MATH. SCAND. 88 (2001), 279–302

EMBEDDING PROBLEMS AND EQUIVALENCE OF QUADRATIC FORMS

ARNE LEDET*

Abstract

If the obstruction to a Galois theoretical embedding problem with kernel of order 2 is the product of two quaternion classes, the criterion for solvability can be reformulated as an equivalence of quadratic forms. In some cases the solutions to the embedding problem can be constructed directly from a matrix expressing this equivalence.

0. Introduction

Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$, and let

$$(*) \qquad 1 \to N \to E \xrightarrow[\pi]{} G \to 1$$

be a short exact sequence of finite groups. We then have a *Galois theoretical embedding problem* given by M/K and $(*)$: Does there exist a Galois extension N/K containing M/K, together with an isomorphism $\varphi\colon \mathrm{Gal}(N/K) \simeq E$, such that $\pi \circ \varphi\colon \mathrm{Gal}(N/K) \to G$ is the restriction map? If so, the problem is said to be *solvable*, and the extension N/K is called a *solution*. If the embedding problem is solvable, the next problem is of course to determine all the solutions.

We will consider only a very special type of embedding problems, namely non-split embedding problem with cyclic kernel of order 2, i.e., N is cyclic of order 2 and the extension $(*)$ is not split-exact. If the fields have characteristic 2, such embedding problems are always solvable, cf. [16]. Hence, we will make the additional assumption that all fields have characteristic $\neq 2$, and we will identify the kernel N of the embedding problem with the group $\mu_2 = \{\pm 1\} \subseteq K^* = K \setminus \{0\}$.

These somewhat special embedding problems are particularly nice because of

* This work was supported by a Queen's University Advisory Research Committee Postdoctoral Fellowship.

Received July 27, 1998.

THEOREM 0.1. *Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$, and let*

$$(**) \qquad 1 \to \mu_2 \to E \to G \to 1$$

be a non-split group extension with characteristic class $\gamma \in H^2(G, \mu_2)$. Also, let $i: H^2(G, \mu_2) \to H^2(G, M^*)$ be the homomorphism induced by the inclusion $\mu_2 \subseteq M^*$. Then the embedding problem given by M/K and $(**)$ is solvable, if and only if $i(\gamma) = 1 \in H^2(G, M^*)$. Furthermore, if $N/K = M(\sqrt{\omega})/K$, $\omega \in M^*$, is a solution to the embedding problem, all the solutions are $M(\sqrt{r\omega})/K$, where r runs through K^*.

Theorem 0.1 is proved in [13] and (for an arbitrary prime instead of just 2) in [8].

For later use we will need the 'if' part of the proof of Theorem 0.1. It goes as follows: Let $c \in Z^2(G, \mu_2)$ represent γ. Then $i(\gamma) = 1$ means that $c \in B^2(G, M^*)$, i.e., that there exists a map $a: G \to M^*$, such that

$$\forall \sigma, \tau \in G: c_{\sigma,\tau} = a_\sigma \, \sigma a_\tau \, a_{\sigma\tau}^{-1}.$$

Since $c_{\sigma,\tau} \in \mu_2$, it follows that $\sigma \mapsto a_\sigma^2$ is a crossed homomorphism $G \to M^*$, and so, by Hilbert 90, there exists an $\omega \in M^*$ with

$$\forall \sigma \in G: \frac{\sigma\omega}{\omega} = a_\sigma^2.$$

Then $M(\sqrt{\omega})/K$ is a solution.

By [11, §30 Satz 2] or [6, Thm. 8.11], $H^2(G, M^*)$ is isomorphic to the relative Brauer group $\mathrm{Br}(M/K)$ of M/K by $[c] \mapsto [M, G, c]$, where $[c] \in H^2(G, M^*)$ is the cohomology class containing $c \in Z^2(G, M^*)$, and $[M, G, c] \in \mathrm{Br}(M/K)$ is the equivalence class of the crossed product algebra (M, G, c), i.e., (M, G, c) is the K-algebra generated by M and elements u_σ, $\sigma \in G$, with relations $u_1 = c_{1,1}$, $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}$ and $u_\sigma x = \sigma x \, u_\sigma$ for $\sigma, \tau \in G$ and $x \in M$.

In particular, c is split, i.e., in $B^2(G, M^*)$, if and only if $(M, G, c) \simeq (M, G, 1)$. If $c \in Z^2(G, \mu_2)$ represents the extension $(**)$, the elements $\pm u_\sigma$, $\sigma \in G$, constitute a subgroup of $\mathrm{GL}(M, G, c)$ isomorphic to E, such that the elements of E operate on M as their images in G. This makes the algebra (M, G, c) easy to describe, and it also makes it easy to recognise splitting factors: If $\varphi: (M, G, c) \simeq (M, G, 1)$ is an isomorphism, we may assume $\varphi(x) = x$ for $x \in M$ by Skolem-Noether, cf. [11, §29 Satz 20] or [6, Thm. 4.9]. Then $\varphi(u_\sigma) = a_\sigma \, u_\sigma$ for some $a_\sigma \in M^*$. The a_σ's are splitting factors for c. On the other hand, if we have splitting factors a_σ, the map given by $u_\sigma \mapsto a_\sigma \, u_\sigma$

is an isomorphism $(M, G, c) \simeq (M, G, 1)$. Hence, the elements $\pm a_\sigma u_\sigma$ in $(M, G, 1)$ constitute a subgroup as above. It follows that we only need to verify that these elements satisfy the relations defining E, and that we only need to do this for $a_\sigma u_\sigma$ in a generating set for E, i.e., for σ in a generating set for G. Also, since we only need a_σ's for σ in a generating set for G in order to find ω, we really only have to consider generating sets. This makes life somewhat easier.

The element in $\mathrm{Br}(M/K)$ corresponding to $i(\gamma) \in H^2(G, M^*)$ is called the *obstruction* to the embedding problem.

0.2. THE CYCLIC GROUP $\boldsymbol{C_4}$. *Let $M/K = K(\sqrt{a})/K$, $a \in K^*$, be a quadratic extension. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to C_4 \to C_2 \to 1$$

is solvable, if and only if a is a norm in M/K, i.e., if and only if

$$\exists \alpha, \beta \in K : \alpha^2 - a\beta^2 = a.$$

In that case, all the solutions to the embedding problem are

$$K\left(\sqrt{r(\alpha + \beta\sqrt{a})}\right)\Big/K, \quad r \in K^*.$$

PROOF. Let σ be the generator of $C_2 = \mathrm{Gal}(M/K)$. The crossed product algebra representing the obstruction is $M[u_\sigma]$, where $u_\sigma^2 = -1$ and $u_\sigma x = \sigma x\, u_\sigma$ for $x \in M$. Thus, the condition on a_σ is $a_\sigma\, \sigma a_\sigma = -1$, i.e., the embedding problem is solvable, if and only if -1 is a norm in M/K. Since $-a$ is a norm, this is equivalent to a being a norm.

Now, if $\alpha^2 - a\beta^2 = a$, the element $a_\sigma = \sqrt{a}/(\alpha + \beta\sqrt{a})$ has norm -1, and we get $\sigma(\alpha + \beta\sqrt{a})/(\alpha + \beta\sqrt{a}) = a_\sigma^2$. Hence, $K\left(\sqrt{\alpha + \beta\sqrt{a}}\right)\Big/K$ is a solution.

That a is a norm in $K(\sqrt{a})/K$ is equivalent to a being a sum of two squares in K. This is the criterion generally given, and the C_4-extensions are then constructed accordingly. See for instance [7, Prop. (III.1.2)] or [1, IX. §6 Ex. 1]. Our reason for preferring the norm criterion is the similarity between the C_4-extensions in 0.2 and the D_4-extensions in 0.4 below.

For $a, b \in K^*$, the *quaternion algebra* $(a, b/K)$ is the K-algebra generated by elements i and j with relations $i^2 = a$, $j^2 = b$ and $ji = -ij$. It is a four-dimensional central simple algebra, and so defines an element in the Brauer

group $\mathrm{Br}(K)$ of K, which we denote (a, b) and call a quaternion *class*.[1] The map $(-,-)\colon K^* \times K^* \to \mathrm{Br}(K)$ is then a symmetric bilinear map defined on the square classes of K, i.e., $(ax^2, by^2) = (a, b)$. In particular, (a, b) has order ≤ 2 in $\mathrm{Br}(K)$.

To the quaternion algebra $(a, b/K)$ we associate the quadratic form $\langle a, b, -ab\rangle$, i.e., the map $K^3 \to K$ given by $(x, y, z) \mapsto ax^2 + by^2 - abz^2$, cf. [11, §30]. It is then easy to see that $(a, b/K)$ is split, if and only if $\langle a, b - ab\rangle$ is isotropic, if and only if b is a norm in $K(\sqrt{a})/K$, and that two quaternion algebras $(a, b/K)$ and $(c, d/K)$ are isomorphic, if and only if the quadratic forms $\langle a, b - ab\rangle$ and $\langle c, d, -cd\rangle$ are equivalent. Thus, the equivalence class of $\langle a, b, -ab\rangle$ is an invariant of $(a, b) \in \mathrm{Br}(K)$.

A little more notation: That quadratic forms $\langle a_1, \ldots, a_n\rangle$ and $\langle b_1, \ldots, b_n\rangle$ are equivalent (over K) means that

$$\mathbf{P}^t \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \mathbf{P} = \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix}$$

for some non-singular $n \times n$ matrix $\mathbf{P}$ over K. Of course, if $a_1, \ldots, a_n, b_1, \ldots, b_n$ are non-zero, $\mathbf{P}$ is necessarily non-singular. We say that $\mathbf{P}$ *expresses* the equivalence of $\langle a_1, \ldots, a_n\rangle$ and $\langle b_1, \ldots, b_n\rangle$. For convenience, we will let

$$\langle a_1, \ldots, a_n\rangle = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},$$

allowing us to write

$$\mathbf{P}^t \langle a_1, \ldots, a_n\rangle \mathbf{P} = \langle b_1, \ldots, b_n\rangle.$$

Now back to embedding problems: In order to treat more complicated cases than 0.2[2] we need

THEOREM 0.3. [6, Thm. 4.7], [9, Cor. 1.7] *Let $\mathfrak{A}$ be a finite-dimensional central simple K-algebra, and let $\mathfrak{B}$ be a central simple subalgebra. Then the centraliser*

$$C_{\mathfrak{A}}(\mathfrak{B}) = \{x \in \mathfrak{A} \mid \forall y \in \mathfrak{B}\colon yx = xy\}$$

is a central simple subalgebra of $\mathfrak{A}$, and

$$\mathfrak{A} \simeq \mathfrak{B} \otimes_K C_{\mathfrak{A}}(\mathfrak{B}).$$

[1] The notation (a, b) is a little unfortunate, since many things in mathematics are denoted (a, b), but it is traditional.

[2] I.e., other cases.

Hence, $[\mathfrak{A}] = [\mathfrak{B}][C_{\mathfrak{A}}(\mathfrak{B})]$ *in* $\mathrm{Br}(K)$.

Using Theorem 0.3, we can hope to 'decompose' the obstruction as a product of quaternion algebras in the following way: We find a quaternion subalgebra Q of $\Gamma = (M, G, c)$, and get $\Gamma \simeq Q \otimes_K \Gamma'$, where $\Gamma' = C_\Gamma(Q)$. The process can then be repeated on Γ'. Of course, finding Q involves some guesswork, and for large obstructions this method may not be practicable, but for a number of embedding problems, including the ones we consider in this paper, it works fine.

The simplest example is the dihedral group of order 8, the group D_4 generated by elements σ and τ with relations $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$. We let V_4 be the Klein Vierergruppe $C_2 \times C_2$.

0.4. The dihedral group $\boldsymbol{D_4}$. *Let* $M/K = K(\sqrt{a}, \sqrt{b})/K$, $a, b \in K^*$, *be a* V_4*-extension, and let* $\sigma, \tau \in V_4 = \mathrm{Gal}(M/K)$ *be given by*

$$\begin{aligned} \sigma\colon &\quad \sqrt{a} \mapsto -\sqrt{a}, &\quad \sqrt{b} &\mapsto \sqrt{b}, \\ \tau\colon &\quad \sqrt{a} \mapsto \sqrt{a}, &\quad \sqrt{b} &\mapsto -\sqrt{b}. \end{aligned}$$

Then the embedding problem given by M/K *and*

$$1 \to \mu_2 \to D_4 \xrightarrow[\tau \mapsto \tau]{\sigma \mapsto \sigma} V_4 \to 1$$

is solvable, if and only if ab *is a norm in* $K(\sqrt{a})/K$, *i.e., if and only if*

$$\exists \alpha, \beta \in K\colon \alpha^2 - a\beta^2 = ab.$$

In that case, all the solutions to the embedding problem are

$$K\left(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b}\right)\Big/K, \quad r \in K^*.$$

Proof. The algebra representing the obstruction is $M[u_\sigma, u_\tau]$, where $u_\sigma^2 = -1$, $u_\tau^2 = 1$, $u_\tau u_\sigma = -u_\sigma u_\tau$, $u_\sigma x = \sigma x\, u_\sigma$ and $u_\tau x = \tau x\, u_\tau$ for $x \in M$. Obviously, $Q = K[\sqrt{a}, \sqrt{b}\, u_\sigma]$ is a subalgebra isomorphic to $(a, -b/K)$, and it is easily seen that the centraliser is $R = K[\sqrt{b}, u_\tau] \simeq (b, 1/K)$. Hence, the obstruction is

$$(a, -b)(b, 1) = (a, -b) = (a, ab) \in \mathrm{Br}(K).$$

This gives the criterion. Now, letting $\omega = \alpha + \beta\sqrt{a}$, $a_\sigma = \sqrt{a}\sqrt{b}/(\alpha + \beta\sqrt{a})$ and $a_\tau = 1$, it is straightforward to check that $K(\sqrt{\omega}, \sqrt{b})/K$ is a solution.

D_4-extensions are well covered in the literature, and the result of 0.4 is virtually folklore. See for instance [7], [8], [12] or [5].

A more general application of Theorem 0.3 is to central products: Let

$$1 \to \mu_2 \to E \xrightarrow[\pi]{} G \to 1$$

and

$$1 \to \mu_2 \to F \xrightarrow[\rho]{} H \to 1$$

be group extensions. The *central product* is then the extension

$$1 \to \mu_2 \to EF \xrightarrow[\pi\rho]{} G \times H \to 1,$$

where $EF = E \times F/\{(1,1),(-1,-1)\}$ and $\pi\rho$ is given by $\pi\rho\overline{(e,f)} = (\pi(e), \rho(f))$.

In referring to central products, we will follow the notation indicated above, with the letters C and D denoting the groups C_4 and D_4. Q will refer to the quaternion group of order 8, i.e., the group Q_8 with generators i and j and relations $i^2 = j^2$ and $ji = i^3 j$. Also, for lack of a better term, x will denote a generator of C_4. The central product EF is generated by copies of the groups E and F. If the groups E and F happen to be the same, we will add a prime (a') to the elements from the second copy to distinguish them.

The connection between Theorem 0.3 and central products is

PROPOSITION 0.5. *Let L/K and M/K be linearly disjoint Galois extensions with Galois groups $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(M/K)$. Let $N/K = LM/K$ be the composite, and identify $\mathrm{Gal}(N/K)$ with $G \times H$ in the obvious way. Also, let $\gamma_L \in \mathrm{Br}(K)$ be the obstruction to the embedding problem given by L/K and the non-split group extension*

$$1 \to \mu_2 \to E \xrightarrow[\pi]{} G \to 1,$$

and let $\gamma_M \in \mathrm{Br}(K)$ be the obstruction to the embedding problem given by M/K and the group extension

$$1 \to \mu_2 \to F \xrightarrow[\rho]{} H \to 1.$$

Then the obstruction to the embedding problem given by N/K and

$$1 \to \mu_2 \to EF \xrightarrow[\pi\rho]{} G \times H \to 1$$

is

$$\gamma_N = \gamma_L \gamma_M \in \mathrm{Br}(K).$$

PROOF. Let Γ_L, Γ_M and Γ_N be the crossed product algebras representing γ_L, γ_M and γ_N. Then $\Gamma_L, \Gamma_M \subseteq \Gamma_N$ and Γ_L centralises Γ_M. For dimensional reasons, Γ_M is the centraliser of Γ_L, and so $\Gamma_N = \Gamma_L \otimes_K \Gamma_M$.

Proposition 0.5 is a special case of [10, Prop. 2.3].

In this paper, we will consider various embedding problems where the obstruction is a product of two quaternion classes, and where the criterion for equivalence is an equivalence of quadratic forms. More specifically, we will construct solutions to these embedding problems from matrices expressing the equivalence. In section 1 below, we look at some cases where the group E has exponent 4, and where the embedding problem is essentially reduced to embedding a quadratic extension in a C_4-extension. In section 2 we cite Witt's criterion for embedding a V_4-extension in a Q_8-extension, where Q_8 is the quaternion group of order 8, and solve three related embedding problems. In section 3 we look at cases where the group E has exponent 8, first solving the problem of embedding a C_4-extension in a C_8-extension, and then reducing the others to this case.

In the case, where the group extension $(**)$ is obtained from the double cover of a symmetric group S_n by embedding G transitively into S_n, Crespo ([2], elaborated in [3]) has produced methods for getting from equivalences of quadratic forms to solutions. This approach is much more powerful than the one used in this paper, but also much less straightforward, relying on isomorphisms between Clifford algebras. Among other things, it covers the case of Q_8, and gives a very elegant derivation of Witt's description of Q_8-extensions.

1. Groups of exponent 4

1.1. THE QUATERNION GROUP $\boldsymbol{Q_8}$. *Let $M/K = K(\sqrt{a}, \sqrt{b})/K$, $a, b \in K^*$, be a V_4-extension. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to Q_8 \to V_4 \to 1$$

is solvable, if and only if the quadratic forms $\langle a, -b, ab\rangle$ and $\langle b, -1, b\rangle$ are equivalent over K. If $\mathbf{P}$ is a 3×3 matrix over K expressing this equivalence, i.e., if

$$\mathbf{P}^t \langle a, -b, ab\rangle \mathbf{P} = \langle b, -1, b\rangle,$$

the solutions are

$$M(\sqrt{r\omega})/K = K(\sqrt{r\omega})/K, \quad r \in K^*,$$

where

$$\omega = p_{22} + p_{32}\sqrt{a} + p_{23}\frac{1}{\sqrt{b}} + p_{33}\frac{\sqrt{a}}{\sqrt{b}}.$$

PROOF. Let $\sigma, \tau \in V_4 = \mathrm{Gal}(M/K)$ be given by $\sigma\sqrt{a} = -\sqrt{a}$, $\sigma\sqrt{b} = \sqrt{b}$, $\tau\sqrt{a} = \sqrt{a}$ and $\tau\sqrt{b} = -\sqrt{b}$. Then the obstruction to the embedding problem is represented by the algebra $M[u_\sigma, u_\tau]$, where $u_\sigma^2 = -1$, $u_\tau^2 = -1$, $u_\tau u_\sigma = -u_\sigma u_\tau$, $u_\sigma x = \sigma x\, u_\sigma$ and $u_\tau x = \tau x\, u_\tau$ for $x \in M$. Clearly, $Q = K[\sqrt{a}, \sqrt{b}\, u_\sigma]$ is a quaternion subalgebra $\simeq (a, -b/K)$, and the centraliser is $R = K[\sqrt{b}, u_\tau] \simeq (b, -1/K)$. Hence, the obstruction to the embedding problem is

$$(a, -b)(b, -1) \in \mathrm{Br}(K),$$

cf. also [4, (7.6)], [10, Cor. 2.6] or [12, Thm. 1.2]. This gives us the criterion.

To prove that $M(\sqrt{\omega})/K$ is a solution, we let

$$a_\sigma = \frac{\sigma\omega\sqrt{b}}{(p_{12} + p_{13}/\sqrt{b})\sqrt{a}},$$

$$a_\tau = \frac{\tau\omega\sqrt{b}}{p_{21} + p_{31}\sqrt{a}}.$$

With $(x, y, z)^t = \mathbf{P}\big(0, 1, 1/\sqrt{b}\big)^t$, we have $x, z \neq 0$ and $ax^2 - by^2 + abz^2 = 0$ and get

$$\frac{\sigma\omega}{\omega} = \frac{\sigma\omega^2}{\omega\sigma\omega} = \frac{\sigma\omega^2}{y^2 - az^2} = \frac{\sigma\omega^2 b}{ax^2} = a_\sigma^2.$$

Similarly, we get $\tau\omega/\omega = a_\tau^2$. Also, $a_\sigma\, \sigma a_\sigma = a_\tau\, \tau a_\tau = -1$, and by using the equalities $ap_{11}^2 - bp_{21}^2 + abp_{31}^2 = ab$ and $p_{11}^2/b - p_{12}^2 - p_{13}^2/b = 1/a$, we get $\tau a_\sigma/a_\sigma = -\sigma a_\tau/a_\tau$. Hence, $M(\sqrt{\omega})/K$ is in fact a Q_8-extension.

The quaternion group Q_8 as Galois group is considered in [8] and [12]. The classical description is Witt's from [16], cf. section 2 below.

In essentially the same way we prove

1.2. THE CENTRAL PRODUCT $\boldsymbol{DC}$. *Let $M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$, $a, b, c \in K^*$, be a $V_4 \times C_2$-extension, and let $\sigma, \tau, \upsilon \in \mathrm{Gal}(M/K)$ be given by*

$$\begin{aligned}
\sigma\colon&\ \sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c},\\
\tau\colon&\ \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto -\sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c},\\
\upsilon\colon&\ \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto -\sqrt{c}.
\end{aligned}$$

Then the embedding problem given by M/K and

$$1 \to \mu_2 \to DC \xrightarrow[\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau\\ x\mapsto\upsilon}]{} V_4 \times C_2 \to 1$$

is solvable, if and only if the quadratic forms $\langle a, -b, ab\rangle$ *and* $\langle c, -1, c\rangle$ *are equivalent over* K. *If* $\mathbf{P}$ *is a* 3×3 *matrix over* K *expressing this equivalence, i.e., if*

$$\mathbf{P}^t \langle a, -b, ab\rangle \mathbf{P} = \langle c, -1, c\rangle,$$

the solutions are

$$M(\sqrt{r\omega})/K = K\big(\sqrt{r\omega}, \sqrt{b}\big)\big/K, \quad r \in K^*,$$

where

$$\omega = p_{22} + p_{32}\sqrt{a} + p_{23}\frac{1}{\sqrt{c}} + p_{33}\frac{\sqrt{a}}{\sqrt{c}}.$$

DC-extensions are considered in [12, Cor. 1.3.(iv) + Thm. A.2] and in [15, Prop. p. 1050]. Both papers provide a description of the solutions. The one given in [15] is similar to 2.3 below.

Inside $M(\sqrt{r\omega})/K$, the fixed field of τ is $K(\sqrt{\omega})$. It follows that $M(\sqrt{r\omega})/K$ is the Galois closure of $K(\sqrt{r\omega})/K$.

1.3. The central product $\boldsymbol{DD}$. *Let* $M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})/K$, $a, b, c, d \in K^*$, *be a* $V_4 \times V_4$*-extension, and let* $\rho, \sigma, \tau, \upsilon \in \mathrm{Gal}(M/K)$ *be given by*

$$\begin{array}{lllll}
\rho\colon & \sqrt{a} \mapsto -\sqrt{a}, & \sqrt{b} \mapsto \sqrt{b}, & \sqrt{c} \mapsto \sqrt{c}, & \sqrt{d} \mapsto \sqrt{d},\\
\sigma\colon & \sqrt{a} \mapsto \sqrt{a}, & \sqrt{b} \mapsto -\sqrt{b}, & \sqrt{c} \mapsto \sqrt{c}, & \sqrt{d} \mapsto \sqrt{d},\\
\tau\colon & \sqrt{a} \mapsto \sqrt{a}, & \sqrt{b} \mapsto \sqrt{b}, & \sqrt{c} \mapsto -\sqrt{c}, & \sqrt{d} \mapsto \sqrt{d},\\
\upsilon\colon & \sqrt{a} \mapsto \sqrt{a}, & \sqrt{b} \mapsto \sqrt{b}, & \sqrt{c} \mapsto \sqrt{c}, & \sqrt{d} \mapsto -\sqrt{d}.
\end{array}$$

Then the embedding problem given by M/K *and*

$$1 \to \mu_2 \to DD \xrightarrow[\substack{\sigma\mapsto\rho\\ \tau\mapsto\sigma\\ \sigma'\mapsto\tau\\ \tau'\mapsto\upsilon}]{} V_4 \times V_4 \to 1$$

is solvable, if and only if the quadratic forms $\langle a, -b, ab\rangle$ *and* $\langle c, -d, cd\rangle$ *are equivalent over* K. *If* $\mathbf{P}$ *is a* 3×3 *matrix over* K *expressing this equivalence, i.e., if*

$$\mathbf{P}^t \langle a, -b, ab\rangle \mathbf{P} = \langle c, -d, cd\rangle,$$

the solutions are

$$M(\sqrt{r\omega})/K = K\big(\sqrt{r\omega}, \sqrt{b}, \sqrt{d}\big)\big/K, \quad r \in K^*,$$

where

$$\omega = p_{22} + p_{32}\sqrt{a} + p_{23}\frac{1}{\sqrt{c}} + p_{33}\frac{\sqrt{a}}{\sqrt{c}}.$$

DD-extensions are considered in [14, Thm. 3.1], and a description of the solutions is given.

The fixed field of τ and τ' in $M(\sqrt{r\omega})/K$ is $K(\sqrt{r\omega})/K$. Thus, $M(\sqrt{r\omega})/K$ is the Galois closure of $K(\sqrt{r\omega})/K$.

REMARK. The description of DD-extensions given in [14] is similar to the description of DC-extensions given in [12], in the same way 1.2 and 1.3 are similar. Also, it is possible to apply the approach of [12] and [14] to Q_8.

2. Witt's criterion

In [16], we find

THEOREM 2.1. (Witt, 1936) *Let $M/K = K(\sqrt{a}, \sqrt{b})/K$, $a, b \in K^*$, be a biquadratic extension. Then M/K can be embedded in a Q_8-extension, if and only if the quadratic forms $\langle a, b, ab\rangle$ and $\langle 1, 1, 1\rangle$ are equivalent over K. If $\mathbf{P}$ is a 3×3 matrix over K expressing this equivalence, i.e., if*

$$\mathbf{P}^t\langle a, b, ab\rangle\mathbf{P} = \langle 1, 1, 1\rangle,$$

we may assume $\det \mathbf{P} = 1/ab$ *and get the solutions*

$$K\left(\sqrt{r\left(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{a}\sqrt{b}\right)}\right)\Big/K, \quad r \in K^*.$$

Witt's criterion is easily obtained from the obstruction given in 1.1, since

$$(a, -b)(b, -1) = (-a, -b)(-1, -b)(b, -1) = (-a, -b)(-1, -1) \in \mathrm{Br}(K).$$

That the extensions given are actually the solutions is proven in [16], as well as in [7, Thm. (I.1.1)]. Also, the proof of 2.2 below is easily modified to prove Theorem 2.1. In fact, the proof of 2.2 is inspired by the proof of Theorem 2.1 given in [7].

It is not hard to see that Witt's result can also be formulated as follows: If $\mathbf{S}$ is a 3×3 matrix over K expressing the equivalence of $\langle 1, 1, 1\rangle$ and $\langle a, b, ab\rangle$, i.e., if

$$\mathbf{S}^t\mathbf{S} = \langle a, b, ab\rangle,$$

we can assume $\det \mathbf{S} = ab$, and the extension

$$K\left(\sqrt{1 + \frac{q_{11}}{\sqrt{a}} + \frac{q_{22}}{\sqrt{b}} + \frac{q_{33}}{\sqrt{a}\sqrt{b}}}\right)\Big/K$$

will be a Q_8-extension containing $K(\sqrt{a}, \sqrt{b})/K$. In fact, we only have to notice that we can let $\mathbf{P} = \mathbf{S}^{-1} = \langle 1/a, 1/b, 1/ab\rangle \mathbf{S}^t$.

These two versions of the result inspire the following:

Let $M = K(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ be a $V_4 \times V_4$-extension, and let ρ, σ, τ and υ in $\mathrm{Gal}(M/K) = V_4 \times V_4$ be given by

$$\begin{aligned}
\rho\colon&\quad \sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c}, \quad \sqrt{d} \mapsto \sqrt{d},\\
\sigma\colon&\quad \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto -\sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c}, \quad \sqrt{d} \mapsto \sqrt{d},\\
\tau\colon&\quad \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto -\sqrt{c}, \quad \sqrt{d} \mapsto \sqrt{d},\\
\upsilon\colon&\quad \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c}, \quad \sqrt{d} \mapsto -\sqrt{d}.
\end{aligned}$$

Then the obstruction to the embedding problem given by M/K and

$$1 \to \mu_2 \to QQ \xrightarrow[\substack{i\mapsto\rho\\ j\mapsto\sigma\\ i'\mapsto\tau\\ j'\mapsto\upsilon}]{} V_4 \times V_4 \to 1$$

is

$$(-1,-1)(-a,-b)(-1,-1)(-c,-d) = (-a,-b)(-c,-d) \in \mathrm{Br}(K),$$

i.e., the embedding problem is solvable, if and only if the quadratic forms $\langle a, b, ab\rangle$ and $\langle c, d, cd\rangle$ are equivalent.

2.2. THE CENTRAL PRODUCT $\boldsymbol{QQ}$. *Let M/K be a $V_4 \times V_4$-extension as above, and consider the embedding problem given by M/K and*

$$1 \to \mu_2 \to QQ \to V_4 \times V_4 \to 1.$$

This embedding problem is solvable, if and only if the quadratic forms $\langle a, b, ab\rangle$ and $\langle c, d, cd\rangle$ are equivalent over K. Furthermore, if $\mathbf{P}$ is a 3×3 matrix over K with determinant cd/ab expressing this equivalence, i.e.,

$$\mathbf{P}^t \langle a, b, ab\rangle \mathbf{P} = \langle c, d, cd\rangle,$$

the solutions are

$$M\left(\sqrt{r\left(1 + p_{11}\frac{\sqrt{a}}{\sqrt{c}} + p_{22}\frac{\sqrt{b}}{\sqrt{d}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}\sqrt{d}}\right)}\right) \Big/ K, \quad r \in K^*.$$

PROOF. Assume $\langle a, b, ab\rangle \sim \langle c, d, cd\rangle$. This means that

$$\mathbf{P}^t \langle a, b, ab\rangle \mathbf{P} = \langle c, d, cd\rangle$$

for some 3×3 matrix $\mathbf{P}$ with determinant cd/ab. From this we get the additional equations $\langle 1/c, 1/d, 1/cd\rangle \mathbf{P}^t \langle a, b, ab\rangle = \mathbf{P}^{-1}$ and $\mathbf{P}\langle 1/c, 1/d, 1/cd\rangle \mathbf{P}^t = \langle 1/a, 1/b, 1/ab\rangle$, and thus (calculating the diagonal elements)

$$\begin{aligned}
&ap_{11}^2 + bp_{21}^2 + abp_{31}^2 = c,\\
&ap_{12}^2 + bp_{22}^2 + abp_{32}^2 = d,\\
&ap_{13}^2 + bp_{23}^2 + abp_{33}^2 = cd,\\
&p_{11} = b/d\,(p_{22}p_{33} - p_{23}p_{32}),\\
&p_{22} = a/c\,(p_{11}p_{33} - p_{13}p_{31}),\\
&p_{33} = p_{11}p_{22} - p_{12}p_{21},\\
&p_{11}^2/c + p_{12}^2/d + p_{13}^2/cd = 1/a,\\
&p_{21}^2/c + p_{22}^2/d + p_{23}^2/cd = 1/b,\\
\text{and}\quad &p_{31}^2/c + p_{32}^2/d + p_{33}^2/cd = 1/ab.
\end{aligned}$$

Now, let

$$\omega = 1 + p_{11}\frac{\sqrt{a}}{\sqrt{c}} + p_{22}\frac{\sqrt{b}}{\sqrt{d}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}\sqrt{d}}.$$

Then

$$\begin{aligned}
\omega\,\rho\omega &= \omega\,\tau\omega\\
&= \big(1 + p_{22}\sqrt{b}/\sqrt{d}\big)^2 - a/c\big(p_{11} + p_{33}\sqrt{b}/\sqrt{d}\big)^2\\
&= \big(1 + b/d\,p_{22}^2 - a/c\,p_{11}^2 - ab/cd\,p_{33}^2\big) + 2\big(p_{22} - a/c\,p_{11}p_{33}\big)\sqrt{b}/\sqrt{d}\\
&= \big(b/c\,p_{21}^2 + ab/c\,p_{31}^2 + b/d\,p_{22}^2 - ab/cd\,p_{33}^2\big) - 2a/c\,p_{13}p_{31}\sqrt{b}/\sqrt{d}\\
&= \big(1 - b/cd\,p_{23}^2 + ab/c\,p_{31}^2 - ab/cd\,p_{33}^2\big) - 2a/c\,p_{13}p_{31}\sqrt{b}/\sqrt{d}\\
&= \big(a/cd\,p_{13}^2 + ab/c\,p_{31}^2\big) - 2a/c\,p_{13}p_{31}\sqrt{b}/\sqrt{d}\\
&= a/c\big(p_{13}/\sqrt{d} - p_{31}\sqrt{b}\big)^2.
\end{aligned}$$

Hence, with

$$a_\rho = a_\tau = \frac{\sqrt{a}}{\omega\sqrt{c}}\left(\frac{p_{13}}{\sqrt{d}} - p_{31}\sqrt{b}\right),$$

we get

$$\frac{\rho\omega}{\omega} = \frac{\tau\omega}{\omega} = a_\rho^2 = a_\tau^2.$$

Clearly,

$$a_\rho\,\rho a_\rho = a_\rho\,\rho a_\tau = a_\tau\,\tau a_\rho = a_\tau\,\tau a_\tau = -1.$$

Similarly,

$$\omega\sigma\omega = \omega\upsilon\omega = b/d\big(p_{23}/\sqrt{c} - p_{32}\sqrt{a}\,\big)^2,$$

and we get

$$\frac{\sigma\omega}{\omega} = \frac{\upsilon\omega}{\omega} = a_\sigma^2 = a_\upsilon^2$$

by letting

$$a_\sigma = a_\upsilon = \frac{\sqrt{b}}{\omega\sqrt{d}}\left(\frac{p_{23}}{\sqrt{c}} - p_{32}\sqrt{a}\right).$$

We then have

$$a_\sigma\,\sigma a_\sigma = a_\sigma\,\sigma a_\upsilon = a_\upsilon\,\upsilon a_\sigma = a_\upsilon\,\upsilon a_\upsilon = -1.$$

Also,

$$\begin{aligned}
\frac{a_\sigma\,\sigma a_\rho}{a_\rho\,\rho a_\sigma} &= \frac{\sqrt{b}\sqrt{c}\,\omega\big(p_{23}/\sqrt{c} - p_{32}\sqrt{a}\,\big)\sqrt{a}\sqrt{d}\,\rho\omega\big(p_{13}/\sqrt{d} + p_{31}\sqrt{b}\,\big)}{\sqrt{a}\sqrt{d}\,\omega\big(p_{13}/\sqrt{d} - p_{31}\sqrt{b}\,\big)\sqrt{b}\sqrt{c}\,\sigma\omega\big(p_{23}/\sqrt{c} + p_{32}\sqrt{a}\,\big)} \\
&= \frac{a/c\big(p_{13}/\sqrt{d} - p_{31}\sqrt{b}\,\big)^2\big(p_{23}/\sqrt{c} - p_{32}\sqrt{a}\,\big)\big(p_{13}/\sqrt{c} + p_{31}\sqrt{b}\,\big)}{b/d\big(p_{23}/\sqrt{c} - p_{32}\sqrt{a}\,\big)^2\big(p_{13}/\sqrt{d} - p_{31}\sqrt{b}\,\big)\big(p_{23}/\sqrt{c} - p_{32}\sqrt{a}\,\big)} \\
&= \frac{ad}{bc}\,\frac{p_{13}^2/d - p_{31}^2 b}{p_{23}^2/d - p_{32}^2 b} = \frac{ap_{13}^2 - abdp_{31}^2}{bp_{23}^2 - abcp_{32}^2} \\
&= \frac{\big(cd - bp_{23}^2 - abp_{33}^2\big) - \big(cd - abcp_{32}^2 - abp_{33}^2\big)}{bp_{23}^2 - abcp_{32}^2} = -1,
\end{aligned}$$

from which it easily follows that

$$\frac{a_\rho\,\rho a_\upsilon}{a_\upsilon\,\upsilon a_\rho} = -\frac{a_\rho\,\rho a_\sigma}{a_\sigma\,\sigma a_\rho} = 1,$$

$$\frac{a_\sigma\,\sigma a_\tau}{a_\tau\,\tau a_\sigma} = -\frac{a_\sigma\,\sigma a_\rho}{a_\rho\,\rho a_\sigma} = 1,$$

and

$$\frac{a_\tau\,\tau a_\upsilon}{a_\upsilon\,\upsilon a_\tau} = -\frac{a_\tau\,\tau a_\sigma}{a_\sigma\,\sigma a_\tau} = -1.$$

Consequently,

$$M(\sqrt{\omega}\,)/K = M\left(\sqrt{1 + p_{11}\frac{\sqrt{a}}{\sqrt{c}} + p_{22}\frac{\sqrt{b}}{\sqrt{d}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}\sqrt{d}}}\right)\Bigg/K$$

is a solution to the embedding problem.

It should be noted that the groups QQ and DD are in fact isomorphic, and that 2.2 and 1.3 are therefore simply different ways of expressing and solving the same embedding problem.

We also note that $K(\omega) = K(\sqrt{a}/\sqrt{c}, \sqrt{b}/\sqrt{d})$, from which it easily follows that $M(\sqrt{\omega})/K$ is the Galois closure of $K(\sqrt{\omega})/K$.

The proof of 2.2 is easily changed to give

2.3. THE CENTRAL PRODUCT $\boldsymbol{QC}$. *Let $M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$, $a, b, c \in K^*$, be a $V_4 \times C_2$-extension, and let $\sigma, \tau, \upsilon \in \mathrm{Gal}(M/K)$ be given by*

$$\begin{aligned}
\sigma\colon&\ \sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c},\\
\tau\colon&\ \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto -\sqrt{b}, \quad \sqrt{c} \mapsto \sqrt{c},\\
\upsilon\colon&\ \sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \quad \sqrt{c} \mapsto -\sqrt{c}.
\end{aligned}$$

Then the embedding problem given by M/K and

$$1 \to \mu_2 \to QC \xrightarrow[\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau\\ x\mapsto\upsilon}]{} V_4 \times C_2 \to 1$$

is solvable, if and only if the quadratic forms $\langle a, b, ab\rangle$ and $\langle 1, c, c\rangle$ are equivalent over K. If $\mathbf{P}$ is a 3×3 matrix over K expressing this equivalence, i.e., if

$$\mathbf{P}^t \langle a, b, ab\rangle \mathbf{P} = \langle 1, c, c\rangle,$$

we can assume $\det \mathbf{P} = c/ab$, *and the solutions are then*

$$M\left(\sqrt{r\left(1 + p_{11}\sqrt{a} + p_{22}\frac{\sqrt{b}}{\sqrt{c}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}}\right)}\right), \quad r \in K^*.$$

The groups QC and DC are isomorphic, and so 2.3 and 1.2 really deal with the same embedding problem.

It is fairly obvious that $M(\sqrt{r\omega})/K$ is the Galois closure of $K(\sqrt{r\omega})/K$. A more direct use of Witt's result is the following: Let $M/K = K\left(\sqrt{\theta}, \sqrt{b}\right)/K$, $\theta = r(\alpha + \beta\sqrt{a})$ be a D_4-extension as in 0.4, and let QD_8 be the quasi-dihedral group of order 16, i.e., QD_8 is generated by elements u and v with relations $u^4 = v^2$ and $vu = u^3 v$. We then have an embedding problem given by M/K and

$$1 \to \mu_2 \to QD_8 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \to 1.$$

By [10, Prop. 4.2], the obstruction to this embedding problem is

$$(-b, -2r\alpha)(-a, -2) \in \mathrm{Br}(K).$$

Assuming $\alpha \neq 0$, the embedding problem is thus 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, i.e., if and only if there exists a matrix $\mathbf{P}$ over K, such that

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

We may assume $\det \mathbf{P} = a/br\alpha$.

Now, the subgroup of QD_8 generated by u^2 and v is isomorphic to Q_8, and so we get the restricted embedding problem given by $M/K(\sqrt{a})$ and

$$1 \to \mu_2 \to Q_8 \to V_4 \to 1.$$

We have $M = K(\sqrt{a})\big(\sqrt{\theta}, \sigma\sqrt{\theta}\big)$ and $\theta\,\sigma\theta = r^2ab$. Hence, to solve the restricted embedding problem by Witt's Theorem, we must find a matrix $\mathbf{S}$ with determinant $1/r^2ab$ expressing the equivalence of $\langle r^2ab, \theta, \sigma\theta\rangle$ and $\langle 1, 1, 1\rangle$ over $K(\sqrt{a})$.[3] This is done by letting

$$\mathbf{S} = \begin{pmatrix} 1/r\sqrt{a} & 0 & 0 \\ 0 & 1 & \sigma\theta/r\sqrt{a} \\ 0 & 1 & -\theta/r\sqrt{a} \end{pmatrix} \mathbf{P} \begin{pmatrix} 1/\sqrt{a} & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2\sqrt{a} & -1/2\sqrt{a} \end{pmatrix}.$$

Hence, a solution to the restricted embedding problem is obtained by adjoining $\sqrt{\omega}$, where

$$\begin{aligned}
\omega &= 1 + s_{11}r\sqrt{a}\sqrt{b} + s_{22}\sqrt{\theta} + s_{33}\,\sigma\sqrt{\theta} \\
&= 1 + p_{11}\sqrt{b}/\sqrt{a} + \tfrac{1}{2}\big[\big(p_{22} + p_{23}/\sqrt{a}\big) + \big(p_{32} + p_{33}/\sqrt{a}\big)\,\sigma\theta/r\sqrt{a}\,\big]\sqrt{\theta} \\
&\qquad + \tfrac{1}{2}\big[\big(p_{22} - p_{23}/\sqrt{a}\big) - \big(p_{32} - p_{33}/\sqrt{a}\big)\,\theta/r\sqrt{a}\,\big]\sigma\sqrt{\theta} \\
&= 1 + p_{11}\sqrt{b}/\sqrt{a} + \tfrac{1}{2}\big[p_{22} + p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}\,\big]\sqrt{\theta} \\
&\qquad + \tfrac{1}{2}\big[p_{22} - p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}\,\big]\sigma\sqrt{\theta}.
\end{aligned}$$

As $\sigma\tau(\sigma\sqrt{\theta}) = \sqrt{\theta}, \sigma\tau\omega = \omega$, and so $M(\sqrt{\omega})/K$ is Galois. Furthermore, the pre-images of $\sigma\tau$ in $\mathrm{Gal}(M(\sqrt{\omega})/K)$ have order 2, and so the Galois group is the quasi-dihedral group. Hence, $M(\sqrt{\omega})/K$ is a solution to the embedding problem.

We summarise:

[3] By Theorem 2.1, it should of course be $\langle\theta, \sigma\theta, r^2ab\rangle$ and $\langle 1, 1, 1\rangle$. However, this makes no difference: Permuting the rows and columns of $\mathbf{S}$ cyclically will not change the determinant.

2.4. THE QUASI-DIHEDRAL GROUP $\boldsymbol{QD_8}$, GENERAL CASE. *Let $M/K = K(\sqrt{\theta}, \sqrt{b})/K$ be a D_4-extension as above, and assume $\alpha \neq 0$. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to QD_8 \xrightarrow[\substack{u\mapsto\sigma\\ v\mapsto\tau}]{} D_4 \to 1$$

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 $\mathbf{P}$, i.e., if

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

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

$$M(\sqrt{s\omega})/K = K(\sqrt{s\omega}, \sqrt{a})/K, \quad s \in K^*,$$

where

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

$\sqrt{s\omega}$ is not a primitive element of $M(\sqrt{s\omega})/K$, since ω has degree 4 over K. However, it is clear that M/K is the Galois closure of $K(\omega)/K$, and hence that $M(\sqrt{s\omega})/K$ is the Galois closure of $K(\sqrt{s\omega})/K$.

QD_8 as Galois group is considered in [8] and [5].

EXAMPLE. Let $K = \mathbb{Q}$, $a = 3$, $b = 2$, $\alpha = 3$, $\beta = 1$ and $r = 1$. The D_4-extension is then $\mathbb{Q}\big(\sqrt{3+\sqrt{3}}, \sqrt{2}\big)/\mathbb{Q}$, and the quadratic forms $\langle 3, 2, 6\rangle$ are $\langle 2, 6, 12\rangle$ are obviously equivalent. We can let

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}$$

and get

$$\omega = 1 + \left(\frac{1}{2\sqrt{3}} + \frac{1}{2\sqrt{6}} - \frac{1}{2\sqrt{2}}\right)\sqrt{3+\sqrt{3}}.$$

Thus, the QD_8-extensions containing $\mathbb{Q}\big(\sqrt{3+\sqrt{3}}, \sqrt{2}\big)/\mathbb{Q}$ are

$$\mathbb{Q}\left(\sqrt{r\left(1 + \left(\frac{1}{2\sqrt{3}} + \frac{1}{2\sqrt{6}} - \frac{1}{2\sqrt{2}}\right)\sqrt{3+\sqrt{3}}\right)}, \sqrt{3}\right)\Big/\mathbb{Q}, \qquad r \in \mathbb{Q}^*.$$

Now, if $\alpha = 0$, we may assume $b = -1$ and $\beta = 1$, replace a by r^2a and get $M = K(\sqrt[4]{a}, i)$ for $i = \sqrt{-1}$. We can then let $\sigma, \tau \in D_4 = \mathrm{Gal}(M/K)$ be given by $\sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$, $\sigma i = i$, $\tau\sqrt[4]{a} = \sqrt[4]{a}$ and $\tau i = -i$. The obstruction is as above, except that $(-b, -2r\alpha) = 1$, and so the embedding problem is solvable, if and only if

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

Let $\omega = (1+i)(p + qi\sqrt{a})\sqrt[4]{a}$, $a_\sigma = (1-i)/(p + qi\sqrt{a})$ and $a_\tau = (1+i)/(p + qi\sqrt{a})$. Then $\sigma\omega/\omega = a_\sigma^2$ and $\tau\omega/\omega = a_\tau^2$, i.e., $M(\sqrt{\omega})/K$ is Galois. And since

$$a_\sigma\, \sigma a_\sigma\, \sigma^2 a_\sigma\, \sigma^3 a_\sigma = -1, \quad a_\tau\, \tau a_\tau = -1, \quad a_\sigma\, \sigma a_\sigma\, \sigma^2 a_\sigma\, \sigma^3 a_\tau = a_\tau\, \tau a_\sigma,$$

$M(\sqrt{\omega})/K$ is a solution to the embedding problem.

Hence, we have

2.5. THE QUASI-DIHEDRAL GROUP $\boldsymbol{QD_8}$, SPECIAL CASE. *Let $M/K = K(\sqrt[4]{a}, i)/K$ be a D_4-extension. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to QD_8 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \to 1$$

is solvable, if and only if

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

The solutions are then

$$M\left(\sqrt{r(1+i)\left(p + qi\sqrt{a}\right)\sqrt[4]{a}}\right)\Big/K$$
$$= K\left(\sqrt{r(1+i)\left(p + qi\sqrt{a}\right)\sqrt[4]{a}},\, i\right)\Big/K, \quad r \in K^*.$$

3. Groups of exponent 8

In 2.4, the D_4-extension M of K is a C_4-extension of $K(\sqrt{b})$. Also, the QD_8-extension is C_8 over $K(\sqrt{b})$. Thus, we have in particular embedded a C_4-extension in a C_8-extension. We remember from section 0 that a C_4-extension is, loosely speaking, just a D_4-extension with $b = 1$. It is therefore plausible that we might solve the problem of embedding a C_4-extension in a C_8-extension by 'letting $b = 1$' in 2.4. And in fact we can:

Let $M/K = K(\sqrt{\theta})/K$, $\theta = r(\alpha + \beta\sqrt{a})$, be a C_4-extension as in 0.2. The obstruction to embedding M/K in a C_8-extension is represented by the

cyclic algebra $\Gamma = M[u_\sigma]$, where $u_\sigma^4 = -1$ and $u_\sigma x = \sigma x\, u_\sigma$ for $x \in M$. Letting $Q = K[u_\sigma + u_\sigma^3, \sqrt{a}\, u_\sigma^2]$ and $R = K[u_\sigma^2, \sqrt{\theta}\, u_\sigma + \sigma\sqrt{\theta}\, u_\sigma^3]$ we see that $\Gamma = Q \otimes_K R$, $Q \simeq (-2, -a/K)$ and $R \simeq (-1, 2r\alpha/K)$. Hence, the obstruction is

$$(-2, -a)(-1, -2r\alpha) \in \mathrm{Br}(K).$$

3.1. THE CYCLIC GROUP $\boldsymbol{C_8}$, GENERAL CASE. *Let $M/K = K\big(\sqrt{\theta}\,\big)/K$ be a C_4-extension as above, and assume $\alpha \neq 0$. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to C_8 \to C_4 \to 1$$

is solvable, if and only if the quadratic forms $\langle 1, 2r\alpha, 2r\alpha\rangle$ and $\langle a, 2, 2a\rangle$ are equivalent over K. If the equivalence is expressed by the matrix $\mathbf{P}$, i.e., if

$$\mathbf{P}^t \langle 1, 2r\alpha, 2r\alpha\rangle \mathbf{P} = \langle a, 2, 2a\rangle,$$

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

$$M(\sqrt{s\omega}\,)/K = K(\sqrt{s\omega}\,)/K, \qquad s \in K^*,$$

where

$$\omega = 1 + p_{11}/\sqrt{a} + \tfrac{1}{2}\big[(p_{22} - p_{32}) + (p_{23} + p_{33})/\sqrt{a}\,\big]\sqrt{\theta} + \tfrac{1}{2}\big[(p_{22} + p_{32}) - (p_{23} - p_{33})/\sqrt{a}\,\big]\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

PROOF. We derive $\mathbf{S}$ from $\mathbf{P}$ as in the proof of 2.4 to get

$$\mathbf{S}^t \langle r^2 a, \theta, \sigma\theta\rangle \mathbf{S} = \mathbf{E}$$

and $\det \mathbf{S} = 1/r^2 a$. Also,

$$\omega = 1 + s_{11} r\sqrt{a} + s_{22}\sqrt{\theta} + s_{33}\,\sigma\sqrt{\theta}.$$

Noting that $s_{33} = \sigma s_{22}$, we get

$$\sigma\omega = 1 - s_{11} r\sqrt{a} - s_{22}\sqrt{\theta} + s_{33}\,\sigma\sqrt{\theta},$$

and by using various equalities (as in the proof of 2.2), we get

$$\omega\,\sigma\omega = r^2 a\big(s_{12} - s_{21}/\sigma\sqrt{\theta}\,\big)^2.$$

Hence, $M(\sqrt{\omega}\,)/K$ is Galois. Also,

$$\omega\,\sigma^2\omega = \big(s_{23}\sqrt{\theta} - s_{32}\,\sigma\sqrt{\theta}\,\big)^2,$$

and letting

$$x = \frac{s_{23}\sqrt{\theta} - s_{32}\,\sigma\sqrt{\theta}}{\omega}$$

we get $\sigma^2\omega/\omega = x^2$ and $x\,\sigma^2 x = -1$. Hence, $M(\sqrt{\omega})/K(\sqrt{a})$ is C_4, and it follows that $M(\sqrt{\omega})/K$ is C_8.

Cyclic extensions of degree 8 are considered in [8].

If $\alpha = 0$, we must have $i \in K^*$, and can assume $M/K = K(\sqrt[4]{a})/K$ and $\sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$. The quaternion factor $(-1, -2r\alpha)$ disappears, and so the obstruction is $(-2, -a) = (2, a) \in \mathrm{Br}(K)$, and the embedding problem is solvable, if and only if

$$\exists p, q \in K\colon p^2 - aq^2 = 2.$$

We let

$$\omega = \left(p + q\sqrt{a}\right)\sqrt[4]{a}$$

and

$$a_\sigma = \frac{1+i}{p+q\sqrt{a}}$$

and get $\sigma\omega/\omega = a_\sigma^2$ and $a_\sigma\,\sigma a_\sigma\,\sigma^2 a_\sigma\,\sigma^2 a_\sigma = -1$. Thus, $M(\sqrt{\omega})/K$ is a solution, and we have

3.2. THE CYCLIC GROUP $\boldsymbol{C_8}$, SPECIAL CASE. *Assume $i \in K^*$, and let $M/K = K(\sqrt[4]{a})/K$ be a C_4-extension. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to C_8 \to C_4 \to 1$$

is solvable, if and only if

$$\exists p, q \in K\colon p^2 - aq^2 = 2,$$

and the solutions are then

$$M\left(\sqrt{r\left(p+q\sqrt{a}\right)\sqrt[4]{a}}\right)\Big/K = K\left(\sqrt{r\left(p+q\sqrt{a}\right)\sqrt[4]{a}}\right)\Big/K, \qquad r \in K^*.$$

We can now use reduction to 3.2 on other embedding problem in the same way we reduced QD_8 to Q_8 in 2.4:

Let D_8 be the dihedral group of order 16, i.e., D_8 is generated by elements σ and τ with relations $\sigma^8 = \tau^2 = 1$ and $\tau\sigma = \sigma^7\tau$.

3.3. THE DIHEDRAL GROUP $\boldsymbol{D_8}$, GENERAL CASE. *Let $M/K = K\big(\sqrt{\theta}, \sqrt{b}\big)/K$ be a D_4-extension as in* 0.4 *and* 2.4*, and assume $\alpha \neq 0$. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to D_8 \to D_4 \to 1$$

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 $\mathbf{P}$, i.e., if

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

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

$$M(\sqrt{s\omega})/K = K\big(\sqrt{s\omega}, \sqrt{b}\big)\big/K, \qquad s \in K^*,$$

where

$$\omega = 1 - p_{11}/\sqrt{a} + \tfrac{1}{2}\big(p_{32} + p_{23}/\sqrt{a}\big)\sqrt{\theta} + \tfrac{1}{2}\big(p_{22}/b - p_{33}/\sqrt{a}\big)\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

D_8 as Galois group is considered in [8] and [5].

PROOF. By [10, Prop. 4.2], the obstruction to the embedding problem is

$$(-ab, -2a)(-b, -r\alpha) \in \mathrm{Br}(K).$$

This gives the criterion.

We now restrict ourselves to the embedding problem given by $M/K(\sqrt{b})$ and

$$1 \to \mu_2 \to C_8 \to C_4 \to 1.$$

$M/K(\sqrt{b})$ has the form required in 3.1, if we replace r, α and β by $r' = r\sqrt{b}$, $\alpha' = \alpha/\sqrt{b}$ and $\beta' = \beta/\sqrt{b}$. Also, letting

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

we get

$$\mathbf{P}'^t\langle 1, 2r\alpha, 2r\alpha\rangle\mathbf{P}' = \langle a, 2, 2a\rangle$$

and $\det \mathbf{P}' = a/r\alpha$. The ω given above is then exactly the one from 3.1, and so $M(\sqrt{\omega})/K(\sqrt{b})$ is C_8. Furthermore, $M(\sqrt{\omega})/K$ is Galois, since $\tau\omega = \omega$, and it is not hard to see that the Galois group is in fact D_8.

$\sqrt{s\omega}$ is not a primitive element of $M(\sqrt{s\omega})/K$, but it is clear that $M(\sqrt{s\omega})/K$ is the Galois closure of $K(\sqrt{s\omega})/K$.

3.4. THE DIHEDRAL GROUP $\boldsymbol{D_8}$, SPECIAL CASE. *Let* $M/K = K\big(\sqrt[4]{a}, i\big)/K$ *be a* D_4*-extension as in* 2.5. *Then the embedding problem given by* M/K *and*

$$1 \to \mu_2 \to D_8 \to D_4 \to 1$$

is solvable, if and only if

$$\exists p, q \in K\colon p^2 - aq^2 = 2.$$

In that case, the solutions are

$$M\Big(\sqrt{r\big(p+q\sqrt{a}\big)\sqrt[4]{a}}\Big)\Big/K = K\Big(\sqrt{r\big(p+q\sqrt{a}\big)\sqrt[4]{a}},\, i\Big)\Big/K, \quad r \in K^*.$$

Now, let $M/K = K\big(\sqrt{\theta}, \sqrt{b}\big)/K$ be a $C_4 \times C_2$-extension, i.e., $K\big(\sqrt{\theta}\big)/K$ is a C_4-extension as above, $K(\sqrt{b})/K$ is a C_2-extension, and $\sqrt{b} \notin K\big(\sqrt{\theta}\big)$. As generators for $C_4 \times C_2 = \mathrm{Gal}(M/K)$ we choose σ and τ, given by

$$\begin{aligned} \sigma\colon &\quad \sqrt{\theta} \mapsto \tfrac{\alpha-\beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}, &&\quad \sqrt{b} \mapsto \sqrt{b}, \\ \tau\colon &\quad \sqrt{\theta} \mapsto \sqrt{\theta}, &&\quad \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

We then have an embedding problem given by M/K and

$$1 \to \mu_2 \to M_{16} \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} C_4 \times C_2 \to 1,$$

where M_{16} is the modular group of order 16, i.e., M_{16} is generated by elements u and v with relations $u^8 = v^2 = 1$ and $vu = u^5 v$.

By [10, Prop. 3.2], the obstruction to this embedding problem is

$$(-2, -a)(-1, -2r\alpha)(a, b) = (-2b, -a)(-1, -2br\alpha) \in \mathrm{Br}(K).$$

3.5. THE MODULAR GROUP $\boldsymbol{M_{16}}$, GENERAL CASE. *Let* $M/K = K\big(\sqrt{\theta}, \sqrt{b}\big)/K$ *be a* $C_4 \times C_2$*-extension as above, and assume* $\alpha \neq 0$. *Then the embedding problem given by* M/K *and*

$$1 \to \mu_2 \to M_{16} \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} C_4 \times C_2 \to 1$$

is solvable if and only if the quadratic forms $\langle 1, 2br\alpha, 2br\alpha\rangle$ *and* $\langle a, 2b, 2ab\rangle$ *are equivalent over* K. *If this equivalence is expressed by the matrix* $\mathbf{P}$, *i.e., if*

$$\mathbf{P}^t\langle 1, 2br\alpha, 2br\alpha\rangle\mathbf{P} = \langle a, 2b, 2ab\rangle,$$

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

$$M(\sqrt{r\omega})/K = K\big(\sqrt{s\omega}, \sqrt{b}\big)\big/K, \quad \in K^*,$$

where

$$\omega = 1 + p_{11}/\sqrt{a} + \tfrac{1}{2}\big[p_{22} + p_{23}/\sqrt{a} - p_{32} + p_{33}/\sqrt{a}\,\big]\sqrt{\theta} + \tfrac{1}{2}\big[p_{22} - p_{23}/\sqrt{a} + p_{32} + p_{33}/\sqrt{a}\,\big]\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

PROOF. The criterion comes directly from the obstruction. Now, letting

$$\mathbf{P}' = \langle 1, \sqrt{b}, \sqrt{b}\rangle\mathbf{P}\langle 1, 1/\sqrt{b}, 1/\sqrt{b}\rangle,$$

we have

$$\mathbf{P}'^t\langle 1, 2r\alpha, 2r\alpha\rangle\mathbf{P}' = \langle a, 2, 2a\rangle$$

and $\det\mathbf{P}' = a/r\alpha$. Thus, by 3.1, $M(\sqrt{\omega})/K(\sqrt{b})$ is a C_8-extension, and $\sigma\omega/\omega = a_\sigma^2$, where

$$a_\sigma = \frac{r\sqrt{a}\big(s_{12} - s_{21}/\sigma\sqrt{\theta}\,\big)}{\omega},$$

$$s_{12} = \frac{p_{12} + p_{13}/\sqrt{a}}{2r\sqrt{a}\sqrt{b}},$$

$$\text{and} \qquad s_{21} = \frac{\sqrt{b}}{\sqrt{a}}\left(p_{21} + p_{31}\frac{\sigma\theta}{r\sqrt{a}}\right).$$

With $a_\tau = 1$ we get $\tau\omega/\omega = a_\tau^2$. Also, $a_\sigma\,\sigma a_\sigma\,\sigma^2 a_\sigma\,\sigma^3 a_\sigma = -1$, $a_\tau\,\tau a_\tau = 1$ and $a_\sigma\,\sigma a_\tau = -a_\tau\,\tau a_\sigma$. Hence, $M(\sqrt{\omega})/K$ is a solution.

M_{16} as Galois group is also considered in [5].

If $\alpha = 0$, we must have $i \in K^*$, and can thus assume $M = K\big(\sqrt[4]{a}, \sqrt{b}\big)$. The elements σ and τ in $C_4 \times C_2$ are then given by

$$\sigma\colon \quad \sqrt[4]{a} \mapsto i\sqrt[4]{a}, \quad \sqrt{b} \mapsto \sqrt{b},$$
$$\tau\colon \quad \sqrt[4]{a} \mapsto \sqrt[4]{a}, \quad \sqrt{b} \mapsto -\sqrt{b},$$

and the obstruction to the embedding problem is $(-2a, -a) = (a, 2b) \in \mathrm{Br}(K)$.

3.6. THE MODULAR GROUP M_{16}, SPECIAL CASE. *Assume $i \in K^*$, and let $M/K = K\left(\sqrt[4]{a}, \sqrt{b}\right)/K$ be a $C_4 \times C_2$-extension as above. Then the embedding problem given by M/K and*

$$1 \to \mu_2 \to M_{16} \xrightarrow[\substack{v \mapsto \sigma \\ v \mapsto \tau}]{} C_4 \times C_2 \to 1$$

is solvable, if and only if

$$\exists p, q \in K\colon p^2 - aq^2 = 2b.$$

In this case the solutions are

$$M\left(\sqrt{r\left(p + q\sqrt{a}\right)\sqrt[4]{a}}\right)\Big/K = K\left(\sqrt{r\left(p + q\sqrt{a}\right)\sqrt[4]{a}}, \sqrt{b}\right)\Big/K, \quad r \in K^*.$$

PROOF. We let $a_\sigma = (1 + i)\sqrt[4]{a}/(p + q\sqrt{a})$ and $a_\tau = 1$.

ACKNOWLEDGMENTS. Thanks to S. Abhyankar for asking the questions that led to this paper. (Although, unfortunately, this paper does not in fact answer his questions.) Also, thanks to N. Yui for reading and commenting on the first versions of paper.

This work was supported by a Queen's University Advisory Research Committee Postdoctoral Fellowship.

REFERENCES

1. Albert, A. A., *Modern Higher Algebra*, Cambridge University Press, 1938.
2. Crespo, T., *Explicit Contruction of $\tilde{A}_n$ Type Fields*, J. Algebra, 127 (1989), 452–461.
3. Crespo, T., *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. 409 (1990), 180–189.
4. Fröhlich, A., *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. 360 (1985), 84–123.
5. Grundman, H. G., Smith, T. L. and Swallow, J. R., *Groups of order* 16 *as Galois groups*, Exposition. Math. 13 (1995), 289–319.
6. Jacobson, N., *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.
7. Jensen, C. U. and Yui, N., *Quaternion Extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, Kinokuniya, Tokyo, 1987, 155–182.
8. Kiming, I., *Explicit Classifications of some* 2*-Extensions of a Field of Characteristic different from* 2, Canad. J. Math. 42 (1990), 825–855.
9. Lam, T. Y., *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
10. Ledet, A., *On* 2*-Groups as Galois Groups*, Canad. J. Math. 47 (1995), 1253–1273.

11. Lorenz, F., *Einführung in die Algebra II*, B. I. Wissenschaftsverlag, Mannheim, 1990.
12. Mináč, J. and Smith, T. L., *A characterization of C-fields via Galois groups*, J. Algebra 137 (1991), 1–11.
13. Schneps, Leila, *Explicit Realisations of Subgroups of* $\mathrm{GL}_2(\mathbf{F}_3)$ *as Galois Groups*, J. Number Theory 39 (1991), 5–13.
14. Smith, T. L., *Extra-special groups of order* 32 *as Galois groups*, Canad. J. Math. 46 (1994), 886–896.
15. Swallow, J. R., *Solutions to central embedding problems are constructible*, J. Algebra 184 (1996), 1041–1051.
16. Witt, E., *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung* p^f, J. Reine Angew. Math. 174 (1936), 237–245.

DEPARTMENT OF MATHEMATICS AND STATISTICS
QUEEN'S UNIVERSITY
KINGSTON, ONTARIO K7L 3N6
CANADA
E-mail: ledet@mast.queensu.ca