Can. J. Math. Vol. **47** (6), 1995 pp. 1253–1273

ON 2-GROUPS AS GALOIS GROUPS

ARNE LEDET

ABSTRACT. Let L/K be a finite Galois extension in characteristic $\neq 2$, and consider a non-split Galois theoretical embedding problem over L/K with cyclic kernel of order 2. In this paper, we prove that if the Galois group of L/K is the direct product of two subgroups, the obstruction to solving the embedding problem can be expressed as the product of the obstructions to related embedding problems over the corresponding subextensions of L/K and certain quaternion algebra factors in the Brauer group of K. In connection with this, the obstructions to realising non-abelian groups of order 8 and 16 as Galois groups over fields of characteristic $\neq 2$ are calculated, and these obstructions are used to consider automatic realisations between groups of order 4, 8 and 16.

1. **Introduction.** Let L/K be a Galois extension of fields, and let

$$1 \longrightarrow N \longrightarrow E \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1 \tag{1}$$

be an extension of pro-finite groups. ($\mathrm{Gal}(L/K)$ denotes the Galois group of the field extension L/K.) The corresponding (Galois theoretical) *embedding problem* then consists in determining whether or not there exists a Galois extension M/K with $L \subseteq M$ and an isomorphism $\varphi: E \longrightarrow \mathrm{Gal}(M/K)$ making the diagram

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{Gal}(L/K) \\ {\scriptstyle\varphi}\downarrow & & \| \\ \mathrm{Gal}(M/K) & \underset{\mathrm{res}}{\longrightarrow} & \mathrm{Gal}(L/K) \end{array}$$

commutative. A pair $(M/K, \varphi)$ satisfying these conditions is called a *solution* to the embedding problem. Also, a Galois extension M/K is called a solution to the embedding problem, if there exists a φ, such that $(M/K, \varphi)$ is a solution.

In this paper we shall consider a special (and important) kind of embedding problems (1), namely the case where N is finite of order 2 and the characteristic of K is $\neq 2$. The group extension then has the form

$$1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1, \tag{2}$$

where $\mu_2 = \{\pm 1\}$ is the group of second roots of unity in the multiplicative group L^* of the field L.

The solvability of an embedding problem (2) depends on the 2-torsion of the Brauer group $\mathrm{Br}(K)$ of the ground field, as the following well known result shows:

Received by the editors May 6, 1994.
AMS subject classification: 12F12.

THEOREM 1.1. *Let L/K be a finite Galois extension in characteristic $\neq 2$, and let*

$$1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1 \tag{2}$$

be a non-split group extension with characteristic class $\gamma \in H^2\big(\mathrm{Gal}(L/K), \mu_2\big)$. (I.e., γ represents the extension (2) in the usual way.) Then the embedding problem given by L/K and (2) is solvable, if and only if $i(\gamma) = 1$ in $H^2\big(\mathrm{Gal}(L/K), L^*\big)$, where the map $i: H^2\big(\mathrm{Gal}(L/K), \mu_2\big) \to H^2\big(\mathrm{Gal}(L/K), L^*\big)$ is induced by the inclusion $\mu_2 \subseteq L^*$.

Furthermore, if $M/K = L(\sqrt{\omega})/K$ is one solution, then all the solutions are $L(\sqrt{r\omega})/K$, $r \in K^*$.

A proof of Theorem 1.1 can be found for instance in [Sc, Lemma 1] or in [Ki, pp. 826–827].

The cohomology group $H^2\big(\mathrm{Gal}(L/K), L^*\big)$ is canonically isomorphic to the relative Brauer group $\mathrm{Br}(L/K)$ of the extension L/K by $[c] \mapsto [L, G, c]$, where $[L, G, c]$ denotes the equivalence class of the crossed product algebra (L, G, c), *cf.* [Ja, Theorem 8.11] or [Lo, Section 30 Satz 2]. Hence, we may consider $i(\gamma)$ as an element of $\mathrm{Br}(L/K)$. This element is called the *obstruction* to the embedding problem.

The result that the solvability of an embedding problem might depend on the splitting of a crossed product algebra is classical: It is essentially the content of [Br, Satz 7].

To us, the advantage of representing the obstruction to an embedding problem by a crossed product algebra instead of a factor system lies in the following theorem:

THEOREM 1.2 [JA, THEOREM 4.7], [LA, COROLLARY 1.7]. *Let $\mathfrak{A}/K$ be a finite-dimensional central simple algebra, and let $\mathfrak{B}/K$ be a central simple subalgebra. Then the centraliser*

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

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

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

In particular, $[\mathfrak{A}] = [\mathfrak{B}][C_{\mathfrak{A}}(\mathfrak{B})]$ in the Brauer group $\mathrm{Br}(K)$.

The obstruction $[L, G, c]$, where $c \in Z^2(G, \mu_2)$ represents γ, is of order ≤ 2 in $\mathrm{Br}(K)$, since $c^2 = 1$. Hence, by Merkurjevs Theorem in [Me], $[L, G, c]$ can be written as a product of quaternion algebras. In reasonably simple cases, such as the ones we will consider, this decomposition can be obtained as follows: Find a quaternion subalgebra Q of $\Gamma = (L, G, c)$. Then $\Gamma \simeq Q \otimes_K C_\Gamma(Q)$ by Theorem 1.2, and $\Gamma' = C_\Gamma(Q)$ is a new finite-dimensional central simple algebra. In $\mathrm{Br}(K)$, we have $[\Gamma] = [Q][\Gamma']$, and so $[\Gamma']$ is again of order ≤ 2. Thus, the process can (perhaps) be continued, ending in a decomposition of Γ as a tensor product of quaternion algebras. (Of course, if the degree of Γ is not a power of 2, Γ is not a tensor product of quaternion algebras. But in that case it might be possible to write Γ as a tensor product of quaternion algebras and an odd-dimensional algebra, which is then automatically split and may be disregarded, since all algebras obtained have order ≤ 2 in $\mathrm{Br}(K)$.)

All relevant facts about Brauer groups and crossed product algebras can be found in [Ja, 4.6–4.7 and 8.4–8.5], [Lo, Sections 29–30] or [La, Chapter 4]. The necessary results about quaternion algebras can be found in [Lo, Section 30] or [La, Chapter 3]. We will use the standard notation for quaternion algebras: For $a, b \in K^*$ the quaternion algebra $(\frac{a,b}{K})$ 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 $(\frac{a,b}{K})$ in $\mathrm{Br}(K)$ will be denoted by (a, b).

EXAMPLE 1.3. Let $K(\sqrt{a})/K$ be a quadratic extension, and consider the embedding problem given by

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathrm{Gal}\big(K(\sqrt{a})/K\big) \longrightarrow 1.$$

The obstruction is then clearly the quaternion algebra $(a, -1) = (a, a)$, and we get another well known result: A quadratic extension $K(\sqrt{a})/K$ can be embedded in a cyclic extension of degree 4, if and only if a is a sum of two squares in K.

And if $a = x^2 + y^2$, $K(\sqrt{a + x\sqrt{a}})/K$ is a cyclic extension of degree 4, hence all solutions are of the form $K\big(\sqrt{r(a + x\sqrt{a})}\big)/K, r \in K^*$.

The purpose of this paper is to determine the decomposition of the obstruction to an embedding problem as a product of quaternion algebras (in the Brauer group) in a number of cases, primarily when G is a 2-group, *i.e.*, a group of 2-power order. In Section 2 we consider the case where $\mathrm{Gal}(L/K)$ is a direct product of finite groups. It is then possible to 'reduce' the problem of determining the obstruction in the general case to that of determining obstructions to the embedding problems obtained by restriction to the direct factors. This is the content of Theorem 2.4 and Corollary 2.5. In Section 3 we determine the obstruction to embedding a $\mathbb{Z}/4\mathbb{Z}$-extension in a $\mathbb{Z}/8\mathbb{Z}$-extension, and the resulting special case of Corollary 2.5 is then used to give an exact criterion for the existence of M_{16}-extensions, where M_{16} is the modular group of order 16. In Section 4 we determine the obstruction to any embedding problem (2), in which $\mathrm{Gal}(L/K)$ is the dihedral group of order 8. As a result, we get criteria for the realisability of several non-abelian groups of order 16 as Galois groups. These criteria are then used in Section 5 to consider questions of automatic realisability.

2. **A reduction theorem.**

In the Sections 2–4, all fields are assumed to have characteristic $\neq 2$.

If G is a finite group, $O^2(G)$ is defined as the intersection of all normal subgroups in G of 2-power index. $O^2(G)$ is then the minimal normal subgroup in G of 2-power index. It is clear that $O^2(G)$ is the composite of all odd-order Sylow subgroups of G, and hence that $O^2(G)$ is the subgroup of G generated by all elements of odd order.

LEMMA 2.1. *Let G and H be finite groups, and let*

$$1 \longrightarrow \mu_2 \longrightarrow E \underset{p}{\longrightarrow} G \times H \longrightarrow 1$$

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

be a group extension. Let $\sigma \in O^2(G)$, $\tau \in H$, *and let* s *and* t *in* E *be pre-images of* $\sigma = (\sigma, 1)$ *and* $\tau = (1, \tau)$. *Then* $ts = st$.

PROOF. By the above remarks we may assume σ to be of odd order. Hence, the two pre-images s and $-s$ of σ have different orders. Since s and tst^{-1} have the same order, $tst^{-1} = -s$ is impossible. ∎

LEMMA 2.2. *Let* G *and* H *be finite groups, and let* $\sigma_1, \dots, \sigma_m \in G$ *and* $\tau_1, \dots, \tau_n \in H$ *represent minimal generating sets for the 2-groups* $G/O^2(G)$ *and* $H/O^2(H)$. *(i.e., the groups* $G/O^2(G)$ *and* $H/O^2(H)$ *are minimally generated by the co-sets* $\sigma_1 O^2(G), \dots, \sigma_m O^2(G)$ *and* $\tau_1 O^2(H), \dots, \tau_n O^2(H)$.*) Let* $k \in \{1, \dots, m\}$ *and* $l \in \{1, \dots, n\}$. *Then there exists an extension*

$$1 \longrightarrow \mu_2 \longrightarrow E_{kl} \xrightarrow[p]{} G \times H \longrightarrow 1 \tag{3}$$

with the following properties:

(1) The restrictions of (3) to G *and* H *are both split exact.*

(2) Let $s_1, \dots, s_m, t_1, \dots, t_n \in E_{kl}$ *be pre-images of* $\sigma_1, \dots, \sigma_m, \tau_1, \dots, \tau_n$. *Then*

$$t_j s_i = s_i t_j, \quad (i,j) \neq (k,l),$$
$$t_l s_k = -s_k t_l.$$

PROOF. By going via $G/O^2(G)$ and $H/O^2(H)$ we see that there exists homomorphisms $\varphi: G \longrightarrow \mathbb{Z}/2\mathbb{Z}$ and $\psi: H \longrightarrow \mathbb{Z}/2\mathbb{Z}$, such that $\varphi(\sigma_i) = \delta_{ik}$ and $\psi(\tau_j) = \delta_{jl}$. ($\delta$ denotes the Kronecker delta.) We then get a homomorphism $\varphi \times \psi: G \times H \longrightarrow V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We consider the extension

$$1 \longrightarrow \mu_2 \longrightarrow D_4 \xrightarrow[q]{} V_4 \longrightarrow 1, \tag{$*$}$$

where D_4 is the dihedral group of order 8, generated by elements σ and τ with $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$, and q is given by $q(\sigma) = (1,1)$ and $q(\tau) = (0,1)$. Inflating this extension to an extension of $G \times H$ via $\varphi \times \psi$ gives

$$1 \longrightarrow \mu_2 \longrightarrow E_{kl} \xrightarrow[(x,y,z)\mapsto(y,z)]{} G \times H \longrightarrow 1,$$

where

$$E_{kl} = \big\{(x,y,z) \in D_4 \times G \times H \mid q(x) = \big(\varphi(y), \psi(z)\big)\big\}.$$

Since the restrictions of ($*$) to $\mathbb{Z}/2\mathbb{Z} \times 0$ and $0 \times \mathbb{Z}/2\mathbb{Z}$ are both split exact, this extension has property (1). As pre-images $s_1, \dots, s_m, t_1, \dots, t_n \in E_{kl}$ we may choose $s_i = (1, \sigma_i, 1)$, $i \neq k$, $s_k = (\sigma\tau, \sigma_k, 1)$, $t_j = (1, 1, \tau_j)$, $j \neq l$, and $t_l = (\tau, 1, \tau_l)$, and (2) is then obvious. ∎

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

REMARK. If H is a subgroup of the group G, and $\gamma \in H^2(G, \mu_2)$ is the characteristic class of an extension

$$1 \longrightarrow \mu_2 \longrightarrow E \underset{p}{\longrightarrow} G \longrightarrow 1,$$

the element $\mathrm{res}_{G\to H}\gamma \in H^2(H, \mu_2)$ is the characteristic class of the extension

$$1 \longrightarrow \mu_2 \longrightarrow p^{-1}(H) \underset{p}{\longrightarrow} H \longrightarrow 1.$$

If $\kappa: F \longrightarrow G$ is a surjective homomorphism, $\inf_{G\to F}\gamma$ is the characteristic class of the extension

$$1 \longrightarrow \mu_2 \longrightarrow E \times_{(p,\kappa)} F \underset{(e,\sigma)\mapsto\sigma}{\longrightarrow} F \longrightarrow 1,$$

where $E \times_{(p,\kappa)} F = \{(e, \sigma) \in E \times F \mid p(e) = \kappa(\sigma)\}$ is the pull-back.

PROPOSITION 2.3. *Let G and H be finite groups, and let*

$$1 \longrightarrow \mu_2 \longrightarrow E \underset{p}{\longrightarrow} G \times H \longrightarrow 1 \tag{4}$$

be a group extension with characteristic class $\gamma \in H^2(G \times H, \mu_2)$. Let $\sigma_1, \ldots, \sigma_m \in G$ and $\tau_1, \ldots, \tau_n \in H$ represent minimal generating sets for the groups $G/O^2(G)$ and $H/O^2(G)$, and let $s_1, \ldots, s_m, t_1, \ldots, t_n \in E$ be pre-images of $\sigma_1, \ldots, \sigma_m, \tau_1, \ldots, \tau_n$. Define $d_{ij} \in \{0, 1\}$ by $t_j s_i = (-1)^{d_{ij}} s_i t_j$. Then

$$\gamma = (\inf_{G\to G\times H} \mathrm{res}_{G\times H\to G}\gamma) \cdot (\inf_{H\to G\times H} \mathrm{res}_{G\times H\to H}\gamma) \cdot \prod_{i,j} \gamma_{ij}^{d_{ij}},$$

where γ_{kl} is the characteristic class of the extension (3) in Lemma 2.2.

PROOF. Let $\lambda = \gamma \cdot (\inf_{G\to G\times H} \mathrm{res}_{G\times H\to G}\gamma) \cdot (\inf_{H\to G\times H} \mathrm{res}_{G\times H\to H}\gamma) \cdot \prod_{i,j} \gamma_{ij}^{d_{ij}}$ and consider the corresponding extension

$$1 \longrightarrow \mu_2 \longrightarrow F \underset{q}{\longrightarrow} G \times H \longrightarrow 1. \tag{$*$}$$

Since $\mathrm{res}_{G\times H\to G} \inf_{G\to G\times H}$ and $\mathrm{res}_{G\times H\to H} \inf_{H\to G\times H}$ are the identity maps on $H^2(G, \mu_2)$ and $H^2(H, \mu_2)$ (and in fact on $Z^2(G, \mu_2)$ and $Z^2(H, \mu_2)$), the restrictions of this extension to G and H are both split exact. Also, if $u_1, \ldots, u_m, v_1, \ldots, v_n \in F$ are pre-images of $\sigma_1, \ldots, \sigma_m, \tau_1, \ldots, \tau_n$, we have $v_j u_i = u_i v_j$ for all i and j: If $t_j s_i = s_i t_j$, we have $d_{ij} = 0$, and λ 'inherits' the relation from γ. If $t_j s_i = -s_i t_j$, we have $d_{ij} = 1$, and λ 'inherits' the relation from $\gamma \cdot \gamma_{ij}$.

Hence, we may choose homomorphisms $s: G \longrightarrow F$ and $t: H \longrightarrow F$ with $qs = 1_G$ and $qt = 1_H$, and get $t(\tau_j)s(\sigma_i) = s(\sigma_i)t(\tau_j)$ for all i and j. By Lemma 2.1, $t(\tau)s(\sigma) = s(\sigma)t(\tau)$ if $\sigma \in O^2(G)$ or $\tau \in O^2(H)$. Since G (H) is generated by $O^2(G), \sigma_1, \ldots, \sigma_m$ ($O^2(H), \tau_1, \ldots, \tau_n$), we get $t(\tau)s(\sigma) = s(\sigma)t(\tau)$ for all $\sigma \in G$ and $\tau \in H$. Thus, $(\sigma, \tau) \mapsto s(\sigma)t(\tau)$ is a homomorphism $G \times H \longrightarrow F$, and $(*)$ is split exact, *i.e.*, $\lambda = 1$. ∎

In particular, the properties (1) and (2) of Lemma 2.2 determines γ_{kl} uniquely.

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

THEOREM 2.4. *Let L/K be a $G \times H$-extension, where G and H are finite groups, and let*

$$1 \longrightarrow \mu_2 \longrightarrow E \xrightarrow[p]{} G \times H \longrightarrow 1 \tag{4}$$

be a nonsplit group extension with characteristic class $\gamma \in H^2(G, \mu_2)$. Let L'/K and L''/K be the subextensions corresponding to the factors G and H. (I.e., L'/K is a G-extension, L''/K is an H-extension, and $L = L'L''$.) Let $\sigma_1, \dots, \sigma_m \in G$ and $\tau_1, \dots, \tau_n \in H$ represent minimal generating sets for the groups $G/O^2(G)$ and $H/O^2(H)$, and choose $a_1, \dots, a_m, b_1, \dots, b_n \in K^*$, such that $\sqrt{a_i} \in (L')^*$, $\sqrt{b_j} \in (L'')^*$, $\sigma_k(\sqrt{a_i}) = (-1)^{\delta_{ik}}\sqrt{a_i}$ and $\tau_l(\sqrt{b_j}) = (-1)^{\delta_{jl}}\sqrt{b_j}$. ($\delta$ denotes the Kronecker delta.) Finally, let $s_1, \dots, s_m$, $t_1, \dots, t_n \in E$ be pre-images of $\sigma_1, \dots, \sigma_m, \tau_1, \dots, \tau_n$, and let $d_{ij} \in \{0, 1\}$ be given by $t_j s_i = (-1)^{d_{ij}} s_i t_j$.

Then the obstruction to the embedding problem given by L/K and (4) is

$$[L', G, \operatorname{res}_{G\times H \to G}\gamma] \cdot [L'', H, \operatorname{res}_{G\times H \to H}\gamma] \cdot \prod_{i,j}(a_i, b_j)^{d_{ij}} \in \operatorname{Br}(K).$$

REMARK. It is possible to choose $a_1, \dots, a_m, b_1, \dots, b_n$ as described, since $\sigma_1, \dots, \sigma_m$ and $\tau_1, \dots, \tau_n$ represent minimal generating sets for the maximal elementary abelian factor groups of $G/O^2(G)$ and $H/O^2(H)$, and hence for the maximal elementary abelian 2-factor groups of G and H.

PROOF. By Proposition 2.3 we have

$$\gamma = (\inf_{G\to G\times H} \operatorname{res}_{G\times H\to G}\gamma) \cdot (\inf_{H\to G\times H} \operatorname{res}_{G\times H\to H}\gamma) \cdot \prod_{i,j}\gamma_{ij}^{d_{ij}}.$$

Hence, the obstruction is

$$[L, G \times H, \inf_{G\to G\times H} \operatorname{res}_{G\times H\to G}\gamma] \cdot [L, G \times H, \inf_{H\to G\times H} \operatorname{res}_{G\times H\to H}\gamma] \cdot \prod_{i,j}[L, G \times H, \gamma_{ij}]^{d_{ij}}.$$

Obviously, the first two terms are $[L', G, \operatorname{res}_{G\times H\to G}\gamma]$ and $[L'', H, \operatorname{res}_{G\times H\to H}\gamma]$, as the inflation corresponds to the inclusion between the relative Brauer groups, *cf.* [Ja, Theorem 8.13] or [Lo, Section 30 F1]. Thus, it remains to prove

$$[L, G \times H, \gamma_{kl}] = (a_k, b_l).$$

In the proof of Lemma 2.2, γ_{kl} was constructed as the inflation from $H^2(V_4, \mu_2)$ of the characteristic class of the extension

$$1 \longrightarrow \mu_2 \longrightarrow D_4 \xrightarrow[q]{} V_4 \longrightarrow 1,$$

where $q(\sigma) = (1, 1)$ and $q(\tau) = (0, 1)$, through a homomorphism $\Phi: G \times H \longrightarrow V_4$, such that $\Phi(\sigma_i, 1) = (\delta_{ik}, 0)$ and $\Phi(1, \tau_j) = (0, \delta_{jl})$. In this case, this inflation can obviously be obtained from the restriction map $G \times H \longrightarrow \operatorname{Gal}(K'/K)$ instead, where $K' =$

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

$K(\sqrt{a_k}, \sqrt{b_l})$, since $\mathrm{Gal}(K'/K) \simeq V_4$, $\sigma_i(\sqrt{a_k}) = (-1)^{\delta_{ik}}\sqrt{a_k}$ and $\tau_j(\sqrt{b_l}) = (-1)^{\delta_{jl}}\sqrt{b_l}$. Replacing V_4 by $\mathrm{Gal}(K'/K)$, the extension becomes

$$(*) \qquad 1 \longrightarrow \mu_2 \longrightarrow D_4 \xrightarrow[q]{} \mathrm{Gal}(K'/K) \longrightarrow 1,$$

where $q(\sigma) = \rho_1\rho_2$, $q(\tau) = \rho_2$, and $\rho_1, \rho_2 \in \mathrm{Gal}(K'/K)$ are given by $\rho_1(\sqrt{a_k}) = -\sqrt{a_k}$, $\rho_1(\sqrt{b_l}) = \sqrt{b_l}$, $\rho_2(\sqrt{a_k}) = \sqrt{a_k}$ and $\rho_2(\sqrt{b_l}) = -\sqrt{b_l}$.

Since inflation corresponds to inclusion, $[L, G \times H, \gamma_{kl}]$ equals the obstruction to the embedding problem given by K'/K and $(*)$. This obstruction is represented by an algebra $\Gamma = K[\sqrt{a_k}, \sqrt{b_l}, u_1, u_2]$, where

$$u_1^2 = u_2^2 = 1,\ u_2u_1 = -u_1u_2,\ u_1x = \rho_1(x)u_1,\ u_2x = \rho_2(x)u_2, \quad \forall x \in K'.$$

Obviously, $K[u, v] \simeq (\frac{1,1}{K})$, and

$$C_\Gamma(K[u, v]) = K[\sqrt{a_k}v, \sqrt{b_l}u] \simeq \left(\frac{a_k, b_l}{K}\right).$$

Hence, $[L, G \times H, \gamma_{kl}] = [\Gamma] = (1, 1)(a_k, b_l) = (a_k, b_l)$ by Theorem 1.2. ∎

A straightforward induction argument gives

COROLLARY 2.5. *Let $G = G_1 \times \cdots \times G_n$, where $G_1, \ldots, G_n$ are finite groups. Let L/K be a G-extension, and let*

$$(5) \qquad 1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow G \longrightarrow 1$$

be a nonsplit extension with characteristic class $\gamma \in H^2(G, \mu_2)$. Let L_i/K be the subextension of L/K corresponding to the factor G_i. (I.e., L_i/K is a G_i-extension, and $L = L_1 \cdots L_n$.) Let $\sigma_{i,1}, \ldots, \sigma_{i,m_i} \in G_i$ represent a minimal generating set for $G_i/O^2(G_i)$, and choose pre-images $s_{i,1}, \ldots, s_{i,m_i} \in E$. Furthermore, let $a_{i,1}, \ldots, a_{i,m_i} \in K^*$, such that $\sqrt{a_{i,h}} \in L_i^*$ and $\sigma_{i,k}(\sqrt{a_{i,h}}) = (-1)^{\delta_{hk}}\sqrt{a_{i,h}}$.

Then the obstruction to the embedding problem given by L/K and (5) is

$$\prod_{i=1}^{n}[L_i, G_i, \mathrm{res}_{G \to G_i}(\gamma)] \cdot \prod_{(i,h,j,k)\in I}(a_{i,h}, a_{j,k})^{d(i,h,j,k)} \in \mathrm{Br}(K),$$

where $I = \{(i, h, j, k) \mid 1 \le i < j \le n,\ 1 \le h \le m_i, 1 \le k \le m_j\}$, and $d(i, h, j, k) \in \{0, 1\}$ is given by $s_{i,h}s_{j,k} = (-1)^{d(i,h,j,k)}s_{j,k}s_{i,h}$.

As an immediate corollary we get the following well known result (*cf.* [Fr, (7.6)] or [M&S, Theorem 1.2]):

COROLLARY 2.6. *Let $L/K = K(\sqrt{a_1}, \ldots, \sqrt{a_n})/K$ be a $(\mathbb{Z}/2\mathbb{Z})^n$-extension, and let $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(L/K)$ be given by $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$. Let*

$$(6) \qquad 1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1$$

be a nonsplit extension, and choose pre-images $s_1, \ldots, s_n \in E$ to $\sigma_1, \ldots, \sigma_n$. Define d_{ij}, $i \le j$, by $s_i^2 = (-1)^{d_{ii}}$ and $s_is_j = (-1)^{d_{ij}}s_js_i$, $i < j$. Then the obstruction to the embedding problem given by L/K and (6) is

$$\prod_{i\le j}(a_i, a_j)^{d_{ij}} \in \mathrm{Br}(K).$$

3. **The modular group.** Our goal is to obtain criteria for the realisability of non-abelian groups of order 16. There are nine such groups:

(1) The direct product $D_4 \times \mathbb{Z}/2\mathbb{Z}$, where D_4 is the dihedral group of order 8, *i.e.*, $D_4 = \langle \sigma, \tau \rangle$, where $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$.

(2) The direct product $Q_8 \times \mathbb{Z}/2\mathbb{Z}$, where Q_8 is the quaternion group of order 8, *i.e.*, Q_8 is the subgroup of $\mathbb{H}^*$ generated by i and j, where $\mathbb{H} = (\frac{-1,-1}{\mathbb{R}})$.

(3) The dihedral group $D_8 = \langle \sigma, \tau \rangle$, where $\sigma^8 = \tau^2 = 1$ and $\tau\sigma = \sigma^7\tau$.

(4) The quasi-dihedral group $QD_8 = \langle x, y \rangle$, where $x^8 = y^2 = 1$ and $yx = x^3y$.

(5) The quaternion group $Q_{16} = \langle x, y \rangle$, where $x^8 = 1, y^2 = x^4$ and $yx = x^7y$.

(6) The modular group $M_{16} = \langle x, y \rangle$, where $x^8 = y^2 = 1$ and $yxy^{-1} = x^5$. (The name 'modular group' can be found in [As, pp. 106–107].)

(7) The semidirect product $C \rtimes C = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} = \langle x, y \rangle$, where $x^4 = y^4 = 1$ and $yx = x^3y$. ($C \rtimes C$ can also be considered as the pull-back of Q_8 and $\mathbb{Z}/4\mathbb{Z}$ with respects to homomorphisms $Q_8, \mathbb{Z}/4\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$. This is the way it is described in [G&S], [GS&S] and [J1].)

(8) The pull-back $D\lambda C = D_4 \times_{(f,g)} \mathbb{Z}/4\mathbb{Z}$, where the homomorphisms $f: D_4 \to \mathbb{Z}/2\mathbb{Z}$ and $g: \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ have kernels $\langle \sigma^2, \tau \rangle$ and $2\mathbb{Z}/4\mathbb{Z}$ respectively, *i.e.*, $D\lambda C = \langle x, y, z \rangle$, where $x^4 = y^2 = z^2 = 1, yx = x^3yz$ and z is central.

(9) The central product $DC = (D_4 \times \mathbb{Z}/4\mathbb{Z})/\langle (\sigma^2, 2) \rangle = \langle x, y, z \rangle$, where $x^4 = y^2 = 1$, $yx = x^3y, x^2 = z^2$ and z is central.

Of these groups (1) and (2) are in a sense uninteresting: A field admits a $D_4 \times \mathbb{Z}/2\mathbb{Z}$-extension if and only if it admits a D_4-extension and has at least eight square classes, and similarly for $Q_8 \times \mathbb{Z}/2\mathbb{Z}$. And criteria for realising D_4- and Q_8-extensions are easily obtained from Corollary 2.6: Let $L/K = K(\sqrt{a}, \sqrt{b})/K$ be a V_4-extension, and let $\rho_1, \rho_2 \in \mathrm{Gal}(L/K) = V_4$ be given by $\rho_1(\sqrt{a}) = -\sqrt{a}$, $\rho_1(\sqrt{b}) = \sqrt{b}$, $\rho_2(\sqrt{a}) = \sqrt{a}$ and $\rho_2(\sqrt{b}) = -\sqrt{b}$. Consider the extensions

$$1 \longrightarrow \mu_2 \underset{-1 \mapsto \sigma^2}{\longrightarrow} D_4 \underset{\substack{\sigma \mapsto \rho_1 \\ \tau \mapsto \rho_2}}{\longrightarrow} V_4 \longrightarrow 1 \tag{7}$$

and

$$1 \longrightarrow \mu_2 \hookrightarrow Q_8 \underset{\substack{i \mapsto \rho_1 \\ j \mapsto \rho_2}}{\longrightarrow} V_4 \longrightarrow 1. \tag{8}$$

By Corollary 2.6 the obstruction to the embedding problem given by L/K and (7) is

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

and the obstruction to the embedding problem given by L/K and (8) is

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

Hence, a V_4-extension $L/K = K(\sqrt{a}, \sqrt{b})/K$ can be embedded in a D_4-extension M/K, such that $M/K(\sqrt{b})$ is cyclic, if and only if $(a, ab) = 1$, and it can be embedded in a Q_8-extension, if and only if $(a, ab) = (b, b)$.

The group DC can be treated directly using Corollary 2.6 as well: Let $L/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$ be a $(\mathbb{Z}/2\mathbb{Z})^3$-extension, and let $\rho, \sigma, \tau \in \mathrm{Gal}(L/K)$ be given by

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

Then we have an extension

$$1 \to \mu_2 \underset{-1 \mapsto x^2}{\longrightarrow} DC \underset{\substack{x \mapsto \rho \\ y \mapsto \sigma \\ z \mapsto \tau}}{\longrightarrow} \mathrm{Gal}(L/K) \to 1, \tag{9}$$

and by Corollary 2.6 the obstruction to the embedding problem given by L/K and (9) is

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

In particular, a field K admits a DC-extension, if and only if there exists quadratically independent elements a, b and c in K^*, such that $(a,ab) = (c,c)$.

These results on D_4-, Q_8- and DC-extensions can all be found in [M&S, Corollary 1.3], with exactly the same proof.

The groups (3)–(5) and (7)–(8) all have D_4 as an epimorphic image and will be treated in the next section.

In this section we will consider the modular group M_{16}. It has $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as an epimorphic image, and it is therefore necessary to extend Corollary 2.6 to finite abelian groups of exponent 4, *i.e.*, it is necessary to describe the map $H^2\big(\mathrm{Gal}(L/K), \mu_2\big) \to \mathrm{Br}(L/K)$, when L/K is cyclic of degree 4:

EXAMPLE 3.1. Consider a cyclic extension L/K of degree 4. We may assume $L = K\Big(\sqrt{r(a+\sqrt{a})}\Big)$, where $a \in K^* \setminus (K^*)^2$ has the form $a = 1 + c^2$, $c \in K$, and $r \in K^*$. The Galois group $\mathrm{Gal}(L/K)$ is then generated by σ, where

$$\sigma\Big(\sqrt{r(a+\sqrt{a})}\Big) = \frac{rc\sqrt{a}}{\sqrt{r(a+\sqrt{a})}}.$$

For ease of notation we let $\theta = r(a+\sqrt{a})$.

The only non-split extension of $\mathrm{Gal}(L/K)$ with μ_2 is

$$1 \to \mu_2 \underset{-1 \mapsto 4}{\longrightarrow} \mathbb{Z}/8\mathbb{Z} \underset{1 \mapsto \sigma}{\longrightarrow} \mathrm{Gal}(L/K) \to 1,$$

and the obstruction to the corresponding embedding problem is represented by the cyclic algebra $\Gamma = (L, \sigma, -1) = L[u]$, where $u^4 = -1$ and $ua = \sigma(a)u$ for $a \in L$. We wish to write this algebra as a tensor product of two quaternion algebras.

Obviously $Q = K[\sqrt{a}, u + u^3] \simeq \left(\frac{a,-2}{K}\right)$ is a quaternion subalgebra of Γ, and by Theorem 1.2 we have $\Gamma \simeq Q \otimes_K C_\Gamma(Q)$. $C_\Gamma(Q)$ is a four-dimensional central simple

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

algebra, and so necessarily a quaternion algebra (*cf.* [Lo, Section 30]). Since $(u^2)^2 = -1$ and $u^2 \in C_\Gamma(Q)$, we seek an $\omega \in \Gamma$ with

$$\omega\sqrt{a} = \sqrt{a}\omega,\ \omega(u+u^3) = (u+u^3)\omega,\ \omega u^2 = -u^2\omega, \quad \omega^2 \in K^*.$$

Calculations show that we can let

$$\omega = \frac{1}{2}\sqrt{\theta}\left(\left(1+\frac{rc\sqrt{a}}{\theta}\right)+\left(1-\frac{rc\sqrt{a}}{\theta}\right)u^2\right),$$

and that $\omega^2 = ra$. Hence, $C_\Gamma(Q) = K[u^2,\omega] \simeq (\frac{-1,ra}{K})$, and the obstruction is

$$[\Gamma] = (a,-2)(-1,ra) = (a,-2)(-1,r)(-1,a) = (a,2)(-1,r) \in \mathrm{Br}(K).$$

We conclude that L/K can be embedded in a $\mathbb{Z}/8\mathbb{Z}$-extension, if and only if $(a,2) = (-1,r)$. This is the same criterion obtained in [Ki, Theorem 3], since $(a,2) = (a,c)$.

Another conclusion is the following: Let $K(\sqrt{a})/K$ be a quadratic extension. Then $K(\sqrt{a})/K$ can be embedded in a cyclic extension of degree 8, if and only if

$$(a,a) = 1 \quad \text{and} \quad \exists r \in K^* : (a,2) = (-1,r).$$

We can now extend Corollary 2.6 in the desired way:

PROPOSITION 3.2. *Let L/K be an $(\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/4\mathbb{Z})^s$-extension. We can write*

$$L = K\left(\sqrt{a_1},\dots,\sqrt{a_r},\sqrt{q_{r+1}(a_{r+1}+\sqrt{a_{r+1}})},\dots,\sqrt{q_{r+s}(a_{r+s}+\sqrt{a_{r+s}})}\right),$$

where $a_1,\dots,a_{r+s} \in K^*$ are quadratically independent, $a_i = 1+c_i^2$ for $i > r$, and $q_i \in K^*$. Let $\sigma_1,\dots,\sigma_{r+s} \in \mathrm{Gal}(L/K)$, such that $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$. Let

$$1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1 \tag{10}$$

be a non-split extension, and choose pre-images $t_1,\dots,t_{r+s} \in E$ to $\sigma_1,\dots,\sigma_{r+s}$. Then the obstruction to the embedding problem given by L/K and (10) is

$$\prod_{i=1}^{r}(a_i,a_i)^{d_i}\cdot\prod_{i=r+1}^{r+s}[(a_i,2)(-1,q_i)]^{d_i}\cdot\prod_{i<j}(a_i,a_j)^{d_{ij}},$$

where $t_i^2 = (-1)^{d_i}$ for $i \le r$, $t_i^4 = (-1)^{d_i}$ for $i > r$, and $t_it_j = (-1)^{d_{ij}}t_jt_i$.

EXAMPLE 3.3. Let $M/K = K\left(\sqrt{r(a+\sqrt{a})},\sqrt{b}\right)/K$ be a $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$-extension, where a and b in K^* are quadratically independent, $a = 1+c^2$ and $r \in K^*$. Let $\sigma,\tau \in \mathrm{Gal}(M/K)$ be given by

$$\sigma:\ \sqrt{r(a+\sqrt{a})} \mapsto \frac{rc\sqrt{a}}{\sqrt{r(a+\sqrt{a})}},\quad \sqrt{b}\mapsto\sqrt{b},$$
$$\tau:\ \sqrt{r(a+\sqrt{a})} \mapsto \sqrt{r(a+\sqrt{a})},\quad \sqrt{b}\mapsto-\sqrt{b}.$$

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

By Proposition 3.2, the obstruction to the embedding problem given by M/K and

$$1 \longrightarrow \mu_2 \underset{-1\mapsto x^4}{\longrightarrow} M_{16} \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} \mathrm{Gal}(M/K) \longrightarrow 1, \tag{11}$$

is

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

In particular, we see that a field K has an M_{16}-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a,a) = 1 \quad \text{and} \quad \exists r \in K^* : (a,2b) = (-1,r).$$

For instance, if -1 and 2 are quadratically independent in K^*, K admits an M_{16}-extension. More generally: If there exists $b \in K^*$, such that $a = 1 + b^2$ and b are $\neq 0$ and quadratically independent, K admits an M_{16}-extension.

An equivalent result on M_{16}-extensions, obtained independently, is given in [GS&S].

REMARK. Let $M/K = K\left(\sqrt{r(a+\sqrt{a})}, \sqrt{b}\right)/K$ be a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension as above. Let $L/K = K\left(\sqrt{r(a+\sqrt{a})}\right)/K$ be the 'canonical' $\mathbb{Z}/4\mathbb{Z}$-subextension. By Example 3.3, the obstruction to the embedding problem given by M/K and (11) is $(a,2)(-1,r)(a,b)$. By Example 3.1, $(a,2)(-1,r) = [L,\sigma,-1]$. (Where σ is considered as an element of $\mathrm{Gal}(L/K)$.) Also, $(a,b) = [L,\sigma,b^2]$ by [Ja, Theorem 8.15]. Hence, the obstruction is $[L,\sigma,-b^2]$, and the embedding problem is solvable, if and only if $-b^2$ is a norm in L/K.

Furthermore, if $-b^2 = N_{L/K}(x)$ for some $x \in L^*$, x^2/b has norm 1 in L/K, and by Hilberts 'Theorem 90' there exists $\omega \in L^*$, such that $\sigma(\omega)/\omega = x^2/b$. An easy calculation now shows that $M(\sqrt{\omega})/K$ is a solution to the embedding problem.

4. **The dihedral group.** In this section we will describe the map $H^2(D_4, \mu_2) \longrightarrow \mathrm{Br}(L/K)$, where L/K is a D_4-extension. This will enable us to obtain criteria for the realisation of all groups of order 16 having D_4 as an epimorphic image, *i.e.*, for the groups D_8, Q_{16}, QD_8, $C \rtimes C$ and $D \curlywedge C$.

First of all we must describe D_4-extensions. In Section 3 we got the following: A biquadratic extension $K(\sqrt{a}, \sqrt{b})/K$ can be embedded in a D_4-extension L/K, such that $L/K(\sqrt{b})$ is cyclic, if and only if $(a,ab) = 1$ in $\mathrm{Br}(K)$. $(a,ab) = 1$ is equivalent to the existence of $\alpha, \beta \in K$ with $\alpha^2 - a\beta^2 = ab$, and since $K(\sqrt{\alpha+\beta\sqrt{a}}, \sqrt{b})/K$ is then easily seen to be a D_4-extension of the desired kind, we see that any such extension is of the form $L/K = K\left(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b}\right)/K$, $r \in K^*$. Also, σ and τ in D_4 may be identified with the automorphisms σ and τ in $\mathrm{Gal}(L/K)$ given by

$$\sigma\left(\sqrt{r(\alpha+\beta\sqrt{a})}\right) = \frac{r\sqrt{ab}}{\sqrt{r(\alpha+\beta\sqrt{a})}}, \quad \sigma(\sqrt{b}) = \sqrt{b},$$
$$\tau\left(\sqrt{r(\alpha+\beta\sqrt{a})}\right) = \sqrt{r(\alpha+\beta\sqrt{a})}, \quad \tau(\sqrt{b}) = -\sqrt{b}.$$

The cohomology group $H^2(D_4, \mu_2)$ is isomorphic to μ_2^3 in the following way: Let $\gamma \in H^2(D_4, \mu_2)$, and consider the corresponding extension

$$1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow D_4 \longrightarrow 1. \tag{12}$$

Let s and t be pre-images of σ and τ respectively. Then we assign to γ the element $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \mu_2^3$ given by

$$s^4 = \varepsilon_1, \quad t^2 = \varepsilon_2, \quad ts = \varepsilon_3 s^3 t.$$

This is an isomorphism: It is clear that the triple $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ and the extension (12) are determined uniquely by each other, and that the map is an injective homomorphism $H^2(D_4, \mu_2) \longrightarrow \mu_2^3$. Also, the triples $(-1, 1, 1)$, $(1, -1, 1)$ and $(1, 1, -1)$ are in the image of $H^2(D_4, \mu_2)$, as the extensions (13), (14) and (17) of D_4 to QD_8, $C \rtimes C$ and $D \curlywedge C$ below shows, and so the map is surjective.

Thus, in order to describe the map $H^2(D_4, \mu_2) \longrightarrow \mathrm{Br}(L/K)$, it is enough to describe the images of the 2-cocycles corresponding to $(-1, 1, 1)$, $(1, -1, 1)$ and $(1, 1, -1)$.

The 2-cocycle corresponding to $(1, -1, 1)$ is obviously the characteristic class of the extension

$$1 \longrightarrow \mu_2 \underset{-1 \mapsto x^2}{\longrightarrow} C \rtimes C \underset{\substack{x \mapsto \sigma \\ y \mapsto \tau}}{\longrightarrow} D_4 \longrightarrow 1. \tag{13}$$

This extension is the inflation of the extension

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

with respect to the homomorphism $D_4 \longrightarrow \mathbb{Z}/2\mathbb{Z}$ with kernel $\langle \sigma \rangle$. In our interpretation of D_4 as a Galois group, this homomorphism corresponds to the restriction map $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}\big(K(\sqrt{b})/K\big)$. As the diagram

$$\begin{array}{ccc} H^2\Big(\mathrm{Gal}\big(K(\sqrt{b})/K\big), \mu_2\Big) & \longrightarrow & \mathrm{Br}\big(K(\sqrt{b})/K\big) \\ {\scriptstyle \mathrm{inf}}\downarrow & & \downarrow \\ H^2(D_4, \mu_2) & \longrightarrow & \mathrm{Br}(L/K) \end{array}$$

is commutative, the obstruction to the embedding problem given by L/K and (13) equals the obstruction to the embedding problem given by $K(\sqrt{b})/K$ and

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathrm{Gal}\big(K(\sqrt{b})/K\big) \longrightarrow 1.$$

By Example 1.3, this second obstruction is $(b, -1) = (b, b)$.

Similarly, the 2-cocycle corresponding to $(1, 1, -1)$ is the inflation of the characteristic class of the extension

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathrm{Gal}\big(K(\sqrt{a})/K\big) \longrightarrow 1,$$

and the image in $\mathrm{Br}(L/K)$ is therefore $(a, -1)$.

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

The last 2-cocycle corresponds to the quasi-dihedral group, and we will determine the obstruction to the associated embedding problem by brute force in the following

EXAMPLE 4.1. Consider the extension

$$1 \longrightarrow \mu_2 \underset{-1\mapsto x^4}{\longrightarrow} QD_8 \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_4 \longrightarrow 1. \tag{14}$$

The obstruction to the embedding problem given by this extension and our D_4-extension L/K is represented by the algebra $\Gamma = L[u_\sigma, u_\tau]$, where

$$u_\sigma^4 = -1,\ u_\tau^2 = 1,\ u_\tau u_\sigma = u_\sigma^3 u_\tau,$$
$$u_\sigma x = \sigma(x)u_\sigma,\ u_\tau x = \tau(x)u_\tau, \quad \forall x \in L.$$

$Q = K[\sqrt{a}, u_\sigma + u_\sigma^3] \simeq (\frac{a,-2}{K})$ is a quaternion subalgebra of Γ, and hence $\Gamma \simeq Q \otimes_K C_\Gamma(Q)$. $C_\Gamma(Q)$ is a 16-dimensional central simple algebra. Obviously, $R = K[\sqrt{b}, u_\tau] \simeq (\frac{b,1}{K})$ is a quaternion subalgebra of $C_\Gamma(Q)$. Thus, $\Gamma \simeq Q \otimes_K R \otimes_K C_{C_\Gamma(Q)}(R)$. $C_{C_\Gamma(Q)}(R) = C_\Gamma(Q \cdot R)$ is a four-dimensional central simple algebra, and hence a quaternion algebra. Since $\sqrt{b}u_\sigma^2 \in C_\Gamma(Q \cdot R)$, we seek $\omega \in C_\Gamma(Q \cdot R)$ with

$$\omega\sqrt{b}u_\sigma^2 = -\sqrt{b}u_\sigma^2\omega, \quad \omega^2 \in K^*.$$

Calculations show that we can let

$$\omega = \left(\frac{r\sqrt{ab}}{\sqrt{r(\alpha + \beta\sqrt{a})}} + \sqrt{r(\alpha + \beta\sqrt{a})}u_\sigma^2 \right)\sqrt{b},$$

and that $\omega^2 = 2\alpha r b$. Hence, $C_\Gamma(Q \cdot R) = K[\sqrt{b}u_\sigma^2, \omega] \simeq (\frac{-b, 2\alpha r b}{K})$, and $\Gamma \simeq (\frac{a,-2}{K}) \otimes_K (\frac{b,1}{K}) \otimes_K (\frac{-b,2\alpha r b}{K})$. The obstruction is then

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

(If $\alpha = 0$, $-b$ is a square in K^*, and $(-b, 2\alpha r)$ is simply the neutral element of $\mathrm{Br}(K)$.)

In particular, K admits a QD_8-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a, ab) = 1 \quad \text{and} \quad \exists x \in K^* : (a,-2) = (-b, x).$$

We now have the following

PROPOSITION 4.2. *Let L/K be a D_4-extension as described above, and let*

$$1 \longrightarrow \mu_2 \longrightarrow E \longrightarrow D_4 \longrightarrow 1 \tag{12}$$

be a non-split extension. Choose pre-images s and t in E of σ and τ respectively. Then the obstruction to the embedding problem given by L/K and (12) is

$$[(a,-2)(-b,2\alpha r)]^i (b,-1)^j (a,-1)^k \in \mathrm{Br}(K),$$

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

where $s^4 = (-1)^i$, $t^2 = (-1)^j$ *and* $ts = (-1)^k s^3 t$.

We are now able to extend Proposition 3.2 to the case, where G is an direct product of copies of $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and D_4. We will not state this result explicitly. Instead we use Proposition 4.2 to write down criteria for the realisability of the groups D_8, Q_{16}, $C \rtimes C$ and $D \leftthreetimes C$:

EXAMPLE 4.3. Let L/K be a D_4-extension as before, and look at the extension

$$1 \longrightarrow \mu_2 \underset{-1\mapsto\sigma^4}{\longrightarrow} D_8 \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} D_4 \longrightarrow 1. \tag{15}$$

By Proposition 4.2 the obstruction to the embedding problem given by L/K and (15) is

$$\begin{aligned}[(a,-2)(-b,2\alpha r)](a,-1) &= (a,2)(-b,2)(-b,\alpha r) = (a,2)(b,2)(-b,\alpha r)\\ &= (ab,2)(-b,\alpha r) \in \mathrm{Br}(K).\end{aligned}$$

In particular, K admits a D_8-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a,ab) = 1 \quad \text{and} \quad \exists x \in K^* : (ab,2) = (-b,x).$$

EXAMPLE 4.4. Consider instead the extension

$$1 \longrightarrow \mu_2 \underset{-1\mapsto x^4}{\longrightarrow} Q_{16} \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_4 \longrightarrow 1. \tag{16}$$

Proposition 4.2 gives us the obstruction

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

Hence, the field K admits a Q_{16}-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a,ab) = 1 \quad \text{and} \quad \exists x \in K^* : (ab,2)(b,-1) = (-b,x).$$

REMARK. If L/K is a Q_{2^n}-extension for some $n \geq 3$ and $K(\sqrt{a},\sqrt{b})/K$, $a, b \in K^*$, is the maximal elementary abelian subextension, a, b and ab are sums of squares in K by [J1, Theorem 1.2]. Also, by the remark following Theorem 1.2 in [J1], there exists a limit, independent of K, to the number of squares necessary. In the case $n = 3$ it is well known that a, b and ab are all sums of three squares. We will now use the result of Example 4.4 to obtain limits in the case $n = 4$:

Let L/K be a Q_{16}-extension and let $K(\sqrt{a},\sqrt{b})/K$ be as above. We may assume $L/K(\sqrt{b})$ to be cyclic. Hence, $(a,ab) = 1$ and $(ab,2)(b,-1) = (-b,x)$ for some $x \in K^*$. If 2 is a square in K, we have $(b,-1) = (-b,x)$. This means that the quadratic forms $\langle b,b,-1\rangle$ and $\langle -b,x,bx\rangle$ are equivalent. Hence, $\langle b,b,-1\rangle$ represents $-b$, *i.e.*, $\langle b,b,b,-1\rangle$ is isotropic, and b is a sum of three squares in K. If 2 is not a square in K, b is a sum of three squares in $K(\sqrt{2})$ by the preceding argument:

$$b = \sum_{i=1}^{3}(x_i + y_i\sqrt{2})^2 = \sum_{i=1}^{3}(x_i^2 + 2y_i^2 + 2x_iy_i\sqrt{2}) = \sum_{i=1}^{3}(x_i^2 + 2y_i^2)$$

for $x_i, y_i \in K$. Hence, b is a sum of nine squares in K.

Now, $(a,-b) = (a,ab) = 1$ means that $\langle 1,-a,b\rangle$ is isotropic, *i.e.*, that $\langle 1,b\rangle$ represents a: $a = bx^2 + y^2$ for some $x, y \in K$. Since b is a sum of nine squares, a is a sum of ten squares in K. By symmetry, so is ab.

We therefore have the following result: If L/K is a Q_{16}-extension with maximal elementary abelian subextension $K(\sqrt{a}, \sqrt{b})/K$ and $L/K(\sqrt{b})$ cyclic, b is a sum of nine squares in K, and a and ab are both sums of ten squares in K.

EXAMPLE 4.5. The obstruction to the embedding problem given by L/K and the extension

$$1 \longrightarrow \mu_2 \underset{-1\mapsto x^2}{\longrightarrow} C \rtimes C \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_4 \longrightarrow 1 \tag{13}$$

is

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

Therefore, the field K admits a $C \rtimes C$-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a,ab) = (b,b) = 1.$$

This criterion is not surprising, since a $C \rtimes C$-extension is the composite of a D_4-extension and a $\mathbb{Z}/4\mathbb{Z}$-extension.

EXAMPLE 4.6. The embedding problem given by L/K and the extension

$$1 \longrightarrow \mu_2 \underset{-1\mapsto z}{\longrightarrow} D \curlywedge C \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_4 \longrightarrow 1 \tag{17}$$

has the obstruction

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

Hence, the field K admits a $D \curlywedge C$-extension, if and only if there exists quadratically independent elements $a, b \in K^*$, such that

$$(a,a) = (a,b) = 1.$$

Again, a $D \curlywedge C$-extension is the composite of a D_4-extension and a $\mathbb{Z}/4\mathbb{Z}$-extension, and so the result is no surprise.

The groups $C \rtimes C$ and $D \curlywedge C$ also have $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as an epimorphic images and could be handled with Proposition 3.2. The results would be the same, however. It is also possible to obtain the obstructions by using the considerations about inflations preceding Example 4.1. This is the way it is done in [GS&S]. Again: The results are the same.

The criteria for the existence of D_8-, QD_8- and Q_{16}-extensions given above can be found also in [Ki, Theorems 6–8], as well as in [GS&S] (without proofs).

REMARK. Using Corollary 2.5, Proposition 3.2 and Proposition 4.2, it is of course possible to find criteria for the realisability of many other 2-groups beside those treated

above. For instance, any group of order 32 having $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, $(\mathbb{Z}/2\mathbb{Z})^4$ or $\mathbb{Z}/2\mathbb{Z} \times D_4$ as a factor. Of these, the case $(\mathbb{Z}/2\mathbb{Z})^4$ is considered in [Sm]. Also, the map $H^2(Q_8, \mu_2) \longrightarrow \mathrm{Br}(L/K)$, where L/K is a Q_8-extension, is easily described, since all elements in $H^2(Q_8, \mu_2)$ are inflations from $H^2(\mathbb{Z}/2\mathbb{Z}, \mu_2)$ via the different epimorphisms $Q_8 \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}/2\mathbb{Z}$. (In fact, it is not even necessary to know what a Q_8-extension looks like. Only the biquadratic subextension is needed.) Hence, groups of order 32 having $\mathbb{Z}/2\mathbb{Z} \times Q_8$ as a factor can be treated as well.

5. **Automatic realisations.** Let G_1 and G_2 be finite groups. If any field K admitting a G_1-extension also admits an G_2-extension, we will write $G_1 \Rightarrow G_2$. A statement $G_1 \Rightarrow G_2$ is called an *automatic realisation*. For instance, it is well known (*cf.* [Wh] or [K&L]) that $\mathbb{Z}/4\mathbb{Z} \Rightarrow \mathbb{Z}/2^n\mathbb{Z}$ for all $n \in \mathbb{N}$. And of course $G \Rightarrow G/N$ whenever $N \triangleleft G$. Also, since any finite abelian group can be realised as a Galois group over a field $\mathbb{C}((X_1)) \cdots ((X_n))$ admitting only abelian extension, no automatic realisation of the form $A \Rightarrow G$, where A is abelian and G is not, can be valid. And if the automatic realisation $G_1 \Rightarrow G_2$ is valid, the minimum number of generators for G_2 is less than or equal to the minimum number of generators for G_1:

Let n be the minimum number of generators for G_1, and let L/K be a G_1-extension. Then there exists n elements $\sigma_1, \ldots, \sigma_n$ in the absolute Galois group $\mathrm{Gal}(K)$ of K, such that $\mathrm{Gal}(L/K)$ is generated by the restrictions of these elements to L. Let K' be the fixed field of $\sigma_1, \ldots, \sigma_n$ in the separable closure of K. Then the absolute Galois group of K' is generated by n elements, and hence the Galois group of any Galois extension of K' is generated by n elements. Since K' obviously admits a G_1-extension (namely LK'/K'), the existence of a G_1-extension cannot imply the existence of a G_2-extension, unless G_2 is generated by n elements.

These remarks concern only 'general' automatic realisations, in which the ground field is an arbitrary field. If attention is restricted to fields with special properties, such as Hilbertian fields or fields with a given level, further automatic realisations may be valid. For instance: If -1 is a square in K, the obstructions to embedding a D_4-extension in D_8-, QD_8- and Q_{16}-extensions coincide, and so we get automatic realisations $D_8 \Leftrightarrow QD_8 \Leftrightarrow Q_{16}$. In fact, an argument similar to the one preceding Proposition 4.2 shows that in this case the obstructions to embedding a D_{2^n}-extension in $D_{2^{n+1}}$-, $QD_{2^{n+1}}$- and $Q_{2^{n+2}}$-extensions are equal for all $n \geq 2$, and so $D_{2^{n+1}} \Leftrightarrow QD_{2^{n+1}} \Leftrightarrow Q_{2^{n+2}}$.

Several non-trivial automatic realisations are known, *cf.* [J1], [J2], [J&Y] and [Sm]. In this section, we will consider automatic realisations between groups of order 4, 8 and 16, using the criteria obtained in the previous sections. (Of course, these criteria work only in characteristic $\neq 2$. But by a theorem of Witt, see [Wi, Satz p. 237] or [Ho, 2.2 and 3.1], automatic realisations between 2-groups in characteristic 2 depends only on the minimum number of generators for the groups involved, and so the results below will all be trivial. For the same reason, we will assume all fields to have characteristic $\neq 2$.) Many of the results of this section can be found in [G&S] as well.

PROPOSITION 5.1. *$Q_{2^n} \Rightarrow C \rtimes C$ for all $n \geq 3$.*

PROOF. We write $Q_{2^n} = \langle x, y \rangle$, where $x^{2^{n-1}} = 1$, $y^2 = x^{2^{n-2}}$ and $yxy^{-1} = x^{-1}$. Let L/K be a Q_{2^n}-extension. If $n = 3$ we have quadratically independent $a, b \in K^*$, such that $(a, ab) = (b, b)$, by the result in Section 3. If $n > 3$ we have a group extension

$$1 \longrightarrow \langle x^4 \rangle \longrightarrow Q_{2^n} \underset{y \mapsto \tau}{\overset{x \mapsto \sigma}{\longrightarrow}} D_4 \longrightarrow 1, \tag{18}$$

and hence quadratically independent $a, b \in K^*$, such that $(a, ab) = 1$, $K(\sqrt{a}, \sqrt{b}) \subseteq L$ and $L/K(\sqrt{b})$ is cyclic. By the remark following Example 4.4, b is a sum of squares in K. If b is a sum of two squares, $(a, ab) = (b, b) = 1$, and K admits a $C \rtimes C$-extension by Example 4.5. If b is not a sum of two squares, there exists $x, y, z \in K$, such that $c = x^2 + y^2 + z^2$ is not a sum of two squares. But then c and $d = x^2 + y^2$ are quadratically independent, and since $(c, cd) = (d, d) = 1$, K admits a $C \rtimes C$-extension. ∎

For $n = 3$ this is [J1, Proposition 1.1].

From the trivial automatic realisations $C \rtimes C \Rightarrow Q_8$, $C \rtimes C \Rightarrow D_4$ and $C \rtimes C \Rightarrow \mathbb{Z}/4\mathbb{Z}$, we get

COROLLARY 5.2. *$Q_{2^n} \Rightarrow Q_8$ for all $n \geq 4$.*

COROLLARY 5.3 [J&Y, THEOREM III.3.6]. *$Q_8 \Rightarrow D_4$.*

Of course, we get $Q_{2^n} \Rightarrow D_4$ for all $n \geq 3$, but for $n > 3$ this is trivial by (18).

COROLLARY 5.4. *$Q_{2^n} \Rightarrow \mathbb{Z}/4\mathbb{Z}$ for all $n \geq 3$.*

Also, we notice that the groups Q_8 and $C \rtimes C$ are in a sense equivalent, as far as realisability is concerned: Any field admitting one of them as a Galois group automatically admits the other as well.

As for the opposite implications: $C \rtimes C \Rightarrow Q_{2^n}$ is not valid for $n \geq 4$, since the field $\hat{\mathbb{Q}}_3$ of 3-adic numbers admits a $C \rtimes C$-extension, but no D_8- or Q_{16}-extensions, and hence no Q_{2^n}-extension for $n \geq 4$. (If p is an odd prime, the field $\hat{\mathbb{Q}}_p$ of p-adic numbers has only four square classes, *cf.* [Se, Corollary p. 18], and so it is easy to check the existence or non-existence of G-extensions, whenever G is one of the groups treated in the preceding sections.) Since $C \rtimes C \Leftrightarrow Q_8$ the implications $Q_8 \Rightarrow Q_{2^n}$, $n \geq 4$, are not valid either. The field $\mathbb{R}((X))$ shows that D_4 does not imply Q_{2^n} for any $n \geq 3$. The implications $\mathbb{Z}/4\mathbb{Z} \Rightarrow Q_{2^n}$ are obviously not valid, since $\mathbb{Z}/4\mathbb{Z}$ can imply nothing but cyclic groups.

LEMMA 5.5. *If $2 \notin (K^*)^2$, the existence of a D_4-extension implies the existence of an M_{16}-extension.*

PROOF. Let $a, b \in K^*$ be quadratically independent, such that $(a, ab) = 1$. If -1 and 2 are quadratically independent in K, K admits an M_{16}-extension by Example 3.3. We may therefore assume -1 and 2 to be quadratically dependent:

If -1 is a square, $(a, a) = 1$. If $2a$ is a square as well, $(a, 2b) = (a, ab) = 1$. Otherwise, 2 and a are quadratically independent, and we can take '$b = 2$': $(a, 2 \cdot 2) = 1$. In both cases we get an M_{16}-extension.

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

If -2 is a square, -1 is a sum of two squares. We may assume that -1 is not a square, and if we choose $b' \in K^*$, such that $a' = -1$ and b' are quadratically independent, we have $(a', a') = 1$ and $(a', 2b') = (-1, 2b') = (-1, x)$ for $x = 2b'$. Hence, we get an M_{16}-extension. ∎

PROPOSITION 5.6. $C \rtimes C \Rightarrow M_{16}$.

PROOF. We have quadratically independent $a, b \in K^*$, such that $(a, ab) = (b, b) = 1$. By Lemma 5.5 we may assume 2 to be a square in K. But then $(b, b) = 1$ and $(b, 2a) = (b, a) = (a, a) = (-1, a)$, and we get an M_{16}-extension. ∎

COROLLARY 5.7. $Q_{2^n} \Rightarrow M_{16}$ *for all* $n \geq 3$.

As the field $\hat{\mathbb{Q}}_5$ shows, the opposite implications are not valid. In fact, $\hat{\mathbb{Q}}_5$ admits no non-abelian group of order 8 or 16, except M_{16}, as a Galois group.

PROPOSITION 5.8. $Q_{16} \Rightarrow D_8$.

PROOF. We have quadratically independent $a, b \in K^*$, such that $(a, ab) = 1$ and $(ab, 2)(b, -1) = (-b, x)$ for some $x \in K^*$. If -1 is a square in K^*, the criteria for realising Q_{16} and D_8 are identical. We may therefore assume that $-1 \notin (K^*)^2$. If 2 is a square, any D_4-extension can be embedded in a D_8-extension. Hence, we can assume $2 \notin (K^*)^2$. If -2 is a square: Let $a' = ab$. Then $(a', a'b) = (ab, a) = 1$ and $(a'b, 2) = (a, 2) = (ab, 2)(b, 2) = (ab, 2)(b, -1) = (-b, x)$, and we get a D_8-extension. If -1 and 2 are quadratically independent, we get a D_8-extension by letting '$a = 2$ and $b = -1$'. ∎

The opposite implication is not valid, as the field $\mathbb{R}((X))$ shows. In fact, $\mathbb{R}((X))$ admits only dihedral groups (including $\mathbb{Z}/2\mathbb{Z}$ and V_4) as Galois groups, and so the only implications $D_8 \Rightarrow G$, where G is a group of order 2^n, $n \leq 4$, are the trivial ones. Similarly, the only possible implications $D_4 \Rightarrow G$, G as before, are the trivial ones and $D_4 \Rightarrow D_8$. Since $\hat{\mathbb{Q}}_3$ admits a D_4-, but no D_8-extension, only the trivial implications are valid. However, we do have

PROPOSITION 5.9. $D_4 \Rightarrow D_8 \vee M_{16}$. *(That is, any field admitting a* D_4*-extension also admits either a* D_8*- or an* M_{16}*-extension.)*

PROOF. We have quadratically independent $a, b \in K^*$, such that $(a, ab) = 1$, and may assume 2 to be a square by Lemma 5.5. But then $(2, ab) = 1$, and we get a D_8-extension. ∎

This result is an improvement of [J1, Theorem 1.7].

The implication $Q_8 \Rightarrow D_8$ is not valid, as $\hat{\mathbb{Q}}_3$ shows. The implications $Q_{2^n} \Rightarrow G$, $G = D_8, D \rtimes C$ or DC, $n = 3, 4$, are not valid, as $\hat{\mathbb{Q}}_7$ shows.

PROPOSITION 5.10. $QD_8 \Rightarrow M_{16}$.

PROOF. We have quadratically independent $a, b \in K^*$, such that $(a, ab) = 1$ and $(a, -2) = (-b, x)$ for some $x \in K^*$. By Lemma 5.5 we may assume 2 to be a square in K: $(a, -1) = (-b, x)$, and the quadratic form $\langle -1, a, a \rangle$ represents $-b$. This means that

https://doi.org/10.4153/CJM-1995-064-3 Published online by Cambridge University Press

the quadratic form $\langle -1, a, a, b\rangle$ is isotropic, and by multiplying with a we get that the quadratic form $\langle 1, 1, -a, ab\rangle$ is isotropic. Hence, $a(1-b) \in K^*$ is a sum of two squares. If $a(1-b)$ is a square, $(a,a) = (a,b) = (1-b,b) = 1$ and $(a,2b) = (a,b) = 1$. If $a(1-b)$ and b are quadratically equivalent, we get

$$1 = \big(a(1-b), a(1-b)\big) = \big(a(1-b), b\big) = (a,b) = (a,a),$$

hence $(a,a) = 1$ and $(a,2b) = 1$. Otherwise, $a' = a(1-b)$ and b are quadratically independent, $(a',a') = 1$ and $(a',2b) = \big(a(1-b),2b\big) = \big(a(1-b),b\big) = (a,b) = (a,a) = (-1,a)$. In all cases, we get an M_{16}-extension. ∎

$M_{16} \Rightarrow \mathbb{Z}/4\mathbb{Z}$ is trivial, and we get

COROLLARY 5.11. $QD_8 \Rightarrow \mathbb{Z}/4\mathbb{Z}$.

Corollaries 5.4 and 5.11 are both special cases of [J1, Corollary 1.3].

The implications $QD_8 \Rightarrow G, G = D_8, Q_{16}, D \curlywedge C$ or DC, are not valid, as $\hat{\mathbb{Q}}_3$ shows. A counterexample to the implications $QD_8 \Rightarrow Q_8$ and $QD_8 \Rightarrow C \rtimes C$ can be constructed as follows: Let K be a subfield of $\mathbb{R}$ maximal with respect to not containing $\sqrt{2}$. The square classes of K are then represented by ± 1, ± 2. In particular, -1 and 2 are quadratically independent, so K admits a QD_8-extension. But an easy calculation shows that K admits no Q_8-extensions.

Since K also admits an $D \curlywedge C$-extension, but no Q_{16}-extensions, we get a counterexample to the implications $D \curlywedge C \Rightarrow Q_8$, $D \curlywedge C \Rightarrow Q_{16}$ and $D \curlywedge C \Rightarrow C \rtimes C$ as well.

PROPOSITION 5.12. $D \curlywedge C \Rightarrow M_{16}$.

PROOF. We have quadratically independent $a, b \in K^*$, such that $(a,a) = (a,b) = 1$, and may again assume 2 to be a square: $(a,a) = 1$ and $(a,2b) = (a,b) = 1$. Hence, we get an M_{16}-extension. ∎

The implication $D \curlywedge C \Rightarrow DC$ is obviously not valid, since DC is not generated by two elements.

PROPOSITION 5.13. $DC \Rightarrow D_4$.

PROOF. By the result in Section 3, we have quadratically independent elements $a, b, c \in K^*$, such that $(a,b) = (c,c)$. By [M&S, Proposition A.1] there exists an $x \in K^*$, such that $(a,bx) = (c,cx) = (ac,x) = 1$. It follows that there exists quadratically independent $p, q \in K^*$, such that $(p,q) = 1$, and hence that K admits a D_4-extension. ∎

Let K be the pythagorean closure of the field $\mathbb{R}(X)$, *i.e.*, the maximal totally positive 2-extension of $\mathbb{R}(X)$, *cf.* [Wa, Lemma 1.4]. Any ordering of $\mathbb{R}(X)$ can then be extended to K, and since the signs of X and $X-1$ in $\mathbb{R}(X)$ can be assigned arbitrarily, -1, X and $X-1$ are quadratically independent in K^*. The quadratic forms $\langle X, X, -1\rangle$ and $\langle X, X-1, -X(X-1)\rangle$ are obviously equivalent, and so we have $(X,X) = \big(X-1, -X(X-1)\big)$. Hence, K admits a DC-extension. But K is pythagorean, admitting no $\mathbb{Z}/4\mathbb{Z}$-extensions. It follows that the implications $DC \Rightarrow G$, $G = \mathbb{Z}/4\mathbb{Z}$, Q_8, Q_{16}, QD_8, M_{16}, $C \rtimes C$ and $D \curlywedge C$, are not valid.

PROPOSITION 5.14. *$D \leftthreetimes C \Rightarrow D_8 \vee DC$ and $D \leftthreetimes C \Rightarrow QD_8 \vee DC$.*

PROOF. We have quadratically independent elements $a, b \in K^*$, such that $(a,a) = (a,b) = 1$.

If -1 and 2 are quadratically independent, we get D_8- and QD_8-extensions by letting $a' = 2$ and $b' = -1$.

If $-1, 2 \notin (K^*)^2$, $-2 \in (K^*)^2$: Any D_4-extension can be embedded in a QD_8-extension. If a and 2 are quadratically independent, we get a D_8-extension by letting $a' = a$ and $b' = 2$, since $(a'b', 2) = (2a, 2) = (a, 2) = (a, -1) = 1$. Otherwise, a and 2 are quadratically equivalent, and we get a D_8-extension, since $(ab, 2) = (2b, 2) = (b, 2) = (-b, 2)$.

If $-1, 2 \in (K^*)^2$, any D_4-extension can be embedded in D_8- and QD_8-extensions.

If $-1 \in (K^*)^2$, $2 \notin (K^*)^2$, a D_4-extension can be embedded in a D_8-extension, if and only if it can be embedded in a QD_8-extension, and so we need only consider D_8: If 2, a and b are quadratically independent, we get a DC-extension by letting $c = 2$. Otherwise, 2 is quadratically equivalent to a, b or ab: If $2 \underset{(2)}{=} a$, $(ab, 2) = (ab, a) = 1$. If $2 \underset{(2)}{=} b$, $(ab, 2) = (ab, b) = (-b, ab)$. If $2 \underset{(2)}{=} ab$, $(ab, 2) = (2, 2) = 1$. In all cases, we get a D_8-extension. ∎

The only nontrivial automatic realisations between the groups $\mathbb{Z}/4\mathbb{Z}$, D_4, Q_8, D_8, Q_{16}, QD_8, M_{16}, $C \rtimes C$, $D \leftthreetimes C$ and DC not covered by the above results are $D \leftthreetimes C \Rightarrow D_8$, $D \leftthreetimes C \Rightarrow QD_8$ and $DC \Rightarrow D_8$. It is clear from the proof of Proposition 5.14 that the automatic realisations $D \leftthreetimes C \Rightarrow D_8$ and $D \leftthreetimes C \Rightarrow QD_8$ are equivalent, and from Proposition 5.14 itself that the automatic realisation $DC \Rightarrow D_8$ would imply the other two. However, the author has not succeeded in giving proofs or counterexamples of any of these three realisations.

REFERENCES

[As] M. Aschbacher, *Finite Group Theory*, Cambridge Stud. Adv. Math. **10**, Cambridge Univ. Press, 1986.

[Br] R. Brauer, *Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind,* J. Reine Angew. Math. **168**(1932), 44–64.

[Fr] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants,* J. Reine Angew. Math. **360**(1985), 84–123.

[G&S] H. G. Grundman and T. L. Smith, *Automatic realizability of Galois groups of order* 16, (1994), preprint.

[GS&S] H. G. Grundman, T. L. Smith and J. R. Swallow, *Groups of order* 16 *as Galois groups,* (1994), preprint.

[Ho] K. Hoechsmann, *Zum Einbettungsproblem,* J. Reine Angew. Math. **229**(1968), 81–106.

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

[J1] C. U. Jensen, *On the representations of a group as a Galois group over an arbitrary field*. In: Théorie des nombres Number Theory, (eds. J.-M. De Koninck and C. Levesque), Walter de Gruyter, 1989, 441–458.

[J2] ———, *Finite groups as Galois groups over arbitrary fields*. In: Contemp. Math. **131**, Proceedings of the international conference of algebra 1989, part 2, Amer. Math. Soc., 1992, 435–448.

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

[Ki] I. Kiming, *Explicit Classifications of some* 2*-Extensions of a Field of Characteristic different from* 2, Canad. J. Math. **42**(1990), 825–855.

[K&L] W. Kuyk and H. W. Lenstra, Jr., *Abelian extensions of arbitrary fields,* Math. Ann. **216**(1975), 99–104.

[La] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.

[Lo] F. Lorenz, *Einführung in die Algebra II*, B. I. Wissenschaftsverlag, Mannheim, 1990.
[Me] A. Merkurjev, *On the norm residue symbol of degree 2,* Soviet Math. Dokl. **24**(1981), 546–551.
[M&S] J. Mináč and T. L. Smith, *A characterization of C-fields via Galois groups,* J. Algebra **137**(1991), 1–11.
[Sc] Leila Schneps, *Explicit Realisations of Subgroups of* $GL_2(F_3)$ *as Galois Groups,* J. Number Theory **39**(1991), 5–13.
[Se] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Math. **7**, Springer-Verlag, 1973.
[Sm] T. Smith, *Extra-special groups of order* 32 *as Galois groups,* Canad. J. Math. **46**(1994), 886–896.
[Wa] R. Ware, *Automorphisms of Pythagorean Fields and their Witt Rings,* Comm. Algebra **17**(1989), 945–969.
[Wh] G. Whaples, *Algebraic extensions of arbitrary fields,* Duke Math. J. **24**(1957), 201–204.
[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Characteristik p zu vorgegebener Gruppe der Ordnung* p^f, J. Reine Angew. Math. **174**(1936), 237–245.

Matematisk Institut
Universitetsparken 5
DK-2100 Copenhagen Ø
Denmark
e-mail: ledet@math.ku.dk