BULL. AUSTRAL. MATH. SOC. 12F10
VOL. 55 (1997) [99–112]

CHARACTERISATIONS OF GALOIS EXTENSIONS OF PRIME CUBED DEGREE

JAMES E. CARTER

Let p be a prime number and let k be a field of characteristic not equal to p. Assuming k contains the appropriate roots of unity, we characterise the non-cyclic Galois extensions of k of degree p^3. Concrete examples of such extensions are given for each possible case which can occur, up to isomorphism.

1. INTRODUCTION

Let p be a prime number. In the course of investigating a problem of algebraic number theory in [1], the author encountered a need for a characterisation of Galois extensions of degree p^3. Assuming certain conditions on the ground field k, he found that these extensions could be described in a straightforward manner utilising methods of a constructive nature which readily yield concrete examples not currently found, to the author's knowledge, in the research literature or in textbooks treating the subject. More specifically, let k be a field of characteristic not equal to p. Furthermore, assume k contains the multiplicative group μ_p of p-th roots of unity. Let G be a finite group and suppose L/k is a Galois extension with Galois group $\mathrm{Gal}(L/k)$ isomorphic to G. In the first part of our presentation we shall characterise the extensions L/k in case G is non-cyclic of order p^3 and G is not the quaternion group (Theorems 4 and 6). The quaternion extensions of k will then be characterised in the second part where we make the additional assumption that k contains μ_4. (Theorems 9 and 10.)

The field extensions described above have been examined elsewhere within the context of the "embedding problem." We do not explicitly touch upon this aspect of the study of these extensions here, but refer the interested reader to [3] .

2. GROUPS OF ORDER p^3

We begin by gathering together some facts about groups of order p^3 which we shall need. Let G be such a group. Then G is either a cyclic group, or the quaternion group, or

$$G = \langle \eta, \tau, \xi \mid \eta^p = \tau^p = 1,\ \xi^p = \eta^\ell,\ [\eta, \tau] = 1 = [\eta, \xi],\ [\tau, \xi] = \eta^s \rangle \tag{1}$$

Received 21st February, 1996
Part of this work appears in the author's Ph.D. thesis. He would like to thank Professor Leon R. McCulloh for his suggestions, and for pointing out Example 4.

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

where s, $\ell \in \{0,1,\dots,p-1\}$. If $s=0$ then G is one of two (up to isomorphism) Abelian groups of order p^3:

(i) $G \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ if $\ell = 0$;
(ii) $G \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$ if $\ell \neq 0$.

If $s \neq 0$ and p is odd then G is one of two (up to isomorphism) nonabelian groups of order p^3. The first, which we shall refer to as type 1, is a split extension of a cyclic group of order p by an elementary Abelian group of type (p,p). The second, referred to as type 2, is a split extension of a cyclic group of order p by a cyclic group of order p^2. We have

(iii) G is of type 1 if $\ell = 0$;
(iv) G is of type 2 if $\ell \neq 0$.

If $s \neq 0$ and $p = 2$ then G is the dihedral group D_4 for either value of $\ell \in \{0,1,\dots,p-1\}$.

In any case of (1), $A = \langle \eta, \tau \rangle$ is a normal subgroup of G and we have an exact sequence of groups

$$1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1. \tag{2}$$

In the nonabelian cases $Z(G) = \langle \eta \rangle$, where $Z(G)$ is the centre of G, and we have the exact sequence

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow H \longrightarrow 1. \tag{3}$$

One easily verifies that H is elementary Abelian of type (p,p).

3. Structure of extensions of degree p^3

In this section and the next we shall consider Galois extensions L/k with $\mathrm{Gal}(L/k) \simeq G$ where G is given by (1). For any field F, $F^\times$ will denote its multiplicative group of nonzero elements, and F^m the multiplicative group of m-th powers of elements of $F^\times$ where m is a positive integer. If S is a subgroup of G we write L^S for the subfield of L fixed by S. We now proceed to describe generators for L/k and the action of η, τ, ξ on these generators. Let $K = L^{\langle\eta\rangle}$, $M = L^{\langle\tau\rangle}$, $E = L^{\langle\eta,\tau\rangle}$, and $F = L^{\langle\eta,\xi\rangle}$. By Galois theory and (1), (2), and (3), L/E and K/k are elementary Abelian extensions of type (p,p). Let $\rho = \xi \mid E$ and $\sigma = \tau \mid F$ be the restrictions of ξ and τ to E and F, respectively. By Galois theory, it follows that $\mathrm{Gal}(E/k) = \langle\rho\rangle$ and $G(F/k) = \langle\sigma\rangle$. By Kummer theory, $E = k(\alpha)$ and $F = k(\beta)$ where $\alpha^p = a$ and $\beta^p = b$ for some elements a and b in $k^\times$ such that $\langle ak^p\rangle$ and $\langle bk^p\rangle$ are distinct cyclic subgroups of $k^\times/k^p$ of order p. Moreover, writing ζ for a primitive p-th root of unity, we may assume α

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

and β chosen so that $\rho(\alpha) = \zeta\alpha$ and $\sigma(\beta) = \zeta\beta$. Consider $\eta \in \mathrm{Gal}(L/k)$. Since $\langle\eta\rangle$ fixes E, $\eta \mid M$ is an E-automorphism of M. Therefore $\eta \mid M \in \mathrm{Gal}(M/E)$. Since $M \not\subseteq K = L^{\langle\eta\rangle}$, $\eta \mid M \neq id_M$. Hence $\mathrm{Gal}(M/E) = \langle\eta \mid M\rangle$. By Kummer theory, $M = E(\gamma)$ where $\gamma^p = c$ for some element c in $E^\times$, and $\langle cE^p\rangle$ and $\langle bE^p\rangle$ are distinct cyclic subgroups of $E^\times/E^p$ of order p. Furthermore, we may assume γ chosen so that $\eta(\gamma) = \zeta\gamma$.

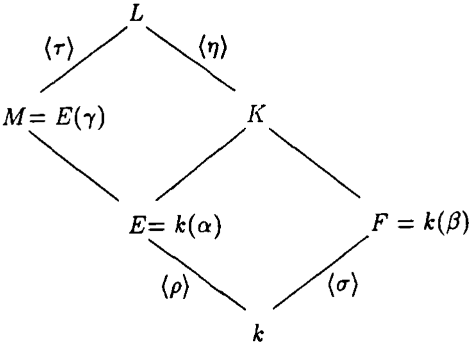

Figure 1

Since $L = k(\alpha, \beta, \gamma)$, any element of $\mathrm{Gal}(L/k)$ is completely determined by its action on the elements α, β, and γ. Thus far we have η fixes α and β and $\eta(\gamma) = \zeta\gamma$, τ fixes α and γ and $\tau(\beta) = \zeta\beta$, and ξ fixes β and $\xi(\alpha) = \zeta\alpha$. It remains to determine $\xi(\gamma)$. If $e \in E$ let $N_{E/k}(e)$ denote the norm of e from E to k.

PROPOSITION 1. *$\xi(\gamma) = \beta^s\gamma e$ for some $e \in E^\times$. Consequently, $b^s = \zeta^\ell/N_{E/k}(e)$.*

PROOF: We show that $\xi(\gamma)/\beta^s\gamma \in E^\times$. From (1) we have $[\tau, \xi] = \eta^s$. Therefore $\tau\xi = \eta^s\xi\tau$. Hence,

$$\tau\left(\frac{\xi(\gamma)}{\beta^s\gamma}\right) = \frac{(\tau\xi)(\gamma)}{\zeta^s\beta^s\gamma} = \frac{(\xi\tau\eta^s)(\gamma)}{\zeta^s\beta^s\gamma} = \frac{(\xi\tau)(\zeta^s\gamma)}{\zeta^s\beta^s\gamma} = \frac{\zeta^s\xi(\gamma)}{\zeta^s\beta^s\gamma} = \frac{\xi(\gamma)}{\beta^s\gamma}.$$

Also,

$$\eta\left(\frac{\xi(\gamma)}{\beta^s\gamma}\right) = \frac{(\eta\xi)(\gamma)}{\beta^s\zeta\gamma} = \frac{\xi(\eta(\gamma))}{\beta^s\zeta\gamma} = \frac{\zeta\xi(\gamma)}{\beta^s\zeta\gamma} = \frac{\xi(\gamma)}{\beta^s\gamma}.$$

Therefore $\xi(\gamma)/\beta^s\gamma \in L^{\langle\eta,\tau\rangle} = E$. It follows that $\xi(\gamma) = \beta^s\gamma e$ for some $e \in E^\times$. By successively applying ξ to both sides of the equation $\xi(\gamma) = \beta^s\gamma e$ we obtain $\xi^p(\gamma) = N_{E/k}(e)b^s\gamma$. On the other hand, $\xi^p = \eta^\ell$ which implies $\xi^p(\gamma) = \eta^\ell(\gamma) = \zeta^\ell\gamma$. Therefore $\zeta^\ell\gamma = N_{E/k}(e)b^s\gamma$ which gives $\zeta^\ell = N_{E/k}(e)b^s$. Hence $b^s = \zeta^\ell/N_{E/k}(e)$. □

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

We display the action of τ, η, and ξ on α, β and γ in the following table:

	α	β	γ
τ	α	$\zeta\beta$	γ
η	α	β	$\zeta\gamma$
ξ	$\zeta\alpha$	β	$\beta^s\gamma e$

Table 1

Corollary 2. *With the notation as in the proposition, if L/k is Abelian and $\ell \neq 0$ then $\mu_p \subseteq N_{E/k}(E^\times)$. If L/k is nonabelian then $b \in \mu_p N_{E/k}(E^\times)$.*

Proof: L/k is Abelian if and only if $s = 0$. Since $b^s = \zeta^\ell / N_{E/k}(e)$ for some $e \in E^\times$ it follows that $\zeta^\ell = N_{E/k}(e)$ when L/k is Abelian. If $\ell \neq 0$ then $\mu_p = \langle \zeta^\ell \rangle \subseteq N_{E/k}(E^\times)$. Now suppose L/k is nonabelian. Then $s \neq 0$ and $b^s \in \mu_p N_{E/k}(E^\times)$. Since $(s, p) = 1$ and $b^p \in k^p \subseteq N_{E/k}(E^\times)$ we have $b \in \mu_p N_{E/k}(E^\times)$. □

Now let $\mathbb{Z}[\langle\rho\rangle]$ be the group ring. Define the elements N and θ in $\mathbb{Z}[\langle\rho\rangle]$ by $N = \sum_{i=0}^{p-1} \rho^i$ and $\theta = \sum_{i=0}^{p-1} i\rho^i$.

Lemma 3. $\rho\theta = \theta - N + p$.

Proof:

$$\begin{aligned}(1-\rho)\theta &= \sum_{i=0}^{p-1} i\rho^i - \sum_{i=0}^{p-1} i\rho^{i+1}\\ &= \sum_{i=1}^{p-1} i\rho^i - \sum_{i=1}^{p} (i-1)\rho^i\\ &= \sum_{i=1}^{p-1} i\rho^i - \sum_{i=1}^{p} i\rho^i + \sum_{i=1}^{p} \rho^i\\ &= -p + \sum_{i=1}^{p} \rho^i\\ &= N - p.\end{aligned}$$

Therefore $\rho\theta = \theta - N + p$. □

If $\sum_{i=0}^{p-1} n_i\rho^i \in \mathbb{Z}[\langle\rho\rangle]$ and $\gamma \in E$ we write $\gamma^{\sum_{i=0}^{p-1} n_i\rho^i}$ for the product $\prod_{i=0}^{p-1} \rho^i(\gamma)^{n_i}$. Recall that $b^s = \zeta^\ell / N_{E/k}(e)$. In terms of the notation just introduced we have $b^s = \zeta^\ell e^{-N}$, and $\rho(\alpha^\ell e^\theta) = \zeta^\ell \alpha^\ell e^{\rho\theta}$. By Lemma 3 this last expression is equal to $\zeta^\ell \alpha^\ell e^\theta e^{-N} e^p = \zeta^\ell e^{-N}(\alpha^\ell e^\theta) e^p = b^s(\alpha^\ell e^\theta)e^p$. Since $\xi(\gamma) = \beta^s\gamma e$ we also have $\rho(c) = b^s c e^p$. Therefore $\rho(c/\alpha^\ell e^\theta) = c/\alpha^\ell e^\theta$. It follows that $c/\alpha^\ell e^\theta \in k^\times$, that is, $c = \kappa\alpha^\ell e^\theta$ where $\kappa \in k^\times$.

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

The results of this section are summarised in the following

Theorem 4. *Let p be any prime and let*

$$G = \langle \eta, \tau, \xi \mid \eta^p = \tau^p = 1,\ \xi^p = \eta^\ell,\ [\eta,\tau] = 1 = [\eta,\xi],\ [\tau,\xi] = \eta^s \rangle$$

where s, $\ell \in \{0, 1, \dots, p-1\}$, and assume k is a field of characteristic not equal to p, containing μ_p. Suppose L/k is a Galois extension of degree p^3 with $\mathrm{Gal}(L/k) = G$. If $K = L^{\langle\eta\rangle}$, $M = L^{\langle\tau\rangle}$, $E = L^{\langle\eta,\tau\rangle}$, and $F = L^{\langle\eta,\xi\rangle}$, then we have the following diagram of subfields of L

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & & \\
M = L^{\langle\tau\rangle} \arrow[dr, dash] & & K = L^{\langle\eta\rangle} \arrow[dl, dash] \arrow[dr, dash] & \\
 & E = L^{\langle\eta,\tau\rangle} \arrow[dr, dash] & & F = L^{\langle\eta,\xi\rangle} \arrow[dl, dash] \\
 & & k &
\end{tikzcd}$$

where $L = MK$, $K = EF$, and there exist elements α, β, $\gamma \in L$ such that $E = k(\alpha)$, $F = k(\beta)$, and $M = E(\gamma)$, and such that $\xi(\alpha) = \zeta\alpha$, $\tau(\beta) = \zeta\beta$, and $\eta(\gamma) = \zeta\gamma$. Then $\alpha^p = a$, $\beta^p = b$, and $\gamma^p = c$ where a, $b \in k^\times$ and $c \in E^\times$.

Furthermore,

(i) *$\langle ak^p \rangle$ and $\langle bk^p \rangle$ are distinct cyclic subgroups of $k^\times/k^p$ of order p;*

(ii) *$\langle bE^p \rangle$ and $\langle cE^p \rangle$ are distinct cyclic subgroups of $E^\times/E^p$ of order p.*

Moreover, if $\rho = \xi \mid E$ then $\mathrm{Gal}(E/k) = \langle\rho\rangle$ and we define N, $\theta \in \mathbb{Z}[\langle\rho\rangle]$ by $N = \sum_{i=0}^{p-1} \rho^i$ and $\theta = \sum_{i=0}^{p-1} i\rho^i$. Finally, there are elements $\kappa \in k^\times$ and $e \in E^\times$ such that $b^s = \zeta^\ell e^{-N}$ and $c = \kappa\alpha^\ell e^\theta$, and such that η, τ, and ξ act as k-automorphisms of L according to the following table.

	α	β	γ
τ	α	$\zeta\beta$	γ
η	α	β	$\zeta\gamma$
ξ	$\zeta\alpha$	β	$\beta^s\gamma e$

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

4. Construction of extensions of degree p^3

In view of the previous two sections we now consider the problem of constructing Galois extensions L/k with $\mathrm{Gal}(L/k) = G$ where G is given by (1) and k is a field of characteristic not equal to p, containing μ_p. If F is any field with $B \subseteq F^\times$, and n is a positive rational integer, write $B^{1/n}$ for the set of n-th roots of elements of B. We shall need the following:

Lemma 5. *Suppose $k \subseteq E \subseteq L$ are arbitrary fields and assume $\mu_n \subseteq E$. If E/k is a Galois extension with Galois group $\mathrm{Gal}(E/k)$ and L/E is a Kummer extension, say $L = E(B^{1/n})$ where $E^\times \supseteq B \supseteq E^n$, then L/k is normal if and only if $\rho(B) = B$ for every $\rho \in \mathrm{Gal}(E/k)$.*

Proof: Suppose L/k is normal. Let $\rho \in \mathrm{Gal}(E/k)$ and choose $\sigma \in \mathrm{Gal}(L/k)$ such that $\sigma \mid E = \rho$. Since $L = E(B^{1/n})$ we have $L = \sigma(L) = \sigma(E(B^{1/n})) = E\left(\rho(B)^{1/n}\right)$. By Kummer theory it follows that $\rho(B) = B$. Conversely, suppose $\rho(B) = B$ for every $\rho \in \mathrm{Gal}(E/k)$. Let σ be a k–embedding of L into an algebraic closure of k. Then $\sigma \mid E = \rho$ for some $\rho \in \mathrm{Gal}(E/k)$. Since $\rho(B) = B$ and $L = E(B^{1/n})$ we have $\sigma(L) = \sigma(E(B^{1/n})) = E\left(\rho(B)^{1/n}\right) = E(B^{1/n}) = L$. Therefore σ is a k–automorphism of L. Hence, L/k is normal. □

For the remainder of this section we assume k is a field of characteristic not equal to p, containing μ_p. Let $a \in k^\times$ such that $\langle ak^p \rangle$ is a cyclic subgroup of $k^\times/k^p$ of order p. Let $E = k(\alpha)$ where $\alpha^p = a$. Then E/k is a Galois extension of degree p and $\mathrm{Gal}(E/k) = \langle \rho \rangle$ where $\rho(\alpha) = \zeta\alpha$. Define the elements N and θ of the group ring $\mathbb{Z}[\langle \rho \rangle]$ by $N = \sum_{i=0}^{p-1} \rho^i$ and $\theta = \sum_{i=0}^{p-1} i\rho^i$. Let s, $\ell \in \{0, 1, \ldots, p-1\}$. Suppose there exists $\kappa \in k^\times$ and $e \in E^\times$ such that $\zeta^\ell e^{-N} = b^s$ for some $b \in k^\times$ of order p (mod k^p), and $c = \kappa\alpha^\ell e^\theta$ has order p (mod E^p). Furthermore, assume $\langle bk^p \rangle \neq \langle ak^p \rangle$ and $\langle bE^p \rangle \neq \langle cE^p \rangle$. Let $F = k(\beta)$ where $\beta^p = b$. Then F/k is a Galois extension of degree p and $\mathrm{Gal}(F/k) = \langle \sigma \rangle$ where $\sigma(\beta) = \zeta\beta$. Moreover, $K = EF$ is a Galois extension of k with $\mathrm{Gal}(K/k) \simeq \langle \rho \rangle \times \langle \sigma \rangle$.

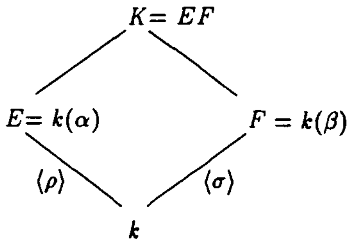

Figure 2

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

Now let $M = E(\gamma)$ where $\gamma^p = c$. Then M is a cyclic extension of E of degree p. Finally, let $L = MK = E(B^{1/p})$ where $B = \langle b, c\rangle E^p$. Then L is an elementary Abelian extension of E of degree p^2 and we have the following diagram of subfields of L.

$$\begin{tikzcd}
 & L = MK \arrow[dl, dash] \arrow[dr, dash] & & \\
M = E(\gamma) \arrow[dr, dash] & & K = EF \arrow[dl, dash] \arrow[dr, dash] & \\
 & E = k(\alpha) \arrow[dr, dash, "\langle\rho\rangle"'] & & F = k(\beta) \arrow[dl, dash, "\langle\sigma\rangle"] \\
 & & k &
\end{tikzcd}$$

Figure 3

Theorem 6. *Let L/k be the extension shown in Figure 3. Then L/k is Galois with* $\operatorname{Gal}(L/k) \simeq G$ *where G is given by (1). Moreover, by replacing e with $\zeta^u e$ for some integer u, we may assume the action of G on L is given by*

	α	β	γ
τ	α	$\zeta\beta$	γ
η	α	β	$\zeta\gamma$
ξ	$\zeta\alpha$	β	$\beta^s\gamma e$

Proof: By Lemma 3, $\rho\theta = \theta - N + p$. Therefore $\rho(c) = \rho(\kappa\alpha^\ell e^\theta) = \kappa\zeta^\ell\alpha^\ell e^{\rho\theta} = \kappa\zeta^\ell\alpha^\ell e^{\theta-N+p} = \zeta^\ell e^{-N}\kappa\alpha^\ell e^\theta e^p = b^s c e^p$. It follows that for every positive integer i $\rho^i(c) \equiv c \pmod{\langle b\rangle E^p}$. Hence, $B = \langle b, c\rangle E^p = \langle b, \rho^i(c)\rangle E^p = \rho^i(B)$ for every positive integer i. This implies that L/k is normal, by Lemma 5. Thus, L/k is Galois since L/k is separable.

We now determine the Galois group $\operatorname{Gal}(L/k)$. Let $\operatorname{Gal}(L/M) = \langle\tau\rangle$ and $\operatorname{Gal}(L/K) = \langle\eta\rangle$ where τ and η are defined by $\tau(\beta) = \zeta\beta$ and $\eta(\gamma) = \zeta\gamma$. Since the sequence

$$1 \to \operatorname{Gal}(L/K) \to \operatorname{Gal}(L/F) \to \operatorname{Gal}(E/k) \to 1$$

is exact, there exists $\xi \in \operatorname{Gal}(L/F)$ such that $\xi \mid E = \rho$. Hence $\xi(\beta) = \beta$ and $\xi(\gamma)^p = \xi(c) = \rho(c) = b^s c e^p$. From $\xi(\gamma)^p = b^s c e^p$ we have $\xi(\gamma) = \zeta^u\beta^s\gamma e$ for some $u \in \{0, 1, \dots, p-1\}$. Suppose $u \neq 0$. Since $(\zeta^u e)^{-N} = e^{-N}$, $(\zeta^u e)^\theta = e^\theta$, and $(\zeta^u e)^p = e^p$ we may replace e with $\zeta^u e$ without affecting any of the arguments of this

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

section, and the above relation becomes $\xi(\gamma) = \beta^s\gamma e$. We display the actions of τ, η, and ξ in the following table.

	α	β	γ
τ	α	$\zeta\beta$	γ
η	α	β	$\zeta\gamma$
ξ	$\zeta\alpha$	β	$\beta^s\gamma e$

Table 2

It remains to show that η, τ, and ξ satisfy the relations of (1). Clearly $\eta^p = \tau^p = 1$ and $[\eta, \tau] = 1$. To show that $\xi^p = \eta^\ell$ it suffices to show $\xi^p(\gamma) = \eta^\ell(\gamma)$ since ξ^p and η^ℓ both fix α and β. By successively applying ξ to both sides of the equation $\xi(\gamma) = \beta^s\gamma e$ one obtains $\xi^p(\gamma) = e^N b^s \gamma$. Since $b^s = \zeta^\ell e^{-N}$ it follows that $\xi^p(\gamma) = \zeta^\ell\gamma = \eta^\ell(\gamma)$. Therefore $\xi^p = \eta^\ell$. We now show $[\eta, \xi] = 1$. Clearly, $\eta\xi$ and $\xi\eta$ agree on α and β. Since also $(\eta\xi)(\gamma) = \eta(\beta^s\gamma e) = \zeta\beta^s\gamma e$ and $(\xi\eta)(\gamma) = \xi(\zeta\gamma) = \zeta\beta^s\gamma e$ it follows that $[\eta, \xi] = 1$. Finally, we show $[\tau, \xi] = \eta^s$. This last equation is equivalent to $\tau\xi = \eta^s\xi\tau$. We have $(\tau\xi)(\alpha) = \zeta\alpha = (\eta^s\xi\tau)(\alpha)$ and $(\tau\xi)(\beta) = \zeta\beta = (\eta^s\xi\tau)(\beta)$. Also, $(\tau\xi)(\gamma) = \tau(\beta^s\gamma e) = \zeta^s\beta^s\gamma e$ and $(\eta^s\xi\tau)(\gamma) = (\eta^s\xi)(\gamma) = \eta^s(\beta^s\gamma e) = \zeta^s\beta^s\gamma e$. Therefore $[\tau, \xi] = \eta^s$. $\square$

REMARK. Let p be any prime. Theorem 4 together with Theorem 6 provide a complete characterisation of noncyclic extensions L/k of degree p^3 of fields k of characteristic not equal to p, containing μ_p, provided such extensions of k exist and L/k is not a quaternion extension.

In the examples which follow immediately, the notation will be as in the statement of Theorem 6. Furthermore, let $\mathbb{Q}$ be the field of rational numbers, and let $i = \sqrt{-1}$. Let ζ_m denote a primitive m-th root of unity. For each example it is not difficult to check that the condition $\zeta^\ell e^{-N} = b^s$ holds. The remaining conditions required by Theorem 6 are easily shown to be satisfied by arguing as follows: (1) Assume the condition does not hold. (2) Write an equation based on the assumption in 1. (3) Derive a contradiction from the equation obtained in 2. In about half the cases, step 3 will begin by taking the obvious norm of both sides of the equation (but see the remark preceding Example 5). Standard facts about cyclotomic fields (see [**2**, Chapter IV] for instance) may also prove helpful in verifying some of the conditions of Examples 4 and 5. In particular, one may find the following facts useful: $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}$, and $p = \prod_{i=1}^{p-1} (1 - \zeta^i)$.

EXAMPLE 1. Let $k = \mathbb{Q}$, $p = 2$, $s = 0$, $\ell = 0$, $a = 3$, $b = 5$, $\kappa = 1$, and $e = 1/(2 + \sqrt{3})$. Then $c = 1/(2 - \sqrt{3})$ and L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

EXAMPLE 2. Let $k = \mathbb{Q}(i)$, $p = 2$, $s = 0$, $\ell = 1$, $a = 2$, $b = 3$, $\kappa = 1$, and $e = i/(3+2\sqrt{2})$. Then $c = i\sqrt{2}/(3-2\sqrt{2})$ and L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

EXAMPLE 3. Let $k = \mathbb{Q}$, $p = 2$, $s = 1$, $\ell = 1$, $a = 2$, $b = -7$, $\kappa = 1$, and $e = 1/(3+\sqrt{2})$. Then $c = \sqrt{2}/(3-\sqrt{2})$ and L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq D_4$.

EXAMPLE 4. Let p be an odd prime. Let $k = \mathbb{Q}(\zeta)$, and let s and ℓ be nonzero. Let $a = p$, and $b = \zeta^{\ell r}$ where r is an integer such that $rs \equiv 1 \pmod{p}$. Let $\kappa = 1$, and $e = 1$. Then $c = \alpha^{\ell}$, where $\alpha^p = p$, and L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq G$, where G is nonabelian of order p^3 of type 2.

REMARK. In the following example, the conditions required by Theorem 6 are verified as outlined in the paragraph preceding Example 1, with the exception of those conditions involving the element c. For these two conditions, carry out steps 1 and 2 as in the previous examples. In step 3, however, apply ρ to both sides of the equation instead of taking norms, and then apply Lemma 3. Now derive a contradiction as before.

EXAMPLE 5. Let p be an odd prime. Let $k = \mathbb{Q}(\zeta)$, and let $s = 1$, $\ell = 0$. Let $a = \zeta$, and $b = 1 - \zeta$. Let $\kappa = 1$, and $e = 1/(1-\zeta_{p^2})$. Then $c = e^{\theta}$, and L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq G$, where G is nonabelian of order p^3 of type 1.

In the remaining sections we shall obtain a characterisation of quaternion extensions of fields L/k where we assume the characteristic of k is not 2, and $\mu_4 \subseteq k$. The development parallels closely that of the previous sections in broad outline, but with essential differences in some of the details.

5. THE QUATERNION GROUP

In terms of generators and relations the quaternion group is given by

$$H_8 = \langle \xi, \tau \mid \xi^4 = 1,\ \xi^2 = \tau^2,\ \tau\xi = \xi^3\tau \rangle. \tag{4}$$

Every subgroup of H_8 is normal. In particular, $Z(H_8) = \langle \xi^2 \rangle$ is the centre of H_8 where $\xi^2 = \tau^2$ is the unique element of order 2 and we have an exact sequence

$$1 \longrightarrow Z(H_8) \longrightarrow H_8 \longrightarrow Q \longrightarrow 1. \tag{5}$$

One easily verifies that Q must be elementary Abelian of type $(2,2)$.

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

6. Structure of quaternion extensions

Suppose k is a field of characteristic not equal to 2, containing μ_4. Let L/k be a normal extension with $\mathrm{Gal}(L/k) \simeq H_8$ where H_8 is given by (4). If S is a subgroup of H_8 we write L^S for the subfield of L fixed by S. We now proceed to describe generators for L/k and the action of ξ and τ on these generators. Let $E = L^{\langle\tau\rangle}$, $F = L^{\langle\xi\rangle}$, and $K = L^{\langle\xi^2\rangle}$. By Galois theory and (5), we have the following diagram of subfields of L where L/K is a quadratic extension and K/k is an elementary Abelian extension of type $(2,2)$.

$$\begin{tikzcd}
 & L \arrow[d, no head] & \\
 & K = L^{\langle\xi^2\rangle} \arrow[dl, no head] \arrow[dr, no head] & \\
E = L^{\langle\tau\rangle} \arrow[dr, no head] & & F = L^{\langle\xi\rangle} \arrow[dl, no head] \\
 & k &
\end{tikzcd}$$

Figure 4

Let $\rho = \xi \mid E$ and $\sigma = \tau \mid F$ be the restrictions of ξ and τ to E and F respectively. By Galois theory it follows that $\mathrm{Gal}(E/k) = \langle\rho\rangle$ and $\mathrm{Gal}(F/k) = \langle\sigma\rangle$. By Kummer theory $E = k(\alpha)$ and $F = K(\beta)$ where $\alpha^2 = a$ and $\beta^2 = b$ are elements of $k^\times$ and $\langle ak^2\rangle$ and $\langle bk^2\rangle$ are distinct cyclic subgroups of $k^\times/k^2$ of order 2. Moreover, $\rho(\alpha) = -\alpha$ and $\sigma(\beta) = -\beta$. Since $\mu_4 \subseteq E$ and L/E is cyclic of degree 4 we have $L = E(\gamma)$ where γ satisfies $f(x) = x^4 - u$ for some $u \in E^\times$. The roots of f are the elements of the set $\{\pm\gamma, \pm i\gamma\}$ where $i^2 = -1$. Since τ is an E–automorphism of L we have $\tau(\gamma) \in \{\pm\gamma, \pm i\gamma\}$. If $\tau(\gamma) = \pm\gamma$ then τ^2 fixes $L = k(\alpha,\gamma)$ which contradicts the fact that τ has order 4. Therefore, we must have $\tau(\gamma) = \pm i\gamma$. If $\tau(\gamma) = -i\gamma$ then $\tau^3(\gamma) = i\gamma$. Also, $\tau^3(\alpha) = \alpha$ and $\tau^3(\beta) = -\beta$. Thus, since $\langle\tau\rangle = \langle\tau^3\rangle$ we may assume $\tau(\gamma) = i\gamma$. Let $c = \gamma^2$. Since $\tau^2(c) = \tau^2(\gamma^2) = \tau^2(\gamma)^2 = (-\gamma)^2 = \gamma^2 = c$ it follows that $c \in L^{\langle\tau^2\rangle} = K$. Thus far we have τ fixes α, $\tau(\beta) = -\beta$, and $\tau(\gamma) = i\gamma$. Also, ξ fixes β and $\xi(\alpha) = -\alpha$. It remains to determine $\xi(\gamma)$.

Lemma 7. *$\xi(\gamma) = i\beta e\gamma$ for some $e \in E^\times$.*

Proof: We show that τ fixes $\xi(\gamma)/i\beta\gamma$. Since $\tau\xi = \xi^3\tau$ and $\xi^2 = \tau^2$ we have

$$\tau\left(\frac{\xi(\gamma)}{i\beta\gamma}\right) = \frac{(\tau\xi)(\gamma)}{-i\beta\tau(\gamma)} = \frac{(\xi^3\tau)(\gamma)}{\beta\gamma} = \frac{i\xi^3(\gamma)}{\beta\gamma} = \frac{i\xi\tau^2(\gamma)}{\beta\gamma} = \frac{-i\xi(\gamma)}{\beta\gamma} = \frac{\xi(\gamma)}{i\beta\gamma}.$$

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

Therefore $\xi(\gamma)/i\beta\gamma \in L^{\langle\tau\rangle} = E$. It follows that $\xi(\gamma) = i\beta e\gamma$ for some $e \in E^\times$. $\square$

The action of τ and ξ on α, β, and γ is displayed in the following table.

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

Table 3

Proposition 8. *If L/k is a normal extension such that $\mathrm{Gal}(L/k) = H_8$ where H_8 is given by (4), then L has subfields as shown in Figure 4 where $b = e^{-N}$ and $c = \kappa\alpha\beta e^\theta$ for some $\kappa \in k^\times$ and $e \in E^\times$ where N and θ are the elements of $\mathbb{Z}[\langle\rho\rangle]$ defined by $N = \sum_{i=0}^{1} \rho^i = 1 + \rho$ and $\theta = \sum_{i=0}^{1} i\rho^i = \rho$.*

Proof: It remains to prove the statements about b and c. We have $\xi(\gamma) = i\beta e\gamma$ by Lemma 7. Hence $-\gamma = \tau^2(\gamma) = \xi^2(\gamma) = -be^N\gamma$. Therefore, $b = e^{-N}$. We now determine c. Since $\xi(c) = \xi(\gamma)^2 = (i\beta e\gamma)^2 = -\beta^2e^2c$ and, by Lemma 3, $\xi(\alpha\beta e^\theta) = -\alpha\beta e^{\theta\rho} = -\alpha\beta e^\theta e^{-N}e^2 = -\alpha\beta e^\theta\beta^2e^2$, we have $\xi(c/\alpha\beta e^\theta) = -\beta^2e^2c/-\beta^2e^2\alpha\beta e^\theta = c/\alpha\beta e^\theta$ which implies $c/\alpha\beta e^\theta \in L^{\langle\xi\rangle} = F$. Also, since $\tau(c) = \tau(\gamma)^2 = -c$ we have $\tau(c/\alpha\beta e^\theta) = -c/-\alpha\beta e^\theta = c/\alpha\beta e^\theta$ which gives $c/\alpha\beta e^\theta \in L^{\langle\tau\rangle} = E$. Hence $c/\alpha\beta e^\theta \in E \cap F = k$. Therefore $c = \kappa\alpha\beta e^\theta$ for some $\kappa \in k^\times$. $\square$

The results of this section are summarised in the following theorem.

Theorem 9. *Let*

$$H_8 = \langle \xi, \tau \mid \xi^4 = 1,\ \xi^2 = \tau^2,\ \tau\xi = \xi^3\tau \rangle$$

and assume k is a field of characteristic not equal to 2, containing μ_4. Suppose L/k is a Galois extension of degree 8 with $\mathrm{Gal}(L/k) = H_8$. If $K = L^{\langle\xi^2\rangle}$, $E = L^{\langle\tau\rangle}$, and $F = L^{\langle\xi\rangle}$, then we have the following diagram of subfields of L

$$\begin{tikzcd}
& L \arrow[d, dash] & \\
& K = L^{\langle\xi^2\rangle} \arrow[dl, dash] \arrow[dr, dash] & \\
E = L^{\langle\tau\rangle} \arrow[dr, dash] & & F = L^{\langle\xi\rangle} \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

where $K = EF$, and there exist elements α, β, $\gamma \in L$ such that $E = k(\alpha)$, $F = k(\beta)$, and $L = K(\gamma)$, and such that $\xi(\alpha) = -\alpha$, $\tau(\beta) = -\beta$ and $\tau(\gamma) = i\gamma$. Then $\alpha^2 = a$, $\beta^2 = b$, and $\gamma^2 = c$ where a, $b \in k^\times$ and $c \in K^\times$. Furthermore,

(i) *$\langle ak^2 \rangle$ and $\langle bk^2 \rangle$ are distinct cyclic subgroups of $k^\times/k^2$ of order 2;*

(ii) *$\langle cK^2 \rangle$ is a cyclic subgroup of $K^\times/K^2$ of order 2.*

Moreover, if $\rho = \xi \mid E$ then $\mathrm{Gal}(E/k) = \langle \rho \rangle$ and we define N, $\theta \in \mathbb{Z}[\langle \rho \rangle]$ by $N = \sum_{i=0}^{1} \rho^i = 1 + \rho$ and $\theta = \sum_{i=0}^{1} i\rho^i = \rho$. Finally, there are elements $\kappa \in k^\times$ and $e \in E^\times$ such that $b = e^{-N}$ and $c = \kappa\alpha\beta e^\theta$, and such that τ and ξ act as k–automorphisms of L according to the following table.

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

7. Construction of quaternion extensions

Suppose k is a field of characteristic not equal to 2, containing μ_4. Let $a \in k^\times$ such that $\langle ak^2 \rangle$ is a subgroup of $k^\times/k^2$ of order 2. Let $E = k(\alpha)$ where $\alpha^2 = a$. Then E/k is a quadratic extension with $\mathrm{Gal}(E/k) = \langle \rho \rangle$, say. Let N, $\theta \in \mathbb{Z}[\langle \rho \rangle]$ be the elements defined in the statement of Proposition 8. Choose $e \in E^\times$ such that $b = e^{-N}$ has order 2 $\left(\mathrm{mod}\ k^2\right)$ and $\langle bk^2 \rangle \neq \langle ak^2 \rangle$. Let $F = k(\beta)$ where $\beta^2 = b$. Then F/k is a quadratic extension with $\mathrm{Gal}(F/k) = \langle \sigma \rangle$, say, and $K = EF$ is an elementary Abelian extension of k of type $(2,2)$. Finally, let $c = \kappa\alpha\beta e^\theta$ where $\kappa \in k^\times$ and assume $c \not\equiv 1$ $\left(\mathrm{mod}\ K^2\right)$. Suppose $\gamma^2 = c$. Then $L = K(\gamma)$ is a quadratic extension of K and we have the following diagram of subfields of L

$$\begin{tikzcd}
 & L = K(\gamma) \arrow[d, dash] & \\
 & K = EF \arrow[dl, dash] \arrow[dr, dash] & \\
E = k(\alpha) \arrow[dr, dash] & & F = k(\beta) \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

Figure 5

Theorem 10. *Let L/k be the extension shown in Figure 5. Then L/k is Galois with $\mathrm{Gal}(L/k) \simeq H_8$.*

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

PROOF: $\mathrm{Gal}(K/k) \simeq \mathrm{Gal}(E/k) \times \mathrm{Gal}(F/k) = \langle\rho\rangle \times \langle\sigma\rangle$. By identifying the elements of the group $\langle\rho\rangle \times \langle\sigma\rangle$ with their preimages under the above isomorphism, we may assume $\mathrm{Gal}(K/k) = \{1_K, \rho, \sigma, \rho\sigma\}$. By Lemma 5, L/k is normal if and only if $\lambda(c) \equiv c \pmod{K^2}$ for every $\lambda \in \mathrm{Gal}(K/k)$. We have $\rho(c) = \rho(\kappa\alpha\beta e^{\theta}) = -\kappa\alpha\beta e^{\theta\rho}$. By Lemma 3 this last expression is equal to $-\kappa\alpha\beta e^{\theta-N+2} = -\kappa\alpha\beta e^{\theta} e^{-N} e^2 = i^2\kappa\alpha\beta e^{\theta}\beta^2 e^2 = ci^2\beta^2 e^2 \equiv c \pmod{K^2}$. Similarly, the condition is verified for the remaining elements of $\mathrm{Gal}(K/k)$. It follows that L/k is a normal extension. Hence, L/k is Galois since L/k is separable.

We shall now show that $\mathrm{Gal}(L/k) \simeq H_8$. Since $\mu_4 \subseteq E$ and $L = E(\gamma)$ where $\gamma^4 \in E$, $\mathrm{Gal}(L/E)$ is cyclic of order 4, say, $\mathrm{Gal}(L/E) = \langle\tau\rangle$. Therefore, $\tau(\alpha) = \alpha$ and we must have $\tau(\beta) = -\beta$, for otherwise $F \subseteq L^{\langle\tau\rangle} = E$ which is a contradiction. Also, by the argument preceding Lemma 7, $\tau(\gamma) = \pm i\gamma$ and we may assume $\tau(\gamma) = i\gamma$. Let $\xi \in \mathrm{Gal}(L/F)$ such that $\xi \mid E = \rho$. Then $\xi(\beta) = \beta$ and we must have $\xi(\alpha) = -\alpha$. Also, $\xi(\gamma)^2 = \xi(c) = \xi(\kappa\alpha\beta e^{\theta}) = -\kappa\alpha\beta e^{\theta\rho} = -\kappa\alpha\beta e^{\theta-N+2}$ (by Lemma 3) $= -\kappa\alpha\beta e^{\theta}\beta^2 e^2$. Therefore $\xi(\gamma) = \pm i\beta e\gamma$. Hence, $\xi^2(\gamma) = \xi(\pm i\beta e\gamma) = \pm i\beta\xi(e)\xi(\gamma) = \pm i\beta\xi(e)(\pm i\beta e\gamma) = -\beta^2 e^{\rho} e\gamma = -e^{-N}e^{N}\gamma = -\gamma = \tau^2(\gamma)$. Since $L = K(\gamma) = k(\alpha,\beta,\gamma)$ and ξ^2 and τ^2 agree on α and β it follows that $\xi^2 = \tau^2$. Therefore ξ has order four which implies $\mathrm{Gal}(L/F) = \langle\xi\rangle$. If $\xi(\gamma) = -i\beta e\gamma$ then $\xi^3(\gamma) = i\beta e\gamma$. Since also $\xi^3(\alpha) = -\alpha$, $\xi^3(\beta) = \beta$, and $\langle\xi\rangle = \langle\xi^3\rangle$, we may assume $\xi(\gamma) = i\beta e\gamma$. The action of τ and ξ on α, β, and γ is displayed in the following table

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

Table 4

We claim that $\mathrm{Gal}(L/k) = \langle \xi, \tau \mid \xi^4 = 1,\ \xi^2 = \tau^2,\ \tau\xi = \xi^3\tau\rangle$. It only remains to show that $\tau\xi = \xi^3\tau$. Clearly, $(\tau\xi)(\alpha) = (\xi^3\tau)(\alpha)$ and $(\tau\xi)(\beta) = (\xi^3\tau)(\beta)$. Also, $(\tau\xi)(\gamma) = \tau(i\beta e\gamma) = -i\beta e i\gamma = \beta e\gamma$ and $(\xi^3\tau)(\gamma) = \xi^3(i\gamma) = i\xi^2(i\beta e\gamma) = i\xi(i\beta e^{\rho} i\beta e\gamma) = -i\xi(\gamma) = -ii\beta e\gamma = \beta e\gamma$. □

REMARK. By Theorem 6 and Theorem 10 we see that if one begins with the elementary Abelian extension K/k of Figure 5, one obtains a normal extension L/k with $\mathrm{Gal}(L/k) \simeq D_4$ by adjoining to E a square root of the element κe^{θ}, for some $\kappa \in k^{\times}$, to obtain M. Then $L = MK$. If, instead, we adjoin to K a square root of the element $\kappa\alpha\beta e^{\theta}$, for some (possibly different) $\kappa \in k^{\times}$, to obtain L, then L/k is a normal extension with $\mathrm{Gal}(L/k) \simeq H_8$. Theorem 9 together with Theorem 10 provide a complete characterisation of quaternion extensions of fields k of characteristic not equal to 2, containing μ_4, provided such extensions of k exist.

In the following examples, the notation will be as in the statement of Theorem 10.

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press

As in the previous examples, the verification that the required conditions are satisfied is left to the reader. Once again, this is easily done as outlined in the paragraph preceding Example 1. The following facts may also be useful in verifying some of the conditions of Example 6: $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ whenever m and n are relatively prime (see [**2**, Chapter IV] for instance), and $2 = -i(1+i)^2$.

EXAMPLE 6. Let $k = \mathbb{Q}(i)$, $a = 2$, $\kappa = 1$, and $e = 1/\left(i+\sqrt{2}\right)$. Then $b = -3$, $c = \sqrt{2}\sqrt{-3}/\left(i-\sqrt{2}\right)$, and L/k is a Galois extension with $\mathrm{Gal}\left(L/k\right) \simeq H_8$.

EXAMPLE 7. In view of the remark following Theorem 10, let k be as in Example 6. In Theorem 6 let $p = 2$, $s = 1$, and $\ell = 0$. Define a, b, κ, and e as in Example 6, but let $c = 1/\left(i-\sqrt{2}\right)$. Then, by Theorem 6, L/k is a Galois extension with $\mathrm{Gal}\left(L/k\right) \simeq D_4$.

REFERENCES

[1] J.E. Carter, *Steinitz classes of tamely ramified nonabelian extensions of algebraic number fields of degree* p^3, Ph.D. Thesis (Dept. of Mathematics, University of Illinois at Urbana-Champaign, 1992).

[2] S. Lang, *Algebraic number theory* (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[3] R. Massy et T. Nguyen-Quang-Do, 'Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale', *J. Reine Angew. Math.* **291** (1977), 149–161.

Department of Mathematics
College of Charleston
Charleston SC 29424-0001
United States of America
e-mail: carter@math.cofc.edu

https://doi.org/10.1017/S0004972700030574 Published online by Cambridge University Press