Journal of Algebra **226,** 375–389 (2000)
doi:10.1006/jabr.1999.8190, available online at http://www.idealibrary.com on IDEAL®

Embedding Obstructions for the Generalized Quaternion Group

Ivo M. Michailov and Nikola P. Ziapkov

Faculty of Mathematics, Informatics and Economics, Constantin Preslavski University, 9700 Shoumen, Bulgaria
E-mail: n.ziapkov@shu-bg.net

Communicated by Walter Feit

Received May 7, 1999

In this paper, we examine the obstructions to the solvability of certain embedding problems with the generalized quaternion group over arbitrary fields of characteristic not 2. First we consider the Galois embedding problem with abelian kernel in cohomological terms. Then we proceed with a number of examples in order to illustrate the role of the properties of the base field on the solvability of the embedding problem. © 2000 Academic Press

1. INTRODUCTION

Let K/k be a finite Galois extension of fields with Galois group F and let

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

be an extension of finite groups. The corresponding embedding problem $(K/k, G, A)$ then consists of determining whether or not there exists a Galois algebra L over the field k containing K in such a way that $G \cong \mathrm{Gal}(L/k)$ and the homomorphism of restriction to K of the automorphisms from G coincides with α. For abuse of notation we also call $(*)$ the embedding problem.

However, the classical formulation of the embedding problem is for Galois extensions as solutions. It is clear that a necessary condition (we call it an obstruction) for the solvability of $(*)$ in terms of Galois algebras is also a necessary condition (an obstruction) for the solvability of $(*)$ in terms of Galois extensions. Such a necessary condition is the compatibility condition found by D. K. Faddeev and H. Hasse.

0021-8693/00 $35.00
Copyright © 2000 by Academic Press
All rights of reproduction in any form reserved.

We give one of its many forms. Namely, let $G \times K$ be the crossed product algebra of the group G and the field K. We say that the group G is compatible with K or the compatibility condition holds for the embedding problem $(*)$ if and only if $G \times K$ is isomorphic to the matrix algebra of order $|F|$ over a subalgebra (see [ILF, II, Sections 1 and 2]).

If the field k has a characteristic $p > 0$, A is a p-group; then the problem $(*)$ is always solvable by [ILF, Theorem 3.10], and the solvability of $(*)$ in terms of Galois extensions depends only on the rank of the groups involved by the famous Witt's result [Wi].

Therefore, we will assume the group A, which is called the kernel of the embedding problem $(*)$, to be abelian of order relatively prime to the characteristic of the base field k. Then the existence of a solution of $(*)$ in terms of Galois algebras is a purely cohomological problem and we give cohomological interpretation of the embedding obstructions to the associated problems. We also give examples with the generalized quanternion group.

In Sections 6 and 7 we consider the quaternion groups Q_8 and Q_{16}, dealing only with Galois extensions of fields with characteristic not 2.

The obstructions to the realizability of groups of order a power of 2 as well as explicit solutions and additional results can be found in [GSS, GS, Ki, Le1]. It is known that the realizability of these groups over k is linked to the splitting of certain products of quaternion algebras in $\mathrm{Br}(k)$.

We will denote by $(a, b/k)$, $a, b \in k^*$, the quaternion algebra generated over k by two anticommuting elements i and j such that $i^2 = a$, $j^2 = b$ and by (a, b) the equivalence class of $(a, b/k)$ in the Brauer group $\mathrm{Br}(k)$. We say that $(a, b/k)$ splits if and only if $(a, b/k) \cong \mathrm{Mat}_2 k$—the matrix algebra; i.e., $(a, b) = 1 \in \mathrm{Br}(k)$. The following two well-known facts about quaternion algebras are often useful.

PROPOSITION 1.1. *Let $a, b, c, d \in k^*$. Then*

(1) $(a, b) = 1 \in \mathrm{Br}(k) \Leftrightarrow \exists x, y \in k$: $a = x^2 - by^2$

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

All necessary results about the Brauer group and quaternion algebras can be found in [La].

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.

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

Obviously, a is rigid if and only if there exists $b \in k^* \setminus k^{*2}$ such that a and b are independent mod k^{*2} and $(a, -b) = 1 \in \mathrm{Br}(k)$.

We denote by $C_n = \langle \rho | \rho^n = 1 \rangle$ the cyclic group of order n, and $C_2^2 = C_2 \times C_2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k)$. 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 $\sqrt{a}^{\rho_1} = -\sqrt{a}$, $\sqrt{b}^{\rho_1} = \sqrt{b}$; $\sqrt{a}^{\rho_2} = \sqrt{a}$, $\sqrt{b}^{\rho_2} = -\sqrt{b}$.

2. THE EMBEDDING PROBLEM WITH ABELIAN KERNEL

Let the problem $(K/k, G, A)$ with abelian kernel be given. For our purposes we follow the approach to the description of embedding conditions given in [ILF, III, Section 13]. Let $\bar{k}$ be the algebraic separable closure of k with profinite Galois group $\bar{F}$. Then we have the group extension $1 \to R \to \bar{F} \to F \to 1$ and the lifting homomorphism λ: $H^2(F, A) \to H^2(\bar{F}, A)$. We denote by c the cohomology class from $H^2(F, A)$ corresponding to the extension $1 \to A \to G \to F \to 1$, and put $\bar{c} = \lambda c$.

THEOREM 2.1 ([ILF, Theorem 3.13.2]). *The embedding problem* $(K/k, G, A)$ *is solvable if and only if* $\bar{c} = 0$.

Let the field K contain a primitive root of unity of degree equal to the order of the kernel A. Then we can define the character group $\hat{A} = \mathrm{Hom}(A, K^*)$ and make it an F-module by $\chi^{\rho}(a) = \chi(a^{\rho})^{\rho^{-1}}$, for $\chi \in \hat{A}$, $a \in A$, $\rho \in F$. Everywhere we mention the character group we will assume that K contains the necessary roots of unity. Let $\mathbf{Z}[\hat{A}]$ be a free abelian group with generators e_{χ} which we make an F-module by the setting $e_{\chi}^{\rho} = e_{\chi^{\rho}}$. Then there is an exact sequence of F-modules

$$0 \to V \to \mathbf{Z}[\hat{A}] \to \hat{A} \to 0;$$

here the epimorphism $\mathbf{Z}[\hat{A}] \to \hat{A}$ is defined by $e_{\chi} \mapsto \chi$, and the kernel V is a free abelian group generated by the elements $e_{\chi_1} + e_{\chi_2} - e_{\chi_1\chi_2}$, $\chi_1, \chi_2 \in \hat{A}$.

By the natural epimorphism $\bar{F} \to F$ all F-modules become $\bar{F}$-modules. The exact sequence $0 \to V \to \mathbf{Z}[\hat{A}] \to \hat{A} \to 0$ implies, by the completeness of the multiplicative group $\bar{k}^*$ of $\bar{k}$, the exact sequence

$$0 \to A \cong \mathrm{Hom}(\hat{A}, \bar{k}^*) \to \mathrm{Hom}(\mathbf{Z}[\hat{A}], \bar{k}^*) \to \mathrm{Hom}(V, \bar{k}^*) \to 0.$$

Since $H^1(\bar{F}, \mathrm{Hom}(\mathbf{Z}[\hat{A}], \bar{k}^*)) = 0$ (see [ILF, III, Section 13.3]), this exact sequence implies the exact cohomology sequence

$$0 \to H^1\big(\bar{F}, \mathrm{Hom}(V, \bar{k}^*)\big) \xrightarrow{\beta} H^2(\bar{F}, A) \xrightarrow{\gamma} H^2\Big(\bar{F}, \mathrm{Hom}\big(\mathbf{Z}[\hat{A}], \bar{k}^*\big)\Big).$$

We call the element $\eta = \gamma\bar{c}$ *the first obstruction*. Its triviality $\eta = 0$ is necessary for the solvability of the problem $(K/k, G, A)$. When the first obstruction is trivial (the compatibility condition) there exists a unique $\xi \in H^1(\bar{F}, \mathrm{Hom}(V, \bar{k}^*))$ such that $\bar{c} = \beta\xi$. We call the element ξ *the second obstruction*. Its triviality $\xi = 0$ is necessary and sufficient for the solvability of the problem $(K/k, G, A)$.

Applying the Hochschild–Serre theorem on cohomology lifting, we obtain the exact sequence

$$0 \to H^1(F, \mathrm{Hom}(V, K^*)) \to H^1\big(\bar{F}, \mathrm{Hom}(V, \bar{k}^*)\big) \to H^1\big(R, \mathrm{Hom}(V, \bar{k}^*)\big).$$

Since $H^1(R, \mathrm{Hom}(V, \bar{k}^*)) = 0$ we have by the arguments given before [ILF, Theorem 3.13.3]

$$H^1\big(\bar{F}, \mathrm{Hom}(V, \bar{k}^*)\big) \cong H^1(F, \mathrm{Hom}(V, K^*)) \cong \mathrm{Ext}_F^1(V, K^*).$$

The exact sequence $0 \to V \to \mathbf{Z}[\hat{A}] \to \hat{A} \to 0$ also implies the exact sequence for Ext,

$$\mathrm{Ext}_F^1\big(\mathbf{Z}[\hat{A}], K^*\big) \to \mathrm{Ext}_F^1(V, K^*) \to \mathrm{Ext}_F^2(\hat{A}, K^*),$$

where $\mathrm{Ext}_F^1(\mathbf{Z}[\hat{A}], K^*) \cong H^1(F, \mathrm{Hom}(\mathbf{Z}[\hat{A}], K^*)) = 0$; therefore $\xi \in \mathrm{Ext}_F^2(\hat{A}, K^*)$. This fact is useful, given additional information about the F-module structure of the character group $\hat{A}$.

3. THE BRAUER PROBLEM

Let $A = \langle a \rangle$ be a cyclic group of order n, and let $\zeta \in K$ be a primitive nth root of unity. Then $\zeta^{\rho} = \zeta^{k_\rho}$, for $\rho \in F$; k_ρ is an integer mod n. When $a^{\rho} = \bar{\rho}^{-1} a \bar{\rho} = a^{k_\rho}$ ($\bar{\rho}$ is a preimage of ρ in G) the problem $(K/k, G, A = \langle a \rangle)$ is called the *Brauer problem*. Applying the techniques in the previous section we can give another proof of [ILF, Theorem 3.1].

THEOREM 3.1. *For the Brauer problem, the compatibility is sufficient for solvability.*

Proof. We take $\chi \in \hat{A}$ such that $\chi(a) = \zeta$. Then $\chi^{\rho}(a) = \chi(a^{\rho})^{\rho^{-1}} = \chi(a^{k_\rho})^{\rho^{-1}} = \zeta^{k_\rho k_{\rho^{-1}}} = \zeta$. Consequently, $\hat{A} = \langle \chi \rangle$, $\mathbf{Z}[\hat{A}]$, and V are modules on which F acts trivially. The group $\mathrm{Hom}(V, K^*)$ is a direct product of several copies of K^* and by Spieser's theorem $H^1(F, \mathrm{Hom}(V, K^*)) = 0$. ∎

Also, we can obtain this fact as a corollary by the following theorem.

THEOREM 3.2. *Let the abelian kernel A be such that $\chi^{\rho} = \chi^{\pm 1}$, $\chi \in \hat{A}$, $\rho \in F$. The problem $(K/k, G, A)$ is solvable if and only if the compatibility condition is satisfied.*

Proof. First we show that for arbitrary $\chi_1, \chi_2 \in \hat{A}$, $\rho \in F$ is satisfied.

$$\chi_1^{\rho} = \chi_1, \chi_2^{\rho} = \chi_2, (\chi_1 \chi_2)^{\rho} = \chi_1 \chi_2 \qquad \text{or}$$

$$\chi_1^{\rho} = \chi_1^{-1}, \chi_2^{\rho} = \chi_2^{-1}, (\chi_1 \chi_2)^{\rho} = \chi_1^{-1}\chi_2^{-1}.$$

Assume $\chi_1^{\rho} = \chi_1^{-1}$ and $\chi_2^{\rho} = \chi_2$. Then we have two cases. In the first case $(\chi_1 \chi_2)^{\rho} = \chi_1^{-1}\chi_2 = \chi_1 \chi_2$, whence $\chi_1^2 = 1$; i.e., $\chi_1^{\rho} = \chi_1^{-1} = \chi_1$. In the second case $(\chi_1 \chi_2)^{\rho} = \chi_1^{-1}\chi_2 = \chi_1^{-1}\chi_2^{-1}$, whence $\chi_2^2 = 1$; i.e., $\chi_2^{\rho} = \chi_2 = \chi_2^{-1}$. This proves our assertion.

Now, we denote by U the free abelian group generated by the elements $e_\chi + e_{\chi^{-1}}$, $\chi \in \hat{A}$. It can be shown that V/U is a free abelian group. The group F acts on U trivially, since $(e_\chi + e_{\chi^{-1}})^{\rho} = e_\chi + e_{\chi^{-1}}$, $\chi \in \hat{A}$, $\rho \in F$. Then the group $\mathrm{Hom}(U, K^*)$ is a direct product of several copies of K^*; therefore $H^1(F, \mathrm{Hom}(U, K^*)) = 0$.

Further, $e_{\chi^{-1}} = -e_\chi + e_\chi + e_{\chi^{-1}}$, whence $e_\chi^{\rho} = e_{\chi^{\rho}} = \pm e_\chi \bmod U$. For an arbitrary generator $\nu = e_{\chi_1} + e_{\chi_2} - e_{\chi_1\chi_2} \in V$ we have $\nu^{\rho} = e_{\chi_1^{\rho}} + e_{\chi_2^{\rho}} - e_{(\chi_1\chi_2)^{\rho}} = \pm \nu \bmod U$ by the above arguments. Therefore $V/U \cong \Sigma \mathbf{Z}\bar{\nu}$, $\bar{\nu} = \nu + U$, $(\mathbf{Z}\bar{\nu})^{\rho} = \mathbf{Z}\bar{\nu}$, whence $\mathrm{Hom}(V/U, K^*)$ is also a direct product of several copies of K^*, and $H^1(F, \mathrm{Hom}(V/U, K^*)) = 0$. The exact sequence $0 \to U \to V \to V/U \to 0$ implies, by applying Hom and then cohomology, the exact sequences

$$0 \to \mathrm{Hom}(V/U, K^*) \to \mathrm{Hom}(V, K^*) \to \mathrm{Hom}(U, K^*) \to 0$$

and

$$0 = H^1(F, \mathrm{Hom}(V/U, K^*)) \to H^1(F, \mathrm{Hom}(V, K^*)) \to H^1(F, \mathrm{Hom}(U, K^*)) = 0.$$

Thus, $H^1(F, \mathrm{Hom}(V, K^*)) = 0$ and the theorem holds. ∎

COROLLARY 3.3 ([ILF, III, Section 4.1]). *The embedding problem $(K/k, G, A)$ with cyclic kernel of order 4 is solvable if and only if the compatibility condition is satisfied.*

Proof. Let the character group $\hat{A}$ be generated by an element χ of order 4. Then for any $\rho \in F$ we have $\chi^{\rho} = \chi^{\pm 1}$, $(\chi^2)^{\rho} = \chi^2$. ∎

If one allows only Galois extensions as solutions for the embedding problem with cyclic kernel of order 4, the compatibility condition is sufficient for solvability if and only if the number of square classes $|k^*/k^{*2}|$ is large enough (see Corollary 3.6 and Example 6.4 and also [Le2]).

We proceed with an example involving the generalized quaternion group of order 2^{n+1} given by the presentation

$$Q_{2^{n+1}} \cong \langle \sigma, \tau \mid \sigma^{2^n} = 1, \tau^2 = \sigma^{2^{n-1}}, \tau\sigma = \sigma^{-1}\tau \rangle.$$

EXAMPLE 3.4. Consider the extension

$$1 \to C_{2^n} \cong \langle \sigma \rangle \to Q_{2^{n+1}} \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{-1})/k\big) \to 1.$$

Let $\zeta \in K = k(\sqrt{-1})$ be a primitive 2^nth root of unity, and let $\zeta^{\rho} = \zeta^{-1}$. We show that the problem $(K/k, Q_{2^{n+1}}, \langle \sigma \rangle)$ is solvable if and only if $(-1,-1) = 1 \in \mathrm{Br}(k)$.

Since the problem is Brauer, we need only to examine the compatibility condition. The character group $\langle \hat{\sigma} \rangle$ is generated by a element χ, where $\chi^i(\sigma) = \zeta^i$, $i = 1, \ldots, 2^n$. The crossed product algebra $Q_{2^{n+1}} \times K \cong \sum_{j=1}^{2^n} (Q_{2^{n+1}} \times K) l_j$, where l_j are the minimal orthogonal idempotents,

$$l_j = \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^i \chi^j(\sigma^i) = \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^i \zeta^{ij}, \; j = 1, \ldots, 2^n.$$

Further,

$$\tau l_j = \frac{1}{2^n} \sum_{j=1}^{2^n} \tau\sigma^i \zeta^{ij} = \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^{-i}\tau\zeta^{ij}$$

$$= \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^{-i}\big(\zeta^{ij}\big)^{\rho}\tau = \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^{-i}\zeta^{-ij}\tau = l_j\tau.$$

Whence,

$$\big(\tau l_j\big)^2 = \tau^2 l_j = \sigma^{2^{n-1}} l_j = \frac{1}{2^n} \sum_{j=1}^{2^n} \sigma^{2^{n-1}+i} \zeta^{ij},$$

but $\zeta^{(2^{n-1}+i)j} = \zeta^{2^{n-1}j}\zeta^{ij} = (-1)^j\zeta^{ij}$. Therefore, $(\tau l_j)^2 = (-1)^j l_j$. Since $(\tau l_j)(\sqrt{-1}\, l_j) = -(\sqrt{-1}\, l_j)(\tau l_j)$ and $(\sqrt{-1}\, l_j)^2 = -l_j$, the elements τl_j and $\sqrt{-1}\, l_j$ generate the quaternion algebra $(Q_{2^{n+1}} \times K) l_j \cong ((-1)^j, -1/k)$. Thus, $(Q_{2^{n+1}} \times K) l_j \cong (1, -1/k) \cong \mathrm{Mat}_2 k$, when j is even and $(Q_{2^{n+1}} \times$

$K)l_j \cong (-1, -1/k)$, when j is odd. Whence $Q_{2^{n+1}} \times K$ is the matrix algebra if and only if $(-1, -1/k) \cong \mathrm{Mat}_2 k$; i.e., $(-1, -1) = 1 \in \mathrm{Br}(k)$. ∎

COROLLARY 3.5 (see Example 7.7). *Given the extension*

$$1 \to C_8 \cong \langle \sigma \rangle \to Q_{16} \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{-1})/k\big) \to 1,$$

where Q_{16} is the quaternion group of order 16 and $2 \in k^{*2}$, the problem $(k(\sqrt{-1})/k, Q_{16}, \langle \sigma \rangle)$ is solvable if and only if $(-1, -1) = 1 \in \mathrm{Br}(k)$.

Proof. It is enough to set $\zeta = \frac{\sqrt{2}}{2} + \sqrt{-1}\,\frac{\sqrt{2}}{2} \in k(\sqrt{-1})$. Indeed, $\zeta^2 = \sqrt{-1}$, $\zeta^4 = -1$, $\zeta^8 = 1$, and $\zeta^\rho = \frac{\sqrt{2}}{2} - \sqrt{-1}\,\frac{\sqrt{2}}{2} = \zeta^{-1}$. ∎

COROLLARY 3.6 (see Example 6.5). *Given the extension*

$$1 \to C_4 \cong \langle \sigma \rangle \to Q_8 \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{-1})/k\big) \to 1,$$

the problem $(k(\sqrt{-1})/k, Q_8, \langle \sigma \rangle)$ is solvable if and only if $(-1, -1) = 1 \in \mathrm{Br}(k)$.

4. ASSOCIATED PROBLEMS OF THE FIRST KIND

An embedding problem whose solvability is necessary for the solvability of a given problem is called an *associated problem*.

Let $\varphi\colon A \to A_1$ be an F-homomorphism. Then φ yields the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\alpha} & F = \mathrm{Gal}(K/k) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
1 & \longrightarrow & A_1 & \longrightarrow & G_1 & \xrightarrow{\alpha_1} & F = \mathrm{Gal}(K/k) & \longrightarrow & 1,
\end{array}$$

for some homomorphism $\psi\colon G \to G_1$. We denote by $c \in H^2(F, A)$ the cohomology class corresponding to the first row, and by $c_1 \in H^2(F, A_1)$ the cohomology class corresponding to the second row. Obviously, c_1 is obtained by applying φ to the 2-cocycles that constitute the class $c \in H^2(F, A)$. From the commutative diagram

$$\begin{array}{ccc}
H^2(F, A) & \xrightarrow{\lambda} & H^2(\bar{F}, A) \\
\downarrow{\scriptstyle \varphi_*} & & \downarrow{\scriptstyle \bar{\varphi}} \\
H^2(F, A_1) & \xrightarrow{\lambda_1} & H^2(\bar{F}, A_1)
\end{array}$$

we have $\bar{c}_1 = \lambda_1 c_1 = \lambda_1 \varphi_* c = \bar{\varphi}\lambda c = \bar{\varphi}\bar{c}$. Therefore, the solvability of the problem $(K/k, G, A)$ implies the solvability of the problem $(K/k, G_1, A_1)$ by Theorem 2.1.

Remark. The same is true even if A and A_1 are non-abelian groups.

EXAMPLE 4.1. Assume $(b, b) = 1$, where $b \in k^* \setminus k^{*2}$. The problem related to the exact sequence

$$1 \to C_{2^n} \cong \langle \sigma \rangle \to Q_{2^{n+1}} \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{b})/k\big) \to 1$$

is solvable. Indeed, we have the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_2 \cong \langle \sigma^{2^{n-1}} \rangle & \longrightarrow & C_4 \cong \langle \tau \rangle & \xrightarrow[\tau \mapsto \rho]{} & C_2 = \mathrm{Gal}(k(\sqrt{b})/k) & \longrightarrow & 1 \\
 & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \\
1 & \longrightarrow & C_{2^n} \cong \langle \sigma \rangle & \longrightarrow & Q_{2^{n+1}} & \xrightarrow[\tau \mapsto \rho]{} & C_2 = \mathrm{Gal}(k(\sqrt{b})/k) & \longrightarrow & 1
\end{array}$$

It is well known that the problem $(k(\sqrt{b})/k, C_4, C_2)$ related to the first row is solvable if and only if $(b, b) = 1$, which is sufficient for the solvability of the problem $(k(\sqrt{b})/k, Q_{2^{n+1}}, \langle \sigma \rangle)$ by the above arguments. However, this is not a necessary condition as the examples in Sections 6 and 7 show. ∎

Now, let φ: $A \to A_1$ be an F-epimorphism. We call the problem $(K/k, G_1, A_1)$ an *associated problem of the first kind*. Then φ induces the injection $\hat{A}_1 = \mathrm{Hom}(A_1, K^*) \to \hat{A} = \mathrm{Hom}(A, K^*)$ and the commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V_1 & \longrightarrow & \mathbf{Z}[\hat{A}_1] & \longrightarrow & \hat{A}_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V & \longrightarrow & \mathbf{Z}[\hat{A}] & \longrightarrow & \hat{A} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V/V_1 & \longrightarrow & \mathbf{Z}[\hat{A}]/\mathbf{Z}[\hat{A}_1] & \longrightarrow & \hat{A}/\hat{A}_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Since $\hat{A}_1 \subset \hat{A}$, $\mathbf{Z}[\hat{A}]/\mathbf{Z}[\hat{A}_1]$, and V/V_1 are free $\mathbf{Z}$-modules. Consequently, the sequence of F-modules

$$0 \to \mathrm{Hom}(V/V_1, K^*) \to \mathrm{Hom}(V, K^*) \xrightarrow{\mu} \mathrm{Hom}(V_1, K^*) \to 0$$

is exact. Further, the maps $\varphi\colon A \to A_1$, $\mu\colon \mathrm{Hom}(V, K^*) \to \mathrm{Hom}(V_1, K^*)$, and $\nu\colon \mathrm{Hom}(\mathbf{Z}[\hat{A}], \bar{k}^*) \to \mathrm{Hom}(\mathbf{Z}[\hat{A}_1], \bar{k}^*)$ induce the commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\bar{F}, \mathrm{Hom}(V, \bar{k}^*)) & \xrightarrow{\beta} & H^2(\bar{F}, A) & \xrightarrow{\gamma} & H^2(\bar{F}, \mathrm{Hom}(\mathbf{Z}[\hat{A}], \bar{k}^*)) \\
 & & \downarrow \bar{\mu} & & \downarrow \bar{\varphi} & & \downarrow \bar{\nu} \\
0 & \longrightarrow & H^1(\bar{F}, \mathrm{Hom}(V_1, \bar{k}^*)) & \xrightarrow{\beta_1} & H^2(\bar{F}, A_1) & \xrightarrow{\gamma_1} & H^2(\bar{F}, \mathrm{Hom}(\mathbf{Z}[\hat{A}_1], \bar{k}^*)).
\end{array}$$

Thus, we have shown the following theorem.

THEOREM 4.2. *Let η and ξ be, respectively, the first and the second obstruction to the problem $(K/k, G, A)$. Then $\bar{\nu}\eta$ and $\bar{\mu}\xi$ are, respectively, the first and the second obstruction to the problem $(K/k, G_1, A_1)$.*

Similarly, the commutative diagram

$$\begin{array}{ccccc}
0 & \longrightarrow & \mathrm{Ext}_F^1(V, K^*) & \longrightarrow & \mathrm{Ext}_F^2(\hat{A}, K^*) \\
 & & \downarrow \mu_* & & \downarrow \varphi_* \\
0 & \longrightarrow & \mathrm{Ext}_F^1(V_1, K^*) & \longrightarrow & \mathrm{Ext}_F^2(\hat{A}_1, K^*),
\end{array}$$

where μ_* and φ_* are induced by the inclusion maps, implies

COROLLARY 4.3. *Let the first obstruction be trivial $(\eta = 0)$. Then $\varphi_* \xi$ is the second obstruction to the problem $(K/k, G_1, A_1)$.*

5. ASSOCIATED PROBLEMS OF THE SECOND KIND

Given a problem $(K/k, G, A)$, let F_1 be a subgroup of F. We put $G_1 = \alpha^{-1}(F_1)$ and denote by k_1 the subfield of F_1-invariant elements in K. We call the problem $(K/k_1, G_1, A)$ an *associated problem of the second kind*. It is clear that a solution of the initial problem is also a solution to the associated problem of the second kind.

We have the restriction map res: $H^2(F, A) \to H^2(F_1, A)$, and the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & G_1 & \xrightarrow{\alpha_1} & F_1 = \mathrm{Gal}(K/k_1) & \longrightarrow & 1 \\ & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\alpha} & F = \mathrm{Gal}(K/k) & \longrightarrow & 1. \end{array}$$

We put $c_1 = \mathrm{res}\, c$, $\overline{F}_1 = \mathrm{Gal}(\overline{k}/k_1)$, and the commutative diagram

$$\begin{array}{ccc} H^2(F, A) & \xrightarrow{\lambda} & H^2(\overline{F}, A) \\ \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\ H^2(F_1, A) & \xrightarrow{\lambda_1} & H^2(\overline{F}_1, A) \end{array}$$

implies $\bar{c}_1 = \lambda_1 c_1 = \lambda_1 \,\mathrm{res}\, c = \mathrm{res}\, \lambda c = \mathrm{res}\, \bar{c}$. Then we obtain the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \longrightarrow H^1(\overline{F}, \mathrm{Hom}(V, \overline{k}^*)) & \xrightarrow{\beta} & H^2(\overline{F}, A) & \xrightarrow{\gamma} & H^2(\overline{F}, \mathrm{Hom}(\mathbf{Z}[\hat{A}], \overline{k}^*)) \\ \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\ 0 \longrightarrow H^1(\overline{F}_1, \mathrm{Hom}(V, \overline{k}^*)) & \xrightarrow{\beta_1} & H^2(\overline{F}_1, A) & \xrightarrow{\gamma_1} & H^2(\overline{F}_1, \mathrm{Hom}(\mathbf{Z}[\hat{A}], \overline{k}^*)), \end{array}$$

where the vertical maps are restriction maps. Thus, we have shown the following analog of theorem 4.2.

THEOREM 5.1. *Let* η *and* ξ *be, respectively, the first and the second obstruction to the problem* $(K/k, G, A)$. *Then* res η *and* res ξ *are, respectively, the first and the second obstruction to the problem* $(K/k_1, G_1, A)$.

Clearly, we can always reduce an embedding problem with abelian kernel to an embedding problem with abelian p-kernel, p being a prime (known as the first Kochendörffer theorem [ILF, Theorem 3.5]).

Now, let A be an abelian p-group, and let F_1 be a Sylow p-subgroup in F. We denote by G_1 the preimage of F_1 in G; $m = |F| = p^r m_p$, $(p, m_p) = 1$, $|F_1| = p^r$. Then we can give a short proof to the well-known Kochendörffer-Faddeev reduction theorem (the second Kochendörffer theorem [ILF, Theorem 3.8; Ko]).

THEOREM 5.2. *The problem* $(K/k, G, A)$ *is solvable if and only if the problem* $(K/k_1, G_1, A)$ *is solvable*.

Proof. Let the associated problem $(K/k_1, G_1, A)$ be solvable. Then $\bar{c}_1 = 0$ and $m_p \bar{c} = 0$, since $\overline{F}$ is a profinite group and $(\overline{F} : \overline{F}_1) = m_p$ (see [Se, I, Section 2.4, Proposition 9]).

Now, let F_2 be a Sylow q-subgroup in F, $q \neq p$. Whence the group extension $1 \to A \to G_2 \to F_2 \to 1$ is split; i.e., $c_2 = 0$, where c_2 is the cohomology class in $H^2(F_2, A)$, corresponding to the extension $1 \to A \to G_2 \to F_2 \to 1$. Therefore, $\bar{c}_2 = 0$; $\bar{c}_2$ is the lifting of c_2 in $H^2(\overline{F}_2, A)$. Thus we have obtained that the restriction of $\bar{c} \in H^2(\overline{F}, A)$ into $H^2(\overline{F}_i, A)$ is zero, for all Sylow p_i-subgroups, F_i in F. This means that $m_{p_i}\, \bar{c} = 0$ for all prime divisors p_i of m and consequently $\bar{c} = 0$; i.e., the problem $(K/k, G, A)$ is solvable. ∎

The two Kochendörffer theorems in effect reduce the embedding problem with abelian kernel to the embedding problem for p-groups.

6. THE QUATERNION GROUP OF ORDER 8

From now on we deal only with Galois extensions over fields with characteristic not 2. In this section, we examine the obstructions to certain embedding problems for the quaternion group of order 8, given by the presentation $Q_8 \cong \langle \sigma, \tau | \sigma^4 = 1,\ \tau^2 = \sigma^2,\ \tau\sigma = \sigma^{-1}\tau \rangle$. The realizability of Q_8 is discussed in many works such as [Wa, Wi, Ki]. In [JY] Jensen and Yui give an explicit construction and a survey of known results. In [Va] is investigated the construction of quaternionic fields over the rational field $\mathbf{Q}$.

Helping our consideration is the following salient theorem.

THEOREM 6.1 (see [ILF, I, Section 10]). *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 $F \cong G/A$. The field $L \supset K$ is a solution of the embedding problem*

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

if and only if the problem

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

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

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

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

Now, let us consider the embedding problem

$$1 \to C_4 \cong \langle \sigma \rangle \to Q_8 \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{b})/k\big) \to 1. \qquad (1)$$

The associated problem

$$1 \to C_2 \cong \langle \sigma \rangle / \langle \sigma^2 \rangle \to C_2^2 \cong Q_8 / \langle \sigma^2 \rangle \to C_2 = \mathrm{Gal}\big(k(\sqrt{b})/k\big) \to 1$$

is solvable if and only if $|k^*/k^{*2}| \geq 4$; i.e., $\exists a \in k^* \setminus k^{*2}$: a and b are independent mod k^{*2}. Then the problem

$$1 \to C_2 \cong \langle \sigma^2 \rangle \to Q_8 \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\to} C_2^2 = \mathrm{Gal}\big(k(\sqrt{a}, \sqrt{b})/k\big) \to 1$$

is solvable if and only if $(a, ab)(b, b) = 1$ [Le1, Section 3; Ki, Theorem 4; GSS, Theorem 3.11]. By Theorem 6.1 the problem (1) is solvable $\Leftrightarrow \exists a \in k^* \setminus k^{*2}$: a and b are independent mod k^{*2} and $1 = (a, ab)(b, b) = (a, a)(a, b)(b, b) = (a, -1)(a, b)(b, b) = (a, -b)(b, b)$.

LEMMA 6.2. *Assume $b \in k^* \setminus k^{*2}$. There exists $a \in k^* \setminus k^{*2}$: a and b are independent* mod k^{*2} *and $(a, -b) = (b, b)$ if and only if b is a sum of three non-zero squares or b is a sum of two squares and b is not rigid.*

Proof. Let $(a, -b)(b, b) = 1$, for some $a \in k^* \setminus k^{*2}$. By Proposition 1.1 $\exists x \in k$: $(-1, ax) = (b, -ax) = (-b, x) = 1$. Then $ax = u^2 + v^2$, for some $u, v \in k$ and $b = w^2 + axy^2 = w^2 + (u^2 + v^2)y^2$, for some $w, y \in k$; i.e., b is a sum of three squares. If b is a sum of two squares then $(a, -b) = (b, b) = 1$; i.e., b is not rigid.

Conversely, let $b = u^2 + v^2 + w^2$, for some $u, v, w \in k$. If $u, v, w \in k^*$ we set $a = u^2 + v^2$ and then $(a, -b)(b, b) = (-1, a)(a, b)(b, -1) = (-1, a)(-a, b) = 1$. If a and b are dependent mod k^{*2} then b is a sum of two squares. When b is a sum of two squares and b is not rigid we have $(a, -b) = (b, b) = 1$, for some $a \in k^* \setminus k^{*2}$: a and b are independent mod k^{*2}. ∎

Whence we immediately get the following.

EXAMPLE 6.3. Assume $b = 2$. The problem (1) is solvable if and only if 2 is not rigid.

EXAMPLE 6.4. Assume $2 \notin k^{*2}$ and $b = y^2 + 1/y^2 \neq 2 \bmod k^{*2}$, for some $y \in k^*$. The problem (1) is always solvable. Indeed, $(b, b) = 1$ and $b = y^2 + 1/y^2 = (y + 1/y)^2 - 2$. Therefore, $(-b, 2) = (-1, 2)(b, 2) = 1$ and we can set $a = 2$. (The special case $k = \mathbf{Q}$ and $a = 2$ is studied in [Co].)

EXAMPLE 6.5 [Wa, Lemma 1]. Assume $b = -1$. The problem (1) is solvable if and only if $|k^*/k^{*2}| \geq 4$ and $s(k) = 2$. Indeed, the obstruction then is $(a, -a)(-1, -1) = (-1, -1) = 1 \Leftrightarrow s(k) = 2$.

COROLLARY 6.6. *Assume* $s(k) = 4$. *The group* Q_8 *is always realizable*.

Proof. Let $-1 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$, $\alpha_i \in k^*$. We put $b = \alpha_1^2 + \alpha_2^2$, $a = \alpha_1^2 + \alpha_2^2 + \alpha_3^2$. Obviously, $(a, -b) = (b, b) = 1$, a and b are independent mod k^{*2}; otherwise $s(k) \leq 2$. ∎

7. THE QUATERNION GROUP OF ORDER 16

Similarly to the previous section, we consider the quaternion group of order 16, given by the presentation $Q_{16} \cong \langle \sigma, \tau \mid \sigma^8 = 1, \tau^2 = \sigma^4, \tau\sigma = \sigma^{-1}\tau \rangle$. Consider the embedding problem

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

It is well known that the associated problem

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

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

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

is solvable if and only if $(ab, 2)(b, b) = (-b, x)$, for some $x \in k^*$ [Le1, Example 4.4; GSS, Theorem 4.6.4]. By Theorem 6.1 the problem (2) is solvable if and only if $(a, ab) = 1$ and $(ab, 2)(b, b) = (-b, x)$, for some $x \in k^*$.

As before, given the extensions

$$1 \to C_8 \cong \langle \sigma \rangle \to Q_{16} \underset{\tau \mapsto \rho}{\to} C_2 = \mathrm{Gal}\big(k(\sqrt{b})/k\big) \to 1, \qquad (3)$$

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

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

the problem (3) 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 $\exists x \in k^*$: $(ab, 2)(b, b) = (-b, x)$. By the remark after Example 4.4 in [Le1] b is a sum of nine squares and

we can write down the following analog of Lemma 6.2 (when b is a sum of two or three non-zero squares).

LEMMA 7.1. *$b \in k^*$ is a sum of three squares $\Leftrightarrow \exists x \in k^*$: $(b, b) = (-b, x)$.*

EXAMPLE 7.2. Assume $a = -2$, $b = 2$. Then $(a, ab) = (-2, -2)$, $(b, b) = (2, 2) = 1$, $(ab, 2) = 1$. Thus, the problem (2) for $a = -2$, $b = 2$ is solvable if and only if $(-2, -2) = 1$.

EXAMPLE 7.3. Assume $a = 2$, $b = -2$, $s(k) = 2$. Then $(a, ab) = (2, -1) = (ab, 2) = 1$ and $(b, b) = (-2, -2) = (-2, -1) = (2, -1)(-1, -1) = (-1, -1) = 1$. Thus, the problem (2) for $a = 2$, $b = -2$, $s(k) = 2$ is solvable.

EXAMPLE 7.4. The problem (2) for $b = -a$ is solvable if and only if a is a sum of two squares and $-a$ is a sum of three squares. Indeed, $(a, ab) = (a, -1) = 1 \Leftrightarrow a$ is a sum of two squares; $(ab, 2) = (2, -1) = 1$ and $(-a, -a) = (a, x)$, for some $x \in k^* \Leftrightarrow -a$ is a sum of three squares by Lemma 7.1.

COROLLARY 7.5. *Assume $s(k) = 4$. The group Q_{16} is always realizable.*

Proof. $s(k) = 4 \Rightarrow \exists \alpha_i \in k^*$, $i = 1, \ldots, 5$, such that $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_5^2 = 0$. If we set $a = \alpha_1^2 + \alpha_2^2$ then $-a = \alpha_3^2 + \alpha_4^2 + \alpha_5^2$. Note that a and $-a$ are independent mod k^{*2}; otherwise $s(k) \leq 2$. Whence the problem (2) for $b = -a$ is solvable by Example 7.4. ∎

Next, we proceed with examples of problems of type (3).

EXAMPLE 7.6. Let $b = -1$ and $-2 \in k^{*2}$. Then $(a, ab) = (a, -a) = 1$, $(ab, 2)(b, b)(-b, x) = (-a, 2)(-1, -1)(1, x) = (-a, -1)(-1, -1) = (a, -1) = 1 \Leftrightarrow a$ is a sum of two squares. Thus, the problem (3) 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 7.7. Let $b = -1$ and $2 \in k^{*2}$. Then $(a, ab) = (a, -a) = 1$, $(ab, 2)(b, b)(-b, x) = (-1, -1) = 1 \Leftrightarrow s(k) = 2$. Thus the problem (3) for $b = -1$ and $2 \in k^{*2}$ is solvable if and only if $|k^*/k^{*2}| \geq 4$ and $s(k) = 2$.

EXAMPLE 7.8. Assume $(-2, -2) = 1$; i.e., $\exists \alpha, \beta \in k$: $\alpha^2 + 2\beta^2 = -2$, and $b = y^2 + 1/y^2$, for some $y \in k^*$. As in Example 6.4 $(b, b) = 1$ and $b = y^2 + 1/y^2 = (y + 1/y)^2 - 2$, whence $(b, 2) = 1$.

Further, consider the element $a = \alpha^2 + b\beta^2$. We have $(a, -b) = 1$, and

$$a = \alpha^2 + b\beta^2 \in k^{*2} \Leftrightarrow b + (\alpha/\beta)^2 \in k^{*2}$$

$$a = \alpha^2 + b\beta^2 \in \beta k^{*2} \Leftrightarrow 1/b + (\beta/\alpha)^2 \in k^{*2}.$$

Also,

$$a = \alpha^2 + (y^2 + 1/y^2)\beta^2 = \alpha^2 + \big((y - 1/y)^2 + 2\big)\beta^2$$
$$= (y - 1/y)^2\beta^2 + \alpha^2 + 2\beta^2 = (y - 1/y)^2\beta^2 - 2,$$

whence $(a, 2) = 1$; therefore $(ab, 2) = (a, 2)(b, 2) = 1$. Thus the problem (3) 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. ∎

REFERENCES

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

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

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

[ILF] V. V. Ishanov, B. B. Lur'e, and D. K. Faddeev, "The Embedding Problem in Galois Theory," Am. Math. Soc., Providence, 1997.

[JY] C. U. Jensen and N. Yui, Quaternion extensions, *Algebraic Geom. Commutative Algebra* (1987), 155–182.

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

[Ko] R. Kochendörffer, Zwei Reduktionssätze zum Einbettungsproblem für Abelschen Algebren, *Math. Nachr.* **10** (1953), 75–84.

[La] T. Y. Lam, "The Algebraic Theory of Quadratic Forms," Benjamin, Reading, MA, 1973.

[Le1] A. Ledet, On 2-groups as Galois groups, *Canad. J. Math.* **47** (1995), 1253–273.

[Le2] A. Ledet, Embedding problems with cyclic kernel of order 4, *Israel J. Algebra* **181** (1998), 109–131.

[Se] J.-P. Serre, "Cohomologie Galoisiene," Springer-Verlag, Berlin, 1965.

[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.