\equiv 7\ (8)$ of b is even.*

Proof. We have that $(a, ab) = (2, b) = 1$ if and only if every odd prime divisor p of b satisfies $p \equiv 1, 7\ (8)$. Since $(a, 2) = (2, 2) = 1$, the condition becomes $(b, b) = (-b, x)$. By lemma 7.1 this can occur if and only if b is not of the form $8s + 7$ (and of course b is natural). This, in turn, can occur if and only if b is even or if b is odd of the desired form. ∎

For $b = 2 : (b, b) = (2, 2) = 1$, so the condition is equivalent to that of D_{16} (see proposition 6.1). Therefore the problem (7.1) is solvable if and only if every odd prime divisor p of a satisfies $p \equiv 1\ (8)$.

Proposition 7.3 *For $a = p$- an odd prime which is relatively prime to b, b is natural $\neq 8s + 7$, the problem (7.1) is solvable if and only if $p \equiv 1, 7\ (8)$ and $(p, -b) = 1$.*

P r o o f. Since $(b,b) = (-b,x), x \in \mathbb{Z}$, the condition is equivalent to $(p,-b) = 1$ and $(p,2) = (-b,y)$, for some $y \in \mathbb{Z}$. By lemma 5.1 this can occur if and only if $p \equiv 1,7\ (8)$. ∎

Let $a = p$ and $b = q$ be distinct odd primes. Then the condition becomes $(p,pq) = 1, (p,2)(q,-1) = (-q,x)$. We consider all possible situations.

1. $p \equiv 1\ (4)$. If $q \equiv 1\ (4)$ or $q \equiv 3\ (8)$, then by proposition 7.3 the problem (7.1) is solvable $\Leftrightarrow$ $p \equiv 1\ (8)$ and $(p|q) = 1$. If $q \equiv 7\ (8)$ we have two subcases:

   (a) $p \equiv 1\ (8), q \equiv 7\ (8)$. Then $(p,2)(q,-1) = (q,-1) = (-q,x)$ can not occur.

   (b) $p \equiv 5\ (8), q \equiv 7\ (8)$. Then $(p,2)(q,-1) = (p,-2)(q,-2) = (pq,-2) = (-q,x) \Leftrightarrow (pq,-2y) = (-p,y) = 1$, for some $y \in \mathbb{N}$. Therefore $(y|p) = 1$ and $(-2y|p) = (-2|p)(y|p) = (-2|p) = 1$, an impossibility.

2. $p \equiv 3\ (4)$. If $q \equiv 1\ (4)$, then $(p,pq) = 1$ can not occur. Let $q \equiv 3\ (4)$. Then the condition becomes $(p,pq) = 1 \Leftrightarrow (p|q) = 1 \Leftrightarrow (q|p) = -1$ and $(pq,2)(q,-1) = (p,2)(q,-2) = (-q,x)$. We consider all possible subcases:

   (a) $p \equiv 3\ (8), q \equiv 3\ (8)$. Then $(p,2)(q,-2) = (p,2) = (-q,x)$ can not occur by lemma 5.1.

   (b) $p \equiv 7\ (8), q \equiv 3\ (8)$. Then $(p,2) = (q,-2) = 1$.

   (c) $p \equiv 3\ (8), q \equiv 7\ (8)$. Since $(p,-2) = (q,2) = 1$, the condition becomes $(p,2)(q,-2) = (p,-1)(q,-1) = (pq,-1) = (-q,x)$. This is equivalent to $(-1,pqy) = (q,y) = 1$, for some $y \in \mathbb{N}$, which can occur only if $y = pqz$, (z- a natural number which does not have prime divisors of the form $4s+3$). Then $(q,pqz) = (q,-pz) = 1$ implies $(q|p) = 1$, an impossibility.

   Finally,

   (d) $p \equiv 7\ (8), q \equiv 7\ (8)$. Then $(p,2)(q,-2) = (q,-1) = (-q,x)$ can not occur.

Thus, we have obtained that for $a = p$ and $b = q$, the problem (7.1) is solvable only in the following cases :

1. $p \equiv 1\ (8), q \equiv 1,3,5\ (8)$ and $(p|q) = 1$;

2. $p \equiv 7\ (8), q \equiv 3\ (8)$ and $(p|q) = 1$.

Finally, let p and q be distinct odd primes, and let $a = p, b = pq$. Again, we must have $(p, q) = 1$, i.e., $(p|q) = 1$, and either p or q is $\equiv 1\ (4)$. Then, the condition becomes $(ab, 2)(b, b) = (q, 2)(pq, -1) = (p, -1)(q, -2) = (-pq, x)$. We consider all possible cases regarding q:

1. $q \equiv 1\ (8)$. Since $(q, 2) = 1, (p, -1)(q, -2) = (pq, -1) = (-pq, x) \Leftrightarrow pq \not\equiv 7\ (8) \Leftrightarrow p \not\equiv 7\ (8)$.

2. $q \equiv 3\ (8)$. Then $p \equiv 1\ (4)$ and $(q, -2) = (p, -1) = 1$.

3. $q \equiv 5\ (8)$. If $p \equiv 1, 7\ (8)$ then $pq \not\equiv 7\ (8)$, therefore $(pq, -1) = (-pq, y)$, for some $y \in \mathbb{Z}$. Whence, the condition $(q, 2) = (-pq, x)$ holds for $x = 2$.

   If $p \equiv 3\ (8)$ then $(p, 2) = (p, -1)$. Therefore, the condition $(p, -1)(q, -2) = (p, 2)(q, 2) = (pq, 2) = (-pq, x)$ holds for $x = 2$.

   If $p \equiv 5\ (8)$ then $(p, -1) = (q, -1) = 1$. Then the condition $(q, 2) = (-pq, x)$ holds, since it is the same as that of SD_{16} and D_{16}.

   Finally, consider

4. $q \equiv 7\ (8)$. Since $(q, 2) = 1$, the condition holds $\Leftrightarrow pq \not\equiv 7\ (8) \Leftrightarrow p \not\equiv 1\ (8)$. Since we must have $p \equiv 1\ (4)$, this means that $p \equiv 5\ (8)$.

Thus, we have obtained that for $a = p$ and $b = pq$, the problem (7.1) is solvable in either of the following cases :

1. $q \equiv 1\ (8), p \equiv 1, 3, 5\ (8)$ and $(p|q) = 1$;

2. $q \equiv 3\ (8), p \equiv 1, 5\ (8)$ and $(p|q) = 1$;

3. $q \equiv 5\ (8)$ and $(p|q) = 1$;

4. $q \equiv 7\ (8), p \equiv 5\ (8)$ and $(p|q) = 1$.

References

[Co] H. Cohn. Quaternionic compositum genus, *J. Number Theory*, **11** (1979), 399-411.

[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.

[JY] Cr. U. Jensen, Noriko Yui. Quaternion extensions, In: *Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata*, Kinokuniya, Tokyo (1987), 155-182.

[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.

[MZ1] I. Michailov, N. Ziapkov. Embedding obstructions for the generalized quaternion group, *J. Algebra*, **226** (2000), 375-389.

[MZ2] I. Michailov, N. Ziapkov. Embedding problems with Galois groups of order 16, *Mathematica Balkanica, New Ser.*, **15** (2001), Fasc. 1-2, 99-108.

[Na] T. Nagel. *Introduction to Number Theory*, John Wiley, New York (1951).

[Re] H. Reichardt. Über Normalkrper mit Quaternionengruppe, *Math. Zeit.*, **41** (1936), 218-221.

[Sa] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris (1967).

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

[Se] J.-P. Serre. *A Course in Arithmetics*, Springer-Verlag, New York (1973).

[Va] T. Vaughan. Constructing quaternionic fields, *Glasgow Math. J.* **34** (1992), 43-54.

[Wa] R. Ware. A note on the quaternion group as Galois group, *Proc. Amer. Math. Soc.* **108** (1990), 621-625.

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

Received: 06.09.2002