CONSTRUCTING QUATERNIONIC FIELDS

by THERESA P. VAUGHAN

(Received 31 July, 1990)

Introduction. Let K be a field of characteristic different from 2, and a, b quadratically independent elements of K. Put $J = K(\sqrt{a}, \sqrt{b})$. In [4], Jensen and Yui discuss the question of quaternionic (Q_8) extensions of J, and give a survey of known results. In [8], Ware discusses (among other things) some general conditions for, and relations between, the existence of Q_8 and D_4 (dihedral) extensions of K. A general theorem of Witt [9] says that J will have a quaternionic extension $J(\sqrt{u})$ if and only if there exists a 3×3 matrix P over K such that $PP^t = \mathrm{diag}(a, b, 1/ab)$, and an appropriate value for u is given in terms of the entries of P. The problem of actually finding P in a particular case is not trivial.

Jensen and Yui give an explicit construction for a suitable P in case -1 is a sum of two squares in K, and in [3], Cohn gives a suitable P for the case when $J = Q(\sqrt{2}, \sqrt{q})$ with q a prime, $q \equiv 1$ or $3 \pmod 8$. There are other characterizations of the problem also. The conditions given by Reichardt [5] consist of the solvability of a set of three simultaneous quadratic equations; Bucht [2] gives conditions which amount to the solution of three simultaneous quartic equations.

The original motivation for this paper, was the construction of quaternionic fields over Q. To this end, we study in some detail the properties which the field J and the defining element u must have in order that $J(\sqrt{u})$ shall be a Q_8 extension of K. In Section 1, we give some preliminaries, and characterize non-cyclic normal (over K) extensions of the form $J(\sqrt{u})$, according to which, and how many of the products $u\sigma(u)$ are square in a quadratic subfield (where σ is a K-automorphism of J).

In Section 2, we define a Q_8 extension L of J to be of Type I if J also admits a dihedral (D_4) extension (and equivalently, a $Z_2 \times Z_4$ extension), and of Type II otherwise. We show that L is of Type I if and only if there exist certain elements x and y in two of the quadratic subfields of J, such that $J(\sqrt{u}) = J(\sqrt{xy})$. In order to construct a Type I extension, it suffices to construct the matching D_4 extension and $Z_2 \times Z_4$ extension.

In Section 3, we give a characterization of Q_8 extensions of $J = Q(\sqrt{n}, \sqrt{m})$ in terms of the norms of algebraic integers in the quadratic subfields of J. In Section 4, we construct several types of quaternionic extensions of Q, and also give a set of sufficient conditions for a Q_8 extension which yields a straightforward construction.

I would like to thank the referees for Corollary 2.6, for the reference [8], and for very helpful suggestions in general.

1. Notation and preliminaries. The notation established in this section will be used throughout this paper.

Let K be a field of characteristic different from 2, and let K^2 denote the set of squares in K. Suppose that K contains elements a_1 and a_2 such that none of a_1, a_2, a_1a_2 is a square in K. Put $a_3 = a_1a_2$. Then $J = K(\sqrt{a_1}, \sqrt{a_2})$ has three quadratic subfields, $K(\sqrt{a_i})$, $1 \le i \le 3$, and the Galois group $\mathrm{Gal}(J/K)$ is $Z_2 \times Z_2$. The three non-trivial K-

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

automorphisms are determined by

$$\sigma_i(\sqrt{a_i}) = \sqrt{a_i}, \qquad \sigma_j(\sqrt{a_i}) = -\sqrt{a_i} \quad \text{for} \quad i \neq j \quad (1 \leq i, j \leq 3).$$

Let $u \in J - J^2$, and $L = J(\sqrt{u})$. Then L is normal over K if and only if $u\sigma_i(u)$ is in J^2 for all $i = 1, 2, 3$, and then $\mathrm{Gal}(L/K)$ must be a non-cyclic group of order 8, that is, one of $Z_2 \times Z_2 \times Z_2$, $Z_4 \times Z_2$, D_4, or Q_8. In what follows, we assume that K has the properties described above, and $L = J(\sqrt{u})$ is normal over K. (In particular, K is not finite, and K has non-cyclic normal extensions of degree 8 over K.)

We will use without comment the well-known fact that if F is any field, and x and y are in F, then $F(\sqrt{x}) = F(\sqrt{y})$ if and only if $xy \in F^2$. Also, the following formal identities will be useful.

LEMMA 1.1. (a) *Suppose that* $x^2 - ny^2 = t^2$. *Then*

$$2(x - t)(x + y\sqrt{n}) = (x - t + y\sqrt{n})^2. \tag{ID1}$$

(b) *Suppose that* $x^2 - ny^2 = kt^2$. *Then*

$$\{\sqrt{x + y\sqrt{n}} + \sqrt{x - y\sqrt{n}}\}^2 = 2x + 2t\sqrt{k} \tag{ID2}$$

Proof. Verify.

COROLLARY 1.2. *If* $\alpha = x + y\sqrt{a} \in K(\sqrt{a})$, *and if* $N_K(\alpha) = x^2 - ay^2 = t^2$ *for some* $t \in K$, *then* $K(\sqrt{a}, \sqrt{\alpha}) = K(\sqrt{a}, \sqrt{b})$ *for some* $b \in K$.

Since $u\sigma_i(u) \in J^2$ $(i = 1, 2, 3)$, and also $u\sigma_i(u) \in K(\sqrt{a_i})$, then for each $i = 1, 2, 3$, one of the following statements must be true:

$$u\sigma_i(u) \in (K(\sqrt{a_i}))^2 \tag{*}$$

$$u\sigma_i(u) \in a_j(K(\sqrt{a_i}))^2 \quad \text{for} \quad i \neq j \quad (1 \leq j \leq 3). \tag{**}$$

The next result follows almost immediately from this observation.

LEMMA 1.3. *If* $L = J(\sqrt{u})$ *is normal over* K, *then there exist* $x_i = K(\sqrt{a_i})$ $(i = 1, 2, 3)$ *such that* $L = J(\sqrt{x_1 x_2 x_3})$.

Proof. Since for each $i = 1, 2, 3$ either (*) or (**) must be true, then $N_K(u)$ must be a square in K. Write $u\sigma_i(u) = m_i y_i^2$, where $m_i \in \{1, a_1, a_2, a_3\}$ and $y_i \in K(\sqrt{a_i})$, $(i = 1, 2, 3)$. Then we have $u^2 N_K(u) = m_1 m_2 m_3 (y_1 y_2 y_3)^2$. The quantity $m_1 m_2 m_3$ must be square in at least one of the fields $K(\sqrt{a_i})$; suppose for example that $m_1 m_2 m_3 = b^2$ for some $b \in K(\sqrt{a_1})$. Then $u = \pm(by_1)y_2 y_3$, and we can take $x_1 = \pm by_1$, $x_2 = y_2$, and $x_3 = y_3$.

We shall see that the truth-values of the statements (*) and (**) determine the field lattice of L over K. First we need a definition.

DEFINITION 1.4. Let $u \in J - J^2$, and assume the notation given above. The ordered triple $S(u) = (s_1, s_2, s_3)$ is defined by: $s_i = 0$ if $u\sigma_i(u) \in (K(\sqrt{a_i}))^2$, and $s_i = 1$ if $u\sigma_i(u) \in a_j(K(\sqrt{a_i}))^2$ for some $i \neq j$, $1 \leq j \leq 3$. If a fuller notation is needed, we will write $s_i = s_i(u)$.

THEOREM 1.5. *Assume all the notation given above. For each* i, $1 \leq i \leq 3$, $s_i = 0$ *if and only if there exists an element* $t \in K(\sqrt{a_i})$ *such that* $tu \in J^2$, *that is, if and only if* $J(\sqrt{u}) = J(\sqrt{t})$.

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

Proof. Fix i, $1 \le i \le 3$, and put $s_i = s$, $\sigma_i = \sigma$, and $a_i = a$. Choose $j \ne i$, and put $b = a_j$. Since $u \in J$, we can write $u = x + y\sqrt{b}$, where $x, y \in K(\sqrt{a})$. Suppose first that $s = 0$; then there is some $z \in K(\sqrt{a})$ such that

$$u\sigma(u) = x^2 - by^2 = z^2$$

and then, from the identity (ID1), we have

$$2(x - z)u = (x - z + y\sqrt{b})^2 \in J^2.$$

Then $J(\sqrt{u}) = J(\sqrt{2(x-z)})$, and $2(x - z) \in K(\sqrt{a})$.

On the other hand, suppose that for some $t \in K(\sqrt{a})$, we have $tu \in J^2$. Then $\sigma(t) = t$, $(tu)\sigma(tu) = t^2 u\sigma(u) \in (K(\sqrt{a})^2$, and so $u\sigma(u) \in (K(\sqrt{a})^2$. Then $s = 0$, and this completes the proof.

COROLLARY 1.6. *Assume the notation above, and fix* i, $1 \le i \le 3$. *Then the Galois group* $\mathrm{Gal}(L/K(\sqrt{a_i}))$ *is* $Z_2 \times Z_2$ *if and only if* $s_i = 0$.

Proof. Suppose first that $s_i = 0$. Then $L = J(\sqrt{t})$ for some $t \in K(\sqrt{a_i})$, such that $tu \in J^2$. Since $u \in J - J^2$, then also $t \in J - J^2$. Hence L must contain the quartic subfield $F = K(\sqrt{a_i}, \sqrt{t})$, and $F \ne J$. Then $\mathrm{Gal}(L/K(\sqrt{a_i}))$ cannot be Z_4, and must be $Z_2 \times Z_2$.

On the other hand, suppose that $\mathrm{Gal}(L/K(\sqrt{a_i}))$ is $Z_2 \times Z_2$. Then L contains a quartic subfield of the form $F = K(\sqrt{a_i}, \sqrt{t})$, with $t \in K(\sqrt{a_i})$, where $F \ne J$. Then for $j \ne i$, we have

$$K(\sqrt{a_i}, \sqrt{t}, \sqrt{a_j}) = L = K(\sqrt{a_i}, \sqrt{a_j}, \sqrt{u}),$$

and it follows that $tu \in J^2$. Then $s_i = 0$.

COROLLARY 1.7. *Using the notation above, the fields* L *for which* $\mathrm{Gal}(L/K)$ *is one of* $Z_2 \times Z_2 \times Z_2$, $Z_4 \times Z_2$, *or* D_4, *are classified and described as follows.*

(A) *The following are equivalent*:
- (a) $\mathrm{Gal}(L/K) = Z_2 \times Z_2 \times Z_2$
- (b) $S(u) = (0, 0, 0)$.
- (c) $L = J(\sqrt{b})$ *for some* $b \in K - J^2$.

(B) *The following are equivalent*:
- (a) $\mathrm{Gal}(L/K) = D_4$ *and* $\mathrm{Gal}(L/K(\sqrt{a_1}))$ *is cyclic*
- (b) $s_1(u) = 1$ *and* $s_k(u) = 0$ *for* $k = 2, 3$,
- (c) *There exists* $x = r + s\sqrt{a_2} \in K(\sqrt{a_2}) - J^2$ *such that* $r^2 - a_2 s^2 = a_3 t^2$ *for some* $t \in K$, *and* $L = J(\sqrt{x})$.

(C) *The following are equivalent*:
- (a) $\mathrm{Gal}(L/K) = Z_4 \times Z_2$ *and* $\mathrm{Gal}(L/K(\sqrt{a_1}))$ *is* $Z_2 \times Z_2$,
- (b) $s_1(u) = 0$ *and* $s_k(u) = 1$ *for* $k = 2, 3$,
- (c) *There exists* $x = r + s\sqrt{a_1} \in K(\sqrt{a_1}) - J^2$ *such that* $r^2 - a_1 s^2 = a_1 t^2$ *for some* $t \in K$, *and* $L = J(\sqrt{x})$.
- (d) *There exist* $y, z \in K$ *such that* $a_1 = y^2 + z^2$.

(D) *The following are equivalent*:
- (a) $\mathrm{Gal}(L/K) = Q_8$
- (b) $s_i(u) = 1$ *for* $i = 1, 2, 3$
- (c) *If* $x = yz$ *where* $y \in K(\sqrt{a_i})$ *and* $z \in K(\sqrt{a_j})$, *then* $L \ne J(\sqrt{x})$

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

Proof. Put $N = s_1(u) + s_2(u) + s_3(u)$. Then by Corollary 1.6, the number of quartic subfields of L is $2(3 - N) + 1$, which is the number of subgroups of order 2 of $\mathrm{Gal}(L/K)$. This number determines a group of order 8, and so we have: $N = 0$ if and only if $\mathrm{Gal}(L/K)$ is $Z_2 \times Z_2 \times Z_2$; $N = 1$ if and only if $\mathrm{Gal}(L/K)$ is D_4, $N = 2$ if and only if $\mathrm{Gal}(L/K)$ is $Z_4 \times Z_2$; and $N = 3$ if and only if $\mathrm{Gal}(L/K)$ is Q_8. (Since L contains J, we need not consider Z_8.)

If $\mathrm{Gal}(L/K)$ is $Z_2 \times Z_2 \times Z_2$, then L contains quadratic subfields (over K) other than $K(\sqrt{a_1})$; if one of these is $K(\sqrt{b})$, then $L = J(\sqrt{b})$, and conversely. This proves (A).

If $\mathrm{Gal}(L/K)$ is D_4 and $s_1(u) = 1$, $s_2(u) = s_3(u) = 0$, and by Corollary 1.6, $\mathrm{Gal}(L/K(a_1))$ is Z_4 and $\mathrm{Gal}(L/K(\sqrt{a_i}))$ is $Z_2 \times Z_2$ for $i = 2, 3$. Then L contains a quadratic extension M of $K(\sqrt{a_2})$, say, $M = K(\sqrt{a_2}, \sqrt{x})$ for some x in $K(\sqrt{a_2})$, and M is not normal over K (since $\mathrm{Gal}(L/K)$ is D_4). Write $x = r + s\sqrt{a_2}$. Then $N_K(x) = r^2 - a_2 s^2$ is not in M^2; it is in J^2 however, so we must have that $N_K(x) = \alpha t^2$, where α is either a_1 or a_3. From the identity (ID2), $K(\sqrt{\alpha})$ will have a quadratic extension other than J, and so α must be a_3. The converse is clear, and this proves (B).

If $\mathrm{Gal}(L/K) = Z_4 \times Z_2$ and $\mathrm{Gal}(L/K(\sqrt{a_1})$ is $Z_2 \times Z_2$, then L must contain a normal (over K) quartic field $M = K(\sqrt{a_1}, \sqrt{x})$ with $x = r + s\sqrt{a_1}$. Since $N_K(x) \in M^2$, we must have $N_K(x) = \alpha t^2$, where α is either 1 or a_1, and $t \in K$. By Corollary 1.2 and (A), if $\alpha = 1$, then $\mathrm{Gal}(L/K)$ is $Z_2 \times Z_2 \times Z_2$, a contradiction. So $\alpha = a_1$ as required. The converse is clear. Finally, if we have $x = r + s\sqrt{a_1}$ where $r^2 - a_1 s^2 = a_1 t^2$, then none of r, s, t is 0, and $r^2 = a_1(s^2 + t^2)$. Take $y = rs/(s^2 + t^2)$ and $z = rt/(s^2 + t^2)$; then $a_1 = y^2 + z^2$, so (d) holds. On the other hand, if we have $a_1 = y^2 + z^2$, then $a_1^2 - a_1 y^2 = a_1 z^2$, and (c) is satisfied. This proves (C).

Now (D) follows from (A), (B), and (C).

2. Quaternionic fields. In this section we discuss some of the relations among statements of the following type (where G and H are non-cyclic groups of order 8):

(a) J can be embedded both in a G-extension and an H-extension

(b) J can be embedded in a G-extension and not in an H-extension

(c) J can be embedded in neither a G-extension nor an H-extension.

We shall see that the fields L with $\mathrm{Gal}(L/Q) = Q_8$, fall naturally into two distinct classes, or types: A field L with $\mathrm{Gal}(L/K) = Q_8$ is of *Type I* if and only if it has any of the following (equivalent) properties: J has a D_4-extension; J has a $Z_2 \times Z_4$-extension; $L = J(\sqrt{u})$ where $u = xy$ with x and y elements of two different quadratic subfields of J. Otherwise, L is of *Type II*.

We use all the notation of Section 1.

LEMMA 2.1. *Let $u, v, uv \in J - J^2$, and assume as always that $L_1 = J(\sqrt{u})$, $L_2 = J(\sqrt{v})$, and $L_3 = J(\sqrt{uv})$ are normal over K. Then we have $S(L_3) \equiv S(L_1) + S(L_2) \pmod 2$.*

Proof. For each i, $1 \le i \le 3$, we can write

$$u\sigma_i(u) = \alpha r^2, \qquad v\sigma_i(v) = \beta s^2, \qquad (uv)\sigma_i(uv) = (\alpha\beta)(rs)^2$$

for some $r, s \in K(\sqrt{a_i})$, where α and β are either 1 or a_j $(j \ne i)$. Clearly, $s_i(uv) = 0$ if $\alpha = \beta$, and is 1 otherwise. Since $\alpha = \beta$ if and only if $s_i(u) = s_i(v)$, the result follows.

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

COROLLARY 2.2. *Fix J, and let $G(J) = G$ be the set of all possible (distinct) ordered triples $S(u)$ for $u \in J - J^2$. Then G, equipped with pointwise addition modulo two, is a group.*

Proof. It was assumed at the beginning that K does have a normal non-cyclic extension of degree 8 (which contains a non-trivial J) and char(K) is not 2. Then $K - J^2$ is not empty, for if $x \in J$ and $x^2 \in K$, then $x = r\sqrt{a_i}$ for some $i = 1, 2$, or 3. Take $b \in K - J^2$; then by Lemma 1.7A(c), $J(\sqrt{b})$ has $S(b) = (0, 0, 0)$ and so $(0, 0, 0)$ is in G. By Lemma 2.1 G is closed under its operation, and every element is its own inverse. So G is a group.

It is not difficult to come up with examples (e.g. with $K = Q$) to show that all possibilities for G are in fact attained. We give a few examples at the end of this section.

DEFINITION 2.3. If $L_1 = J(\sqrt{u})$ and $L_2 = J(\sqrt{v})$ are normal extensions of K such that $S(u) + S(v) \equiv (1, 1, 1) \pmod 2$, then we say that L_1 and L_2 are *complementary* extensions. If $S(u) = S(v)$, then L_1 and L_2 are *matching* extensions.

The next Corollary gives some easy consequences of the fact that $G(J)$ is a group.

COROLLARY 2.4. *Suppose that J has normal (over K) extensions $L_1 = J(\sqrt{u})$ and $L_2 = J(\sqrt{v})$.*

(a) *L_1 and L_2 are matching extensions if and only if there exists some element $b \in K$ such that $buv \in J$, that is, $L_2 = J(\sqrt{bu})$.*

(b) *J has a Q_8 extension if and only if J has at least one pair of complementary extensions.*

(c) *If J has a Q_8 extension, then J has a D_4 extension if and only if J has a $Z_2 \times Z_4$ extension.*

(d) *If J has three D_4 extensions which are pairwise not matching, then $G(J)$ has order 8, and J has extensions of every kind.*

The next result characterizes Q_8 extensions of Type I according to the properties of the defining element u.

THEOREM 2.5. *Suppose that $L = J(\sqrt{u})$ with $\mathrm{Gal}(L/Q) = Q_8$. Then the following are equivalent:*

(a) *J has a D_4 extension*

(b) *J has a $Z_2 \times Z_4$ extension*

(c) *For some $i \neq j$, $1 \leq i, j \leq 3$, there exist elements $x \in K(\sqrt{a_i}) - K$ and $y \in K(\sqrt{a_j}) - K$ such that $L = J(\sqrt{xy})$.*

Proof. The equivalence of (a) and (b) is given in Corollary 2.4. Assume (a); suppose that J has a D_4 extension M cyclic over $K(\sqrt{a_1})$. By Corollary 1.7, L has a quartic subfield $M = J(\sqrt{x})$ where $x \in K(\sqrt{a_2}) - K$. We have $S(u) = (1, 1, 1)$ by assumption, and $S(x) = (1, 0, 0)$. Then $S(ux) = (0, 1, 1)$, so that $N = J(\sqrt{ux})$ has $\mathrm{Gal}(N/K) = Z_2 \times Z_4$. Again by Corollary 1.7, there is an element $y \in K(\sqrt{a_1}) - K$ so that $N = J(\sqrt{y})$. Now it follows that $uxy \in J^2$, that is, $L = J(\sqrt{u}) = J(\sqrt{xy})$.

Now assume (c); suppose that $x \in K(\sqrt{a_1}) - K$ and $y \in K(\sqrt{a_2}) - K$. Since L is normal and $\mathrm{Gal}(L/K) = Q_8$, then neither x nor y is in J^2, and we have $(xy)\sigma_1(xy) = x^2 y\sigma_1(y) \in a_2(K(\sqrt{a_1}))^2$. Since $y\sigma_1(y) \in K$, we must have either $y\sigma_1(y) \in a_2K^2$ or $y\sigma_1(y) \in$

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

$a_1a_2K^2$. Then $J(\sqrt{y})$ is a normal field, and its Galois group is either D_4 (and (a) holds) or $Z_2 \times Z_4$ (and (b) holds). This completes the proof.

The argument of Theorem 2.5 indicates a method of construction for a Q_8 extension of Type I, that is, one need only find appropriate x and y in quadratic subfields of J, satisfying (respectively) conditions $B(c)$ and $C(c)$ of Corollary 1.7.

If K has a D_4 extension L_1 and a $Z_2 \times Z_4$ extension L_2, which are complementary, then the composite field $M = L_1L_2$ is normal over K and has degree 16 over K. Thus we have the following corollary.

COROLLARY 2.6. *J has a Q_8 extension of Type I if and only if J can be embedded into a normal extension M of K where* $\mathrm{Gal}(M/K)$ *is the group of order* 16 *generated by two elements ρ and τ satisfying the relations*

$$\rho^4 = \tau^4 = \rho\tau\rho\tau^{-1} = 1.$$

Proof. In [**6**], Thomas and Wood give the subgroup lattices for all groups of order 16. Since M is a composite field, $M = L_1L_2$, it is easy to count up the subfields of M according to their degree over K: there are three of degree 2, seven of degree 4, and three of degree 8. Since $\mathrm{Gal}(M/K)$ is not abelian, there is only one possibility; it has generators as described.

We now give some examples to illustrate the possibilities. We use some of the work of the next section, on quaternionic extensions of Q.

EXAMPLE 2.7. A Q_8 extension of Type I. Let $K = Q$, $J = Q(\sqrt{2}, \sqrt{3})$. Take $u = 2 + \sqrt{2}$, and $v = 3 + \sqrt{3}$. Then $L_1 = J(\sqrt{u})$ has $\mathrm{Gal}(L_1) = Z_2 \times Z_4$, and $L_2 = J(\sqrt{v})$ has $\mathrm{Gal}(L_2) = D_4$; furthermore, L_1 and L_2 are complementary. Then $J(\sqrt{uv})$ is quaternionic, and of Type I.

EXAMPLE 2.8. A Q_8 extension of Type II. Let $K = Q$, $J = Q(\sqrt{3}, \sqrt{14})$. Take $x = 5 + 3\sqrt{3}$, $y = 7 + 2\sqrt{14}$, and $z = 6 + \sqrt{42}$. Then put $u = xyz$, and $L = J(\sqrt{u})$. We have $u\sigma_1(u) = 42x^2$, $u\sigma_2(u) = 12y^2$ and $u\sigma_3(u) = 14z^2$, so that $\mathrm{Gal}(L) = Q_8$. Since none of 3, 14, 42 is a sum of two integer squares, J has no $Z_2 \times Z_4$ extensions, and hence no D_4 extensions.

EXAMPLE 2.9. A field with a D_4 extension, but no Q_8 extension. Let $K = Q$, and $J = Q(\sqrt{2}, \sqrt{7})$. Then if $x = 3 + \sqrt{2}$, $L_1 = J(\sqrt{x})$ is dihedral. By a result of Reichardt [**4**], since $7 \equiv 7 \pmod 8$, J has no Q_8 extension.

3. Type II extensions. In this section, K is the rational field Q. The results hold for Q_8 extensions of both types, but the primary interest is in their application as a method for constructing Q_8 extensions of Type II. We assume that $a_1 = m$, $a_2 = n$, and $a_3 = k = mn/\gcd(m, n)^2$ are positive squarefree integers, with mn not square. (Recall that a Q_8 extension of Q is a real field.) Otherwise, we use the notation of Section 1.

LEMMA 3.1. *Suppose that $u = x_1x_2x_3$, where $x_i \in K(\sqrt{a_i})$, for $i = 1, 2, 3$, and that $L = J(\sqrt{u})$ is normal over Q. Assume that each x_i is an algebraic integer, and put $r_1 = N(x_2)N(x_3)$, $r_2 = N(x_1)N(x_3)$, and $r_3 = N(x_1)N(x_2)$. Then each r_i is a rational integer, and we write $r_i = m_it_i^2$, where m_i and t_i are integers and m_i is squarefree.* (a) *For $i = 1, 2, 3$, $m_i \in \{1, m, n, k\}$.* (b) *If any two of m_1, m_2, m_3 are equal, then* $\mathrm{Gal}(L/Q)$ *is not Q_8.*

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

Proof. Since L is normal over Q, then $u\sigma_i(u) = r_i x_i^2$ is square in J for each $i = 1, 2, 3$, so that r_i is square in J. Then there is some $a \in \{1, m, n, k\}$, such that ar_i is a rational square. Since a is squarefree and r_i is an integer, (a) follows. To see (b), suppose e.g. that $m_1 = m_2$. Then $r_1 r_2 = r_3 N(x_3)^2$ is a rational square, and then r_3 is a rational square, and $u\sigma_3(u) = r_3 x_3^2$ is square in J. This proves (b).

COROLLARY 3.2. *If* $\mathrm{Gal}(L/Q) = Q_8$, *then* (m_1, m_2, m_3) *is either* (a_2, a_3, a_1) *or* (a_3, a_1, a_2).

REMARK. At this point, it is easy to see that if K has a Q_8 extension L as in Lemma 3.1, then K also has a D_4 extension: one of the fields $K(\sqrt{a_i}, \sqrt{x_i})$ must have D_4 as its normal closure. Stronger results of this nature are proved in [**8**].

We are interested in constructing Q_8 extensions of $J = Q(\sqrt{m}, \sqrt{n})$ using properties of the integers in the quadratic subfields of J. Obviously, some of our results could be generalized directly to any field K with a sufficiently well-behaved ring of integers.

THEOREM 3.3. *Let* $K = Q$, *and suppose* $a_1 = m$, $a_2 = n$ *are squarefree integers such that* mn *is not square. Define* $D = \gcd(m, n)$, *and write* $m = MD$, $n = ND$. *Put* $a_3 = k = MN$, *and* $J = Q(\sqrt{m}, \sqrt{n})$. *Then* J *has a* Q_8 *extension* L *if and only if there exist rational integers* $j, m_1, m_2, n_1, n_2, d_1, d_2$, *and integers* $x \in Q(\sqrt{m})$, $y \in Q(\sqrt{n})$, $z \in Q(\sqrt{k})$, *such that*

(1) $M = m_1 m_2$, $N = n_1 n_2$, $D = d_1 d_2$
(2) $N(x) = n_1 m_1 d_1 j t^2$
(3) $N(y) = n_2 m_1 d_2 j r^2$
(4) $N(z) = n_1 m_2 d_2 j s^2$

for some $r, s, t \in Q$.

Proof. Suppose first that all the conditions above are satisfied, and put $u = xyz$. Then $u\sigma_1(u) = x^2 N(y) N(z) = NM(x d_2 jrs)^2 = k\alpha^2$ with $\alpha \in Q(\sqrt{m})$; similarly $u\sigma_2(u) = m\beta^2$ for some $\beta \in Q(\sqrt{n})$ and $u\sigma_3(u) = n\gamma^2$ for some $\gamma \in Q(\sqrt{k})$. Then $S(u) = (1, 1, 1)$ and $\mathrm{Gal}(J(\sqrt{u}))$ is Q_8.

Conversely, suppose that $S(u) = (1, 1, 1)$. By Lemma 1.3, and multiplying by a rational integer square if necessary, we may assume that $u = xyz$, where $x \in Q(\sqrt{m})$, $y \in Q(\sqrt{n})$, and $z \in Q(\sqrt{k})$, are algebraic integers. Then the norms $N(x)$, $N(y)$, $N(z)$ are rational integers, and by Corollary 3.2, the integers $kN(y)N(z)$, $mN(x)N(z)$, and $nN(x)N(y)$ are rational squares. The argument is based on the fact that M, N, and D are squarefree, positive, and pairwise relatively prime.

If $kN(y)N(z)$ is square, then (since $k = MN$) there are integers so that $N(y) = n_2 m_1 a$ and $N(z) = n_1 m_2 b$ with $n_1 n_2 = N$ and $m_1 m_2 = M$. Then if $mN(x)N(z)$ is square, there must be integers so that $N(x) = m_1 d_1 c$ and $N(z) = m_2 d_2 d$, where $d_1 d_2 = D$. It follows that $N(z) = n_1 m_2 d_2 \alpha$ for some rational integer α. Similarly, $N(y) = n_2 m_1 d_2 \beta$ and $N(x) = n_1 m_1 d_1 \gamma$, for rational integers β and γ. Now $kN(y)N(z) = kNMd_2^2 \alpha\beta = (kd_2)^2 \alpha\beta$ is a rational square, and so α and β must have the same squarefree part. The same is true for α and γ, and for β and γ. Put j equal to this common squarefree part, and conditions (1)–(4) are satisfied.

NOTATION. If p is an odd prime and a is an integer, then we use the notation $(a \mid p)$ for the Legendre symbol: if $(a, p) = 1$, then $(a \mid p) = 1$ is a square mod p, and is -1 otherwise.

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

General residuacity conditions for the existence of a Q_8 extension of J are known; see e.g. [2] or [4]. The next theorem gives detailed conditions involving the integers n_i, m_i, d_i of Theorem 3.3.

THEOREM 3.4. *We use the notation of Theorem* 3.3. *Let* $J(\sqrt{xyz})$ *be a* Q_8 *extension of* J, *such that conditions* (1)–(4) *of Theorem* 3.3 *are satsified. Let* p *be an odd prime.*

(a) *If* $p \mid m_1 n_1 d_2$, *then* $p \equiv 1 \pmod 4$.

(b) *If* $p \mid N$, *then* $(-m \mid p) = 1$.

(c) *If* $p \mid M$, *then* $(-n \mid p) = 1$.

(d) *If* $p \mid D$ *then* $(-k \mid p) = 1$.

Proof. Let p be an odd prime, and write $x = a + b\sqrt{m}$, $y = c + d\sqrt{n}$, $z = e + f\sqrt{k}$, where a, b, c, d, e, f are rational numbers with denominator 1 or 2. Since p is an odd prime, we may as well assume that they are all integers; we can also assume that each of $\gcd(a,b)$, $\gcd(c,d)$, and $\gcd(e,f)$ is 1 or 2. Then

(i) $N(x) = a^2 - mb^2 = n_1 m_1 d_1 j t^2$

(ii) $N(y) = c^2 - nd^2 = n_2 m_1 d_2 j r^2$

(iii) $N(z) = e^2 - kf^2 = n_1 m_2 d_2 j s^2$.

(a) Suppose first that $p(m_1)$. Then $p \mid m$, and from (i), $p \mid a$, so equation (i) is divisible by p. We also have $p \mid k$, and so equations (i) and (iii) yield the congruences

$$-(m/p)b^2 \equiv n_1(m_1/p)d_1 j t^2 \pmod p,$$
$$e^2 \equiv n_1 m_2 d_2 j s^2 \pmod p.$$

Since $m = m_1 m_2 d_1 d_2$, then multiplying these together gives

$$-(m/p)b^2 e^2 \equiv n_1^2 (m/p) j^2 t^2 s^2 \pmod p.$$

Since $\gcd(a,b)$ and $\gcd(e,f)$ can only be 1 or 2, and p is odd, then $\gcd(b,p) = 1$ and $\gcd(e,p) = 1$. Of course $\gcd((m/p),p) = 1$, and so $(-1 \mid p) = 1$, and $p \equiv 1 \pmod 4$. The proof is similar if $p \mid n_1$ or $p \mid d_2$.

The statements (b), (c), (d) are all proved in the same way; we give the argument for (c). If $p \mid m_1$, then $(n \mid p) = 1$ from equation (ii). Since $(-1 \mid p) = 1$ also, then $(-n \mid p) = 1$. Suppose now that $p \mid m_2$. Since $k = MN$, then $m_2 \mid k$, and then $p \mid e$, so equation (iii) is divisible by p. Then equations (i) and (iii) give the congruences

$$-(k/p)f^2 \equiv n_1(m_2/p)d_2 j s^2 \pmod p.$$
$$a^2 \equiv n_1 m_1 d_1 j t^2 \pmod p.$$

Multiplying these together gives

$$-(k/p)f^2 a^2 \equiv n_1^2 (M/p) D j^2 s^2 t^2 \pmod p.$$

and since $(k/p) = N(M/P)$ and $n = ND$, it follows that $(-n \mid p) = 1$.

The next Corollary is helpful in finding solutions to the equations (1)–(4) of Theorem 3.3.

COROLLARY 3.5. *Suppose that* J *has a* Q_8 *extension, and assume the notation of Theorem* 3.3. *Suppose that* p *is an odd prime divisor of* mn. *Then* p *is inert in one of the*

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

quadratic subfields of J if and only if $p \equiv 3 \pmod 4$, and p splits in one of the quadratic subfields of J if and only if $p \equiv 1 \pmod 4$.

Proof. It is well known that a prime p splits (resp. is inert) in a quadratic field $Q(\sqrt{j})$ if and only if $\gcd(j,p)=1$, and $(j \mid p)=1$ (resp. $(j \mid p)=-1$). The result follows immediately from Theorem 3.4.

4. Applications. We work out some specific constructions for n, m such that $J=Q(\sqrt{m},\sqrt{n})$ has a Q_8 extension. As before, m and n are positive squarefree integers such that mn is not square. We use, without much comment, various special properties of quadratic fields; for instance if $x \in Q(\sqrt{j})$ and $j<0$, then $N(x) \geq 0$; the multiplicative properties of norms, and so on.

The residuacity conditions for odd primes are easily computed from Theorem 3.4 or otherwise. Congruence conditions on (m,n,k) modulo 8 are given by Reichardt in [4]: we must have either (a) $m \equiv n \equiv 1 \pmod 4$, or else (b) $m \equiv n \equiv 2 \bmod 4$), and $(m/2, n/2, k)$ congruent to one of $(1,1,1)$, $(3,7,5)$, $(5,5,1)$, $(1,3,3)$, $(5,7,3) \pmod 8$.

In the examples below, one of n, m is a prime. The following lemma gives some useful consequences of Lemma 1.1 for rational integers.

LEMMA 4.1. *Let p be an odd prime, and let $n=\pm p$. Suppose that x, y are integers such that $\gcd(x,y)=1$.* (a) *If t is odd and $x^2-ny^2=t^2$, then one of the quantities $\pm(x+y\sqrt{n})$ is a square in $Q(\sqrt{n})$.* (b) *If t is odd and $x^2-ny^2=4t^2$, then there exist integers α, β such that $\alpha^2 \pm p\beta^2 = \pm 4t$.*

Proof. (a) From the assumptions, $(x-t)/2$ and $(x+t)/2$ are relatively prime integers, and their product is $\pm p(y/2)^2$. Then since p is prime, we have, say, $(x-t)/2 = \pm p\alpha^2$ and $(x+t)/2 = \pm\beta^2$, for integers α and β. Then by the identity (ID1) of Lemma 1.1, one of $\pm(x+y\sqrt{n})$ is square. Similarly, for (b), one of the quantities $\pm(x-2t)$ is square in $Q(\sqrt{n})$. That is, one of $\pm 2(x+y\sqrt{n})$ is equal to a square, say, $(\alpha+\beta\sqrt{n})^2$. Then $\alpha^2-n\beta^2=\pm 4t$.

EXAMPLE 4.2. $J=Q(\sqrt{2},\sqrt{n})$ has a Q_8 extension if and only if every odd prime factor p of n satisfies $p \equiv 1$ or $3 \pmod 8$.

Since $2=1^2+1^2$, a Q_8 extension of J must be of Type I. Suppose that n is odd. Let $y=2+\sqrt{2}$; then y satisfies condition C(c) of Corollary 1.7. It remains to find an $x \in Q(\sqrt{2n})$ satisfying condition B(c) of Corollary 1.7, that is,

$$x = a + b\sqrt{2n} \quad \text{and} \quad N(x) = a^2 - 2nb^2 = nt^2 \tag{1}$$

(where we may assume a, b and t are rational integers). If $a^2-2nb^2=nt^2$, then (since n is squarefree) $n \mid a$, say $a=nc$. Then $n^2c^2-2nb^2=nt^2$, and $nc^2-2b^2=t^2$, from which we have $nc^2=t^2+2b^2$. Since $Q(\sqrt{-2})$ is a PID, this equation is solvable if and only if $n \equiv 1$ or $3 \pmod 8$; in this case, there is a solution x for (1), and then $J(\sqrt{xy})$ is a Q_8 extension.

EXAMPLE 4.3. Let $p \equiv q \equiv 1 \pmod 4$ be primes. Then $J=Q(\sqrt{p},\sqrt{q})$ has a Q_8 extension if and only if $(p \mid q)=1$.

Any Q_8 extension must be of Type I. We need a solution to $x^2-py^2=qt^2$. Since $Q(\sqrt{p})$ has odd class number (see e.g. [1]), say $h=2r+1$, we can always solve either

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

$x^2 - py^2 = q^h$ or $x^2 - py^2 = 4q^h$ (in integers x, y). Then we can take $t = q^r$ or $2q^r$, accordingly, and let $X = x + y\sqrt{p}$. Next, there are integers u, v so that $pq = u^2 + v^2$. Put $Y = pq + u\sqrt{pq}$. Then $J(\sqrt{XY})$ is a Q_8 extension.

EXAMPLE 4.4. Let $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Then $J = Q(\sqrt{p}, \sqrt{2q})$ has a Q_8 if and only if $p \equiv 5 \pmod 8$ and $(p \mid q) = -1$.

Any Q_8 extension must be of Type I. We need a solution to the equation $x^2 - 2qy^2 = 2pqt^2$, or equivalently, a solution to $a^2 + pb^2 = 2qc^2$.

In $Q(\sqrt{-p})$, the class group has even order, and we have the prime ideal factorizations: $(2) = P^2$ and $(q) = Q_1Q_2$. Suppose that Q_1 were of odd order t in the class group. Then there exist integers x, y such that $x^2 + py^2 = q^t$; x and y must be of opposite parity since q^t is odd. But then $x^2 + py^2 \equiv 1 \pmod 4$, while $q^t \equiv 3 \pmod 4$, a contradiction. Thus Q_1 has even order, say $2j$, in the class group.

Now there must be integers x, y so that $x^2 + py^2 = q^{2j}$. From Lemma 4.1, if x is odd, then one of $\pm(x + y\sqrt{-p})$ is square, and $2j$ is not minimal. So x must be even. We next show that j is odd. Since $(x - q^j)(x + q^j) = -py^2$, we may suppose that $x - q^j = \pm s^2$ and $x + q^j = \pm pr^2$, with $rs = y$. Then (with appropriate choice of sign)

$$\pm 2(x + y\sqrt{-p}) = [s + (y/s)\sqrt{-p}]^2 = Y^2$$

where $N(Y) = 2q^j$. Since $p = 5 \pmod 8$, the equation $u^2 + pv^2 = 2z^2$ has no integral solutions, so $N(Y) = 2q^j$ implies that j must be odd, say $j = 2i + 1$. Now we can write $N(Y) = 2q(q^i)^2$, as required. Write $Y = a + b\sqrt{-p}$ and $N(Y) = 2qc^2$, and let $Z = 2qc - a\sqrt{2q}$. Then $N(Z) = 2pqb^2$. Finally, write $p = r^2 + s^2$, and let $X = p + r\sqrt{p}$. Then $J(\sqrt{XZ})$ is a Q_8 extension.

The construction of a Type I extension is probably most easily accomplished by the method of the examples above. We do not have anything this simple for Type II extensions, but the next theorem gives a construction for a large class of Type II extensions. This theorem can also be used for Type I extensions.

THEOREM 4.5. *Let* $\gcd(m, n) = 1$, *and* $J = Q(\sqrt{m}, \sqrt{n})$. *Suppose that there are integers such that*

(i) $n = ak$
(ii) $a = A^2 + B^2$
(iii) $(Ar)^2 + ms^2 = kt^2$
(iv) $u^2 + av^2 = mw^2$.

Then define algebraic integers X, Y, *and* Z *by*

$$X = (Br + s\sqrt{m})(u + w\sqrt{m}) = (Bru + msw) + (us + Brw)\sqrt{m}$$

$$Y = kt^2 + tr\sqrt{n}$$

$$Z = ams + tB\sqrt{nm}$$

Then $J(\sqrt{XYZ})$ *is a* Q_8 *extension of* J.

Proof. We will show that conditions (1)–(4) of Theorem 3.3 are satisfied. We have $M = m$, $N = n$, $D = 1$, and we take $m_1 = 1$, $m_2 = m$, $n_1 = a$ and $n_2 = k$. Since $D = 1$, $d_1 = d_2 = 1$ can be ignored. Define the integer $j = kt^2 - ar^2$. Then $-j = (Br)^2 - ms^2$, and

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

from (iv), we have $u^2 - mw^2 = -av^2$. Then since $n = ak$,

$$N(X) = ((Br)^2 - ms^2)(u^2 - mw^2) = ajv^2 = n_1 m_1 jv^2$$
$$N(Y) = (kt^2)^2 - nt^2 r^2 = kt^2(kt^2 - ar^2) = kjt^2 = n_2 m_1 jt^2$$
$$N(Z) = (ams)^2 - nm(tB)^2 = am(ams^2 - kt^2 B^2) = amjA^2 = n_1 m_2 jA^2$$

and the conditions of Theorem 3.3 are satisfied. Then $J(\sqrt{XYZ})$ is a Q_8 extension.

EXAMPLE 4.6. $J = Q(\sqrt{3}, \sqrt{n})$ has a Q_8 extension if and only if $n = 2 \pmod 4$ and every odd prime divisor p of n satisfies $p \equiv 1$ or $7 \pmod{12}$. The necessity of these conditions follows from the general residuacity conditions given by Reichardt. To see the sufficiency, write $n = 2k$. Since $Q(\sqrt{-3})$ is a PID, and every prime divisor of k splits in $Q(\sqrt{-3})$, then there exist integers r, s so that $r^2 + 3s^2 = k$. Then in the notation of Theorem 4.5, we take: $m = 3$, $n = 2k$, $a = 2$, $A = B = 1$, $t = 1$, $u = v = w = 1$, and r, s so that $r^2 + 3s^2 = k$. The corresponding X, Y, Z produce the desired Q_8 extension.

Similar results are possible for $J = Q(\sqrt{p}, \sqrt{2k})$, where p is a prime, $p = 3 \pmod 8$, as in the next example.

EXAMPLE 4.7. Let $p \equiv 3 \pmod 8$ and $q \equiv 3 \pmod 4$. Then $J = Q(\sqrt{p}, \sqrt{2q})$ has a Q_8 extension if and only if $(p \mid q) = -1$. Again we need only establish sufficiency. We use Theorem 4.5 with $m = p$, $n = 2q$, $m_1 = 1$, $m_2 = p$, $n_1 = 2$, $n_2 = q$, $D = d_1 = d_2 = 1$. Take $a = 2$, $A = B = 1$, and $k = q$. Since $Q(\sqrt{-2})$ is a PID, and since $p \equiv 3 \pmod 8$, there are integers u, v so that $u^2 + 2v^2 = p$. We need only show that $r^2 + ps^2 = qt^2$ has a solution. Since $(p \mid q) = -1$ and $q \equiv 3 \pmod 4$, then $(-p \mid q) = 1$, and q splits in $Q(\sqrt{-p})$. Then there is some minimal integer j so that, for some $x, y \in Z$, either

$$\text{(a) } x^2 + py^2 = q^j \quad \text{or} \quad \text{(b) } x^2 + py^2 = 4q^j.$$

If (a) holds, then x and y have opposite parity. Suppose that j is even, $j = 2i$. Then $q^j \equiv 1 \pmod 4$, and since $p \equiv 3 \pmod 8$, we must have x odd and $y \equiv 0 \pmod 4$. Then by Lemma 4.1, one of $\pm(x + y\sqrt{-p})$ is square, and its square roots has norm q^i; then j is not minimal. Thus in case (a), j must be odd.

If (b) holds, then x and y are odd. If j is even, $j = 2i$, then by Lemma 4.1, there would be an element of norm $4q^i$ and j would not be minimal. So in case (b) also, j must be odd.

It follows that the equation $r^2 + ps^2 = qt^2$ has an integral solution. Then the conditions of Theorem 4.5 are satisfied, and the corresponding X, Y, and Z give a Q_8 extension $J(\sqrt{XYZ})$.

4.8. Let $m \equiv 3 \pmod 8$, $n \equiv 2 \pmod 4$, with $\gcd(m, n) = 1$, and suppose that both $Q(\sqrt{m})$ and $Q(\sqrt{-m})$ are PID's. If all the residuacity conditions are satisfied, then $J = Q(\sqrt{m}, \sqrt{n})$ has a Q_8 extension.

Proof. We use Theorem 4.5. Write $n = ak$, where k is the product of all the prime factors of n which are congruent to $3 \pmod 4$, and a is the product of the remaining factors. Then $a = A^2 + B^2$ for some integers A, B, and $a \equiv 2 \pmod 8$. If $p \mid k$, then $(-m \mid p) = 1$, and so since $Q(\sqrt{-m})$ is a PID, the equation $x^2 + my^2 = k$ has an integral solution. Multiplying through by A^2, we have a solution to the equation $(Ar)^2 + ms^2 = kt^2$.

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press

If $p \mid a$ and p is odd, then $p \equiv 1 \pmod 4$, so $(-m \mid p) = 1$ implies $(m \mid p) = 1$. Since $m \equiv 3 \pmod 8$, 2 ramifies in $Q(\sqrt{m})$. Now since $Q(\sqrt{m})$ is a PID, there must be a solution to either $x^2 - my^2 = a$, or to $x^2 - my^2 = -a$. Since $m = 3 \pmod 8$ and $a \equiv 2 \pmod 8$, the equation $x^2 - my^2 = a$ is not possible. Then there is a solution to $x^2 - my^2 = -a$, and then $x^2 + a = my^2$. Now take $m_1 = 1$, $m_2 = m$, $n_1 = a$, and $n_2 = k$, and we have the solution given in Theorem 4.5.

REFERENCES

1. Ezra Brown, Class numbers of real quadratic fields, *Trans. Amer. Math. Soc.* **190** (1974), 99–107.

2. G. Bucht, Uber einige algebraische Korper achten Grades, *Arkiv for Matematik, Astronomi och Fysik, Bd. 6*, **30** (1910), 1–36.

3. Harvey Cohn, Quaternionic compositum genus, *J. Number Theory*, **11,** (1979), 399–411.

4. Christian U. Jensen and Noriko Yui, Quaternion Extensions, *Algebraic Geometry and Commutative Algebra* (1987), 155–182.

5. H. Reichardt, Uber Normalkorper mit Qaternionengruppe, *Math. Zeitschrift* **41,** (1936), 218–221.

6. Emanuel Rosenbluth, Die Arithmetische Theorie und die Konstruktion der Quaternionenkorper auf klassenkorpertheoretischer Grundlage, *Monatshefte fur Math. u. Phys.* **41** (1934), 85–125.

7. A. D. Thomas and G. V. Wood, *Group tables* (Shiva Publishing, 1980).

8. Roger Ware, A note on the quaternion group as Galois group, *Proc. Amer. Math. Soc.* **108,** (1990), 621–625.

9. E. Witt, Konstruktion von galoisschen Korpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1936), 237–245.

UNIVERSITY OF NORTH CAROLINA AT GREENSBORO,
GREENSBORO,
NC 27412,
USA

https://doi.org/10.1017/S0017089500008533 Published online by Cambridge University Press