Serdica

Mathematical Journal

Сердика

Математическо списание

Serdica Math. J. **31** (2005), 217–228

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

QUATERNION EXTENSIONS OF ORDER 16

Ivo M. Michailov

Communicated by V. Drensky

We describe several types of Galois extensions having as Galois group the quaternion group Q_{16} of order 16.

1. Introduction.

The realization of small 2-groups as Galois groups over arbitrary field of characteristic not 2 has been an object of many papers in recent years. Most commonly among them are investigated the nonabelian groups of orders 8 and 16. The goals, which are pursued in these works, are mainly in two directions. Firstly, there is looked for the conditions (or obstructions) under which the groups are realizable. Secondly, there is looked for a description of all Galois extensions, realizing these groups. The conditions under which the groups are realizable are often expressed by the so-called *obstructions*, which are usually products of quaternion classes in the Brauer group. When the obstruction is expressed as a product of two quaternion classes, an explicit parameterization of all Galois extensions is being given. This is done in [2], [5], [6]. Since the obstruction to realizability of the quaternion group Q_{16} is a product of three

2000 *Mathematics Subject Classification:* 12F12
Key words: embedding problem, extension, Galois, quaternion
This work is partially supported by project of Shumen University

quaternion classes, such a description can not be made. That is why the Q_{16} extensions are not considered in the mentioned works. Some interesting results about realizability of Q_{16} as a Galois group over algebraic fields are obtained in [1].

Our goal is to give a description of Q_{16} extensions in specific situations. In Section 3 we give three types of Q_{16} extensions, which make use of extensions realizing other nonabelian groups of order 16. There is used the equivalence of quadratic forms. This theory is well developed in [6]. In Section 4 we give a different kind of description of Q_{16} extensions in a specific situation. Namely, we give all Q_{16} extensions that contain a given quadratic extension, which in turn, contains a primitive 8th root of unity.

2. The dihedral and quasidihedral (semidihedral) groups of order 16. We begin by giving the Galois extensions realizing the groups QD_{16} and D_{16}, as we find them in [5, 6]. By QD_{16} we denote the quasidihedral group (by Ledet's notation QD_8) generated by elements u and v, such that $u^8 = 1, v^2 = u^4$ and $vu = u^3v$. By D_{16} we denote the dihedral group (by Ledet's notation D_8) generated by elements u and v, such that $u^8 = v^2 = 1$ and $vu = u^{-1}v$.

Now, let $a, b \in k^*$ (k has characteristic $\neq 2$) be quadratically independent, i.e., a, b and ab are not in k^2. Let also $(a, ab) = 1 \in \mathrm{Br}(k)$, i.e., D_8 is realizable. Then there exist $\alpha, \beta \in k^*$, such that $\alpha^2 - a\beta^2 = ab$, hence all D_8 extensions are $\{k(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b})/k,\ r \in k^*\}$. Denote

$$\varphi = \sqrt{r(\alpha + \beta\sqrt{a})} \text{ and } \psi = \sqrt{r(\alpha - \beta\sqrt{a})} = \frac{\alpha - \beta\sqrt{a}}{\sqrt{ab}}\varphi,$$

so D_8 is generated by the elements σ and τ, such that

$$\sigma : \varphi \mapsto \psi, \sqrt{b} \mapsto \sqrt{b}; \quad \tau : \varphi \mapsto \varphi, \sqrt{b} \mapsto -\sqrt{b}.$$

Note also that we have

$$\sigma : \psi \mapsto -\varphi, \quad \tau : \psi \mapsto -\psi.$$

From [6], we have the following theorems describing the QD_{16} and D_{16} extensions:

Theorem 2.1. *Let $\alpha \neq 0$. The embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension*

$$1 \to \mu_2 \to QD_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.1}$$

is solvable if and only if the quadratic forms $\langle b, 2r\alpha, 2br\alpha\rangle$ *and* $\langle a, 2, 2a\rangle$ *are equivalent over* k*. If this equivalence is expressed by the matrix* $\mathbf{P}$*:*

$$\mathbf{P}^t\langle b, 2r\alpha, 2br\alpha\rangle\mathbf{P} = \langle a, 2, 2a\rangle,$$

we can assume $\det \mathbf{P} = a/br\alpha$ *and get the solutions*

$$K(\sqrt{s\omega_{QD}})/k = k(\sqrt{s\omega_{QD}}, \sqrt{b})/k, \quad s \in k^*,$$

where

$$\omega_{QD} = 1 + p_{11}\sqrt{b}/\sqrt{a} + \frac{1}{2}(p_{22} + p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a})\varphi$$
$$+ \frac{1}{2}(p_{22} - p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a})\psi.$$

Theorem 2.2. *Let* $\alpha \neq 0$*. The embedding problem given by* $K/k = k(\varphi, \sqrt{b})/k$ *and the group extension*

$$1 \to \mu_2 \to D_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.2}$$

is solvable if and only if the quadratic forms $\langle b, r\alpha, br\alpha\rangle$ *and* $\langle ab, 2b, 2a\rangle$ *are equivalent over* k*. If this equivalence is expressed by the matrix* $\mathbf{P}$*:*

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2b, 2a\rangle,$$

we can assume $\det \mathbf{P} = 2a/r\alpha$ *and get the solutions*

$$K(\sqrt{s\omega_D})/k = k(\sqrt{s\omega_D}, \sqrt{b})/k, \quad s \in k^*,$$

where

$$\omega_D = 1 - p_{11}/\sqrt{a} + \frac{1}{2}(p_{32} + p_{23}/\sqrt{a})\varphi + \frac{1}{2}(p_{22}/\sqrt{b} - p_{33}\sqrt{b}/\sqrt{a})\psi.$$

The obstructions to the embedding problems given by (2.1) and (2.2) are, respectively, $(-b, -2r\alpha)(-a, -2) \in Br(k)$ and $(-ab, -2a)(-b, -r\alpha)$. In the special case $b = -1$ we can assume that all D_8 extensions are $k(\sqrt[4]{a}, i)/k$ and the action of the generators of D_8 is

$$\sigma : \sqrt[4]{a} \mapsto \sqrt[4]{a}i, \sigma : i \mapsto i; \quad \tau : \sqrt[4]{a} \mapsto \sqrt[4]{a}, \tau : i \mapsto -i.$$

Theorem 2.3. *The embedding problem given by $K/k = k(\sqrt[4]{a}, i)/k$, with Galois group D_8, and the group extension*

$$1 \to \mu_2 \to QD_{16} \underset{\substack{u\mapsto\sigma\\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.1}$$

is solvable if and only if

$$\exists p, q \in k : p^2 + aq^2 = -2.$$

The solutions are:

$$K(\sqrt{r\omega_{QD}})/k = k(\sqrt{r\omega_{QD}}, i)/k, \quad r \in k^*,$$

where $\omega_{QD} = (1+i)(p+qi\sqrt{a})\sqrt[4]{a}$.

Theorem 2.4. *The embedding problem given by $K/k = k(\sqrt[4]{a}, i)/k$, with Galois group D_8, and the group extension*

$$1 \to \mu_2 \to D_{16} \underset{\substack{u\mapsto\sigma\\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.2}$$

is solvable if and only if

$$\exists p, q \in k : p^2 - aq^2 = 2.$$

The solutions are:

$$K(\sqrt{r\omega_D})/k = k(\sqrt{r\omega_D}, i)/k, \quad r \in k^*,$$

where $\omega_D = (p+q\sqrt{a})\sqrt[4]{a}$.

Now, we turn our attention to the semidihedral group SD_{16}, generated by elements u and v, such that $u^8 = v^2 = 1$ and $vu = u^3v$. The group SD_{16} is in fact isomorphic to the group QD_{16}, but it has different obstruction, hence different parameterization of the solutions. The obstruction to embedding the D_8 extension into an SD_{16} extension is $(a,-2)(-b,2r\alpha) = (-ab,-2)(-b,-r\alpha) \in \mathrm{Br}(k)$, as is shown in [4, 7]. Whence, given $\alpha \neq 0$, the embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension

$$1 \to \mu_2 \to SD_{16} \underset{\substack{u\mapsto\sigma\\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.3}$$

is solvable if and only if $\langle b, r\alpha, br\alpha\rangle$ is equivalent to $\langle ab, 2, 2ab\rangle$ over k. Let this equivalence be expressed by the matrix $\mathbf{P}$:

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2, 2ab\rangle,$$

and assume det $\mathbf{P} = 2a/r\alpha$. With similar argument as to the group D_{16} given in [6] we define the matrix $\mathbf{P}'$:

$$\mathbf{P}' = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2 & -1/2 \end{pmatrix} \langle\sqrt{b}, 1, \sqrt{b}\rangle \mathbf{P} \langle 1/\sqrt{b}, 1, 1/\sqrt{b}\rangle.$$

We can assume det $\mathbf{P}' = a/r\alpha$ and denote $\alpha' = \alpha/\sqrt{b}, \beta' = \beta/\sqrt{b}$. Now we put

$$\begin{aligned}\omega = 1 + p'_{11}/\sqrt{a} + \frac{1}{2}[(p'_{22} - p'_{32}) + (p'_{23} + p'_{33})/\sqrt{a}]\varphi \\ + \frac{1}{2}[(p'_{22} + p'_{32}) - (p'_{23} - p'_{33})/\sqrt{a}]\frac{\alpha' - \beta'\sqrt{a}}{\sqrt{a}}\varphi,\end{aligned}$$

where p'_{ij}s are the entries of the matrix $\mathbf{P}'$. Then

$$\omega = 1 - p_{11}/\sqrt{a} + \frac{1}{2}[\sqrt{b}p_{32} + p_{23}/\sqrt{ab}]\varphi + \frac{1}{2}[p_{22} - p_{33}/\sqrt{a}]\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}\sqrt{b}}\varphi,$$

whence $K(\sqrt{\omega})/k(\sqrt{b})$ is a C_8 extension. Now we may put

$$\omega_{SD} = \sigma\omega = 1 + p_{11}/\sqrt{a} + \frac{1}{2}(p_{32}\sqrt{b} - p_{23}/\sqrt{ab})\psi - \frac{1}{2}[p_{22} + p_{33}/\sqrt{a}]\varphi.$$

Then we have $\tau\omega_{SD} = \omega_{SD}$, so $K(\sqrt{\omega_{SD}})/k$ is Galois, and since the preimage of $\tau\sigma$ in the Galois group is of order 4, the Galois group is SD_{16}. Thus we have:

Theorem 2.5. *Let $\alpha \neq 0$. The embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension*

$$1 \to \mu_2 \to SD_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \to 1 \tag{2.3}$$

is solvable if and only if the quadratic forms $\langle b, r\alpha, br\alpha\rangle$ and $\langle ab, 2, 2ab\rangle$ are equivalent over k. If this equivalence is expressed by the matrix $\mathbf{P}$:

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2, 2ab\rangle,$$

we can assume det $\mathbf{P} = 2a/r\alpha$ *and get the solutions*

$$K(\sqrt{s\omega_{SD}})/k = k(\sqrt{s\omega_{SD}}, \sqrt{b})/k, \quad s \in k^*,$$

where ω_{SD} is as above.

For $b = -1$ we have:

Theorem 2.6. *The embedding problem given by $K/k = k(\sqrt[4]{a}, i)/k$, with Galois group D_8, and the group extension*

$$1 \to \mu_2 \to SD_{16} \underset{\substack{u \mapsto \sigma \\ v \mapsto \tau}}{\longrightarrow} D_8 \to 1 \tag{2.3}$$

is solvable if and only if

$$\exists p, q \in k : p^2 - aq^2 = -2.$$

The solutions are:

$$K(\sqrt{r\omega_{SD}})/k = k(\sqrt{r\omega_{SD}}, i)/k, \quad r \in k^*,$$

where $\omega_{SD} = (p + q\sqrt{a})\sqrt[4]{a}$.

3. The quaternion group of order 16. In this section we give three types of Galois extensions having the group Q_{16} as Galois group which are obtained easily by the dihedral, quasidihedral and semidihedral Galois extensions described in the previous section. Let the quaternion group Q_{16} be generated by elements u and v, such that $u^8 = 1, v^2 = u^4$ and $vu = u^{-1}v$. Then the embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension

$$1 \to \mu_2 \to Q_{16} \underset{\substack{u \mapsto \sigma \\ v \mapsto \tau}}{\longrightarrow} D_8 \to 1 \tag{3.1}$$

is solvable if and only if $(ab, 2)(b, -1)(-b, r\alpha) = 1 \in \mathrm{Br}(k)$ (see [4]).

We will consider three special cases, where one of the elements a, b, ab is a sum of two squares. We use this simple argument: If a group G is of exponent 8, and

$$1 \to \mu_2 \to G \underset{\substack{u \mapsto \sigma \\ v \mapsto \tau}}{\longrightarrow} D_8 \to 1$$

is a non-split group extension, then G is isomorphic to one of the groups QD_{16} (SD_{16}), D_{16} or Q_{16}. Moreover, the group G is determined uniquely by the orders of the pre-images u, v, uv of the generators $\sigma, \tau, \sigma\tau \in D_8$.

Proposition 3.1. *Let $(a, -1) = 1 \in \mathrm{Br}(k)$, i.e., $\exists x, y \in k$ such that $a = x^2 - ay^2$. Then all the solutions of the embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension* (3.1) *are*

$$K\left(\sqrt{s(x + y\sqrt{a})\omega_{QD}}\right) \Big/ k = k\left(\sqrt{s(x + y\sqrt{a})\omega_{QD}}, \sqrt{b}\right) \Big/ k, \quad s \in k^*,$$

where ω_{QD} is as in theorems 2.1 *or* 2.3.

Proof. The obstruction is

$$(ab,2)(b,-1)(-b,r\alpha)=(ab,-2)(ab,-1)(b,-1)(-b,r\alpha)=(ab,-2)(-b,r\alpha)\in\mathrm{Br}(k),$$

which is exactly the obstruction to realizability of QD_{16}. Now, let $(ab,-2)(-b,r\alpha) = 1 \in \mathrm{Br}(k)$ and ω_{QD} give the QD_{16} extension. Then $\sigma\tau\omega_{QD} = \omega_{QD}$, and we put $\omega_Q = (x + y\sqrt{a})\omega_{QD}$. We have $\sigma\tau\omega_Q = a^2_{\sigma\tau}\omega_Q$, where

$$a_{\sigma\tau} = \frac{\sqrt{a}}{x + y\sqrt{a}}.$$

Thus $K(\sqrt{\omega_Q})/k$ is Galois and the pre-images of $\sigma\tau$ and τ in the Galois group G are of order 4, since $a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = -1$. Hence $K(\sqrt{s\omega_Q})/k$ is Q_{16} extension. □

Proposition 3.2. *Let $(b,-1) = 1 \in \mathrm{Br}(k)$, i.e., $\exists x, y \in k$ such that $b = x^2 - by^2$. Then all the solutions of the embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension* (3.1) *are*

$$K\left(\sqrt{s(x + y\sqrt{b})\omega_D}\right)\Big/k = k\left(\sqrt{s(x + y\sqrt{b})\omega_D}, \sqrt{b}\right)\Big/k, \quad s \in k^*,$$

where ω_D is as in theorems 2.2 *or* 2.4.

Proof. The obstruction is $(ab,2)(b,-1)(-b,r\alpha) = (ab,2)(-b,r\alpha) \in \mathrm{Br}(k)$, which is exactly the obstruction to realizability of D_{16}. Now, let $(ab,2)(-b,r\alpha) = 1 \in \mathrm{Br}(k)$ and ω_D give the D_{16} extension. Here $\tau\omega_D = \omega_D, \sigma\tau\omega_D = a^2_{\sigma\tau}\omega_D$; the pre-images of τ and σ in D_{16} are of order 2, and we put $\omega_Q = (x + y\sqrt{b})\omega_D$. Now we have $\tau\omega_Q = a^2_\tau\omega_Q$ and $\sigma\tau\omega_Q = a'^2_{\sigma\tau}\omega_Q$, where

$$a_\tau = \frac{\sqrt{b}}{x + y\sqrt{b}}, \quad a'_{\sigma\tau} = a_\tau a_{\sigma\tau}.$$

From $a_\tau\tau a_\tau = -1, a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = 1$ we get $a'_{\sigma\tau}\sigma\tau a'_{\sigma\tau} = a_\tau\tau a_\tau a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = -1$, so the pre-images of τ and $\sigma\tau$ in G are of order 4. Thus $K(\sqrt{s\omega_Q})/k$ is Galois Q_{16} extension. □

Proposition 3.3. *Let $(ab,-1) = 1 \in \mathrm{Br}(k)$, i.e., $\exists x, y \in k$ such that $ab = x^2 - aby^2$. Then all the solutions of the embedding problem given by $K/k = k(\varphi, \sqrt{b})/k$ and the group extension* (3.1) *are*

$$K\left(\sqrt{s(x + y\sqrt{ab})\omega_{SD}}\right)\Big/k = k\left(\sqrt{s(x + y\sqrt{ab})\omega_{SD}}, \sqrt{b}\right)\Big/k, \quad s \in k^*,$$

where ω_{SD} is as in theorems 2.5 *or* 2.6.

Proof. The obstruction is

$$(-ab,-2)(ab,-1)(-1,-2)(b,-1)(-b,r\alpha)=(-ab,-2)(-b,-r\alpha)\in \mathrm{Br}(k),$$

which is exactly the obstruction to realizability of SD_{16}. Now, $(-ab,-2)(-b,-r\alpha) = 1 \in \mathrm{Br}(k)$ and ω_{SD} give the SD_{16} extension. Here $\tau\omega_{SD}=\omega_{SD}, \sigma\tau\omega_{SD}= a_{\sigma\tau}^2\omega_{SD}$; the pre-image of τ is of order 2 and the pre-image of $\sigma\tau$ is of order 4 (in SD_{16}), and we put $\omega_Q=(x+y\sqrt{ab})\omega_{SD}$. Now we have $\tau\omega_Q=a_\tau^2\omega_Q$ and $\sigma\tau\omega_Q=a_{\sigma\tau}^2\omega_Q$, where

$$a_\tau=\frac{\sqrt{ab}}{x+y\sqrt{ab}}.$$

From $a_\tau\tau a_\tau=-1$ and $a_{\sigma\tau}\sigma\tau a_{\sigma\tau}=-1$ we get that the pre-images of τ and $\sigma\tau$ in G are of order 4. Thus $K(\sqrt{s\omega_Q})/k$ is Galois Q_{16} extension. □

4. Quaternion extensions over quadratic extensions that contain a primitive 8th root of unity.

Let $b\in k^*\setminus(k^*)^2$, let $L=k(\sqrt{b})$ and let L contain a primitive 8th root of unity ζ. Our goal is to describe all Galois extensions M/k, which are solutions to the embedding problem given by L/k and the group extension

$$1\to C_8=\langle u\rangle\to Q_{16}\to C_2\cong \mathrm{Gal}(L/k)\to 1, \tag{4.1}$$

where Q_{16} is generated by u and v the same way as in Section 3.

Now, assume M is cyclic over L of degree 8. Then $M=L(\omega^{1/8})$ by Kummer theory. If $\mathrm{Gal}(L/k)=\{1,v\}$, then M is Galois over k if and only if $v(\omega)=\omega^t\beta^8$, where $\beta\in L^*$ and $t^2\equiv 1 \pmod 8$. So, we must give a detailed description of the element ω.

If G is a group of order 16, which contains a cyclic subgroup $\langle u\rangle$ of order 8, then G is generated by elements u and v such that

1. $|u|=8,\ v\notin\langle u\rangle$;
2. $vuv^{-1}=u^j,\ v^2=u^l$;
3. $j^2\equiv 1 \pmod 8),\ l(j-1)\equiv 0 \pmod 8)$.

It is known that $G\cong Q_{16}$ if and only if $j\equiv -1$ and $l\equiv 4 \pmod 8$. Since $\zeta\in L$, we have $v(\zeta)=\zeta^r$, where r is an integer, such that $\gcd(r,8)=1$, i.e., r is odd. Assume $\zeta=\dfrac{\sqrt{2}}{2}(1+i)$, where $i=\sqrt{-1}$. Then we have the following four cases:

1. $r \equiv 1$, i.e., $\zeta \in k$;

2. $r \equiv -1$, i.e., $\sqrt{2} \in k$ and $b =_2 -1$;

3. $r \equiv 5$, i.e., $i \in k$ and $b =_2 2$;

4. $r \equiv -5$, i.e., $\sqrt{-2} \in k$ and $b =_2 -1 =_2 2$.

The embedding problem given by $L/k = k(\sqrt{b})/k$ and the group extension (4.1) is solvable if and only if there exists $a \in k$, such that a and b are quadratically independent over k, $(a, ab) = 1 \in Br(k)$ and $(ab, 2)(b, b)(-b, x) = 1 \in Br(k)$, for some $x \in k$ (see [8]). We denote by N the norm map $N_{L/k} : L \to k$. Now, consider the four cases, described above.

If $r \equiv 1$, i.e., $\zeta \in k$, then the embedding problem given by L/k and (4.1) is solvable if and only if there exists a, such that $(a, b) = 1$, i.e., $\exists \gamma \in L$, such that $a = N(\gamma)$ and b are quadratically independent. The description of all Q_{16} extensions is given in Theorem 4.5.

If $r \equiv -1$, i.e., $\sqrt{2} \in k$ and $b =_2 -1$, then the embedding problem is solvable if and only if there exists a, such that a and -1 are quadratically independent and $(-1, -1) = 1$, i.e., $-1 = N(\gamma)$ for some $\gamma \in L$. The description of all Q_{16} extensions is given in Theorem 4.6.

If $r \equiv 5$, i.e., $i \in k$ and $b =_2 2$, then the embedding problem is solvable if and only if there exists a, such that $(a, 2) = 1$ and also $a = N(\gamma)$ and 2 are quadratically independent. The description of all Q_{16} extensions is given in Theorem 4.7.

If $r \equiv -5$, i.e., $\sqrt{-2} \in k$ and $b =_2 -1 =_2 2$, then the embedding problem is solvable if and only if there exists a, such that $(a, 2) = 1$ and $a = N(\gamma)$ and 2 are quadratically independent. The description of all Q_{16} extensions is given in Theorem 4.8.

Now, we will write down several lemmas, which are particular cases of results obtained in [3].

Lemma 4.1. *If $\delta, \delta' \in L^*$ and $v(\delta)/\delta = v(\delta')/\delta'$, then $\delta' = d\delta$, with $d \in k$.*

Lemma 4.2. *Assume $\zeta = \dfrac{\sqrt{2}}{2}(1 + i) \in L$. Let $M = L(\sqrt[8]{\omega})$, where $\omega \in L$ and assume $[M : L] = 8$. Then M/k realizes Q_{16} as Galois group if and only if $v(\omega) = \omega^t \beta^8$, with $t \equiv -r \pmod 8$ and $\omega^{(t^2-1)/8}\beta^t v(\beta) = \zeta^{l_1}$, where $l_1 \equiv 4 \pmod 8$.*

Lemma 4.3. *If $b \notin -k^2$ (i.e., $L = k(\sqrt{b}) \neq k(i)$), then $k \cap L^8 = k^8 \cup b^4 k^8$ and $k \cap L^4 = k^4 \cup b^2 k^4$.*

Lemma 4.4. *$L \neq k(i)$ (i.e., $i \in k$) if and only if $r \equiv 1 \pmod 4$; $\zeta \in k$ if and only if $r \equiv 1 \pmod 8$.*

With the help of these lemmas we will prove the following theorems.

Theorem 4.5. *Let $L = k(\sqrt{b}), \omega \in L$ and let $\zeta \in k$. Then $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension if and only if $\omega = (c\sqrt{b})^4 N(\gamma)/\gamma^2$, where $c \in k^*, \gamma \in L^*$ and $N(\gamma) \notin k^2 \cup bk^2$.*

Proof. Assume that ω is given by the formula in the statement of this theorem. Then $\sqrt{\omega} = \pm c^2 b \sqrt{N(\gamma)}/\gamma$. Since $a = N(\gamma)$ and b are quadratically independent, we have $[L(\sqrt{\omega}) : L] = 2, L(\sqrt{\omega}) = k(\sqrt{a}, \sqrt{b})$ – a biquadratic extension over k and $[M : L] = 8$. Furthermore, $N(\omega) = (c\sqrt{b})^8 = \delta^8$, where $\delta = c\sqrt{b} \in L^*$. Therefore $v(\omega) = \omega^{-1}\delta^8$, hence M/k is Galois and $t = -1$. Also, $\rho = \omega^{(t^2-1)/8}\delta^t v(\delta) = v(\delta)/\delta = -1 = \zeta^{l_1}$, so $l_1 \equiv 4$ and M/k is a Q_{16} extension.

Now, assume that $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension. Then $t = -1$ and $N(\omega) = \delta^8$ for $\delta \in L^*$. From Lemma 4.3 follows that $\delta^8 \in k \cap L^8 = k^8 \cup b^4k^8$. If $\delta^8 \in k^8$, then $\delta \in k$, since $\zeta \in k$. In this case, $\rho = v(\delta)/\delta = 1 = \zeta^{l_1}$, whence $l_1 \equiv 0$, so M/k is not a Q_{16} extension, a contradiction. Therefore, $\delta^8 \in b^4k^8$, i.e., $\delta = c\sqrt{b}, c \in k^*$. Then $\rho = v(\delta)/\delta = -1$, so $l_1 \equiv 4$. Furthermore, $(\omega/\delta^4)v(\omega/\delta^4) = N(\omega)/\delta^8 = 1$ and Hilbert's Theorem 90 implies $\omega/\delta^4 = v(\gamma)/\gamma$, for some $\gamma \in L^*$. Whence $\omega = \delta^4 v(\gamma)/\gamma = (c\sqrt{b})^4 N(\gamma)/\gamma^2$. Now, assume $u(\sqrt[8]{\omega}) = \sqrt[8]{\omega}\zeta$. Then $\sqrt{\omega}$ is contained in the fixed field of u^2, which must be a biquadratic extension over k. Therefore, $a = N(\gamma)$ and b are quadratically independent. □

Theorem 4.6. *Let $\sqrt{2} \in k, L = k(i)$ and let $\omega \in L^*$. Then $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension if and only if*

$$\omega = \begin{cases} c_1 i, & \text{if } c_1 \in k, -1 = \alpha^8, N(\alpha) = -1, \text{ and } c_1 \notin k^2 \cup -k^2; \\ c_2(1+\gamma^8), & \text{if } c_2 \in k, N(\gamma) = -1, 1+\gamma^8 = d\delta^2, d \in k^*, \delta \in L^*, \text{ and} \\ & c_2 d \notin k^2 \cup -k^2. \end{cases}$$

Proof. Assume that ω is given by the formula in the statement of this theorem. If $\omega = c_1 i$, then $\sqrt{\omega} = \pm\sqrt{c_1\alpha^4} = \pm\sqrt{c_1}\alpha^2$. Whence $L(\sqrt{\omega}) = k(\sqrt{c_1}, \sqrt{b})$ is biquadratic over k and $[M : L] = 8$. Furthermore, $v(\omega) = -\omega = \omega\alpha^8$, so $t = 1$ and $r \equiv -1$. Also, $\rho = \alpha v(\alpha) = N(\alpha) = -1 = \zeta^{l_1}$, so $l_1 \equiv 4$ and M/k is a Q_{16} extension. If $\omega = c_2(1+\gamma^8)$, then $\sqrt{\omega} = \pm\sqrt{c_2 d}\delta$. Whence $[M : L] = 8$. Furthermore, $v(\omega) = c_2(1 + v(\gamma^8)) = \omega\beta^8$, where $\beta = v(\gamma)$. Since $N(\beta) = N(\gamma) = -1 = \zeta^{l_1}$, M/k is a Q_{16} extension.

Now, let M/k be a Q_{16} extension. If $v(\omega) = -\omega$, then $\omega = c_1 i, c_1 \in k$. Since $r \equiv -1$, we have $t = 1$, i.e., $v(\omega) = \omega\alpha^8, \alpha \in L^*$, so $\alpha^8 = -1$. Also,

$\rho = \alpha v(\alpha) = N(\alpha) = -1 = \zeta^4$, since $l_1 \equiv 4$. Furthermore, the fixed field of u^2 is biquadratic over k, so $u^2(\sqrt{\omega}) = \sqrt{\omega} = \pm\sqrt{c_1}\alpha^2$. Whence c_1 and -1 are quadratically independent, i.e., $k(\sqrt{c_1}, i)/k$ is a biquadratic extension. If $v(\omega) \neq -\omega$, then $v(\omega)/\omega = \beta^8 \neq -1$, therefore $1 + v(\beta^8) \neq 0$. From $N(\beta^8) = 1$, follows that

$$v(\omega)/\omega = \beta^8 = \frac{1+\beta^8}{1+v(\beta^8)} = \frac{v(1+v(\beta^8))}{1+v(\beta^8)},$$

and Lemma 4.1 implies that $\omega = c_2(1+\gamma^8)$, where $\gamma = v(\beta)$ and $N(\gamma^8) = 1$. Now, from $\rho = N(\beta) = -1$ follows that $N(\gamma) = -1$. Since the fixed field of u^2 must be biquadratic over k, we have that $1+\gamma^8 = d\delta^2$, where $d \in k^*$ and $\delta \in L^*$. We have then $\sqrt{\omega} = \pm\sqrt{c_2 d}\delta$, so $c_2 d$ and -1 must be quadratically independent over k. □

Theorem 4.7. *Let $i \in k, L = k(\sqrt{2})$ and let $\omega \in L^*$. Then $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension if and only if $\omega = c^3/\gamma^2$, where $c \in k^*, \gamma \in L^*, N(\gamma) = -c$ and $c \notin k^2 \cup 2k^2$.*

Proof. Assume that ω is given by the formula in the statement of this theorem. From $c \notin k^2 \cup 2k^2$ follows that $L(\sqrt{\omega}) = k(\sqrt{c}, \sqrt{2})$ is biquadratic over k and $[M : L] = 8$. Furthermore, $v(\omega)/\omega^3 = \gamma^8/c^6 N(\gamma^2) = \beta^8$, where $\beta = \gamma/c$. Therefore $t = 3$ and $(t^2-1)/8 = 1$, so $\rho = \omega\beta^3 v(\beta) = N(\gamma)/c = -1 = \zeta^{l_1}$. Thus M/k is a Q_{16} extension.

Now, assume that $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension. Then $v(\omega) = \omega^3\beta^8, \beta \in L^*$, hence $N(\omega) = (\omega\beta^2)^4 \in L^4 \cap k$. Then Lemma 4.3 implies that $L^4 \cap k = k^4 \cup 4k^4$, whence $\omega\beta^2 = c$ or $\omega\beta^2 = \sqrt{2}c$ for $c \in k$. We have that $N(\omega) \in k^2$. On the other hand, if $\omega\beta^2 = \sqrt{2}c$, then $N(\omega\beta^2) = -2c^2 \in -2k^2 = 2k^2 \neq k^2$, a contradiction. Thus the only possibility that remains is $\omega\beta^2 = c$. Let $\gamma = c\beta$. Then $\omega = c/\beta^2 = c^3/\gamma^2$ and $N(\gamma^2) = c^4 N(c/\omega) = c^2$, i.e., $N(\gamma) = \pm c$. If $N(\gamma) = c$, then $\rho = \omega\beta^3 v(\beta) = N(\gamma)/c = 1 = \zeta^{l_1}$, so $l_1 \equiv 0$, a contradiction. Thus remains that $N(\gamma) = -c$. Also, c and 2 must be quadratically independent over k, since $[M : L] = 8$. □

Theorem 4.8. *Let $\sqrt{-2} \in k, L = k(\sqrt{i})$ and let $\omega \in L^*$. Then $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension if and only if $\omega = N(\gamma)\eta^2/\gamma^4$, where $\eta \in ik, \gamma \in L^*$ and $N(\gamma) \notin k^2 \cup -k^2$.*

Proof. Assume that ω is given by the formula in the statement of this theorem. From $N(\gamma) \notin k^2 \cup -k^2$ follows that $L(\sqrt{\omega})$ is biquadratic over k and $[M : L] = 8$. Since $r \equiv 3$, we must show that $t = 5$ and $l_1 \equiv 4$. Indeed, $v(\omega)/\omega^4 = \omega\beta^8$, where $\beta = \gamma^2/v(\gamma)\eta$. Also, $\rho = \omega^3\beta^5 v(\beta) = \eta/v(\eta) = -1$, so $l_1 \equiv 4$. Therefore, $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension.

Now, assume that $M/k = L(\sqrt[8]{\omega})/k$ is a Q_{16} extension. Then $v(\omega) = \omega^5\beta^8$, where $\beta \in L^*$ and $l_1 \equiv 4$. Hence $v(\omega)/\omega = (\omega\beta^2)^4$. Let $\alpha = N(\omega\beta^2) \in k$.

Then $\alpha^4 = N((\omega\beta^2)^4) = N(v(\omega)/\omega) = 1$. Therefore, $\alpha^2 = \pm 1$. If $\alpha^2 = -1$, then $\alpha = \pm i \in k$, a contradiction. Then $\alpha^2 = 1$, so $\alpha = \pm 1$. Let $\delta = \omega\beta^2$. If $N(\delta) = 1$, we have $\delta = \gamma/v(\gamma)$, for some $\gamma \in L^*$. Therefore, $\omega = \gamma/v(\gamma)\beta^2 = N(\gamma)\eta^2/\gamma^4$, where $\eta = \gamma^2/v(\gamma)\beta$. Also, $\rho = \omega^3\beta^5 v(\beta) = \eta/v(\eta) = \zeta^4 = -1$, so $v(\eta) = -\eta$, i.e., $\eta \in ik$. If $\alpha = -1$, i.e., $N(\delta) = -1$, then $v(\omega\delta^2) = \omega\delta^4 v(\delta^2) = \omega\delta^2$, i.e., $\omega\delta^2 \in k$. Therefore, $N(\omega\delta^2) \in k^2$ and $N(\omega) \in k^2$. But then $-1 = N(\omega\beta^2) = N(\delta) \in k^2$, a contradiction. Thus we have $\omega = N(\gamma)\eta^2/\gamma^4$, where $\eta \in ik$. Finally, since $k(\sqrt{\omega}, i)/k$ must be a biquadratic extension, we have that $a = N(\gamma)$ and -1 must be quadratically independent over k. □

REFERENCES

[1] P. Damey. Extensions quaternioniennes d'un corps de nombres. *Mem. Soc. Math. Fr.*, tome **37** (1974), 35–38.

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

[3] Y.-S. Hwang, D. B. Leep, A. R. Wadsworth. Galois groups of order $2n$ that contain a cyclic subgroup of order n. Available at `http://arxiv.org/find/math`.

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

[5] A. Ledet. Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16. *Proc. Amer. Math. Soc.* **128** (2000), 2213–2222.

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

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

[8] I. Michailov, N. Ziapkov. Embedding problems with Galois groups of order 16. *Math. Balkanica (N.S.)* **15**, *1–2* (2001), 99–108.

Faculty of Mathematics, Informatics and Economics
Constantin Preslavski University
9700 Shumen, Bulgaria
e-mail ivo_michailov@yahoo.com

Received January 28, 2005