ISRAEL JOURNAL OF MATHEMATICS 106 (1998), 109–131

EMBEDDING PROBLEMS WITH CYCLIC KERNEL OF ORDER 4

BY

ARNE LEDET

Department of Mathematics, Queen's University
Kingston, Ontario K7L 3N6, Canada
e-mail: ledet@mast.queensu.ca

ABSTRACT

We consider Galois theoretical embedding problems with kernel C_4, and prove that such an embedding problem can be 'constructively' reduced to two embedding problems, where the kernels are groups of roots of unity.

1. Introduction

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

$$(1.1) \qquad 1 \to N \to E \underset{\pi}{\to} G \to 1$$

be an extension of G with the finite group N. It is then natural to ask whether there exists a Galois extension F/K with $M \subseteq F$ and an isomorphism $\varphi : \mathrm{Gal}(F/K) \to E$, such that $\pi \circ \varphi = \mathrm{res}$, where res: $\mathrm{Gal}(F/K) \to \mathrm{Gal}(M/K)$ is the restriction map. This is the *(Galois theoreticalm) embedding problem* given by M/K and (1.1). A Galois extension F/K with the described properties is called a **proper solution** to the embedding problem. A Galois extension F/K with $M \subseteq F$ is called a **(weak) solution** to the embedding problem, if there exists a monomorphism φ: $\mathrm{Gal}(F/K) \hookrightarrow E$, such that $\pi \circ \varphi = \mathrm{res}$. The group N is called the **kernel** of the embedding problem.

In this paper, we will consider embedding problems with cyclic kernel of order 4 over a field of characteristic $\neq 2$. In particular, we will assume all fields to have characteristic $\neq 2$. The central result is Theorem 1.1 below, where the embedding

Received January 12, 1997

problem is reduced to two simpler embedding problems. In order to formulate Theorem 1.1, we need to introduce some notation:

Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$, and assume that $i = \sqrt{-1}$ is in M. Also, let

$$1 \to C_4 \to E \underset{\pi}{\to} G \to 1, \tag{1.2}$$

be a group extension, where C_4 is the cyclic group of order 4.

We identify C_4 (as an abstract group) with the group μ_4 of primitive fourth roots of unity. We then have two G-module actions on $\mu_4 = C_4$: The Galois action of G on μ_4, which we will write as $(\sigma, \zeta) \mapsto \sigma\zeta$, and the action of G on C_4 induced by (1.2), which we will write as $(\sigma, \zeta) \mapsto {}^{\sigma}\zeta$. (Here σ is an element of G and ζ an element of $\mu_4 = C_4$.)

We now have two induced group extensions: One obtained by restriction of (1.2) to the subgroup $N = \{\sigma \in G \mid \sigma i = {}^{\sigma}i\}$ of G, and one obtained from (1.2) by means of the homomorphism $\zeta \mapsto \zeta^2$ of C_4 onto μ_2. In both cases the kernel is a group of roots of unity, since μ_4 and C_4 are identical as N-modules.

THEOREM 1.1: *Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$ and $i \in M$. Let*

$$1 \to C_4 \to E \underset{\pi}{\to} G \to 1 \tag{1.2}$$

be a group extension. Let L be the fixed field of $N = \{\sigma \in G \mid \sigma i = {}^{\sigma}i\}$. Then the embedding problem given by M/K and (1.2) is solvable, if and only if the embedding problems given by M/L and

$$1 \to \mu_4 \to \pi^{-1}(N) \underset{\pi}{\to} N \to 1, \tag{1.3}$$

resp. by M/K and

$$1 \to \mu_2 \to E/C_2 \underset{\pi'}{\to} G \to 1, \tag{1.4}$$

are solvable.

We will prove Theorem 1.1 in section 2 below. Theorem 1.1 and its proof is an explicit special case of [Ho, (3.8)].

Embedding problems in which the kernel is a group of roots of unity (with Galois action) are called **Brauer type** embedding problems. The advantage of Brauer type embedding problems is a nice criterion for solvability in terms of crossed product algebras, cf. [Br, Satz 7]. The two special cases (kernel μ_4 and μ_2) we need will be formulated explicitly in Propositions 2.2 and 2.4 below.

In sections 2–3 below, Theorem 1.1 and its Corollary 2.5 are used to obtain criteria for embedding cyclic extensions of degree 4 in cyclic extensions of degree 16 (Theorem 2.8) and for embedding dihedral extensions of degree 8 in dihedral, quasi-dihedral and quaternion extensions of degree 32 (Theorems 3.6–3.8).

As an application of these (somewhat technical) criteria, we consider automatic realisations. An **automatic realisation** $G \Rightarrow H$, where G and H are finite groups, is a statement that any field admitting a G-extension also admits an H-extension. Automatic realisations have been considered by several authors. See [Le] and [G&S] for references. We prove the following two results:

PROPOSITION 1.2: $Q_{32} \Rightarrow D_{16}$.

Remark: The automatic realisation $Q_8 \Rightarrow D_4$ is well known, and is proved e.g. in [J&Y, Th. (III.3.6)]. The automatic realisation $Q_{16} \Rightarrow D_8$ is proved in [Le, Prop. 5.8]. The result of Proposition 1.2 is therefore not surprising, and it is a reasonable conjecture that $Q_{2^{n+1}} \Rightarrow D_{2^n}$ for all $n > 1$.

PROPOSITION 1.3: $D_8 \Rightarrow D_{16} \vee Q_{16}$. *(That is, any field admitting a D_8-extension also admits a D_{16}- or a Q_{16}-extension.)*

Of course, the criteria of sections 2–3 work only in characteristic $\neq 2$. But by a result of Witt, [Wi, Satz p. 237], Propositions 1.2 and 1.3 are trivial in characteristic 2.

2. Embedding problems with kernel C_4

Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$. We will consider the embedding problem given by M/K and a group extension

$$(2.1) \qquad 1 \to C_4 \to E \xrightarrow[\pi]{} G \to 1.$$

If $i \notin M$, we consider the Galois extension $M(i)/K$ instead. Obviously, this extension has Galois group $G \times C_2$, and we have an embedding problem given by $M(i)/K$ and the group extension

$$(2.1') \qquad 1 \to C_4 \to E \times C_2 \xrightarrow[\pi\times 1]{} G \times C_2 \to 1.$$

Since the embedding problem given by M/K and (2.1) is solvable, if and only if the embedding problem given by $M(i)/K$ and (2.1′) is, we may replace M/K by $M(i)/K$ and assume $i \in M$.

As above, we identify C_4 and μ_4, and write the two G-module actions as $(\sigma,\zeta) \mapsto {}^\sigma\zeta$ and $(\sigma,\zeta) \mapsto \sigma\zeta$, respectively. We then define homomorphisms $e, f, g\colon G \to \{1,-1\}$ by $\sigma i = i^{e_\sigma}$, ${}^\sigma i = i^{f_\sigma}$ and $g_\sigma = e_\sigma f_\sigma$ for $\sigma \in G$. Also, we define a new G-module structure on M^* by

$$ {}^\sigma x = \sigma x^{g_\sigma}, \quad x \in M^*,\ \sigma \in G. $$

When M^* is considered a G-module in this way, we denote it $M^\times$. We then have $C_4 \subseteq M^\times$, as well as an induced G-action on $M^\times/4 = M^\times/(M^\times)^4$.

Lemma 2.1: *Let $\omega \in M^\times$. Then $F/K = M(\sqrt[4]{\omega})/K$ is Galois and a solution to the embedding problem given by M/K and some extension*

$$ 1 \to C_4 \to E \underset{\pi}{\to} G \to 1, \tag{2.1} $$

if and only if $\bar\omega \in (M^\times/4)^G = H^0(G, M^\times/4)$. In that case there exists $a_\sigma \in M^\times$ for $\sigma \in G$, such that ${}^\sigma\omega/\omega = a_\sigma^4$, and (2.1) *may be chosen to have characteristic class $[c] \in H^2(G, C_4)$, where*

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

Proof: By Kummer theory, F/K is Galois, if and only if there exists $i_\sigma \in \{1,-1\}$ and $b_\sigma \in M^*$ for $\sigma \in G$, such that $\sigma\omega/\omega^{i_\sigma} = b_\sigma^4$. If this is the case, we can extend $\sigma \in G$ to $\mathrm{Gal}(F/K)$ by

$$ \sigma(\sqrt[4]{\omega}) = \zeta_\sigma b_\sigma\, (\sqrt[4]{\omega})^{i_\sigma} $$

for a suitable $\zeta_\sigma \in \mu_4$. Now, let κ generate $\mathrm{Gal}(F/M)$, i.e., $\kappa(\sqrt[4]{\omega}) = \zeta \cdot \sqrt[4]{\omega}$ for some $\zeta \in \mu_4$. Then we have

$$ \sigma\kappa(\sqrt[4]{\omega}) = \zeta^{e_\sigma}\zeta_\sigma b_\sigma\, (\sqrt[4]{\omega})^{i_\sigma} $$

and

$$ \kappa^{f_\sigma}\sigma(\sqrt[4]{\omega}) = \zeta^{f_\sigma i_\sigma}\zeta_\sigma b_\sigma\, (\sqrt[4]{\omega})^{i_\sigma} $$

for $\sigma \in G$. Hence, we must have $\zeta^{e_\sigma} = \zeta^{f_\sigma i_\sigma}$. If $\bar\omega \in (M^\times/4)^G$, we may assume $i_\sigma = g_\sigma$, and so the condition is fulfilled for $a_\sigma = b_\sigma^{g_\sigma}$. Conversely: If $\omega \in (M^\times)^4$, we have $\bar\omega = 1 \in (M^\times/4)^G$. If $\omega \in (M^\times)^2 \smallsetminus (M^\times)^4$, we write $\omega = \xi^2$ for some $\xi \in M^\times$. Then $F = M(\sqrt{\xi})$, and so $\zeta = -1$. Since i_σ and g_σ are both odd, we can let $a_\sigma = b_\sigma^{g_\sigma}\xi^{(i_\sigma g_\sigma - 1)/2}$ and get ${}^\sigma\omega/\omega = a_\sigma^4$, and thus $\bar\omega \in (M^*/4)^G$. Finally, if $\omega \notin (M^*)^2$, we can choose $\zeta = i$ and get $i_\sigma = g_\sigma$. Then ${}^\sigma\omega/\omega = a_\sigma^4$ for $a_\sigma = b_\sigma^{g_\sigma}$.

Now, assume ${}^\sigma\omega/\omega = a_\sigma^4$ for $\sigma \in G$, and extend σ to $\bar\sigma \in \mathrm{Gal}(F/K)$ by

$$\bar\sigma(\sqrt[4]{\omega}) = (\zeta_\sigma a_\sigma \sqrt[4]{\omega})^{g_\sigma},$$

where $\zeta_\sigma \in \mu_4$. Also, let $\kappa_{\sigma,\tau} \in \mathrm{Gal}(F/M)$ be given by $\bar\sigma\bar\tau = \kappa_{\sigma,\tau}\overline{\sigma\tau}$ for $\sigma, \tau \in G$. Then $\kappa_{\sigma,\tau}(\sqrt[4]{\omega}) = \zeta_{\sigma,\tau}\sqrt[4]{\omega}$ for some $\zeta_{\sigma,\tau} \in \mu_4$, and the factor system $(\sigma, \tau) \mapsto \zeta_{\sigma,\tau}$ represents (2.1). As

$$\bar\sigma\bar\tau(\sqrt[4]{\omega}) = \bar\sigma(\zeta_\tau a_\tau \sqrt[4]{\omega})^{g_\tau} = \sigma\zeta_\tau^{g_\tau}\sigma a_\tau^{g_\tau}\zeta_\sigma^{g_{\sigma\tau}}a_\sigma^{g_{\sigma\tau}}(\sqrt[4]{\omega})^{g_{\sigma\tau}} = (\zeta_\sigma{}^\sigma\zeta_\tau\, a_\sigma{}^\sigma a_\tau \sqrt[4]{\omega})^{g_{\sigma\tau}}$$

and

$$\kappa_{\sigma,\tau}\overline{\sigma\tau}(\sqrt[4]{\omega}) = \kappa_{\sigma,\tau}(\zeta_{\sigma\tau}a_{\sigma\tau}\sqrt[4]{\omega})^{g_{\sigma\tau}} = (\zeta_{\sigma\tau}\, a_{\sigma\tau}\, \zeta_{\sigma,\tau} \sqrt[4]{\omega})^{g_{\sigma\tau}},$$

we get

$$\zeta_{\sigma,\tau} = \zeta_\sigma{}^\sigma\zeta_\tau\, \zeta_{\sigma\tau}^{-1} \cdot c_{\sigma,\tau},$$

and hence $[\zeta] = [c] \in H^2(G, C_4)$. ∎

It is clear from the proof of Lemma 2.1 that $[c]$ is independent of the choice of a_σ's. Also, if $\lambda = x^4\omega$ for $x \in M^\times$, we can let $b_\sigma = a_\sigma{}^\sigma x/x$ and get ${}^\sigma\lambda/\lambda^{g_\sigma} = b_\sigma^4$. The factor system obtained from λ and the b_σ's is then c. Thus, we have a well-defined homomorphism $\Delta\colon (M^\times/4)^G \to H^2(G, C_4)$, given by $\Delta(\bar\omega) = [c]$.

Obviously, $M(\sqrt[4]{\omega})/K$, $\omega \in M^\times$, is a solution to the embedding problem given by M/K and $\gamma \in H^2(G, C_4)$, if and only if $\bar\omega \in (M^\times/4)^G$ and $\Delta(\bar\omega)$ equals either γ or γ^{-1}. In particular, if $M(\sqrt[4]{\omega})/K$ *is* a solution, all the solutions are $M(\sqrt[4]{r\omega})/K$, where r runs through a set of representatives for the elements of $\ker\Delta$.

Remark: The map $\Delta\colon (M^\times/4)^G \to H^2(G, C_4)$ can be obtained as the composite of two connecting homomorphisms in analogy with the argument in [Ki, pp. 826–827]: From the short-exact sequences

$$1 \to (M^\times)^4 \to M^\times \to M^\times/4 \to 1$$

and

$$1 \to C_4 \to M^\times \to (M^\times)^4 \to 1$$

we get long-exact cohomology sequences

$$(M^\times/4)^G \xrightarrow[\delta_1]{} H^1(G, (M^\times)^4) \to H^1(G, M^\times)$$

and

$$H^1(G, M^\times) \to H^1(G, M^\times)^4) \xrightarrow[\delta_2]{} H^2(G, C_4) \to H^2(G, M^\times),$$

and Δ is then the composite $\delta_2 \circ \delta_1$. However, unlike the situation in [Ki], we do not get an exact sequence

$$(M^\times/4)^G \underset{\Delta}{\to} H^2(G, C_4) \to H^2(G, M^\times),$$

since $H^1(G, M^\times)$ is not necessarily trivial. In fact, if L is the fixed field of the kernel of g, we have $H^1(G, M^\times) \simeq K^*/\mathrm{N}_{L/K}(L^*)$. Thus, the existence of splitting factors a_σ as in Lemma 2.1 does not ensure the existence of an ω.

From Lemma 2.1 we get

Proposition 2.2: *Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$ and $\mu_4 \subseteq M^*$. Let*

$$1 \to \mu_4 \to E \underset{\pi}{\to} G \to 1 \tag{2.2}$$

be a group extension with characteristic class $\gamma \in H^2(G, \mu_4)$. Then the embedding problem given by M/K and (2.2) is solvable, if and only if $i(\gamma) = 1 \in H^2(G, M^*)$, where i: $H^2(G, \mu_4) \to H^2(G, M^*)$ is the homomorphism induced by the inclusion $\mu_4 \subseteq M^*$. Furthermore, if $M(\sqrt[4]{\omega})/K$, $\omega \in M^*$, is a solution, all the solutions are $M(\sqrt[4]{r\omega})/K$, $r \in K^*$.

Thus, if the G-modules C_4 and μ_4 are identical, we have a criterion for solvability of the embedding problem given by M/K and (2.1) in terms of the Brauer group $\mathrm{Br}(K)$: We identify the cohomology group $H^2(G, M^*)$ with the relative Brauer group $\mathrm{Br}(M/K)$ of the extension M/K in the usual way, cf. [Ja, Th. 8.11] or [Lo, §30 Satz 2], by letting the cohomology class $[c]$ containing a factor system $c \in Z^2(G, M^*)$ correspond to the equivalence class $[M, G, c]$ of the crossed product algebra (M, G, c). The element $i(\gamma) \in \mathrm{Br}(M/K)$ from Proposition 2.2 (and Proposition 2.4 below) we will call the **obstruction** to the embedding problem.

If C_4 and μ_4 are not identical as G-modules, we let $N = \ker g$. This is is then a subgroup of G of index 2.

Lemma 2.3: *Let M/K be finite Galois with Galois group $G = \mathrm{Gal}(M/K)$, and let $N \subseteq G$ be a subgroup of index 2. Let d: $N \to M^*$ be a crossed homomorphism, and let $\kappa \in G \setminus N$, $a \in M^*$. Then d can be extended to a crossed homomorphism d': $G \to M^*$, such that $d'_\kappa = a$, if and only if $a\kappa a = d_{\kappa^2}$ and $\forall \sigma \in N$: $\sigma a/a = \kappa d_{\kappa^{-1}\sigma\kappa}/d_\sigma$.*

Proof: 'Only if' is clear, since we must have

$$d_{\kappa^2} = d'_{\kappa^2} = d'_\kappa \kappa d'_\kappa = a\kappa a$$

and

$$\forall \sigma \in N\colon d_\sigma\, \sigma a = d'_\sigma\, \sigma d'_\kappa = d'_{\sigma\kappa} = d'_{\kappa\kappa^{-1}\sigma\kappa} = d'_\kappa\, \kappa d'_{\kappa^{-1}\sigma\kappa} = a\, \kappa d_{\kappa^{-1}\sigma\kappa}.$$

'If': Direct calculations show that $d'\colon G \to M^*$, given by $d'_\sigma = d_\sigma$ and $d'_{\sigma\kappa} = d_\sigma\, \sigma a$ for $\sigma \in N$, is a crossed homomorphism. ∎

Let $L = \mathcal{F}(N)$ be the fixed field of N, and let $\kappa \in G \setminus N$. Choose a representative $c \in Z^2(G, C_4)$ of the characteristic class of

$$(2.1) \qquad 1 \to C_4 \to E \xrightarrow[\pi]{} G \to 1.$$

We may assume $c_{\sigma,\kappa} = 1$ for $\sigma \in N$.

The embedding problem given by M/K and (2.1) gives rise to two other embedding problems: One given by M/L and

$$(2.3) \qquad 1 \to \mu_4 \to \pi^{-1}(N) \xrightarrow[\pi]{} N \to 1,$$

which is solvable, if and only if $[c|_{N\times N}] = 1 \in H^2(N, M^*)$, cf. Proposition 2.2, and another given by M/K and

$$(2.4) \qquad 1 \to \mu_2 \to E/C_2 \xrightarrow[\pi']{} G \to 1,$$

where (2.4) has characteristic class $[c^2] \in H^2(G, \mu_2)$. To handle this second embedding problem, we need the following well-known result:

Proposition 2.4: *Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$. Also, let*

$$(2.5) \qquad 1 \to \mu_2 \to E \xrightarrow[\pi]{} G \to 1$$

be a group extension with characteristic class $\gamma \in H^2(G, \mu_2)$. Then the embedding problem given by M/K and (2.5) is solvable, if and only if $i(\gamma) = 1 \in H^2(G, M^*)$, where $i\colon H^2(G, \mu_2) \to H^2(G, M^*)$ is the homomorphism induced by the inclusion $\mu_2 \subseteq M^*$. Furthermore, if $M(\sqrt{\omega})/K$, $\omega \in M^*$, is a solution, all the solutions are $M(\sqrt{r\omega})/K$, $r \in K^*$.

A proof of Proposition 2.4 can be found in [Sch].

Thus, the embedding problem given by M/K and (2.4) is solvable, if and only if $[c^2] = 1 \in H^2(G, M^*)$.

Clearly, the embedding problems given by M/L and (2.3), resp. M/K and (2.4), are solvable, if the embedding problem given by M/K and (2.1) is.

Now, assume that the embedding problems given by M/L and (2.3), resp. M/K and (2.4), are solvable. Then there exist maps a: $N \to M^*$ and b: $G \to M^*$, such that

$$c_{\sigma,\tau} = a_\sigma \, \sigma a_\tau \, a_{\sigma\tau}^{-1}, \quad \sigma, \tau \in N,$$

and

$$c_{\sigma,\tau}^2 = b_\sigma \, \sigma b_\tau \, b_{\sigma\tau}^{-1}, \quad \sigma, \tau \in G.$$

The map $\sigma \mapsto a_\sigma \, \kappa a_{\kappa^{-1}\sigma\kappa} \, c_{\kappa,\kappa^{-1}\sigma\kappa}$ is a crossed homomorphism $N \to M^*$, and with $a = a_{\kappa^2} \, c_{\kappa,\kappa}$ the conditions of Lemma 2.3 are fulfilled. Hence, there exists $r \in M^*$, such that

$$\forall \sigma \in N\colon \frac{\sigma r}{r} = a_\sigma \, \kappa a_{\kappa^{-1}\sigma\kappa} \, c_{\kappa,\kappa^{-1}\sigma\kappa}$$

and

$$\frac{\kappa r}{r} = a_{\kappa^2} \, c_{\kappa,\kappa}.$$

The map $\sigma \mapsto a_\sigma^2/b_\sigma$ is also a crossed homomorphism, and so there exists $s \in M^*$, such that

$$\forall \sigma \in N\colon \frac{\sigma s}{s} = \frac{a_\sigma^2}{b_\sigma}.$$

Let

$$\omega = \frac{r^2 s}{b_\kappa \, \kappa s}.$$

Then $\sigma\omega/\omega = a_\sigma^4$ for $\sigma \in N$, and ${}^\kappa\omega/\omega = 1/r^4$. We extend a to G by

$$a_{\sigma\kappa} = a_\sigma/\sigma r, \quad \sigma \in N,$$

and get

$$\forall \sigma \in G\colon \frac{{}^\sigma\omega}{\omega} = a_\sigma^4.$$

Direct calculations now show that

$$c_{\sigma,\tau} = a_\sigma \, {}^\sigma a_\tau \, a_{\sigma\tau}^{-1}, \quad \sigma, \tau \in G,$$

and so $M(\sqrt[4]{\omega})/K$ is a solution to the embedding problem given by M/K and (2.1). This completes the proof of Theorem 1.1.

Remark: If $i \in L$, we can determine all solutions to the embedding problem given by M/K and (2.1) from one solution, since we can describe the kernel of Δ: From the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & C_4 \arrow[r] \arrow[d, equal] & C_4 \rtimes G \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\text{res}"] & 1 \\
1 \arrow[r] & C_4 \arrow[r] & C_4 \rtimes H \arrow[r] & H \arrow[r] & 1,
\end{tikzcd}$$

where $H = \mathrm{Gal}(L/K)$, we conclude that any solution to the split-exact embedding problem over M/K is the composite of M/K and a solution to the split-exact embedding problem over L/K. Thus, we need only find $\ker\Delta$ in the case $M = L$:

If $L = K$, the map Δ is trivial, and the kernel is $K^*/4$. Hence, the elements of the kernel are reprensented by the elements of K^*. This corresponds to the situation in Proposition 2.2.

If $L \neq K$: We seek all pairs $(\omega, a) \in L^\times \times L^\times$, such that ${}^\kappa\omega/\omega = a^4$ and $a^\kappa a = 1$. Since $g_\kappa = -1$, we get $\omega\,\kappa\omega = a^{-4}$ and $\kappa a/a = 1$, i.e., $\omega\,\kappa\omega = a^{-4}$ and $a \in K^*$. This means that $(a^2\omega)\kappa(a^2\omega) = 1$, and hence $a^2\omega = \kappa x/x$ for some $x \in L^*$ by Hilbert 90. On the other hand: If we let $\omega = a^{-2}\kappa x/x$ for $a \in K^*$ and $x \in L^*$, the conditions are fulfilled. Thus, the elements in $\ker\Delta$ are represented by the elements $b^2\kappa x/x$, where $b \in K^*$ and $x \in L^*$.

In particular, if (2.1) is central we can describe the full set of solutions to the embedding problem.

COROLLARY 2.5: *Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$ and $i \notin M$. Let*

$$1 \to C_4 \to E \underset{\pi}{\to} G \to 1 \tag{2.1}$$

be a group extension. Extend the elements $\sigma \in G$ to $M(i)$ by $\sigma i = i$, and let κ be the generator of $\mathrm{Gal}(M(i)/M)$. Let $N = \{\sigma \in G \mid {}^\sigma i = i\}$, $\mathcal{F}(N) = K(\sqrt{b})$ and $L = K(i\sqrt{b})$. Then $\mathrm{Gal}(M(i)/L) \simeq G$ by restriction, and the embedding problem given by M/K and (2.1) is solvable, if and only if the embedding problems given by M/K and

$$1 \to \mu_2 \to E/\mu_2 \underset{\pi'}{\to} G \to 1, \tag{2.4}$$

resp. by $M(i)/L$ and

$$1 \to \mu_4 \to E \underset{\pi}{\to} G \to 1, \tag{2.2}$$

are solvable.

Remark: Theorem 1.1 and Corollary 2.5 allow us to get criteria for solving embedding problems with kernel C_4 in terms of Brauer groups. However, a number of special cases must be considered, corresponding to the location of $K(i)$ within $M(i)$. If the maximal elementary abelian 2-factor group of G is isomorphic to $(\mathbb{Z}/2)^n$, there are 2^n+1 cases.

By Theorem 1.1, an embedding problem with kernel C_4 has two obstructions, corresponding to the two reduced embedding problems. In order to simplify these, we need

THEOREM 2.6 ([Ja, Th. 4.7]): *Let $\mathfrak{A}/K$ be a finite-dimensional central simple algebra, and let $\mathfrak{B}/K$ 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

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

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

Since solvability of the embedding problem given by M/K and (2.4) implies that the obstruction to the embedding problem given by M/L and (2.3) has order at most 2 in $\mathrm{Br}(L)$, we can attempt to decompose this obstruction as a product of quaternion algebras by means of Theorem 2.6.

We use the standard notation for quaternion algebras: 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 $ji=-ij$. The equivalence class of $(a,b/K)$ in $\mathrm{Br}(K)$ is denoted (a,b). General references for Brauer groups, crossed product algebras and quaternion algebras are [Ja, 4.6–4.7, 8.4–8.5] and [Lo, §§29–30]. For $a \in K^*$, the algebra generated by elements i and $j \neq 0$ with relations $i^2=a^2$, $j^2=0$ and $ji=-ij$ is split, and we will therefore use $(a^2,0)$ and $(0,a^2)$ to denote the neutral element 1 of $\mathrm{Br}(K)$.

For elements $a,b \in K^*$, we write $a =_2 b$, if a and b are quadratically equivalent, i.e., if $a/b \in (K^*)^2$.

PROPOSITION 2.7 (The cyclic group of order 8): *Let $M/K = K(\sqrt{a})/K$ be a quadratic extension, and let σ be the generator for $G = \mathrm{Gal}(M/K)$. Then the embedding problem given by M/K and*

$$1 \to C_4 \to C_8 \underset{\pi}{\to} G \to 1 \tag{2.6}$$

is solvable, if and only if the embedding problems given by M/K and

$$(2.7) \qquad 1 \to \mu_2 \to C_4 \underset{\pi'}{\longrightarrow} G \to 1,$$

resp. by $M(i)/K(i)$ and

$$(2.8) \qquad 1 \to \mu_4 \to \pi^{-1}(\mathrm{Gal}(M(i)/K(i))) \underset{\pi}{\longrightarrow} \mathrm{Gal}(M(i)/K(i)) \to 1,$$

are solvable. In fact, we have the following 3 cases:

1. *$i \in K$. M/K can be embedded in a C_8-extension, if and only if $i \in \mathrm{N}_{M/K}(M^*)$. If $i = \mathrm{N}_{M/K}(x)$ for some $x \in M^*$, we get a solution $M(\sqrt[4]{\omega})/K = K(\sqrt[4]{\omega})/K$ by letting $\omega = \sigma x^2 \cdot \sqrt{a}$.*
2. *$a = -1$. M/K can be embedded in a C_8-extension, if and only if $-1 \in \mathrm{N}_{M/K}(M^*)$. If $-1 = \mathrm{N}_{M/K}(x)$ for some $x \in M^*$, we get a solution $K(\sqrt[4]{\omega})/K$ by letting $\omega = 2ix$.*
3. *-1 and a are quadratically independent. We identify G and $\mathrm{Gal}(M(i)/K(i))$, and let κ generate $\mathrm{Gal}(M(i)/M)$. M/K can be embedded in a C_8-extension, if and only if $i \in \mathrm{N}_{M(i)/K(i)}(M(i)^*)$ and $-1 \in \mathrm{N}_{M/K}(M^*)$. If $-1 = \mathrm{N}_{M/K}(x)$ and $i = \mathrm{N}_{M(i)/K(i)}(y)$ for $x \in M^*$ and $y \in M(i)^*$, we choose $r \in M^*$ and $s \in M(i)^*$, such that $\sigma r/r = y\kappa y$ and $\sigma s/s = y^2/x$, and let $\omega = r^2 s/\kappa s$. A solution to the embedding problem is then*

$$M(\sqrt[4]{\omega} + r/\sqrt[4]{\omega}) = K(\sqrt[4]{\omega} + r/\sqrt[4]{\omega}).$$

Proof: Most of the theorem is obtained directly from Theorem 1.1 and Corollary 2.5, since the crossed product algebras representing the obstructions are all cyclic, cf. [Ja, 8.8] or [Lo, §30.4]. The last part of (3) is proved as follows: $M(i, \sqrt[4]{\omega})/K$ is a $C_8 \times C_2$-extension containing a solution to the embedding problem. We extend κ to $M(i, \sqrt[4]{\omega})$ by $\kappa(\sqrt[4]{\omega}) = r/\sqrt[4]{\omega}$ and get $\kappa^2 = 1$. The solution contained in $M(i, \sqrt[4]{\omega})/K$ is then the fixed field $\mathcal{F}(\kappa)/K$. This fixed field is $M(\sqrt[4]{\omega} + 1/\sqrt[4]{\omega})$, since

$$\sqrt[4]{\omega} + r/\sqrt[4]{\omega} = \sqrt[4]{\omega} + \kappa(\sqrt[4]{\omega}) \in \mathcal{F}(\kappa) \setminus M(i, \sqrt{\omega}). \qquad \blacksquare$$

THEOREM 2.8 (The cyclic group of order 16): *Let M/K be a C_4-extension, let σ be a generator for $\mathrm{Gal}(M/K)$, and consider the embedding problem given by M/K and*

$$(2.9) \qquad 1 \to C_4 \to C_{16} \underset{\pi}{\longrightarrow} \mathrm{Gal}(M/K) \to 1.$$

It is solvable, if and only if the embedding problems given by M/K and

$$(2.10) \qquad 1 \to \mu_2 \to C_8 \underset{\pi'}{\longrightarrow} \mathrm{Gal}(M/K) \to 1,$$

resp. by $M(i)/K(i)$ and

$$(2.11) \qquad 1 \to C_4 \to \pi^{-1}(\mathrm{Gal}(M(i)/K(i))) \underset{\pi}{\longrightarrow} \mathrm{Gal}(M(i)/K(i)) \to 1,$$

are solvable. We get the following three cases:

(1) *$i \in K$. We can then write $M = K(\sqrt[4]{a})$ for some $a \in K^*$, and let σ be given by $\sigma(\sqrt[4]{a}) = i \cdot \sqrt[4]{a}$. The embedding problem is solvable, if and only if $i \in \mathrm{N}_{M/K}(M^*)$. And if $i = \mathrm{N}_{M/K}(x)$ for some $x \in M^*$, we get a solution $M(\sqrt[4]{\omega})/K = K(\sqrt[4]{\omega})/K$ by letting $\omega = \sigma x\, \sigma^2 x^2\, \sigma^3 x^3 \cdot \sqrt[4]{a}$.*

In terms of obstructions: It is necessary for solvability that there exists $\alpha, \beta \in K$, $\alpha \neq 0$, such that $\alpha^2 - a\beta^2 = i$. The obstruction to the embedding problem is then

$$(a, \alpha)(i, \alpha\beta) \in \mathrm{Br}(K).$$

In particular: The quadratic extension $K(\sqrt{a})/K$ can be embedded in a C_{16}-extension, if and only if $(a, i) = 1 \in \mathrm{Br}(K)$ and

$$(a, \alpha) = (i, r\alpha\beta) \in \mathrm{Br}(K)$$

for some $r \in K^*$, where $\alpha \in K^*$ and $\beta \in K$ are chosen, such that $\alpha^2 - a\beta^2 = i$.

(2) *$a = -1$: We must have $-1 = u^2 + v^2$ for some $u, v \in K$, and $M = K(\sqrt{r(1 - iu)})$, where $r \in K^*$. The embedding problem is then solvable, if and only if M/K and $M/K(i)$ can be embedded in C_8-extensions, if and only if $-1 \in \mathrm{N}_{M/K}(M^*)$ and $i \in \mathrm{N}_{M/K(i)}(M^*)$. If $\mathrm{N}_{M/K}(x) = -1$ and $\mathrm{N}_{M/K(i)}(y) = i$ for some $x, y \in M^*$, we choose $r, s \in M^*$, such that $\sigma r/r = y$ and $\sigma^2 s/s = y^2/x$, and get a solution $M(\sqrt[4]{\omega})/K$ by letting $\omega = r^2 s/x\, \sigma s$.*

In terms of obstructions, the embedding problem is solvable, if and only if

$$(-1, r) = 1 \in \mathrm{Br}(K) \quad \textit{and} \quad (r(1 - iu), i) = 1 \in \mathrm{Br}(K(i)).$$

In particular: $K(i)/K$ can be embedded in a C_{16}-extension, if and only if $(-1, -1) = 1 \in \mathrm{Br}(K)$ and

$$(-1, r) = 1 \in \mathrm{Br}(K) \quad \textit{and} \quad (r(1 - iu), i) = 1 \in \mathrm{Br}(K(i))$$

for some $r \in K^*$, where $u, v \in K$, such that $-1 = u^2 + v^2$.

(3) *a and -1 are quadratically independent. We identify G and $\mathrm{Gal}(M(i)/K(i))$, and let κ generate $\mathrm{Gal}(M(i)/K)$, Also, we may assume $a = 1 + c^2$ for some $c \in K$, and $M = K(\sqrt{r(a+\sqrt{a})})$, where $r \in K^*$. The embedding problem is then solvable, if and only if M/K can be embedded in a C_8-extension and $M(i)/K(i)$ can be embedded in a C_{16}-extension, if and only if $-1 \in \mathrm{N}_{M/K}(M^*)$ and $i \in \mathrm{N}_{M(i)/K(i)}(M(i)^*)$. If $\mathrm{N}_{M/K}(x) = -1$ and $\mathrm{N}_{M(i)/K(i)}(y) = i$ for some $x \in M^*$ and $y \in M(i)^*$, we choose $r \in M^*$ and $s \in M(i)^*$, such that $\sigma r/r = y\,\kappa y$ and $\sigma s/s = y^2/x$, and let $\omega = r^2 s/x\,\kappa s$. A solution to the embedding problem is then*

$$M(\sqrt[4]{\omega} + r/\sqrt[4]{\omega})/K = K(\sqrt[4]{\omega} + r/\sqrt[4]{\omega})/K.$$

Since $M(i) = K(i, \sqrt[4]{\lambda})$, where $\lambda = 4r^2(1-ic)^2 a = [2r(1-ic)]^2 a$, we get the following criterion in terms of obstructions: M/K can be embedded in a C_{16}-extension, if and only if $(a, 2) = (-1, r) \in \mathrm{Br}(K)$ and

$$(a, \alpha) = (i, r(1-ic)\alpha\beta) \in \mathrm{Br}(K(i)),$$

where $\alpha \in K(i)^*$ and $\beta \in K(i)$ are chosen, such that $\alpha^2 - a\beta^2 = i$. (Such α, β exist by the first part of the criterion, since $(a, i) = (a, 2) = 1 \in \mathrm{Br}(K(i))$.)

In particular: The quadratic extension $K(\sqrt{a})/K$ can be embedded in a C_{16}-extension, if and only if

$$(a, a) = 1 \in \mathrm{Br}(K), \quad (a, 2) = (-1, r) \in \mathrm{Br}(K), \quad \text{and}$$
$$(a, \alpha) = (i, r(x-iy)\alpha\beta) \in \mathrm{Br}(K(i)),$$

for some $r \in K^*$, where $x, y \in K$, such that $a = x^2 + y^2$, and $\alpha \in K(i)^*$, $\beta \in K(i)$, such that $\alpha^2 - a\beta^2 = i$.

Proof: (1) The obstruction to the embedding problem is the cyclic algebra $\Gamma = (M, \sigma, i) = M[u]$, where $u^4 = i$ and $ux = \sigma(x)u$ for $x \in M$. We will write this algebra as a product of quaternion algebras: Obviously, M/K cannot be embedded in a C_{16}-extension, unless $K(\sqrt{a})/K$ can be embedded in a C_8-extension. By Proposition 2.7 this is possible, if and only if i is a norm in $K(\sqrt{a})/K$. Thus, we must have $\alpha, \beta \in K$, such that $\alpha^2 - a\beta^2 = i$. If $\alpha = 0$, we replace α and β by $i+1$ and $i\beta$ to obtain $\alpha \neq 0$. Let

$$i_1 = \sqrt{a}, \quad j_1 = (\alpha + \beta\sqrt{a} + iu^2)u,$$
$$i_2 = u^2, \quad j_2 = \sqrt[4]{a}\,(\alpha + \beta i\sqrt{a} + u^2).$$

Then $i_2^2 = a$, $j_1^2 = -2\alpha$, $j_1 i_1 = -i_1 j_1$, $i_2^2 = i$, $j_2^2 = 2\alpha\beta i a$, $j_2 i_2 = -i_2 j_2$, $i_1 i_2 = i_2 i_1$, $j_1 i_2 = i_2 j_1$, $i_1 j_2 = j_2 i_1$ and $j_1 j_2 = j_2 j_1$. Hence, the quaternion subalgebras $K[i_1, j_1] \simeq (a, -2\alpha/K)$ and $K[i_2, j_2] \simeq (i, 2\alpha\beta/K)$ centralise each other, and we have

$$[\Gamma] = (a, -2\alpha)(i, 2\alpha\beta i a) = (a, \alpha)(i, \alpha\beta) \in \mathrm{Br}(K).$$

The last part follows, since $K(\sqrt{a})/K$ can be embedded in a C_{16}-extension, if and only if $K(\sqrt[4]{r^2 a})/K$ can for some $r \in K^*$.

(2) The obstruction to embedding M/K in a C_8-extension is $(2, -1)(-1, r) = (-1, r) \in \mathrm{Br}(K)$ by [Le, Ex. 3.1].

(3) As in the proof of Proposition 2.7, we extend κ to $M(i, \sqrt[4]{\omega})$ by $\kappa(\sqrt[4]{\omega}) = r/\sqrt[4]{\omega}$, and get the fixed field $\mathcal{F}(\kappa)/K$ as a solution. $\blacksquare$

Remark: The norm criteria of Proposition 2.7 and Theorem 2.8 are both special cases of [AFS&S, Th. 3].

3. The dihedral, quasi-dihedral and quaternion groups of order 32

First some notation: When $n \geq 2$, the **dihedral group** D_{2^n} is the group of order 2^{n+1} generated by elements σ and τ with relations $\sigma^{2^n} = \tau^2 = 1$ and $\tau\sigma = \sigma^{2^n-1}\tau$, the **quasi-dihedral group** QD_{2^n} is the group of order 2^{n+1} generated by elements x and y with relations $x^{2^n} = y^2 = 1$ and $yx = x^{2^{n-1}-1}y$, and the **quaternion group** $Q_{2^{n+1}}$ is the group of order 2^{n+1} generated by elements x and y with relations $x^{2^n} = 1$, $y^2 = x^{2^{n-1}}$ and $yx = x^{2^n-1}y$. Also, V_4 is the 'Klein Vierergruppe' $C_2 \times C_2$.

In this section, we will give criteria for embedding a D_4-extension M/K in D_{16}-, QD_{16}- and Q_{32}-extensions. To do this, we need to solve some auxiliary embedding problems:

Let $M/K = K(\sqrt{a}, i)/K$, $a \in K^*$, $i = \sqrt{-1}$, be a V_4-extension, and let $\sigma, \tau \in V_4 = \mathrm{Gal}(M/K)$ be given by $\sigma\sqrt{a} = -\sqrt{a}$, $\sigma i = i$, $\tau\sqrt{a} = \sqrt{a}$ and $\tau i = -i$.

Lemma 3.1: *The obstruction to the embedding problem given by M/K and*

(3.1)
$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto\sigma^2"'] & D_8 \arrow[r, "\substack{\sigma\mapsto\sigma \\ \tau\mapsto\tau}"'] & V_4 \arrow[r] & 1 \end{tikzcd}$$

is

$$(a, 2) \in \mathrm{Br}(K).$$

Remark: Moreover, if $p, q \in K$ are chosen, such that $p^2 - aq^2 = 2$, then

$$K(\sqrt{(p + q\sqrt{a}) \cdot \sqrt[4]{a}}, i)/K$$

will be a solution to the embedding problem.

Proof: The obstruction is represented by the algebra $\Gamma = M[u, v]$, where $u^2 = i$, $v^2 = 1$, $vu = -iuv$, $ux = \sigma(x)u$ and $vx = \tau(x)v$ for $x \in M$. We then have a quaternion subalgebra $Q = K[i, v] \simeq (-1, 1/K)$ and find

$$C_\Gamma(Q) = K[\sqrt{a}, (1 - i)u] \simeq \left(\frac{a, 2}{K}\right).$$

Hence, $\Gamma \simeq (-1, 1/K) \otimes_K (a, 2/K)$, and $[\Gamma] = (a, 2)$. ∎

A similar argument gives

LEMMA 3.2: *The obstruction to the embedding problem given by M/K and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i \mapsto \sigma^2"'] & Q_{16} \arrow[r, "\substack{x \mapsto \sigma \\ y \mapsto \tau}"'] & V_4 \arrow[r] & 1 \end{tikzcd} \tag{3.2}$$

is

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

Now, let $M/K = K(\sqrt[4]{a}, i)/K$, $a \in K^*$, be a D_4-extension, and let $\sigma, \tau \in D_4 = \mathrm{Gal}(M/K)$ be given by $\sigma(\sqrt[4]{a}) = i \cdot \sqrt[4]{a}$, $\sigma i = i$, $\tau(\sqrt[4]{a}) = \sqrt[4]{a}$ and $\tau i = -i$.

LEMMA 3.3: *For the embedding problem given by M/K and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i \mapsto \sigma^4"'] & D_{16} \arrow[r, "\substack{\sigma \mapsto \sigma \\ \tau \mapsto \tau}"'] & D_4 \arrow[r] & 1 \end{tikzcd} \tag{3.3}$$

to be solvable, it is necessary that there exists $\alpha, \beta \in K$, $\alpha \neq 0$, such that $\alpha^2 + a\beta^2 = 2$. In that case, the obstruction is

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

Remark: If there exists $\alpha, \beta \in K$, such that $\alpha^2 + a\beta^2 = 2$, we can obtain $\alpha \neq 0$: If $\alpha = 0$ and char $K \neq 3$, we can let $\alpha' = \frac{4}{3}$ and $\beta' = \frac{1}{3}\beta$. If $\alpha = 0$ and char $K = 3$, we can let $\alpha' = a - 1/a$ and $\beta' = (a + 1/a)\beta$.

Proof: By Proposition 2.2, the embedding problem is solvable, if and only if the crossed product algebra $\Gamma = (M, D_4, c)$ is split, where $c \in Z^2(D_4, \mu_4)$ represents (3.3).

Obviously, the embedding problem given by M/K and (3.3) cannot be solvable, unless M/K can be embedded in a D_8-extension. By [Le, Ex. 4.3], the obstruction to this embedding problem is $(2,-a) \in \mathrm{Br}(K)$. Hence, there must exist $\alpha, \beta \in K$, such that $\alpha^2 + a\beta^2 = 2$. By the remark above, we can assume $\alpha \neq 0$.

The algebra Γ is generated over M by elements u and v, such that $u^4 = i$, $v^2 = 1$, $vu = -iu^3v$, $ux = \sigma(x)u$ and $vx = \tau(x)v$ for $x \in M$. We let

$$\begin{aligned} i_1 &= i, & j_1 &= v, \\ i_2 &= (1-i)u^2, & j_2 &= \sqrt[4]{a}\,(\alpha + \beta\sqrt{a} + (1-i)u^2), \\ i_3 &= \sqrt{a}, & j_3 &= [2-(1+i)(\alpha - \beta i\sqrt{a})]u - i[2-(1-i)(\alpha + \beta i\sqrt{a})]u^3. \end{aligned}$$

Then $i_1^2 = -1$, $j_1^2 = 1$, $j_1i_1 = -i_1j_1$, $i_2^2 = 2$, $j_2^2 = 2a\alpha\beta$, $j_2i_2 = -i_2j_2$, $i_3^2 = a$, $j_3^2 = 8\alpha(\alpha-1)$ and $j_3i_3 = -i_3j_3$. Hence, we have quaternion subalgebras $Q_1 = K[i_1,j_1] = (-1,1/K)$, $Q_2 = K[i_2,j_2] = (2,-2a\alpha\beta/K)$ and $Q_3 = K[i_3,j_3] = (a, 8\alpha(\alpha-1)/K)$ of Γ. Furthermore, for $p \neq q$, the elements i_p and j_p commute with i_q and j_q. Thus, the tensor product $Q_1 \otimes Q_2 \otimes Q_3$ is contained in Γ, and so $\Gamma \simeq Q_1 \otimes Q_2 \otimes Q_3$. In $\mathrm{Br}(K)$, we get

$$[\Gamma] = (-1,1)(2,2a\alpha\beta)(a,8\alpha(\alpha-1)) = (2,\alpha\beta)(a,\alpha(\alpha-1)). \qquad \blacksquare$$

Similar arguments give

LEMMA 3.4: *For the embedding problem given by M/K and*

$$(3.4) \qquad 1 \to \mu_4 \xrightarrow[i\mapsto x^4]{} QD_{16} \xrightarrow[\substack{x\mapsto\sigma \\ y\mapsto\tau}]{} D_4 \to 1$$

to be solvable, it is necessary that there exists $\alpha, \beta \in K$, $\alpha \neq 0$, such that $\alpha^2 + a\beta^2 = 2$. In that case, the obstruction is

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

LEMMA 3.5: *For the embedding problem given by M/K and*

$$(3.5) \qquad 1 \to \mu_4 \xrightarrow[i\mapsto x^4]{} Q_{32} \xrightarrow[\substack{x\mapsto\sigma \\ y\mapsto\tau}]{} D_4 \to 1$$

to be solvable, it is necessary that there exists $\alpha, \beta \in K$, $\alpha \neq 0$, such that $\alpha^2 + a\beta^2 = 2$. In that case, the obstruction is

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

Now, let M/K be a general D_4-extension. D_4-extensions are well-described, and we use the description in [Le]: $M/K = K(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b})/K$, where a and b in K^* are quadratically equivalent, $r \in K^*$, and $\alpha, \beta \in K$ with $\alpha^2 - a\beta^2 = ab$. Also, $\sigma, \tau \in D_4 = \mathrm{Gal}(M/K)$ are given by

$$\begin{aligned} \sigma\colon\quad & \sqrt{r(\alpha+\beta\sqrt{a})} \mapsto \frac{\sqrt{a}\sqrt{b}}{\alpha+\beta\sqrt{a}}\sqrt{r(\alpha+\beta\sqrt{a})}, && \sqrt{b} \mapsto \sqrt{b}, \\ \tau\colon\quad & \sqrt{r(\alpha+\beta\sqrt{a})} \mapsto \sqrt{r(\alpha+\beta\sqrt{a})}, && \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

For convenience we let $\theta = r(\alpha+\beta\sqrt{a})$.

THEOREM 3.6 (The dihedral group): *Consider the embedding problem given by M/K and*

$$(3.6)\qquad \begin{tikzcd} 1 \arrow[r] & C_4 \arrow[r, "i\mapsto\sigma^4"'] & D_{16} \arrow[r, "\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}"'] & D_4 \arrow[r] & 1. \end{tikzcd}$$

It is a necessary condition for solvability of this embedding problem that the embedding problem given by M/K and

$$(3.7)\qquad \begin{tikzcd} 1 \arrow[r] & \mu_2 \arrow[r] & D_8 \arrow[r, "\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}"'] & D_4 \arrow[r] & 1 \end{tikzcd}$$

is solvable. The obstruction to this embedding problem is

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

by [Le, Ex. 4.3]. We will therefore assume $(2, ab) = (-b, r\alpha)$.

There are now five cases:

(1) $i \in K$: The N of Theorem 1.1 is $\langle\sigma\rangle$. Hence, $L = \mathcal{F}(N) = K(\sqrt{b})$, and the restricted embedding problem is given by M/L and

$$1 \to \mu_4 \to C_{16} \to C_4 \to 1.$$

The obstruction to this embedding problem is

$$(a', \alpha')(i, \alpha'\beta') \in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a = \left([(\alpha-\beta\sqrt{a})i + \sqrt{a}\sqrt{b}]\sqrt{\theta}\right)^4$ (i.e., $M = L(\sqrt[4]{a'})$ and $\sigma(\sqrt[4]{a'}) = i\cdot\sqrt[4]{a'}$) and $\alpha', \beta' \in L$, such that $\alpha' \neq 0$ and $\alpha'^2 - a'\beta'^2 = i$. (Such

α', β' exists, since $(a', i) = (a, 2) = (-a, 2) = (ab, 2) = (-b, r\alpha) = (1, r\alpha) = 1 \in \mathrm{Br}(L)$.)

(2) $a =_2 -1$: We then have $N = \langle \sigma^2, \sigma\tau \rangle$ and $L = K(i\sqrt{b})$. The restricted embedding problem is given by M/L and

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto\sigma^2"'] & D_8 \arrow[r, "\substack{\sigma\mapsto\sigma^2\\ \tau\mapsto\sigma\tau}"'] & V_4 \arrow[r] & 1. \end{tikzcd}$$

By Lemma 3.1, the obstruction to this embedding problem is

$$(2, r(\alpha + i\sqrt{b})) \in \mathrm{Br}(L),$$

since $M = L(\sqrt{\theta} + \sigma\sqrt{\theta}, i)$ and $(\sqrt{\theta} + \sigma\sqrt{\theta})^2 = 2r(\alpha + i\sqrt{b})$.

(3) $b = -1$: This is the case considered in Lemma 3.3: We may assume $r = \beta = 1$ and $\alpha = 0$, and get the obstruction

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

where $\alpha', \beta' \in K$, $\alpha' \neq 0$, such that $\alpha'^2 + a\beta'^2 = 2$.

(4) $ab =_2 -1$: We have $N = \langle \sigma^2, \tau \rangle$ and $L = K(\sqrt{a})$. The restricted embedding problem is given by M/L and

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto\sigma^2"'] & D_8 \arrow[r, "\substack{\sigma\mapsto\sigma^2\\ \tau\mapsto\tau}"'] & V_4 \arrow[r] & 1, \end{tikzcd}$$

and the obstruction is

$$(2, r(\alpha + \beta\sqrt{a})) \in \mathrm{Br}(L).$$

(5) a, b and -1 are quadratically independent: Let κ generate $\mathrm{Gal}(M(i)/M)$, and identify $\mathrm{Gal}(M/K)$ with $\mathrm{Gal}(M(i)/K(i))$. By Corollary 2.5, we must consider the subgroup $N = \langle \sigma, \tau\kappa \rangle \simeq D_4$ of $\mathrm{Gal}(M(i)/K)$, and let $L = K(i\sqrt{b})$. The restricted embedding problem is then given by by $M(i)/L$ and

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto\sigma^4"'] & D_{16} \arrow[r, "\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau\kappa}"'] & N \arrow[r] & 1. \end{tikzcd}$$

This is the embedding problem considered in Lemma 3.3, and the obstruction is

$$(2, \alpha'\beta')(a', \alpha'(\alpha' - 1)) \in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a$ (and hence $M(i) = L(\sqrt[4]{a'}, i)$), and $\alpha', \beta' \in L$, $\alpha' \neq 0$, such that $\alpha'^2 + a'\beta'^2 = 2$.

THEOREM 3.7 (The quasi-dihedral group): *Consider the embedding problem given by M/K and*

$$\begin{tikzcd} 1 \arrow[r] & C_4 \arrow[r, "i\mapsto x^4"'] & QD_{16} \arrow[r, "\substack{x\mapsto\sigma \\ y\mapsto\tau}"'] & D_4 \arrow[r] & 1. \end{tikzcd} \tag{3.8}$$

It is a necessary condition for solvability of this embedding problem that the embedding problem given by M/K and

$$\begin{tikzcd} 1 \arrow[r] & \mu_2 \arrow[r] & D_8 \arrow[r, "\substack{\sigma\mapsto\sigma \\ \tau\mapsto\tau}"'] & D_4 \arrow[r] & 1 \end{tikzcd} \tag{3.7}$$

is solvable. Hence, as above we will assume $(2, ab) = (-b, r\alpha)$.

Again there are five cases:

(1) $i \in K$: The N of Theorem 1.1 is $\langle\sigma\rangle$. Hence, $L = K(\sqrt{b})$, and the restricted embedding problem is given by M/L and

$$1 \to \mu_4 \to C_{16} \to C_4 \to 1.$$

The obstruction to this embedding problem is

$$(a', \alpha')(i, \alpha'\beta') \in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a = \left([(\alpha + \beta\sqrt{a})i + \sqrt{a}\sqrt{b}]\sqrt{\theta}\right)^4$ and $\alpha', \beta' \in L$, such that $\alpha' \neq 0$ and $\alpha'^2 - a'\beta'^2 = i$. This is exactly the same criterion as in case (1) *of Theorem 3.6* above.

(2) *$a = -1$: We then have $N = \langle\sigma^2, \sigma\tau\rangle$ and $L = K(i\sqrt{b})$. The restricted embedding problem is given by M/L and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto x^2"'] & Q_{16} \arrow[r, "\substack{x\mapsto\sigma^2 \\ y\mapsto\sigma\tau}"'] & V_4 \arrow[r] & 1. \end{tikzcd}$$

By Lemma 3.2, the obstruction to this embedding problem is

$$(2, r(\alpha + i\sqrt{b}))(-1, -1) \in \mathrm{Br}(L),$$

cf. case (2) *of Theorem 3.6.*

(3) *$b = -1$: This is the case considered in Lemma 3.4: We may assume $r = \beta = 1$ and $\alpha = 0$, and get the obstruction*

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

where $\alpha', \beta' \in K$, $\alpha' \neq 0$, such that $\alpha'^2 + a\beta'^2 = 2$.

(4) *$ab =_2 -1$: We have $N = \langle \sigma^2, \tau \rangle$ and $L = K(\sqrt{a})$. The restricted embedding problem is given by M/L and*

$$1 \to \mu_4 \xrightarrow[i \mapsto \sigma^2]{} D_8 \xrightarrow[\substack{\sigma \mapsto \sigma^2 \\ \tau \mapsto \tau}]{} V_4 \to 1,$$

and the obstruction is

$$(2, r(\alpha + \beta\sqrt{a})) \in \mathrm{Br}(L),$$

as in case (4) *of Theorem 3.6.*

(5) *a, b and -1 are quadratically independent: Let κ generate $\mathrm{Gal}(M(i)/M)$, and identify $\mathrm{Gal}(M/K)$ with $\mathrm{Gal}(M(i)/K(i))$. By Corollary 2.5, we must consider the subgroup $N = \langle \sigma, \tau\kappa \rangle \simeq D_4$ of $\mathrm{Gal}(M(i)/K)$, and let $L = K(i\sqrt{b})$. The restricted embedding problem is then given by by $M(i)/L$ and*

$$1 \to \mu_4 \xrightarrow[i \mapsto x^4]{} QD_{16} \xrightarrow[\substack{x \mapsto \sigma \\ y \mapsto \tau\kappa}]{} N \to 1.$$

This is the embedding problem considered in Lemma 3.4, and the obstruction is

$$(2, \alpha'\beta')(a', -\alpha'(\alpha' - 1)) \in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a$ and $\alpha', \beta' \in L$, $\alpha' \neq 0$, such that $\alpha'^2 + a'\beta'^2 = 2$, cf. case (5) *of Theorem 3.6.*

THEOREM 3.8 (The quaternion group): *Consider the embedding problem given by M/K and*

$$(3.9) \qquad 1 \to C_4 \xrightarrow[i \mapsto x^4]{} Q_{32} \xrightarrow[\substack{x \mapsto \sigma \\ y \mapsto \tau}]{} D_4 \to 1.$$

As above, it is a necessary condition for solvability of this embedding problem that the embedding problem given by M/K and

$$(3.7) \qquad 1 \to \mu_2 \to D_8 \xrightarrow[\substack{\sigma \mapsto \sigma \\ \tau \mapsto \tau}]{} D_4 \to 1$$

is solvable. Hence, we will again assume $(2, ab) = (-b, r\alpha)$.

There are now the usual five cases:

(1) *$i \in K$: We have $N = \langle \sigma \rangle$ and $L = K(\sqrt{b})$. The restricted embedding problem is thus given by M/L and*

$$1 \to \mu_4 \to C_{16} \to C_4 \to 1.$$

The obstruction to this embedding problem is

$$(a',\alpha')(i,\alpha'\beta')\in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a = \left([(\alpha-\beta\sqrt{a})i+\sqrt{a}\sqrt{b}]\sqrt{\theta}\right)^4$ *and* $\alpha',\beta'\in L$, *such that* $\alpha'\neq 0$ *and* $\alpha'^2 - a'\beta'^2 = i$. *Again, this is exactly the same criterion as in the cases (1) above.*

(2) $a=-1$: $N=\langle\sigma^2,\sigma\tau\rangle$ *and* $L=K(i\sqrt{b})$. *The restricted embedding problem is given by* M/L *and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto x^2"'] & Q_{16} \arrow[r, "\substack{x\mapsto\sigma^2\\ y\mapsto\sigma\tau}"'] & V_4 \arrow[r] & 1. \end{tikzcd}$$

By Lemma 3.2, the obstruction to this embedding problem is

$$(2,r(\alpha+i\sqrt{b}))(-1,-1)\in\mathrm{Br}(L),$$

as in case (2) *of the quasi-dihedral group.*

(3) $b=-1$: *This is the case considered in Lemma 3.5: We may assume* $r=\beta=1$ *and* $\alpha=0$, *and get the obstruction*

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

where $\alpha',\beta'\in K$, $\alpha'\neq 0$, *such that* $\alpha'^2+a\beta'^2=2$.

(4) $ab =_2 -1$: *We have* $N=\langle\sigma^2,\tau\rangle$ *and* $L=K(\sqrt{a})$. *The restricted embedding problem is given by* M/L *and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto x^2"'] & Q_{16} \arrow[r, "\substack{x\mapsto\sigma^2\\ y\mapsto\tau}"'] & V_4 \arrow[r] & 1, \end{tikzcd}$$

and the obstruction is

$$(2,r(\alpha+\beta\sqrt{a}))(-1,-1)\in\mathrm{Br}(L)$$

by Lemma 3.2.

(5) a, b *and* -1 *are quadratically independent: Let* κ *generate* $\mathrm{Gal}(M(i)/M)$, *and identify* $\mathrm{Gal}(M/K)$ *with* $\mathrm{Gal}(M(i)/K(i))$. *By Corollary 2.5, we must consider the subgroup* $N=\langle\sigma,\tau\kappa\rangle\simeq D_4$ *of* $\mathrm{Gal}(M(i)/K)$, *and let* $L=K(i\sqrt{b})$. *The restricted embedding problem is then given by by* $M(i)/L$ *and*

$$\begin{tikzcd} 1 \arrow[r] & \mu_4 \arrow[r, "i\mapsto x^4"'] & Q_{32} \arrow[r, "\substack{x\mapsto\sigma\\ y\mapsto\tau\kappa}"'] & N \arrow[r] & 1. \end{tikzcd}$$

This is the embedding problem considered in Lemma 3.5, and the obstruction is

$$(2,\alpha'\beta')(a',\alpha'(\alpha'-1))(-1,-1) \in \mathrm{Br}(L),$$

where $a' = [2rab(\beta - i\sqrt{b})]^2 a$ *and* $\alpha', \beta' \in L$, $\alpha' \neq 0$, *such that* $\alpha'^2 + a'\beta'^2 = 2$, *cf. the cases* (5) *above.*

Proof of Proposition 1.2: If -1 and 2 are quadratically independent in the ground field K, the D_4-extension $K(\sqrt[4]{2}, i)/K$ can be embedded in a D_{16}-extension by Lemma 3.3: K must have characteristic $\neq 3$, and we have $(4/3)^2 + 2(1/3)^2 = 2$. Hence, we can let $\alpha = 4/3$ and $\beta = 1/3$, and get

$$(2,\alpha\beta)(a,\alpha(\alpha-1)) = (2,4/9)(2,4/9) = 1 \in \mathrm{Br}(K).$$

If $-1 \in (K^*)^2$, the criteria for embedding a D_4-extension in D_{16}- and Q_{32}-extensions are identical. In the other cases, the obstructions differ by a factor $(-1,-1) \in \mathrm{Br}(K)$. Thus, we may assume that -1 and 2 are not quadratically independent in K^* and that -1 is not a sum of two squares in K. In particular, -2 is not a square, and so we must have $\sqrt{2} \in K^*$.

Let $M/K = K(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b})/K$ be a D_4-extension as in section 3, and assume M/K embeddable in a Q_{32}-extension. The cases $a =_2 -1$ and $ab =_2 -1$ are impossible, since they both include criteria of the form $(2,x) = (-1,-1)$ in $\mathrm{Br}(K)$, contradicting $(2,x) = 1$ and $(-1,-1) \neq 1$. We must therefore have one of the cases $b =_2 -1$ and $a, b, -1$ quadratically independent. In both cases we get $(a, 2-\sqrt{2}) = (-1,-1)$ by letting $\alpha' = \sqrt{2}$ and $\beta' = 0$. It follows that $2-\sqrt{2}$ is not a square in K^*, since $(-1,-1) \neq 1$. However, $2-\sqrt{2} = (1-\sqrt{2}/2)^2 + (1/\sqrt{2})^2$ is a sum of two squares, and so $2-\sqrt{2}$ and -1 are quadratically independent. By Lemma 3.3, the D_4-extension $K(\sqrt[4]{2-\sqrt{2}}, i)/K$ can be embedded in a D_{16}-extension. ∎

Proof of Proposition 1.3: We have quadratically independent $a, b \in K^*$, such that $(a,ab) = 1$ and $(2,ab) = (-b,x)$ for some $x \in K^*$.

If -1 and 2 are quadratically independent, we get a D_{16}-extension as in the proof of Proposition 1.2.

If $-1 \in (K^*)^2$, we have $D_8 \Leftrightarrow Q_{16}$ by [Le, Exs. 4.3–4.4].

If $-2 \in (K^*)^2$: Let $a' = ab$. Then $(a',a'b) = 1$ and $(2,a'b)(b,-1) = (-b,x)$, and so we get a Q_{16}-extension by [Le, Ex. 4.4].

$2 \in (K^*)^2$: Assume first that there exists $a' \in K^*$, such that a' is a sum of three squares in K, but not a sum of two squares. Write $a' = p^2 + q^2 + r^2$, and let $b' = p^2 + q^2$. Then $(a', a'b') = 1$ and $(2, a'b')(b', -1) = 1 = (-b', 1)$. Thus, we have a Q_{16}-extension. Otherwise every sum of squares in K is a sum of two squares: If K is not formally real, we then have $(2, ab)(b, -1) = 1$, and so get a Q_{16}-extension. If K is formally real: We can let $\alpha = \sqrt{2}$ and $\beta = 0$. The obstruction to embedding $K(\sqrt[4]{a'}, i)/K$ in a D_{16}-extension is then $(a', 2 - \sqrt{2})$. If $2 - \sqrt{2} \in (K^*)^2$, we can use any $a' \in K^* \setminus (K^*)^2$. If $2 - \sqrt{2} \notin (K^*)^2$, we can let $a' = 4 + \sqrt{2}$, since $2 - \sqrt{2}$ is a sum of two squares. Thus, we get a D_{16}-extension. ∎

References

[AFSandS] J. K. Arason, B. Fein, M. Schacher and J. Sonn, *Cyclic extensions of $K(\sqrt{-1})/K$*, Transactions of the American Mathematical Society **313** (1989), 843–851.

[Br] R. Brauer, *Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind*, Journal für die reine und angewandte Mathematik **168** (1932), 44–64.

[GandS] H. G. Grundman and T. L. Smith, *Automatic realizability of Galois groups of order* 16, Proceedings of the American Mathematical Society **124** (1996), 2631–2640.

[Ho] K. Hoechsmann, *Zum Einbettungsproblem*, Journal für die reine und angewandte Mathematik **229** (1968), 81–106.

[Ja] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.

[J&Y] C. U. Jensen and N. Yui, *Quaternion extensions*, in *Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata*, Kinokuniya, Tokyo, 1987, pp. 155–182.

[Ki] I. Kiming, *Explicit classifications of some* 2*-extensions of a field of characteristic different from* 2, Canadian Journal of Mathematics **42** (1990), 825–855.

[Le] A. Ledet, *On* 2*-groups as Galois groups*, Canadian Journal of Mathematics **47** (1995), 1253–1273.

[Lo] F. Lorenz, *Einführung in die Algebra II*, B. I. Wissenschaftsverlag, Mannheim, 1990.

[Sch] Leila Schneps, *Explicit realisations of subgroups of* $\mathrm{GL}_2(\mathbf{F}_3)$ *as Galois groups*, Journal of Number Theory **39** (1991), 5–13.

[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, Journal für die reine und angewandte Mathematik **174** (1936), 237–245.