Can. J. Math. Vol. XLII, No. 5, 1990 pp. 825–855

EXPLICIT CLASSIFICATIONS OF SOME 2-EXTENSIONS OF A FIELD OF CHARACTERISTIC DIFFERENT FROM 2

IAN KIMING

1. Introduction. Let p be a prime number. Let k be a field of characteristic different from p and containing the p-th roots of unity. Let $\mathfrak{G}$ be a finite group. Let L/k be a finite normal extension with Galois group $\mathfrak{G}$ and let c be a 2-cocycle on $\mathfrak{G}$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$, where $\mathfrak{G}$ acts trivially on $\mathbb{Z}/p\mathbb{Z}$. By $\mathrm{Emb}(L/k, c)$ we denote the question of the existence of a finite normal extension M of k, such that M contains L, such that $[M{:}\,L] = p$, and such that, denoting by $\mathfrak{G}_1$ the Galois group of M/k, the extension

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathfrak{G}_1 \longrightarrow \mathfrak{G} \longrightarrow 1$$

is given by the class of c.

Therefore we are confronted with the problem of expressing explicitly in terms of the structure of L/k the condition for c to split when perceived as a 2-cocycle in $Z^2(\mathfrak{G}, L^\times)$ (see the introductory remarks in "The reductive method" below). This problem has been solved in [**3**] in the case that $\mathfrak{G}$ is an elementary abelian p-group.

If $\mathfrak{N}$ is a normal subgroup of $\mathfrak{G}$, K is the fixed field of $\mathfrak{N}$ and $\operatorname{res} c$ is the restriction of c to $\mathfrak{N}$, then assuming that the question $\mathrm{Emb}(L/K, \operatorname{res} c)$ has an affirmative answer we shall present an explicit method of reducing the question $\mathrm{Emb}(L/k, c)$ to a question about the structure of a solution to $\mathrm{Emb}(L/K, \operatorname{res} c)$, of K/k and of the extension, $\mathfrak{G}$, of $\mathfrak{N}$ by $\mathfrak{G}/\mathfrak{N}$. Here the word "explicit" is to be interpreted in the following manner: If the fact that $H^1(\mathfrak{N}, L^\times) = 0$ were proved constructively then the reduction could be performed constructively.

If $\mathfrak{G}$ is a finite group, k is a field and L/k is finite normal extension with Galois group $\mathfrak{G}$, then for brevity we shall refer to L/k as a $\mathfrak{G}$-extension.

As an application of the method, we shall give explicit information about the structure of $\mathfrak{G}$-extensions of k when k is a field of characteristic different from 2 and $\mathfrak{G}$ is cyclic of order 8, dihedral of order 8 or 16, quaternion of order 8 or 16 or quasi-dihedral of order 16. These groups will denoted by $\mathbb{Z}/8\mathbb{Z}$, D_4, D_8,Q_8, Q_{16} and QD_8 respectively.

In [**1**] the problem of the existence of certain embeddings of quadratic extensions into dihedral—or quaternion—extensions is solved in the case that k is an algebraic

Received February 3rd, 1989.

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

number field. However, the methods used in [**1**] do not work in the general case. Let us furthermore note that the general central embedding problem has been solved in [**5**] in the case where $\mathfrak{G}$ is a p-group and k has characteristic p.

2. The Reductive Method. In what follows k will denote a field of characteristic different from p and containing the p-th roots of unity. Also, if $\mathfrak{G}$ is a finite group, A is a $\mathfrak{G}$-module and $\sigma \in Z^s(\mathfrak{G}, A)$, then we shall denote by $\overline{\sigma}$ the class of σ in $H^s(\mathfrak{G}, A)$.

Let L be a finite normal extension of k with Galois group $\mathfrak{G}$. Let ε be a primitive p-th root of unity in k. We shall identify $\langle \varepsilon \rangle$ with $\mathbb{Z}/p\mathbb{Z}$. Under the Galois action of $\mathfrak{G}$ on $L^\times$ the group $\langle \varepsilon \rangle$ is fixed and $\mathfrak{G}$ acts trivially on this group. Thus we may identify $H^s(\mathfrak{G}, \mathbb{Z}/p\mathbb{Z})$, where $\mathfrak{G}$ acts trivially on $\mathbb{Z}/p\mathbb{Z}$, with $H^s(\mathfrak{G}, \langle \varepsilon \rangle)$.

As is well know or easily seen, the extensions of order p of L which are normal over k are in 1–1 correspondence with the elements of $H^0\big(\mathfrak{G}, L^\times/(L^\times)^p\big)$ (where the action of $\mathfrak{G}$ on $L^\times$ is the Galois action). For $\alpha \in L^\times$ we denote by $\bar{\alpha}$ the class of α in $L^\times/(L^\times)^p$. If $\alpha \in L^\times$ and $\bar{\alpha} \in H^0\big(\mathfrak{G}, L^\times/(L^\times)^p\big)$ then $\bar{\alpha}$ corresponds to the extension $L(\alpha^{1/p})/k$. An extension of order p of L which is normal over k has the form $L(\alpha^{1/p})/L$ for some $\alpha \in L^\times$ and for such an α we have $\bar{\alpha} \in H^0\big(\mathfrak{G}, L^\times/(L^\times)^p\big)$ and the extension $L(\alpha^{1/p})/k$ corresponds to $\bar{\alpha}$.

We have the exact diagram

$$\begin{tikzcd}
 & & 1 \arrow[d] & & \\
 & & \langle \varepsilon \rangle \arrow[d] & & \\
1 \arrow[r] & (L^\times)^p \arrow[r] & L^\times \arrow[r] \arrow[d] & L^\times/(L^\times)^p \arrow[r] & 1 \\
 & & (L^\times)^p \arrow[d] & & \\
 & & 1 & &
\end{tikzcd}$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

with natural maps. From this diagram we get the exact diagram

$$\begin{tikzcd}
H^0\big(\mathfrak{G}, L^\times/(L^\times)^p\big) \arrow[r, "\psi"] & H^1\big(\mathfrak{G},(L^\times)^p\big) \arrow[r] \arrow[d, "\delta"'] & H^1\big(\mathfrak{G},(L^\times)\big) = 0 \\
& H^2(\mathfrak{G}, \langle \varepsilon \rangle) \arrow[d, "\varphi"'] & \\
& H^2(\mathfrak{G}, L^\times) &
\end{tikzcd}$$

with Galois action. Using this diagram and some easy computations we can derive: If $\alpha \in L^\times$ and $\overline{\alpha} \in H^0\big(\mathfrak{G}, L^\times/(L^\times)^p\big)$ then $\mathrm{Gal}\big(L(\alpha^{1/p})/k\big)$ is the extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathfrak{G}$ determined by $\delta\psi\overline{\alpha}$.

In this way we see that if $c \in Z^2(\mathfrak{G}, \mathbb{Z}/\mathbb{Z}p)$ and $\bar{c} \neq 0$ then $\mathrm{Emb}(L/k, c)$ has an affirmative answer if and only if $\varphi\bar{c} = 0$.

We also see that if $L(\alpha^{1/p})/k$ is a solution to $\mathrm{Emb}(L/k, c)$ then any other solution has the form $L((q\alpha)^{1/p})/k$, where $q \in k^\times$.

If $\mathfrak{N}$ is a subgroup in $\mathfrak{G}$ then we note, letting φ denote also the map $H^2(\mathfrak{N}, \langle\varepsilon\rangle) \longrightarrow H^2(\mathfrak{N}, L^\times)$, that φ commutes with restriction to $\mathfrak{N}$.

For group elements G and H we put $G^H = H^{-1}GH$. The letter E always denotes the neutral element of a given group.

THEOREM 1. *Let $\mathfrak{G}$ be a finite group, let L/k be a $\mathfrak{G}$-extension, let $\mathfrak{N}$ be a normal subgroup in $\mathfrak{G}$ and let K be the fixed field on $\mathfrak{N}$ in L. Let $c \in Z^2(\mathfrak{G}, L^\times)$ be such that $c(E,G) = c(G,E) = 1$ for all $G \in \mathfrak{G}$ and suppose that* res $\bar{c} = 0$ *in $H^2(\mathfrak{N}, L^\times)$ where* res *is restriction to $\mathfrak{N}$. Thus there exists a function $f\colon \mathfrak{N} \longrightarrow L^\times$ such that*

$$c(N_1, N_2) = \frac{f(N_1)\big(N_1 f(N_2)\big)}{f(N_1N_2)} \qquad \textit{for all } N_1, N_2 \in \mathfrak{N}.$$

Let $\mathfrak{G} = \bigcup_{X \in \mathfrak{G}/\mathfrak{N}} G(X)\mathfrak{N}$ be a coset decomposition and let $N(,)$ be the corresponding factor system, that is,

$$G(X)G(Y) = G(XY)N(X,Y) \qquad \text{for all } X, Y \in \mathfrak{G}/\mathfrak{N}.$$

Then the following assertions hold:

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

(1) For $X \in \mathfrak{G}/\mathfrak{N}$ the function $\Omega_X\colon \mathfrak{N} \longrightarrow L^\times$ given by

$$\Omega_X(N) = \frac{c\big(N, G(X)\big)}{c\big(G(X), N^{G(X)}\big)} \cdot \frac{G(X)f\big(N^{G(X)}\big)}{f(N)}$$

is a 1-cocycle on $\mathfrak{N}$.

For every $X \in \mathfrak{G}/\mathfrak{N}$ we choose $a_X \in L^\times$ such that

$$\Omega_X(N) = a_X^{-1}(Na_X) \qquad \text{for all } N \in \mathfrak{N}.$$

(2) With X and Y ranging over $\mathfrak{G}/\mathfrak{N}$ the expression

$$s(X, Y) = \frac{c\big(G(X), G(Y)\big)}{c\big(G(XY), N(X, Y)\big)} \cdot \Big(G(XY)f\big(N(X, Y)\big)\Big) \cdot \frac{a_{XY}}{a_X\big(G(X)a_Y\big)}$$

defines an element of $Z^2\big(\mathfrak{G}/\mathfrak{N}, K^\times\big)$.

(3) Under the inflation map $H^2\big(\mathfrak{G}/\mathfrak{N}, K^\times\big) \longrightarrow H^2(\mathfrak{G}, L^\times)$ the element $\bar{s}$ given in (2) is mapped to $\bar{c}$.

(4) $\bar{c} = 0$ in $H^2(\mathfrak{G}, L^\times)$ if and only if $\bar{s} = 0$ in $H^2(\mathfrak{G}/\mathfrak{N}, K^\times)$, where $\bar{s}$ is the element given in (2).

(5) Defining $h\colon \mathfrak{G} \longrightarrow L^\times$ by

$$h\big(G(X)N\big) = a_X \cdot \frac{G(X)f(N)}{c\big(G(X), N\big)} \qquad \text{for } X \in \mathfrak{G}/\mathfrak{N}, N \in \mathfrak{N},$$

we have for elements $G_1, G_2 \in \mathfrak{G}$ with classes X resp. Y in $\mathfrak{G}/\mathfrak{N}$ that

$$c(G_1, G_2) = s(X, Y) \cdot \frac{h(G_1)\big(G_1 h(G_2)\big)}{h(G_1 G_2)}.$$

PROOF. Put $M = \mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[\mathfrak{G}], L^\times\big)$. Then M is a $\mathfrak{G}$-module with $\mathfrak{G}$ acting by

$$(G.m)(H) = m(HG) \qquad \text{for } m \in M, G, H \in \mathfrak{G}.$$

Putting $l(G) = Gl$ for $G \in \mathfrak{G}$, $l \in L^\times$ we may consider $L^\times$ as embedded in M. If the element $m \in M$ actually belongs to $L^\times$ then the embedding of this element in $L^\times$ is $m(E)$. As M is co-induced we have $H^i(\mathfrak{G}, M) = 0$ for $i \geq 1$.

By the inflation- and restriction-maps we get the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & H^1\big(\mathfrak{G}/\mathfrak{N}, (M/L^\times)^{\mathfrak{N}}\big) \arrow[r, "\text{infl}"] \arrow[d, "\delta_1"] & H^1(\mathfrak{G}, M/L^\times) \arrow[r, "\text{res}"] \arrow[d, "\delta_2"] & H^1(\mathfrak{N}, M/L^\times) \arrow[d, "\delta_3"] \\
0 \arrow[r] & H^2\big(\mathfrak{G}/\mathfrak{N}, K^\times\big) \arrow[r, "\text{infl}"] & H^2\big(\mathfrak{G}, L^\times\big) \arrow[r, "\text{res}"] & H^2\big(\mathfrak{N}, L^\times\big).
\end{tikzcd}$$

Here the maps δ_1, δ_2 and δ_3 are connecting homomorphisms derived from the exact sequence

$$1 \longrightarrow L^\times \longrightarrow M \longrightarrow M/L^\times \longrightarrow 1$$

and it is well known or easily seen that these maps are isomorphisms. A remark about δ_1 is appropriate:

$M^{\mathfrak{N}}/K^\times$ is identified with $(M/L^\times)^{\mathfrak{N}}$ in the following way: If m is an element of M such that the class of m modulo $L^\times$ belongs to $(M/L^\times)^{\mathfrak{N}}$, then there is a function $g\colon \mathfrak{N} \longrightarrow L^\times$ such that $N.m = mg(N)$ for all $N \in \mathfrak{N}$. Then $g \in Z^1(\mathfrak{N}, L^\times)$ and thus there exists $a \in L^\times$ such that $g(N) = a(Na)^{-1}$ for all $N \in \mathfrak{N}$. Then $am \in M^{\mathfrak{N}}$.

If $m \in M$ and if the class of m modulo $K^\times$ belongs to $M^{\mathfrak{N}}/K^\times$ then the class of m modulo $L^\times$ belongs to $(M/L^\times)^{\mathfrak{N}}$.

If $\mu' \in Z^1(\mathfrak{G}, M/L^\times)$ and if $\mu\colon \mathfrak{G} \longrightarrow M$ is a "lifting" of μ', that is, for every $G \in \mathfrak{G}$ the (modulo $L^\times$)-class of $\mu(G)$ is $\mu'(G)$, then $\delta_2\mu$ denotes the 2-cocycle given by

$$(\delta_2\mu)(G_1, G_2) = \left(\frac{\mu(G_1)\big(G_1\mu(G_2)\big)}{\mu(G_1G_2)}\right)(E).$$

In this way the element $\delta_2\overline{\mu}' \in H^2(\mathfrak{G}, L^\times)$ is the 2-cocycle-class containing $\delta_2\mu$. Similar abuse of notation is employed in connection with the maps δ_1 and δ_3.

Let $\theta : \mathfrak{G} \longrightarrow M$ be given by

$$\theta(G)(G_1) = c(G_1, G) \qquad \text{for } G, G_1 \in \mathfrak{G},$$

and let β be the element of M given by

$$\beta\big(G(X)N\big) = \frac{c\big(G(X), N\big)}{G(X)f(N)} \qquad \text{for } X \in \mathfrak{G}/\mathfrak{N},\ N \in \mathfrak{N}.$$

Let $\eta(G) = \theta(G)\beta(G\beta)^{-1}$ for $G \in \mathfrak{G}$, and let $\eta'\colon \mathfrak{G} \longrightarrow M/L^\times$ be given by demanding that $\eta'(G)$ be the class of $\eta(G)$ modulo $L^\times$.

For $G, G_1, G_2 \in \mathfrak{G}$ we have

$$(+) \qquad c(G, G_1, G_2)\big(Gc(G_1, G_2)\big) = c(G, G_1)c(GG_1, G_2)$$

and this shows that η' is a 1-cocycle.

Obviously, $\delta_2\eta = c$.

Using (+) with $G = G(X)$, $G_1 = N$, $G_2 = N_1$ for $X \in \mathfrak{G}/\mathfrak{N}$ and $N, N_1 \in \mathfrak{N}$ we see that $\operatorname{res}\eta' = 0$.

Defining $\xi : \mathfrak{G}/\mathfrak{N} \longrightarrow M$ by

$$\xi(X) = \eta\big(G(X)\big) \quad \text{for } X \in \mathfrak{G}/\mathfrak{N}$$

and $\xi' : \mathfrak{G}/\mathfrak{N} \longrightarrow M/L^{\times}$ so that $\xi'(G)$ is the class modulo $L^{\times}$ of $\xi(G)$, we see that ξ' is a 1-cocycle on $\mathfrak{G}/\mathfrak{N}$ with coefficients in $(M/L^{\times})^{\mathfrak{N}}$ such that

$$\eta' = \mathrm{infl}(\xi').$$

If $X \in \mathfrak{G}/\mathfrak{N}$ and $N \in \mathfrak{N}$ then $\Omega_X(N) = \big(N\xi(X)\big)\big(\xi(X)\big)^{-1}$ is an element of $L^{\times}$ and this element is

$$\begin{aligned}\left(\frac{N\xi(X)}{\xi(X)}\right)(E) &= \frac{\xi(X)(N)}{\xi(X)(E)} \\ &= \frac{\eta\big(G(X)\big)(N)}{\eta\big(G(X)\big)(E)} \\ &= c\big(N, G(X)\big) \cdot \frac{\beta(N)}{\beta\big(G(X)N^{G(X)}\big)} \cdot \frac{\beta\big(G(X)\big)}{\beta(E)} \cdot \frac{1}{c\big(E, G(X)\big)} \\ &= \frac{c\big(N, G(X)\big)}{c\big(G(X), N^{G(X)}\big)} \cdot \frac{G(X)f\big(N^{G(X)}\big)}{f(N)},\end{aligned}$$

and the chosen elements $a_X \in L^{\times}$ satisfy

$$\Omega_X(N) = \big(Na_X\big)a_X^{-1}.$$

Define $\zeta(X) = \xi(X)a_X^{-1}$ for $X \in \mathfrak{G}/\mathfrak{N}$; then $\delta_1\xi'$ is represented by the 2-cocycle $s = \delta_1\zeta \in Z^2\big(\mathfrak{G}/\mathfrak{N}, K^{\times}\big)$. Explicitly we get for $X, Y \in \mathfrak{G}/\mathfrak{N}$ that

$$\begin{aligned} s(X, Y) &= \left(\frac{\zeta(X)\big(X\zeta(Y)\big)}{\zeta(XY)}\right)(E) \\ &= \left(\frac{\zeta(X)\big(G(X)\zeta(Y)\big)}{\zeta(XY)}\right)(E) \\ &= \frac{\eta\big(G(X)\big)(E)\eta\big(G(Y)\big)\big(G(X)\big)}{\eta\big(G(XY)\big)(E)} \cdot \frac{a_{XY}}{a_X\big(G(X)a_Y\big)} \\ &= \frac{c\big(G(X), G(Y)\big)\beta\big(G(X)\big)\beta\big(G(XY)\big)}{\beta\big(G(X)\big)\beta\big(G(X)G(Y)\big)} \cdot \frac{a_{XY}}{a_X\big(G(X)a_Y\big)} \\ &= \frac{c\big(G(X), G(Y)\big)}{\beta\big(G(XY)N(X, Y)\big)} \cdot \frac{a_{XY}}{a_X\big(G(X)a_Y\big)} \\ &= \frac{c\big(G(X), G(Y)\big)}{c\big(G(XY), N(X, Y)\big)} \cdot \big(G(XY)f\big(N(X, Y)\big)\big) \cdot \frac{a_{XY}}{a_X\big(G(X)a_Y\big)}.\end{aligned}$$

Now we have proved the assertions (1), (2), (3) and (4), since (4) is obvious.

Finally we get

$$c = \delta_2 \eta = \delta_2\Big((\operatorname{infl} \zeta)\big(\frac{\eta}{\operatorname{infl} \zeta}\big)\Big).$$

Now, $\delta_2(\operatorname{infl} \zeta) = \operatorname{infl}(\delta_1 \zeta) = \operatorname{infl}(s)$ and for $X \in \mathfrak{G} / \mathfrak{N}$ and $N \in \mathfrak{N}$ we have

$$\begin{aligned}\left(\frac{\eta\big(G(X)N\big)}{(\operatorname{infl} \zeta)\big(G(X)N\big)}\right)(E) &= \frac{\eta\big(G(X)N\big)(E)}{\zeta(X)(E)} \\ &= a_X \cdot \frac{\eta\big(G(X)N\big)(E)}{\eta\big(G(X)\big)(E)} \\ &= a_X \cdot \frac{G(X)f(N)}{c\big(G(X), N\big)},\end{aligned}$$

which proves (5). Q. E. D.

REMARK. The assumption that $c(E, G) = c(G, E) = 1$ in the formulation of Theorem 1 is not necessary and is made only for practical reasons.

Theorem 1 and the remarks preceding it clearly provide us with a "reductive" method of the required type for $\operatorname{Emb}(L/k, c)$.

As an immediate consequence of Theorem 1 we have the following elementary theorem about cyclic p-extensions.

THEOREM 2. *Let p be a prime number and let n be a natural number. Let k be a field of characteristic different from p and containing the p^n-th roots of unity. Let $\varepsilon \in k$ be a primitive p^n-th root of unity. Suppose that $a \in k^\times \setminus (k^\times)^p$ and let $L = k(a^{1/p^n})$. Put $K = k(a^{1/p})$. Then L is a normal extension of k with Galois group $\mathbb{Z}/p^n\mathbb{Z}$ and L can be embedded in a normal extension of k with Galois group $\mathbb{Z}/p^{n+1}\mathbb{Z}$ if and only if ε is a norm from K/k.*

PROOF. Put $\zeta = \varepsilon^{p^{n-1}}$. Let C be a generator of $\mathfrak{G} = \operatorname{Gal}(L/k)$. Put $\mathfrak{N} = \langle C^p \rangle$ and let $\overline{G}$ denote the class of G mod $\mathfrak{N}$ for $G \in \mathfrak{G}$. The cyclic group of order p^{n+1} is the extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathfrak{G}$ given by the 2-cocycle

$$c(C^i, C^j) = \begin{cases} 1 & \text{for } i+j \leq p^n - 1 \\ \zeta & \text{for } i+j \geq p^n. \end{cases}$$

Let $f(C^{pi}) = \varepsilon^i$ for $i = 0, \ldots, p^{n-1} - 1$. Then we see that

$$c(C^{pi}, C^{pj}) f(C^{p(i+j)}) = f(C^{pi}) f(C^{pj}).$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

Using the notation of Theorem 1 we get $\Omega_{\overline{C}^u} = 1$, $a_{\overline{C}^u} = 1$, and for $0 \leq u, v \leq p-1$,

$$s(\overline{C}^u, \overline{C}^v) = \begin{cases} 1 & \text{for } u+v \leq p-1 \\ \varepsilon & \text{for } u+v \geq p. \end{cases}$$

So, s is a 2-coboundary if and only if ε is a norm from K/k.

Q. E. D.

3. 2-Extensions. In what follows, k denotes a field of characteristic different from 2.

Suppose that $a \in k^{\times} \setminus (k^{\times})^2$ and consider the quadratic extension $k(\sqrt{a})/k$. According to Theorem 2 this extension can be embedded in a $(\mathbb{Z}/4\mathbb{Z})$-extension of k if and only if -1 is a norm from $k(\sqrt{a})/k$, i.e., if and only if a is a sum of two squares in k (if -1 is a square in k then every element of k is a sum of two squares in k). Using Theorem 1 and Theorem 2 (or by direct verification) we then see that the $(\mathbb{Z}/4\mathbb{Z})$-extensions of k are the extensions

$$k\left(\left(q(a+u\sqrt{a})\right)^{1/2}\right)/k,$$

where

$$a = u^2 + v^2 \notin (k^{\times})^2, \quad u, v \in k, \quad q \in k^{\times}.$$

(If -1 is a square there is of course a simpler parametrisation but we do not need that.)

For $a, b \in k^{\times}$ the symbol (a, b) denotes as usual the element of the Brauer-group of k represented by the 2-cocycle on the absolute Galois group of k sending (G_1, G_2) into

$$\sqrt{a}^{\varphi(G_1)+\varphi(G_2)-\varphi(G_1G_2)},$$

where

$$\varphi(G) = \begin{cases} 0 & \text{if } G\sqrt{b} = \sqrt{b} \\ 1 & \text{if } G\sqrt{b} = -\sqrt{b}. \end{cases}$$

By abuse of notation we shall, whenever it is convenient, also let (a, b) denote this 2-cocycle.

As is well known we have $(a, b) = (b, a)$ and thus $(a, b) = 1$ if and only if a is a a norm from $k(\sqrt{b})/k$, and if and only if b is a norm from $k(\sqrt{a})/k$.

The next theorem classifies the $(\mathbb{Z}/8\mathbb{Z})$-extensions of k.

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

THEOREM 3. *Let $a = u^2 + v^2 \in k^\times \setminus (k^\times)^2$, where $u, v \in k$. Put $\theta = a + u\sqrt{a}$. We distinguish the following two cases:*

1° — a is a square in k. In this case we shall assume that $a = -1$.

2° — a is not a square in k.

For $x \in k(\sqrt{a})$ we denote by x' the conjugate of x in $k(\sqrt{a})$.
(1) For $q \in k^\times$ the $(\mathbb{Z}/4\mathbb{Z})$-extension $k(q\theta)^{1/2}/k$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of k if and only if

$$\left(a, \frac{v}{u}\right)(q, -1) = 1.$$

(2) $k(\sqrt{a})/k$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of k if and only if the equation

$$(+) \qquad X^2 - aY^2 - \frac{v}{u}Z^2 - a\frac{v}{u}V^2 = 0$$

has a solution $(X, Y, Z, V) \neq (0, 0, 0, 0)$ with $X, Y, Z, V \in k$.

In case 1° this condition is satisfied.
(3) If the condition under (2) is satisfied then all $(\mathbb{Z}/8\mathbb{Z})$-extensions of k containing $k(\sqrt{a})$ are obtained as follows:
In case 1° we choose $x, y \in k$ such that $x^2 + y^2 \neq 0$ and put $q = x^2 + y^2$. We put

$$\varphi = \frac{1 + \sqrt{-1}}{(x + y\sqrt{-1})\big((v + 1) + u\sqrt{-1}\big)}.$$

Then the element

$$\xi = \frac{q\theta^2}{v\sqrt{-1}}\varphi^2 \in k(\sqrt{a})$$

has norm 1 (over k) and we choose $\eta \in k(\sqrt{a})^\times$ such that

$$\eta' = \eta\xi.$$

Then $k\Big(\sqrt{a}, \big(\eta(q\theta)^{1/2}\big)^{1/2}\Big)/k$ is a $(\mathbb{Z}/8\mathbb{Z})$-extension containing $k(\sqrt{a})$. In case 2°: we choose a solution $(X, Y, Z, V) \neq (0, 0, 0, 0)$ with $X, Y, Z, V \in k$ to (+) and $y \in k$ such that $1 + y^2 \neq 0$. We put

$$\begin{aligned} q &= (1 + y^2)(Z^2 + aV^2) \\ &= (-Zy + V\sqrt{a})^2 + (Z + Vy\sqrt{a})^2 \in k^\times. \end{aligned}$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

Put

$$\begin{aligned} W_1 &= \frac{1}{2}\Big(\big(Z\big(-y\big(u+v\big)+(u-v)\big)+aV(1+y)\big) \\ &\qquad + \big(Z(1-y)+V\big((u+v)+y(u-v)\big)\big)\sqrt{a}\Big) \\ W_2 &= \frac{1}{2}\Big(\big(Z\big(-(u+v)-y(u-v)\big)+aV(1-y)\big) \\ &\qquad + \big(-Z(1+y)+V\big((u-v)-y(u+v)\big)\big)\sqrt{a}\Big) \\ \varphi &= \frac{W_1}{(X+Y\sqrt{a})\big((y-\frac{u}{v})+\frac{1}{v}\sqrt{a}\big)\big((u+v)+\sqrt{a}\big)}. \end{aligned}$$

Then the element

$$\xi = \frac{W_1}{W_1'}\cdot\frac{u+\sqrt{a}}{v}\cdot\frac{2}{W_1W_1'}(W_1W_1' - W_2W_2' + qv\sqrt{a})\varphi^2 \in k(\sqrt{a})$$

has norm 1. We choose $\eta \in k(\sqrt{a})^\times$ such that

$$\eta' = \eta\xi.$$

Then $k\Big((q\theta)^{1/2}, \big(\eta\big(q\theta + W_2(q\theta)\big)^{1/2}\big)^{1/2}\Big)$ is a $(\mathbb{Z}/8\mathbb{Z})$-extension of k containing $k(\sqrt{a})$.

PROOF. We divide the proof into two parts. In (a) we choose $q \in k^\times$ and assume that the $(\mathbb{Z}/4\mathbb{Z})$-extension $k\big((q\theta)^{1/2}\big)/k$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of k. Then we perform some preliminary computations concerning the structure of such a $(\mathbb{Z}/8\mathbb{Z})$-extension. In this process the theorem will be proved completely for the case 1°. In (b) we finish the proof of the theorem for the case 2°.

(a) Let $q \in k^\times$ and consider the $(\mathbb{Z}/4\mathbb{Z})$-extension $k\big((q\theta)^{1/2}\big)/k$. Let $\mathfrak{G} = \langle C\rangle$ be the Galois group where C is chosen such that $C(q\theta)^{1/2} = qv\sqrt{a}(q\theta)^{-1/2}$. Put $\mathfrak{N} = \langle C^2\rangle$ and let c be the "natural" 2-cocycle giving the extension

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \to \mathfrak{G} \to 0.$$

The restriction of c to $\mathfrak{N}$ is a 2-coboundary in $B^2\big(\mathfrak{N}, k\big((q\theta)^{1/2}\big)^\times\big)$ if and only if $q\theta$ is a sum of two squares in $k(\sqrt{a})$. In case 1° this condition is satisfied.

Let us assume that if we are in case 2° then

$$q\theta = W_1^2 + W_2^2 \quad \text{for certain } W_1, W_2 \in k(\sqrt{a}).$$

With the notation from Theorem 1 we put

$$f(C^2) = f = \begin{cases} \sqrt{-1} & \text{in case } 1^\circ \\ \frac{1}{W_1}(W_2 - (q\theta)^{1/2}) & \text{in case } 2^\circ \end{cases}$$

and $f(E) = 1$. Denoting by $\overline{G}$ the class of $G \in \mathfrak{G}$ modulo $\mathfrak{N}$ we compute

$$\Omega_{\overline{C}}(C^2) = \begin{cases} -1 & \text{in case } 1^\circ \\ \frac{Cf}{f} & \text{in case } 2^\circ \end{cases}$$

and put

$$A = \begin{cases} (q\theta)^{1/2} & \text{in case } 1^\circ \\ 1 + \frac{f}{Cf} & \text{in case } 2^\circ. \end{cases}$$

If in case 2° we had $Cf = -f$ then $\theta CW_1 = W_1 v\sqrt{a}$ and for $W_1 = x + y\sqrt{a}$ this would give $x = y(u - v)$ and $x(u+v) = ya$ and so $y(u^2 - v^2) = ya = y(u^2 + v^2)$ and so $y = 0$. Then $W_1 \in k$ and since $C\frac{W_2}{W_1} = -\frac{W_2}{W_1}$ we would also deduce $W_2\sqrt{a} \in k$ which is impossible. Consequently, $A \neq 0$ in all cases and we may put $a_{\overline{C}} = A$. We find

$$s(\overline{C}, \overline{C}) = \frac{f}{ACA} \in k,$$

and $k((q\theta)^{1/2})/k$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of k if and only if $s(\bar{C}, \bar{C})$ is a norm from $k(\sqrt{a})/k$. Still using the notation from Theorem 1 we have

$$h(C) = A,$$

and if $s(\overline{C}, \overline{C})$ is a norm from $k(\sqrt{a})/k$, say $s(\overline{C}, \overline{C}) = \varphi\varphi'$ for some $\varphi \in k(\sqrt{a})$, then all $(\mathbb{Z}/8\mathbb{Z})$-extensions of k containing $k((q\theta)^{1/2})$ have the form $k((q\theta)^{1/2}), \chi^{1/2})/k$ where $\chi \in k((q\theta)^{1/2})$ is such that

$$C\chi = \chi(A\varphi)^2.$$

In case 1° we get $s(\overline{C}, \overline{C}) = \frac{1}{qv}$ and $s(\overline{C}, \overline{C})$ is a norm from $k(\sqrt{a})/k$ if and only if $(qv, -1) = 1$. Now, $v = \frac{1}{2}\big((v+1)^2 + u^2\big)$, so $(v, -1) = 1$, and hence the conditon says that $(q, -1) = 1$. By similar reasoning we have $(\frac{v}{u}, -1) = 1$. Consequently the quadratic extension $k(\sqrt{-1})/k$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of k. The equation

$$X^2 + Y^2 - \frac{v}{u}(Z^2 - V^2) = 0$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

has a solution $(X, Y, Z, V) \neq (0,0,0,0)$ with $X, Y, Z, V \in k$. If $(q, -1) = 1$ we put $\chi = \eta(q\theta)^{1/2}$ where $\eta \in k(\sqrt{-1})$ and the condition on η is then

$$\begin{aligned}\frac{\eta'}{\eta} &= \frac{(q\theta)^{1/2}}{C(q\theta)^{1/2}} \cdot (q\theta)\varphi^2 \\ &= \frac{q\theta^2}{v\sqrt{-1}}\varphi^2,\end{aligned}$$

where φ is as stated in the theorem.

Hereby we have proved the theorem for the case 1° and for the rest of the proof we shall assume that case 2° prevails.

We compute

$$\begin{aligned}\frac{ACA}{f} &= -(1 + C + C^2 + C^3)(f) \\ &= -2\left(\frac{W_2}{W_1} + C\frac{W_2}{W_1}\right).\end{aligned}$$

We may put $\chi = \eta(q\theta + W_2(q\theta)^{1/2})$ where $\eta \in k(\sqrt{a})$ and with $\omega = q\theta + W_2(q\theta)^{1/2}$ the condition on η becomes

$$\frac{\eta'}{\eta} = \frac{\omega}{C\omega}A^2\varphi^2,$$

where φ is such that $s(\overline{C}, \overline{C}) = \varphi\varphi'$, and since $\omega = W_1(q\theta)^{1/2}C^2 f = W_1(q\theta)^{1/2}\left(-\frac{1}{f}\right)$ we get

$$\begin{aligned}\frac{\omega}{C\omega}A^2 &= \frac{W_1}{W_1'} \cdot \frac{\theta}{v\sqrt{a}} \cdot \frac{Cf}{f}\left(1 + \frac{f}{Cf}\right)^2 \\ &= \frac{W_1}{W_1'} \cdot \frac{u + \sqrt{a}}{v}(1 + C^2)\left(1 + \frac{f}{Cf}\right) \\ &= \frac{W_1}{W_1'} \cdot \frac{u + \sqrt{a}}{v}\frac{2}{W_1 W_1'}(W_1 W_1' - W_2 W_2' + qv\sqrt{a}).\end{aligned}$$

(b) Let $q \in k^{\times}$.

Let us first assume that $q \notin k(\sqrt{a})^2$. Let C_1 be the non-trivial automorphism in $k(\sqrt{q})$. We consider C and C_1 as automorphisms in $k(\sqrt{q}, \sqrt{\theta})/k$ with $C_1(q\theta)^{1/2} = (q\theta)^{1/2}$ and $C\sqrt{q} = \sqrt{q}$. The Galois group of $k(\sqrt{q}, \sqrt{\theta})/k$ is $\langle C \rangle \times \langle C_1 \rangle$ and the fixed field of $\langle C^2 C_1 \rangle$ is $k(\sqrt{\theta})$. We have $c(-1, q)(C^2C_1, C^2C_1) = 1$ and we see that $\tilde{c} = c(-1, q)$ gives us the "natural" 2-cocycle on $\langle C, C_1 \rangle / \langle C^2 C_1 \rangle = \mathrm{Gal}(k(\sqrt{\theta})/k)$ mentioned under (a). Now,

$$\theta = \left(\frac{u+v}{2} + \frac{1}{2}\sqrt{a}\right)^2 + \left(\frac{u-v}{2} + \frac{1}{2}\sqrt{a}\right)^2.$$

Put

$$\alpha = \frac{u+v}{2} + \frac{1}{2}\sqrt{a}, \quad \beta = \frac{u-v}{2} + \frac{1}{2}\sqrt{a}.$$

Then

$$-2\left(\frac{\beta}{\alpha} + \frac{\beta'}{\alpha'}\right) = 4\frac{v}{u}$$

and so $\tilde{c}$ has class 0 in $\mathrm{Br}(k)$ if and only if $(a, \frac{v}{u}) = 1$. We conclude that c has class 0 in $\mathrm{Br}(k)$ if and only if $(a, \frac{v}{u})(q, -1) = 1$. If $q \in k(\sqrt{a})^2$ then $k((q\theta)^{1/2}) = k(\theta^{1/2})$, and we see that the conclusion is still true (since $(a, -1) = 1$).

Hereby (1) is proved.

If $q \in k^\times$ and $(a, \frac{v}{u})(q, -1) = 1$ then q must be a sum of two squares in $k(\sqrt{a})$. An elementary computation shows that this is the case if and only if q has the form

$$(++) \qquad q = (1 + y^2)(Z^2 + aV^2) \quad \text{with } y, Z, V \in k.$$

If (++) is satisfied we get $q = (-Zy + V\sqrt{a})^2 + (Z + Vy\sqrt{a})^2$ and

$$q\theta = W_1^2 + W_2^2$$

where W_1 and W_2 are as in the theorem. Furthermore, $(q, -1) = (Z^2 + aV^2, -1) = (Z^2 + aV^2, a)$ and so $(a, \frac{v}{u})(q, -1) = (a, \frac{v}{u}(Z^2 + aV^2)) = 1$ and thus the equation (+) has a solution $(X, Y, Z, V) \neq (0, 0, 0, 0)$ with $X, Y, Z, V \in k$.

If the equation (+) has a solution $(X, Y, Z, V) \neq (0, 0, 0, 0)$ with $X, Y, Z, V \in k$ we must have $Z^2 + aV^2 \neq 0$. Putting $q = Z^2 + aV^2$ we then see that $(a, \frac{v}{u}q) = 1$ and since $(q, -1) = (q, a)$ we deduce $(a, \frac{v}{u})(q, -1) = 1$.

With this, (2) is proved.

To complete the proof, we have only to show that if q has the form (++) where $(X, Z, Y, V) \neq (0, 0, 0, 0)$ is a solution to (+) with $X, Z, Y, V \in k$ then $s(\overline{C}, \overline{C}) = \varphi\varphi'$ where $s(\overline{C}, \overline{C})$ is the element computed under (a) and $\varphi \in k(\sqrt{a})$ is the element given in the formulation of the theorem. This can be verified by a completely elementary computation which is left to the reader.

Q. E. D.

The next theorem gives a classification of Q_8-extensions of k, Q_8 being the quaternion group of order 8. These extensions of k have been classified in [**5**] but

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

our theorem gives a somewhat different classification. The article [**2**] also gives a classification of the Q_8-extensions of k, but the method of proof and the form of the classification given [**2**] are both different from what will be presented here. We use the following presentation of Q_8:

$$Q_8 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = E,\ \tilde{N}^4 = \tilde{S}^2,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1} \rangle.$$

THEOREM 4. *Let $a, b \in k^\times$ be such that none of a, b, ab is a square in k. Let $\mathfrak{G} = \langle N, S \rangle$ be the Galois group of $k(\sqrt{a}, \sqrt{b})/k$ where $N\sqrt{a} = -\sqrt{a}, N\sqrt{b} = \sqrt{b}, S\sqrt{a} = \sqrt{a}$ and $S\sqrt{b} = -\sqrt{b}$. The extension $k(\sqrt{a}, \sqrt{b})/k$ can be embedded in a Q_8-extension of k if and only if*

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

if and only if there exist $\alpha, \beta, \gamma, \lambda, \mu, \nu \in k$ such that

$$\begin{aligned} a &= \alpha^2 + \beta^2 + \gamma^2 \\ b &= \lambda^2 + \mu^2 + \nu^2 \quad \text{and} \\ \alpha\lambda &+ \beta\mu + \gamma\nu = 0. \end{aligned}$$

If this is the case we put

$$\theta = 1 + \frac{\alpha}{\sqrt{a}} + \frac{\nu}{\sqrt{b}} + \frac{\alpha\nu - \gamma\lambda}{\sqrt{ab}}$$

and then we have

$$\begin{aligned} \theta S\theta &= \left(\frac{\mu}{\sqrt{b}} + \frac{\alpha\mu - \beta\lambda}{\sqrt{ab}} \right)^2, \\ \theta N\theta &= \left(\frac{\beta}{\sqrt{a}} + \frac{\beta\nu - \gamma\mu}{\sqrt{ab}} \right)^2, \\ \theta NS\theta &= \left(\frac{\lambda}{\sqrt{b}} - \frac{\gamma}{\sqrt{a}} \right)^2, \end{aligned}$$

and the extensions $k(\sqrt{a}, \sqrt{b}, (q\theta)^{1/2})/k$ where $q \in k^\times$ are the Q_8-extensions of k containing $k(\sqrt{a}, \sqrt{b})$.

PROOF. Let c be the "natural" 2-cocycle giving the extension of $\mathbb{Z}/2\mathbb{Z}$ to Q_8 with $\mathfrak{G}$ as quotient, i.e., c is obtained from the isomorphism $Q_8/\langle \tilde{N}^2 \rangle \cong \mathfrak{G}$, where Q_8 has the presentation given above, given by $\tilde{N} \longmapsto N$ and $\tilde{S} \longmapsto S$. We have $c(N, S) = 1, c(S, N) = -1$ and $c(N, N) = c(S, S) = -1$. Let $\mathfrak{N} = \langle S \rangle$. Putting

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

$\tilde{c} = c(-1, b)$ we get $\tilde{c}(S, S) = 1$. With the notation of Theorem 1 we put, denoting by $\overline{G}$ the class of $G \in \mathfrak{G}$ modulo $\mathfrak{N}$, $f = f(S) = 1$, $\Omega_{\overline{N}}(S) = -1$, and $A = a_{\overline{N}} = \sqrt{b}$. Then, $s(\overline{N}, \overline{N}) = -\frac{1}{b}$. Thus $\tilde{c}$ has class 0 in $\mathrm{Br}(k)$ if and only if $(a, -b) = 1$ and consequently c has class 0 in $\mathrm{Br}(k)$ if and only if $(a, -b)(b, -1) = 1$, and if and only if $(a, b)(ab, -1) = 1$.

If $(a, b)(ab, -1) = 1$ then b is a sum of two squares in $k(\sqrt{a})$. As we previously have seen this means that b has the form $b = (1 + x^2)(y^2 + az^2)$ where $x, y, z \in k$. Then $(b, -1) = (y^2 + az^2, -1) = (y^2 + az^2, a)$ and so $1 = (a, b)(ab, -1) = (a, -1)(a, b(y^2 + az^2)) = (a, -(1 + x^2))$. So, a has the form $a = X^2 + (1 + x^2)Y^2$ where $X, Y \in k$. Then

$$\begin{aligned} b &= (y^2 + (Xz)^2 + (1 + x^2)(Yz)^2)(1 + x^2) \\ &= ((1 + x^2)Yz)^2 + (y - Xxz)^2 + (yx + Xz)^2. \end{aligned}$$

Putting $\alpha = X, \beta = Yx, \gamma = -Y, \lambda = (1 + x^2)Yz, \mu = y - Xxz$ and $\nu = yx + Xz$ we then get $a = \alpha^2 + \beta^2 + \gamma^2, b = \lambda^2 + \mu^2 + \nu^2$ and $\alpha\lambda + \beta\mu + \gamma\nu = 0$.

Conversely, if there exist $\alpha, \beta, \gamma, \lambda, \mu, \nu \in k$ such that $a = \alpha^2 + \beta^2 + \gamma^2$, $b = \lambda^2 + \mu^2 + \nu^2$ and $\alpha\lambda + \beta\mu + \gamma\nu = 0$ then we may assume that $\gamma \neq 0$. Since $\beta^2 + \gamma^2 \neq 0$ we see that it is possible to determine $X, Y, x, y, z \in k$ such that $a = X^2 + (1 + x^2)Y^2$ and $b = (1 + x^2)(y^2 + az^2)$ and so $(a, b)(ab, -1) = (a, -(1 + x^2)) = 1$. Furthermore it can be seen by elementary computations that if we put

$$\begin{aligned} \psi(E) &= 1, \\ \psi(S) &= \frac{1}{\theta}\left(\frac{\mu}{\sqrt{b}} + \frac{\alpha\mu - \beta\lambda}{\sqrt{ab}}\right), \\ \psi(N) &= \frac{1}{\theta}\left(\frac{\beta}{\sqrt{a}} + \frac{\beta\nu - \gamma\mu}{\sqrt{ab}}\right) \quad \text{and} \\ \psi(NS) &= \frac{1}{\theta}\left(\frac{\lambda}{\sqrt{b}} + \frac{\gamma}{\sqrt{a}}\right), \end{aligned}$$

then $c(G_1, G_2)\psi(G_1G_2) = \psi(G_1)G_1\psi(G_2)$ for $G_1, G_2 \in \mathfrak{G}$. Note that $ab = (\alpha\mu - \beta\lambda)^2 + (\beta\nu - \gamma\mu)^2 + (\gamma\lambda - \alpha\nu)^2$. As a consequence, the extension $k(\sqrt{a}, \sqrt{b}, \sqrt{\theta})/k$ is a Q_8-extension of k.

Q. E. D.

REMARK. We have $(a, b)(ab, -1) = (-a, -b)(-1, -1)$, and from the theory of quadratic forms it follows that $(a, b)(ab, -1) = 1$ if and only if the quadratic forms $(ab)^{-1}X^2 + aY^2 + bZ^2$ and $X^2 + Y^2 + Z^2$ are equivalent over k. If this is the case it is a possible to obtain in a natural way the expressions giving $\psi(S)$, $\psi(N)$ and $\psi(NS)$ by means of a transformation matrix defining the equivalence of the two quadratic forms.

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

In the following theorems we shall discuss construction and classification of extensions with Galois group isomorphic to the dihedral or quasi-dihedral group of order 16. Let us recall that the dihedral group of order 16, D_8, has the presentation

$$D_8 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = \tilde{S}^2 = E,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1} \rangle,$$

and that the quasi-dihedral group of order 16, QD_8, has the presentation

$$QD_8 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = \tilde{S}^2 = E,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^3 \rangle.$$

First we prove a simple theorem on D_4-extensions, D_4 being the dihedral group of order 8.

THEOREM 5. *(1) Let $a, b \in k^\times$ be such that none of a, b, ab is a square in k. The extension $k(\sqrt{a}, \sqrt{b})/k$ can be embedded in a D_4-extension of k cyclic over $k(\sqrt{b})$ if and only if $(a, -b) = 1$, i.e. iff there exist $x, y \in k$ such that $b = ay^2 - x^2$. If this the case then the D_4-extensions of k containing $k(\sqrt{a}, \sqrt{b})$ and cyclic over $k(\sqrt{b})$ are exactly the extensions of the form $k(\sqrt{a}, \sqrt{b}, (q(ay + x\sqrt{a}))^{1/2})/k$ where $q \in k^\times$.*

(2) The D_4-extensions of k are the following:

$$k(\sqrt{a}, \sqrt{a-1}, (q(a + \sqrt{a}))^{1/2})/k$$

where $a, q \in k^\times$ are such that none of $a, a-1, a(a-1)$ is a square in k, and

$$k(\sqrt{-1}, \sqrt{q}a^{1/4})/k$$

where $a, q \in k^\times$ are such that none of $-1, a, -a$ is a square in k.

PROOF. Let $\mathfrak{G} = \langle N, S \rangle$ be the Galois group of $k(\sqrt{a}, \sqrt{b})/k$ where $N\sqrt{a} = -\sqrt{a}$, $N\sqrt{b} = \sqrt{b}$, $S\sqrt{a} = \sqrt{a}$, $S\sqrt{b} = -\sqrt{b}$. Considering the presentation

$$D_4 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^4 = \tilde{S}^2 = E,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1} \rangle,$$

the isomorphism $D_4/\langle \tilde{N}^2 \rangle \cong \mathfrak{G}$ given by $\tilde{N} \longmapsto N$, $\tilde{S} \longmapsto S$ provides us with a 2-cocycle, c, on $\mathfrak{G}$ with coefficients in $\{\pm 1\}$ giving the extension of $\mathbb{Z}/2\mathbb{Z}$ to D_4 with $\mathfrak{G}$ as quotient. An embedding of $k(\sqrt{a}, \sqrt{b})/k$ in a D_4-extension cyclic over $k(\sqrt{b})$ is possible if and only if c is a 2-coboundary in $B^2(\mathfrak{G}, k(\sqrt{a}, \sqrt{b})^\times)$.

We have $c(S, S) = 1$. Put $\mathfrak{N} = \langle S \rangle$. Using the notation from Theorem 1 we get, denoting by $\overline{G}$ the class modulo $\mathfrak{N}$ of $G \in \mathfrak{G}$, $f = f(S) = 1$, $\Omega_{\overline{N}}(S) = -1$, $a_{\overline{N}} = \sqrt{b}$ and $s(\overline{N}, \overline{N}) = -\frac{1}{b}$. The embedding problem under consideration is thus solvable if and only if $(a, -b) = 1$.

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

If this is the case there exist $x, y \in k$ such that $-b = x^2 - ay^2$. Still using the notation from Theorem 1 we find $h(E) = h(S) = 1$, $h(N) = h(NS) = \sqrt{b}$ and the given embedding problem is solved by the extensions $k(\sqrt{a}, \sqrt{b}, \sqrt{\theta})/k$ where $\theta \in k(\sqrt{a}, \sqrt{b})^{\times}$ satisfies

$$S\theta = \theta \text{ and}$$
$$(+) \qquad N\theta = NS\theta = \theta\left(\frac{x - y\sqrt{a}}{\sqrt{b}}\right)^2.$$

The solutions to (+) are $\theta = q(ay + x\sqrt{a})$ where $q \in k^{\times}$.

The rest of the statements in the theorem are now obvious.

Q. E. D.

THEOREM 6. *We consider the presentation*

$$D_8 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = \tilde{S}^2 = E,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1} \rangle.$$

(1) The D_4-extension

$$k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)/k$$

where $a, b, q \in k^{\times}$ are such that none of a, b, ab is a square in k and either

$$1^\circ \quad b = a - 1, \quad \theta = a + \sqrt{a}$$

or

$$2^\circ \quad b = -1, \quad \theta = \sqrt{a}$$

can be embedded in a D_8-extension cyclic over $k(\sqrt{b})$ if and only if

$$(a, 2)(q, -b) = 1.$$

(2) If a and b are as in (1) there exists $q \in k^{\times}$ such that $(a, 2)(q, -b) = 1$ if and only if the equation

$$X^2 - aY^2 - 2Z^2 - 2abV^2 = 0$$

has a solution with $X, Y, Z, V \in k$ and $(X, Y) \neq (0, 0)$.

(3) The following two familites of D_8-extensions of k give all D_8-extensions of k:

$$(I) \qquad k\Big(\sqrt{-1}, (q\sqrt{a})^{1/2}, \big((X + Y\sqrt{a})(q\sqrt{a})^{1/2}\big)^{1/2}\Big)/k$$

where $a, q \in k^{\times}$, none of $-1, a, -a$ is a square in $k, (a, 2) = 1$ and (X, Y) is a solution to the equation

$$2 = X^2 - aY^2$$

with $X, Y \in k$;

$$(II) \qquad k\left(\sqrt{a}, \sqrt{a-1}, (2q\theta)^{1/2}, \left(\eta \cdot \frac{1}{W_2}\left(2q\theta + W_1(2q\theta)^{1/2}\right)\right)^{1/2}\right)/k$$

where $a \in k^{\times}, b = a - 1 \in k^{\times}$ are such that none of a, b, ab is a square in k, $\theta = a + \sqrt{a}$, $(X, Y, Z, V) \in (k)^4$ is a solution to the equation

$$X^2 - aY^2 - 2Z^2 - 2abV^2 = 0$$

with $(X, Y) \neq (0, 0)$, $x, y \in k$ are such that $x^2 + by^2 \neq 0$, $q = (x^2 + by^2)(Z^2 + abV^2)$,

$$W_1 = \big(Z(x - by) - abyV\big) + \big(Zx - b(x + y)V\big)\sqrt{a},$$
$$W_2 = \big(Z(x + y) + axV\big) + \big(Zy + (x - by)V\big)\sqrt{a},$$
$$\varphi = \frac{W_2}{2}\,\frac{b}{(X + Y\sqrt{a})(1 + \sqrt{a})\big((by - x) + x\sqrt{a}\big)},$$

and $\eta \in k(\sqrt{a})^{\times}$ is chosen in the following way. It is shown that the element $\xi \in k(\sqrt{a})$ defined by

$$\xi = 4(1 + \sqrt{a}) \cdot \frac{W_1W_2' + W_1'W_2 + 2q\sqrt{a}}{bW_2W_2'}\varphi^2,$$

where $x \longmapsto x'$ denotes the conjugation in $k(\sqrt{a})$, has norm 1 over k, and η is chosen such that

$$\eta' = \eta\xi.$$

PROOF. We divide the proof into three parts. In (a) we perform some preliminary computations and prove (1). In (b) we prove (2), and in (c) we finish the proof of the theorem.

(a) Let $a, b, q \in k^{\times}$ be such that none of a, b, ab is a square in k and that $b = a - 1$ or $b = -1$. With $\theta = a + \sqrt{a}$ for $b = a - 1$ and $\theta = \sqrt{a}$ for $b = -1$ the extension $k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)/k$ is a D_4-extension of k. The Galois group is generated by N and S where $N\sqrt{a} = -\sqrt{a}$, $N\sqrt{b} = \sqrt{b}$, $N(2q\theta)^{1/2} = 2q\sqrt{a}\sqrt{b}(2q\theta)^{-1/2}$,

$S\sqrt{a} = \sqrt{a}, S(2q\theta)^{1/2} = (2q\theta)^{1/2}, S\sqrt{b} = -\sqrt{b}$. The isomorphism $D_8/\langle \tilde{N}^2\rangle \cong \langle N, S\rangle$ given by $\tilde{N} \longmapsto N$, $\tilde{S} \longmapsto S$ gives rise to a 2-cocycle, c, on $\mathfrak{G}$ with coefficients in $\{\pm 1\}$. To prove (1) we have to show that $c \in B^2\big(\mathfrak{G}, k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)^{\times}\big)$ if and only if $(a,2)(q,-b) = 1$.

Put $K = k(\sqrt{a})$. Let us first assume that the restriction of c to $\mathfrak{N} = \langle N^2, S\rangle$ splits. This is equivalent to the assumption that the extension $K\big((2q\theta)^{1/2}, \sqrt{b}\big)/K$ can be embedded in a D_4-extension of K cyclic over $K(\sqrt{b})$. According to Theorem 5 this possible if and only if $(2q\theta, -b) = 1$ over K, i. e., if and only if there exist $X, Y \in K$ such that

$$2q\theta = X^2 + bY^2.$$

Let us assume that this the case. The $Y \neq 0$ and c splits in $\mathrm{Br}(K)$ as $c = \delta f$ (where δ is the coboundary operator) where

$$f(E) = f(S) = 1,\ f(N^2) = f(N^2S) = f = \frac{1}{\sqrt{b}}\left(\frac{X}{Y} - \frac{1}{Y}(2q\theta)^{1/2}\right),$$

as follows from the proof of Theorem 5 (or by direct verification). Using the notation of Theorem 1 we now compute, denoting by $\overline{N}$ the class of N in $\langle N, S\rangle / \langle N^2, S\rangle$, that

$$\Omega_{\overline{N}}(E) = 1,\ \Omega_{\overline{N}}(N^2) = \frac{Nf}{f},\ \Omega_{\overline{N}}(S) = -Nf \text{ and } \Omega_{\overline{N}}(N^2S) = \frac{1}{f}.$$

Consider $A = 1 + \frac{f}{Nf} - \frac{1}{Nf} + f$. We have $GA = A\Omega_{\overline{N}}(G)$ for $G \in \mathfrak{N}$. If $A = 0$ we would have $Nf + f - 1 + fNf = 0$ and since

$$f = \frac{1}{Y\sqrt{b}}\big(X - (2q\theta)^{1/2}\big),$$

$$Nf = \frac{1}{\sqrt{b}Y'}\big(X' - \frac{\sqrt{a}\sqrt{b}}{\theta}(2q\theta)^{1/2}\big)$$

and

$$fNf = \frac{1}{bYY'}\big(XX' + 2q\sqrt{a}\sqrt{b} + (2q\theta)^{1/2}(-X\frac{\sqrt{a}\sqrt{b}}{\theta} - X')\big)$$

(denoting by $x \longmapsto x'$ the conjugation in $K = k(\sqrt{a})$), we would deduce

$$X'\sqrt{b}Y + X\sqrt{b}Y' - bYY' + XX' + 2q\sqrt{a}\sqrt{b} = 0$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

which is impossible. Thus $A \neq 0$ and we put $a_{\overline{N}} = A$ and find $s(\overline{N},\overline{N}) = \frac{f}{ANA}$. We compute

$$\begin{aligned}\frac{ANA}{f} &= \frac{1}{f}\left(1 + \frac{f}{Nf} - \frac{1}{Nf} + f\right)(1 - fNf + f + Nf)\\ &= 4 + \frac{Nf}{f} - \frac{1}{fNf} + \frac{f}{Nf} - fNf\\ &= (1 + N + N^2 + N^3)(1 - fNf)\\ &= 4\left(1 - \frac{XX'}{bYY'}\right).\end{aligned}$$

Supposing furthermore that $s(\overline{N},\overline{N}) = \varphi\varphi'$ for some $\varphi \in K$, we see that c splits in $\mathrm{Br}(k)$, say $c = \delta\psi$, and the D_8-extensions containing $K\left((2q\theta)^{1/2}, \sqrt{b}\right)$ and cyclic over $k(\sqrt{b})$ are the extensions $K\left((2q\theta)^{1/2}, \sqrt{b}, \sqrt{\chi}\right)/k$ where $\chi \in K\left((2q\theta)^{1/2}, \sqrt{b}\right)^{\times}$ is such that

$$G\chi = \chi\psi(G)^2 \text{ for } G \in \langle N, S\rangle.$$

According to Theorem 5, χ has the form $\chi = \eta\omega$ for some $\eta \in k(\sqrt{a})$ and $\omega = \frac{1}{Y}\left(2q\theta + X(2q\theta)^{1/2}\right)$. Since $\psi(N) = A\varphi$ we get for the determination of η, that

$$\frac{\eta'}{\eta} = \frac{\omega}{N\omega}A^2\varphi^2.$$

Since $\omega = -\frac{1}{f}\sqrt{b}(2q\theta)^{1/2}$ we find

$$\begin{aligned}\frac{\omega}{N\omega}A^2 &= \frac{\theta}{\sqrt{a}\sqrt{b}} \cdot \frac{Nf}{f}A^2\\ &= \frac{\theta}{\sqrt{a}\sqrt{b}}\left(\frac{Nf}{f} + \frac{f}{Nf} + \frac{1}{fNf} + fNf - \frac{2}{f} + 2Nf - \frac{2}{Nf} + 2f\right)\\ &= \frac{\theta}{\sqrt{a}\sqrt{b}}(1 + N^2)\left(2f + 2Nf + fNf + \frac{Nf}{f}\right)\\ &= 4 \cdot \frac{\theta}{\sqrt{a}} \cdot \frac{XY' + X'Y + 2q\sqrt{a}}{bYY'}.\end{aligned}$$

In the case $b = -1, \theta = \sqrt{a}$ the above reasoning can be brought into a simpler form. Obviously, $(2q\theta, -b) = 1$ and c splits in $\mathrm{Br}(K)$ as $c = \delta f$ where $f(E) = f(S) = 1$ and $f(N^2) = f(N^2S) = \sqrt{-1}$. Putting $A = 1 + \sqrt{-1}$ we compute that

$$s(\overline{N},\overline{N}) = \frac{f(N^2)}{ANA} = \frac{1}{2}.$$

Assuming furthermore that $(a,2) = 1$ we may write $2 = X^2 - aY^2$ where $X, Y \in k$. Then $s(\overline{N}, \overline{N}) = \varphi\varphi'$ where $\varphi = (X + Y\sqrt{a})^{-1}$. Again we put $\chi = \eta\omega$ but here $\omega = (2q\theta)^{1/2}$. For the determination of η we get

$$\frac{\eta'}{\eta} = \frac{\omega}{N\omega}A^2\varphi^2 = 2\varphi^2.$$

Since $1 + (2\varphi^2)^{-1} = X(X + Y\sqrt{a})$ we may choose $\eta = X + Y\sqrt{a}$ (since this choice is obviously possible if $X = 0$).

Now let us return to the original situation without the additional assumptions. Let us however first assume that $q \notin k(\sqrt{a}, \sqrt{b})^2$. Let C be the conjugation in $k(\sqrt{q})$. We extend N, S and C to automorphisms in $k\big(\sqrt{a}, \sqrt{b}, \sqrt{q}, (2q\theta)^{1/2}\big)/k$ by $N\sqrt{q} = S\sqrt{q} = \sqrt{q}$ and $C\sqrt{a} = \sqrt{a}, C\sqrt{b} = \sqrt{b}, C(2q\theta)^{1/2} = (2q\theta)^{1/2}$. The Galois group of this extension is $\langle N, S\rangle \times \langle C\rangle, k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)$ is the fixed field of $\langle C\rangle$ and $k\big(\sqrt{a}, \sqrt{b}, (2\theta)^{1/2}\big)$ is the fixed field of $\langle N^2C\rangle$. We have

$$\langle N, S\rangle \times \langle C\rangle / \langle N^2C\rangle \cong \langle N, S\rangle$$

where the isomorphism is given by $N \longmapsto N$, $S \longmapsto S$, $C \longmapsto N^2$. Now consider the "natural" 2-cocycle, c_1, on $\langle N, S\rangle \times \langle C\rangle / \langle N^2C\rangle$ which is attached to the problem of embedding the extension $k\big(\sqrt{a}, \sqrt{b}, (2\theta)^{1/2}\big)/k$ into a D_8-extension of k cyclic over $k(\sqrt{b})$. Via the inflation maps we may view c_1 and c as 2-cocycles on $\langle N, S\rangle \times \langle C\rangle$. Thus we have

$$c_1(N^{\alpha_1}S^{\beta_1}C^{\gamma_1}, N^{\alpha_2}S^{\beta_2}C^{\gamma_2}) = c(N^{\alpha_1+2\gamma_1}S^{\beta_1}, N^{\alpha_2+2\gamma_2}S^{\beta_2}).$$

Consider $\psi\colon \langle N, S\rangle \times \langle C\rangle \longrightarrow k(\sqrt{b})^\times$ given by $\psi(E) = 1$, $\psi(C) = \sqrt{b}$ and $\psi(GC^\alpha) = \psi(C^\alpha)$ for $G \in \langle N, S\rangle$, and consider the 2-cocycle $\sigma = \frac{c}{c_1}(-\frac{1}{b}, q)\delta\psi$ on $\langle N, S\rangle \times \langle C\rangle$. We state that σ is a 2-coboundary. One way of realizing this is to use Theorem 1. First we note that

$$\sigma(C, C) = (-1)\cdot(-\frac{1}{b})(\sqrt{b}C\sqrt{b}) = 1,$$

and secondly we compute, identifying $\langle N, S\rangle$ with $\langle N, S\rangle \times \langle C\rangle / \langle C\rangle$, for $G \in \langle N, S\rangle$

$$\begin{aligned}\Omega_G(C) &= \frac{\sigma(C,G)}{\sigma(G,C)} \\ &= \frac{c(C,G)c_1(G,C)}{c(G,C)c_1(C,G)}\cdot\frac{\psi(C)}{G\psi(C)} \\ &= \frac{c(G,N^2)}{c(N^2,G)}\cdot\frac{\sqrt{b}}{G\sqrt{b}} \\ &= 1,\end{aligned}$$

which shows the statement to be true.

That c is cohomologous to $(a, 2)(q, -b)$ in case 2° we have already seen.

In case 1° we note that

$$2\theta = (1 + \sqrt{a})^2 + b,$$

and that

$$1 - \frac{1}{b}(1 + \sqrt{a})(1 - \sqrt{a}) = 2$$

whence it follows from the above that c_1 is cohomologous to $(a, 2)$. Thus c is cohomologous to $(a, 2)(q, -b)$.

Finally, if $q \in k(\sqrt{a}, \sqrt{b})^2$ the conclusion is clearly still true since in that case either $(q, -b) = (1, -b), (q, -b) = (a, -b), (q, -b) = (b, -b)$ or $(q, -b) = (ab, -b)$.

Hereby (1) is proved.

(b) Let again $a, b \in k^\times$ be such that none of a, b, ab is a square in k and either $b = a - 1$ or $b = -1$. If $b = -1$ the statement in (2) is trivial so we assume that $b = a - 1$.

If $q \in k^\times$ is such that $(a, 2)(q, -b) = 1$ then $(q, -b) = 1$ over $k(\sqrt{a})$. Therefore there exist $x_1, x_2, y_1, y_2 \in k$ such that

$$q = (x_1 + x_2\sqrt{a})^2 + b(y_1 + y_2\sqrt{a})^2.$$

From this we see that q has the form

$$(+) \qquad q = (x^2 + by^2)(Z^2 + abV^2),$$

where $x, y, Z, V \in k$. Then $(q, -b) = (Z^2 + abV^2, a)$ and so $1 = (a, 2)(q, -b) = \big(a, 2(Z^2 + abV^2)\big)$ and thus the equation $X^2 - aY^2 = 2(Z^2 + abV^2)$ has a solution with $X, Y \in k$ and $(X, Y) \neq (0, 0)$.

If the equation $X^2 - aY^2 - 2Z^2 - 2abV^2 = 0$ has a solution with $X, Y, Z, V \in k$ and $(X, Y) \neq (0, 0)$, then we must have $Z^2 + abV^2 \neq 0$. Choosing $x, y \in k$ such that $x^2 + by^2 \neq 0$ and putting $q = (x^2 + by^2)(Z^2 + abV^2)$, we then find $(a, 2)(q, -b) = 1$.

Hereby (2) is proved and we have found the construction of the 'possible' values of q from solutions to the equation in (2).

(c) The results in (3) follow from the results obtained in (a) and (b) once, in connection with the family in (II), we observe the following fact:

With

$$\begin{aligned} q &= (x^2 + by^2)(Z^2 + abV^2), \\ &= (Zx - byV\sqrt{a})^2 + b(yZ + Vx\sqrt{a})^2 \end{aligned}$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

we get, since $2\theta = (1+\sqrt{a})^2 + b$, that

$$2q\theta = W_1^2 + bW_2^2$$

where W_1 and W_2 are as specified in (II). Furthermore, it can be computed that

$$W_2W_2' - \frac{1}{b}W_1W_1' = 2(x^2 - by^2 + 2xy)(Z^2 + abV^2)$$

and we have

$$x^2 - by^2 + 2xy = (1-a)\Big(\big(y - \frac{x}{b}\big)^2 - a\big(\frac{x}{b}\big)^2\Big).$$

Q. E. D.

The investigation of QD_8-extensions is completely analogous to Theorem 6.

THEOREM 7. *We consider the presentation*

$$QD_8 = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = \tilde{S}^2 = E, \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^3 \rangle .$$

(1) The D_4-extension

$$k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)/k$$

where $a, b, q \in k^\times$ are such that none of a, b, ab is a square in k and either

$$1^\circ \quad b = a - 1, \quad \theta = a + \sqrt{a}$$

or

$$2^\circ \quad b = -1, \quad \theta = \sqrt{a}$$

can be embedded in a QD_8-extension cyclic over $k(\sqrt{b})$ and dihedral over $k(\sqrt{a})$ if and only if

$$(a, -2)(q, -b) = 1.$$

(2) If a and b are as in (1) there exists $q \in k^\times$ such that

$$(a, -2)(q, -b) = 1$$

if and only if the equation

$$X^2 - aY^2 + 2Z^2 + 2abV^2 = 0$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

has a solution with $X, Y, Z, V \in k$ and $(X, Y) \neq (0, 0)$.

(3) The following two families of QD_8-extensions of k give all the QD_8-extensions of k:

$$(I) \qquad k\Big(\sqrt{-1}, (q\sqrt{a})^{1/2}, \big((X + Y\sqrt{a})(q\sqrt{a})^{1/2}\big)^{1/2}\Big)/k$$

where $a, q \in k^\times$ are such that none of $a, -1, -a$ is a square in k, $(a, -2) = 1$ and (X, Y) is a solution to the equation

$$-2 = X^2 - aY^2$$

with $X, Y \in k$.

$$(II) \qquad k\Big(\sqrt{a}, \sqrt{a-1}, (2q\theta)^{1/2}, \Big(\eta \cdot \frac{1}{W_2}\big(2q\theta + W_1(2q\theta)^{1/2}\big)\Big)^{1/2}\Big)/k$$

where $a \in k^\times$ and $b = a - 1 \in k^\times$ are such that none of a, b, ab is a square in $k, \theta = a + \sqrt{a}, (X, Y, Z, V) \in (k)^4$ is a solution to the equation

$$X^2 - aY^2 + 2Z^2 + 2abV^2 = 0$$

with $(X, Y) \neq (0, 0)$, $x, y \in k$ are such that $x^2 + by^2 \neq 0$, $q = (x^2 + by^2)(Z^2 + abV^2)$,

$$\begin{aligned} W_1 &= \big(Z(x - by) - abyV\big) + \big(Zx - b(x + y)V\big)\sqrt{a}, \\ W_2 &= \big(Z(x + y) + axV\big) + \big(Zy + (x - by)V\big)\sqrt{a}, \\ \varphi &= \frac{W_2}{2} \cdot \frac{b}{(X + Y\sqrt{a})(1 + \sqrt{a})\big((by - x) + x\sqrt{a}\big)}, \end{aligned}$$

and $\eta \in k(\sqrt{a})^\times$ is chosen in the following way. It is shown that the element $\xi \in k(\sqrt{a})$ defined by

$$\xi = 4(1 + \sqrt{a}) \cdot \frac{-W_1W_2' - W_1'W_2 + 2q\sqrt{a}}{bW_2W_2'}\varphi^2,$$

where $x \mapsto x'$ denotes the conjugation in $k(\sqrt{a})$, has norm 1 over k, and η is chosen such that

$$\eta' = \eta\xi.$$

PROOF. The proof is completely analogous to the proof of Theorem 6. We have only to remark that the following changes in the proof of (a) have to be made:

We compute $\Omega_{\overline{N}}(E) = 1$, $\Omega_{\overline{N}}(N^2) = \frac{Nf}{f}$, $\Omega_{\overline{N}}(S) = Nf$, $\Omega_{\overline{N}}(N^2S) = -\frac{1}{f}$ and we put $A = 1 + \frac{f}{Nf} + \frac{1}{Nf} - f$ and deduce $A \neq 0$.

In the special case $b = -1, \theta = \sqrt{a}$, we put $A = 1 - \sqrt{-1}$.

Q. E. D.

Finally we shall investigate the structure of Q_{16}-extensions of k, Q_{16} being the quaternion group of order 16. We use the presentation

$$(+) \qquad Q_{16} = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = E, \tilde{S}^2 = \tilde{N}^4, \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1} \rangle.$$

THEOREM 8. *We consider the presentation (+) of Q_{16}.*

(1) The D_4-extension

$$k\left(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\right)/k$$

where $a, b, q \in k^\times$ are such that none of a, b, ab is a square in k and either

$$1^\circ \quad b = a - 1, \quad \theta = a + \sqrt{a}$$

or

$$2^\circ \quad b = -1, \quad \theta = \sqrt{a}$$

can be embedded in a Q_{16}-extension cyclic over $k(\sqrt{b})$ if and only if

$$(a, 2)(b, -1)(q, -b) = 1.$$

(2) Suppose that $K/k = k\left(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\right)/k$ is an extension of the type in (1) which can be embedded in a Q_{16}-extensions of k cyclic over $k(\sqrt{b})$. Let $\langle N, S\rangle$ be the Galois group of K/k using the same notation as in the proof of Theorem 6. Denote by x' the conjugate of x for $x \in k(\sqrt{a})$.

Then there exist $\alpha, \beta, \gamma, \lambda, \mu, \nu \in k(\sqrt{a})$ such that

$$\begin{aligned} 2q\theta &= \alpha^2 + \beta^2 + \gamma^2, \\ b &= \lambda^2 + \mu^2 + \nu^2 \quad \text{and} \\ \alpha\lambda &+ \beta\mu + \gamma\nu = 0. \end{aligned}$$

Put

$$\chi = 1 + \frac{\alpha}{(2q\theta)^{1/2}} + \frac{\nu}{\sqrt{b}} + \frac{\alpha\nu - \gamma\lambda}{\sqrt{b}(2q\theta)^{1/2}},$$

$$\psi_1 = \frac{\mu}{\sqrt{b}} + \frac{\alpha\mu - \beta\lambda}{\sqrt{b}(2q\theta)^{1/2}},$$

$$\psi_2 = \frac{\beta}{(2q\theta)^{1/2}} + \frac{\beta\nu - \gamma\mu}{\sqrt{b}(2q\theta)^{1/2}}, \text{ and}$$

$$\psi_3 = \frac{\lambda}{\sqrt{b}} - \frac{\gamma}{(2q\theta)^{1/2}}.$$

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

Let Tr (resp. Tr_1) be the trace for K/k (resp. $K/k(\sqrt{a})$) and suppose that

$$\zeta = \mathrm{Tr}\Big(\frac{\chi}{\psi_2} + \frac{1}{2}\cdot\frac{N\chi}{\psi_2}\Big(\frac{\psi_3}{N\psi_1} - \frac{\psi_1}{N\psi_3}\Big)\Big) \neq 0.$$

Then ζ is a norm from $k(\sqrt{a})/k$ and all Q_{16}-extensions containing K and cyclic over $k(\sqrt{b})$ are obtained in the following way:

Choose $\varphi \in k(\sqrt{a})$ such that

$$\frac{1}{\zeta} = \varphi\varphi'.$$

Then

$$\xi = \varphi^2\mathrm{Tr}_1\left(\frac{\chi}{N\chi} + \frac{\psi_2}{N\psi_2} + \frac{\psi_3}{N\psi_1} - \frac{\psi_1}{N\psi_3}\right) \in k(\sqrt{a})$$

has norm 1. We choose $\eta \in k(\sqrt{a})$ such that

$$\eta' = \eta\xi.$$

Then $K\big((\eta\chi)^{1/2}\big)/k$ is a Q_{16}-extension of the required type.

PROOF. (1) Consider a D_4-extension $K/k = k\big(\sqrt{a}, \sqrt{b}, (2q\theta)^{1/2}\big)/k$ where a, b and q are as in the formulation of the theorem except possibly for the validity of the condition $(a,2)(b,-1)(q,-b) = 1$. We let $\mathfrak{G} = \langle N, S\rangle$ be the Galois group of K/k using the same notation as in the proof of Theorem 6.

The problem of embedding K/k in a D_8- or Q_{16}-extensions of k cyclic over $k(\sqrt{b})$ is equivalent to the problem of the splitting in $H^2(\mathfrak{G}, K^\times)$ of the 2-cocycle, c (resp. c_1), on $\mathfrak{G}$ with coefficients in $\{\pm 1\}$ obtained from the natural isomorphisms

$$D_8/\langle \tilde{N}^4\rangle = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = \tilde{S}^2 = E,\ \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1}\rangle / \langle \tilde{N}^4\rangle \cong \mathfrak{G}$$

$$(\text{resp.}\quad Q_{16}/\langle \tilde{N}^4\rangle = \langle \tilde{N}, \tilde{S} \mid \tilde{N}^8 = E, \tilde{S}^2 = \tilde{N}^4, \tilde{S}^{-1}\tilde{N}\tilde{S} = \tilde{N}^{-1}\rangle / \tilde{N}^4 \cong \mathfrak{G}).$$

We state that $c_1 = c(-1,b)$ in $Z^2(\mathfrak{G}, K^\times)$. This can be demonstrated by using Theorem 1 on $\sigma = c_1\big(c(-1,b)\big)^{-1}$ for $\mathfrak{N} = \langle N\rangle$. Note that $\sigma(S,S) = 1$.

According to Theorem 6 and the proof of it, c is cohomologous to $(a,2)(q,-b)$ in $Z^2(\mathfrak{G}, K^\times)$. It follows that c_1 is cohomologous to $(a,2)(b,-1)(q,-b)$ in $Z^2(\mathfrak{G}, K^\times)$, which proves (1).

(2) The extension $K/k(\sqrt{a})$ is a biquadratic extension and can, according to assumption, be embedded in a Q_8-extension of $k(\sqrt{a})$. According to Theorem 4 there exist $\alpha, \beta, \gamma, \lambda, \mu, \nu \in k(\sqrt{a})$ with the properties stated and according to the

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

proof of Theorem 4 the restriction to $\mathfrak{N} = \langle N^2, S\rangle$ of the 2-cocycle, c_1, considered in (1) splits as $c_1 = \delta\psi$ where

$$\psi(E) = 1,\ \psi(S) = \frac{1}{\chi}\psi_1,\ \psi(N^2) = \frac{1}{\chi}\psi_2,\ \text{ and }\ \psi(N^2S) = \frac{1}{\chi}\psi_3.$$

We now apply Theorem 1 and retaining the notation of that theorem we find

$$\begin{aligned}
\Omega_{\overline{N}}(E) &= 1,\\
\Omega_{\overline{N}}(S) &= -\frac{\chi}{N\chi}\cdot\frac{N\psi_3}{\psi_1},\\
\Omega_{\overline{N}}(N^2) &= \frac{\chi}{N\chi}\cdot\frac{N\psi_2}{\psi_2},\ \text{and}\\
\Omega_{\overline{N}}(N^2S) &= \frac{\chi}{N\chi}\cdot\frac{N\psi_1}{\psi_3},
\end{aligned}$$

where $\overline{N}$ denotes the class of N modulo $\mathfrak{N}$.

Put

$$A = 1 + \frac{N\chi}{\chi}\left(\frac{\psi_2}{N\psi_2} + \frac{\psi_3}{N\psi_1} - \frac{\psi_1}{N\psi_3}\right).$$

Then $GA = \Omega_{\overline{N}}(G)A$ for $G \in \mathfrak{N}$, and if $A \neq 0$ we find

$$s(\overline{N},\overline{N}) = \frac{\psi(N^2)}{ANA} = \frac{\psi_2}{\chi(ANA)}.$$

We compute (using $c_1 = \delta\psi$ on $\mathfrak{N}$) that

$$\begin{aligned}
&(ANA)\cdot\frac{\chi}{\psi_2}\\
&\quad= \left(\chi + \frac{\psi_2N\chi}{N\psi_2} + \frac{\psi_3N\chi}{N\psi_1} - \frac{\psi_1N\chi}{N\psi_3}\right)\\
&\qquad\qquad\left(\frac{1}{\psi_2} - \frac{N\psi_2}{\chi N\chi} + \frac{N\psi_3}{\psi_3N\chi} + \frac{N\psi_1}{\psi_1N\chi}\right)\\
&\quad= \frac{\chi}{\psi_2} + \frac{N\chi}{N\psi_2} - \frac{\psi_2}{\chi} - \frac{N\psi_2}{N\chi} - \frac{\psi_1}{\psi_3} - \frac{N\psi_1}{N\psi_3} + \frac{\psi_3}{\psi_1} + \frac{N\psi_3}{N\psi_1}\\
&\qquad + \frac{\psi_3N\chi}{\psi_2N\psi_1} + \frac{\psi_2N\psi_3}{\psi_3N\psi_2} + \frac{\psi_1N\psi_2}{\chi N\psi_3} + \frac{\chi N\psi_1}{\psi_1N\chi}\\
&\qquad - \frac{\psi_1N\chi}{\psi_2N\psi_3} + \frac{\psi_2N\psi_1}{\psi_1N\psi_2} - \frac{\psi_3N\psi_2}{\chi N\psi_1} + \frac{\chi N\psi_3}{\psi_3N\chi}\\
&\quad= \mathrm{Tr}\left(\frac{\chi}{\psi_2}\right) + (1+N+N^2+N^3)\left(\frac{\psi_3N\chi}{\psi_2N\psi_1} - \frac{\psi_1N\chi}{\psi_2N\psi_3}\right),
\end{aligned}$$

and since

$$S\left(\frac{\psi_3 N\chi}{\psi_2 N\psi_1}\right) = N\left(\frac{\psi_3 N\chi}{\psi_2 N\psi_1}\right)$$

and

$$S\left(\frac{\psi_1 N\chi}{\psi_2 N\psi_3}\right) = N^3\left(\frac{\psi_1 N\chi}{\psi_2 N\psi_3}\right)$$

we get

$$\begin{aligned}(ANA)\cdot\frac{\chi}{\psi_2} &= \operatorname{Tr}\left(\frac{\chi}{\psi_2}+\frac{1}{2}\cdot\frac{N\chi}{\psi_2}\left(\frac{\psi_3}{N\psi_1}-\frac{\psi_1}{N\psi_3}\right)\right)\\ &= \zeta\end{aligned}$$

which according to assumption is non-zero. Thus $A \neq 0$. According to assumption there is $\varphi \in k(\sqrt{a})$ such that

$$\begin{aligned}\varphi\varphi' &= s(\overline{N},\overline{N})\\ &= \frac{1}{\zeta}.\end{aligned}$$

The Q_{16}-extensions of k of the required type have the form $K\big((\eta\chi)^{1/2}\big)/k$ for some $\eta \in k(\sqrt{a})$. For the determination of η we get, retaining the notation of Theorem 1,

$$N(\eta\chi) = (\eta\chi)\varphi^2 h(N)^2 = (\eta\chi)A^2\varphi^2,$$

that is,

$$\frac{\eta'}{\eta} = \frac{\chi}{N\chi}\cdot A^2\varphi^{2}$$

Now we compute (using $c_1 = \delta\psi$ on $\mathfrak{R}$) that

$$\begin{aligned}\frac{\chi}{N\chi}A^2 &= \frac{\chi}{N\chi}+\frac{N\chi}{\chi}\left(\frac{\psi_2^2}{N\psi_2^2}+\frac{\psi_3^2}{N\psi_1^2}+\frac{\psi_1^2}{N\psi_3^2}\right)\\ &\quad +2\frac{\psi_2}{N\psi_2}-2\frac{N\chi}{\chi}\cdot\frac{\psi_1\psi_3}{N(\psi_1\psi_3)}\\ &\quad +2\frac{\psi_3}{N\psi_1}-2\frac{N\chi}{\chi}\cdot\frac{\psi_1\psi_2}{N(\psi_2\psi_3)}\\ &\quad -2\frac{\psi_1}{N\psi_3}+2\frac{N\chi}{\chi}\cdot\frac{\psi_2\psi_3}{N(\psi_1\psi_2)}\\ &= \operatorname{Tr}_1\left(\frac{\chi}{N\chi}+\frac{\psi_2}{N\psi_2}+\frac{\psi_3}{N\psi_1}-\frac{\psi_1}{N\psi_3}\right).\end{aligned}$$

Q. E. D.

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press

EXAMPLE: Consider $k = \mathbb{Q}$. According to Theorem 8 the D_4-extension $K/\mathbb{Q} = \mathbb{Q}\left(\sqrt{7}, \sqrt{6}, (7+\sqrt{7})^{1/2}\right)/\mathbb{Q}$ can be embedded in a Q_{16}-extension of $\mathbb{Q}$ cyclic over $\mathbb{Q}(\sqrt{6})$ because $(7,2) = 1$ and $(6,-1)(2,-6) = (6,-2) = 1$. We have

$$\begin{aligned} 7+\sqrt{7} &= 1^2 + (-\frac{1}{2}+\frac{1}{2}\sqrt{7})^2 + (\frac{3}{2}+\frac{1}{2}\sqrt{7})^2, \\ 6 &= 2^2 + 1^2 + (-1)^2 \quad \text{and} \\ 2 &+ (-\frac{1}{2}+\frac{1}{2}\sqrt{7}) - (\frac{3}{2}+\frac{1}{2}\sqrt{7}) = 0. \end{aligned}$$

With the notation of Theorem 8, (2) we put

$$\chi = \frac{1}{\sqrt{6}}\left(\sqrt{6} - 1 + (-4+\sqrt{6}-\sqrt{7})(7+\sqrt{7})^{-1/2}\right)$$

and we choose $\eta \in \mathbb{Q}(\sqrt{7})$ such that

$$\frac{\eta'}{\eta} = \frac{11789 - 3116\sqrt{7}}{3.53^2}$$

where $x \longmapsto x'$ denotes conjugation in $\mathbb{Q}(\sqrt{7})$. For example we may choose

$$\eta = 6\sqrt{7}(41 + 38\sqrt{7}).$$

Thus $\mathbb{Q}(\sqrt{6}, \sqrt{7}, \sqrt{\theta})/\mathbb{Q}$ where

$$\theta = \sqrt{6}\sqrt{7}(41+38\sqrt{7})\left((\sqrt{6}-1) + (-4+\sqrt{6}-\sqrt{7})(7+\sqrt{7})^{-1/2}\right)$$

is a Q_{16}-extension of $\mathbb{Q}$ containing K.

A direct verification of this fact can be obtained by using Theorem 1, (5) and Theorem 8, (2). It is sufficient to prove normality of $\mathbb{Q}\sqrt{6}, \sqrt{7}, (\eta\chi)^{1/2}/\mathbb{Q}$. Denoting by N the automorphism in K/k given by $N\sqrt{7} = -\sqrt{7}$, $N\sqrt{6} = \sqrt{6}$, $N(7+\sqrt{7})^{1/2} = \sqrt{6}\sqrt{7}(7+\sqrt{7})^{-1/2}$, it is sufficient to prove the existence of an element $y \in K$ such that

$$N(\eta\chi) = (\eta\chi)y^2.$$

We compute

$$\begin{aligned} \frac{\chi}{N\chi} = \frac{1}{2 \cdot 53^2}&(14854 + 1495\sqrt{6} - 1846\sqrt{7} - 769\sqrt{6}\sqrt{7}) \\ &+ (-3508 - 1507\sqrt{6} + 1470\sqrt{7} + 95\sqrt{6}\sqrt{7})(7+\sqrt{7})^{1/2}). \end{aligned}$$

Put

$$\begin{aligned}U &= \frac{5+7\sqrt{7}}{12} \text{ and}\\ V &= \frac{1}{53^2}\Big((696+403\sqrt{6}-234\sqrt{7}-305\sqrt{6}\sqrt{7})\\ &\qquad +(-164-621\sqrt{6}+152\sqrt{7}+233\sqrt{6}\sqrt{7})(7+\sqrt{7})^{1/2}\Big).\end{aligned}$$

Then we find

$$\begin{aligned}U^2 &= \frac{1}{72}(184+35\sqrt{7}),\\ V^2 &= \frac{4}{53^4}\Big((6681066+1150071\sqrt{6}-2380326\sqrt{7}-442527\sqrt{6}\sqrt{7})\\ &\qquad +(-2424714-602241\sqrt{6}+921996\sqrt{7}\\ &\qquad\qquad +209379\sqrt{6}\sqrt{7})(7+\sqrt{7})^{1/2}\Big)\end{aligned}$$

and

$$\begin{aligned}&\frac{N\eta}{\eta}\cdot\frac{\chi}{N\chi}\\ &= \frac{1}{2\cdot 3\cdot 53^4}\Big((215378758-68047558\sqrt{7}+34397983\sqrt{6}\\ &\qquad\qquad -13724161\sqrt{6}\sqrt{7})\\ &\qquad +(-73419452+28260758\sqrt{7}-19838163\sqrt{6}\\ &\qquad\qquad +5815767\sqrt{6}\sqrt{7})(7+\sqrt{7})^{1/2}\Big)\\ &= U^2V^2.\end{aligned}$$

REMARK. Let $\mathfrak{G}$ be a finite group. For the study of $\mathfrak{G}$-extensions of $\mathbb{Q}$ the question of existence of "regular" $\mathfrak{G}$-extensions of $\mathbb{Q}(t)$, where t is a transcendental over $\mathbb{Q}$, is of interest. (A "regular" $\mathfrak{G}$-extension of $\mathbb{Q}(t)$ is a $\mathfrak{G}$-extension $K/\mathbb{Q}(t)$ such that any element of K which is algebraic over $\mathbb{Q}$ belongs to $\mathbb{Q}$.) The reason for this is that the existence of a regular $\mathfrak{G}$-extension of $\mathbb{Q}(t)$ is, by elementary Galois theory and by the Hilbert irreducibility theorem for $\mathbb{Q}$, seen to imply the existence of infinitely many $\mathfrak{G}$-extensions of $\mathbb{Q}$.

Using the theorems above we can deduce the existence of a regular $\mathfrak{G}$-extension of $\mathbb{Q}(t)$ when $\mathfrak{G}$ is any of the 2-groups considered:

According to Theorem 3 the extension $\mathbb{Q}\big((1+t^4)^{1/2}\big)/\mathbb{Q}(t)$ can be embedded in a $(\mathbb{Z}/8\mathbb{Z})$-extension of $\mathbb{Q}(t)$ (and any $(\mathbb{Z}/8\mathbb{Z})$-extension of $\mathbb{Q}(t)$ containing $(1+t^4)^{1/2}$ must be regular).

According to Theorem 4 the extension $\mathbb{Q}\left((t^2+2)^{1/2},(2t^2+6)^{1/2}\right)/\,\mathbb{Q}(t)$ can be embedded in a Q_8-extension of $\mathbb{Q}(t)$ since

$$\begin{aligned} t^2+2 &= t^2+1^2+(-1)^2,\\ 2t^2+6 &= 2^2+(1-t)^2+(1+t)^2. \end{aligned}$$

Such a Q_8-extension of $\mathbb{Q}(t)$ is obviously regular.

According to Theorem 6 the extension

$$\mathbb{Q}\left((t^2-2)^{1/2},(t^2-3)^{1/2},\left(2\left((t^2-2)+(t^2-2)^{1/2}\right)\right)^{1/2}\right)/\,\mathbb{Q}(t)$$

can be embedded in a D_8-extension of $\mathbb{Q}(t)$ and such a D_8-extension of $\mathbb{Q}(t)$ is obviously regular.

According to Theorem 7 the extension

$$\mathbb{Q}\left((t^2+2)^{1/2},(t^2+1)^{1/2},\left(2\left((t^2+2)+(t^2+2)^{1/2}\right)\right)^{1/2}\right)/\,\mathbb{Q}(t)$$

can be embedded in a QD_8-extension of $\mathbb{Q}(t)$ and such an extension is regular.

According to Theorem 8 the extension $\mathbb{Q}(\sqrt{a},\sqrt{b},\sqrt{2\theta})/\,\mathbb{Q}(t)$ where

$$\begin{aligned} a &= 4t^4+8t^2+2 = (2t^2+2)^2-2,\\ b &= a-1 = 4t^4+8t^2+1 = (2t^2+1)^2+(2t)^2 \text{ and}\\ \theta &= a+\sqrt{a} \end{aligned}$$

can be embedded in a Q_{16}-extension of $\mathbb{Q}(t)$ and such an extension is regular.

Using different methods, Lamprecht has given some constructions of cyclic, regular extensions of $\mathbb{Q}(t)$ in [**4**].

REFERENCES

1. P. Damey, J. Martinet, *Plongement d'une extension quadratique dans une extension quaternionienne*, J. reine angew. Math. **262/263** (1974) 323–338.

2. C. U. Jensen, N. Yui, *Quaternion Extensions*, Algebraic Geormetry and Commutative Algebra in Honour of Masayoshi **NAGATA**, Kinokuniya, Tokyo (1987) 155–182.

3. R. Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique differénte de p*, J. Algebra **109** (1987) 508–535.

4. E. Lamprecht, *Zur Charakterisierung zyklischer Erweiterungen rationaler Funktionenkörper, II*, Arch. Math. (Basel) **13** (1962) 488–497.

5. E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. reine angew. Math. **174** (1936) 237–245.

Inst. for Experimental Math.
Ellernstraße 29
4300 Essen
Germany

https://doi.org/10.4153/CJM-1990-043-6 Published online by Cambridge University Press