PACIFIC JOURNAL OF MATHEMATICS
Vol. 175, No. 1, 1996

MAXIMAL SUBFIELDS OF $Q(i)$-DIVISION RINGS

STEVEN LIEDAHL

In this paper we determine the $Q(i)$-division rings which have maximal subfields of the form $E(i)$, where E/Q is cyclic and $i = \sqrt{-1}$. These are precisely the $Q(i)$-division rings having maximal subfields which are abelian over Q. More generally we determine the $Q(i)$-division rings having maximal subfields which are Galois over Q. We show that a division ring D contains such subfields if and only if the same is true for the 2-part of the Sylow decomposition of D.

1. Introduction and Preliminaries.

Let K be a field, and let D be a finite-dimensional K-central division ring. The dimension $[D : K] = m^2$ is a square, and one defines the index of D by $\text{ind}(D) = m$. The maximal subfields of D are precisely those subfields which contain K and which have degree m over K. In case D has a maximal subfield L which is Galois over K, there exists a 2-cocycle $f : G \times G \to L^*$ such that D is isomorphic to the crossed product algebra $(L/K, f)$. This is proved in the chapter on simple algebras in [**Hers**], and we will assume familiarity with the results given there. It is well known that if K is a number field, then D has a maximal subfield which is cyclic of degree m over K. In [**Alb**], A.A. Albert posed the following rationality question: if F is a subfield of K, does there exist a cyclic extension E/F of degree m such that EK is a maximal subfield of D? He showed that such E need not exist, but considered conditions on $\text{ind}(D)$ and $[K : F]$ under which such E could be found (e.g., Proposition 6, below).

The results of the present paper are motivated by this question in the special case $K = Q(i)$, $F = Q$. If E/Q is a cyclic extension of degree m such that $E(i)$ is a maximal subfield of a $Q(i)$-division ring D, then $E(i)$ is, in particular, an abelian extension of Q. It turns out that, conversely, if D has maximal subfields abelian over Q, then it has one of the form $E(i)$, where E/Q is cyclic. This raises the question of whether a $Q(i)$-division ring has maximal subfields which are cyclic, abelian, or even Galois over Q. We determine the $Q(i)$-division rings having such subfields in our main theorems 7, 8, and 12, according to the local indices of D. To define these,

let K be any number field, let p denote a finite or infinite prime of K, and let K_p denote the completion of K at p. Then $K_p \otimes_K D$ is a matrix ring over a K_p-division ring D_p, and we define $\mathrm{ind}_p(D) = \mathrm{ind}(D_p) = m_p$. The K-division ring D is determined uniquely up to K-isomorphism by its Hasse invariants $\mathrm{inv}_p(D) = r_p/m_p \in Q/Z$, where $(r_p, m_p) = 1$. For their definition, we refer to [**A-T**] and especially to [**Rein**]. The invariants satisfy

(i) $r_p/m_p = 0$ for all but finitely many p,

(ii) $r_p/m_p = 0$ or $1/2$ if p is real, $r_p/m_p = 0$ if p is complex, and

(iii) $\sum_p (r_p/m_p) = 0$.

Moreover, given fractions r_p/m_p in Q/Z satisfying (i), (ii), and (iii), with the nonzero r_p/m_p satisfying $(r_p, m_p) = 1$, there is a unique K-division ring D such that $\mathrm{inv}_p(D) = r_p/m_p$, and one has $\mathrm{ind}(D) = \text{l.c.m. } \{m_p\}$. If L is a finite extension of K then $L \otimes_K D$ is a central simple L-algebra. Its invariant at a prime $\wp$ dividing p is given by $\mathrm{inv}_\wp(L \otimes_K D) = [L_\wp : K_p] \cdot \mathrm{inv}_p(D)$. Let $\mathrm{Br}(K)$ denote the Brauer group of K, and denote the Brauer class of D by $[D]$. Let Res denote the restriction homomorphism from $\mathrm{Br}(K)$ to $\mathrm{Br}(L)$ induced by $D \to L \otimes_K D$.

We recall the splitting behavior of rational primes in $Q(i)$. The primes $p = 2$ and $p = p_\infty$ are the only ramified primes; they have unique extensions to $Q(i)$. A prime $p \equiv 1 \pmod 4$ has two divisors $\wp, \bar{\wp}$ in $Q(i)$ which are conjugate under the action of $\mathrm{Gal}(Q(i)/Q)$ on the set of primes of $Q(i)$. The primes $p \equiv 3 \pmod 4$ remain prime in $Q(i)$.

Finally, we will need a description of the Galois extensions of degree ef of a local field F such that the ramification index e is prime to the residue characteristic p of F. Accordingly, let F be a finite extension of Q_p, let q denote the number of elements of the residue field of F. Let T/F be the unramified extension of degree f. Choose a prime element π_F of F and a root of unity $\zeta \in T$ of order $q^f - 1$.

Theorem 1 ([**Alb**, **Has**]). *Assume e, f, and i are integers such that $q^f \equiv 1 \pmod e$, $e | i(q-1)$, $0 \le i < q^f - 1$, and $(e, p) = 1$. Then the field $K = F(\zeta, \pi_K)$ defined by $\pi_K^e = \zeta^i \pi_F$ is a Galois extension whose Galois group is generated by elements x, y with defining relations $x^e = 1$, $y^f = x^i$, $y^{-1}xy = x^q$. Conversely, each Galois extension of F having degree ef and ramification index e is obtained in this manner by a choice of integer i satisfying the congruence conditions above.*

This paper is based on part of the author's U.C.L.A. doctoral dissertation, which was written under the kind supervision of Professor M. Schacher, and which was supported by a U.S. Department of Education Dissertation Year

Grant.

2. Maximal Subfields.

We shall give necessary and sufficient conditions for a $Q(i)$-division ring to have maximal subfields which are cyclic, abelian, or Galois over Q in terms of the local indices $\mathrm{ind}_\wp(D)$. Assume D is a $Q(i)$-division ring for which the class $[D]$ lies in the image of Res : $\mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$, with $[Q(i) \otimes_Q \Delta] = [D]$ for some Q-division ring Δ. Then either $Q(i) \otimes_Q \Delta \cong D$ or $Q(i) \otimes_Q \Delta \cong M_2(D)$ and $\mathrm{ind}(D) = \frac{1}{2}\mathrm{ind}(\Delta)$. In the first case, if L/Q is a cyclic maximal subfield of Δ, then $L(i)$ is a maximal subfield of D and is an abelian extension of Q. By contrast, it may happen in the second case that no maximal subfield of D is Galois over Q. These cases are distinguished in the following proposition.

Proposition 2. *For a Q-division ring Δ, the following are equivalent:*

(i) $Q(i) \otimes_Q \Delta$ *is a $Q(i)$-division ring,*

(ii) $\sqrt{-1} \notin \Delta$,

(iii) *If* $\mathrm{ind}(\Delta) = 2^t \cdot m$, m *odd, then* 2^t *divides* $\mathrm{ind}_p(\Delta)$ *for a prime* $p \equiv 1 (\mathrm{mod}\, 4)$.

Proof. (i) $\Rightarrow$ (ii). If $\sqrt{-1} \in \Delta$ then $Q(i) \otimes \Delta$ contains $Q(i) \otimes Q(i) \cong Q(i) \otimes Q[X]/(X^2+1) \cong Q(i)[X]/(X^2+1) \cong Q(i) \oplus Q(i)$, which contains zero-divisors.

(ii) $\Rightarrow$ (i). The regular representation gives $Q(i) \subseteq M_2(Q)$, therefore $Q(i) \otimes_Q \Delta \subseteq M_2(Q) \otimes_Q \Delta = M_2(\Delta)$. If $Q(i) \otimes_Q \Delta$ is not a division ring then $Q(i) \otimes_Q \Delta \cong M_2(D)$ contains a copy of $M_2(Q)$ centralized by $Z(Q(i) \otimes_Q \Delta) = Q(i)$. By [**Hers**, Thm. 4.4.2], $M_2(\Delta) = M_2(Q) \otimes_Q C$, where C is the centralizer of $M_2(Q)$ in $M_2(\Delta)$. Then C is a central simple Q-algebra, so $C \cong \Delta$ and there is an embedding $Q(i) \subseteq \Delta$.

(i) $\Leftrightarrow$ (iii). The index of $D = Q(i) \otimes_Q \Delta$ equals the l.c.m. of the indices $\mathrm{ind}_\wp(D)$. So $Q(i) \otimes_Q \Delta$ is a division ring iff 2^t divides $\mathrm{ind}_p(\Delta)/[Q(i)_\wp : Q_p]$ for some p iff 2^t divides $\mathrm{ind}_p(\Delta)$ for some p split completely in $Q(i)$. □

It is known from [**Sch1**] that if Δ is a Q-division ring which is a crossed product algebra for G, then each Sylow subgroup of G is metacyclic, i.e., a Sylow subgroup P has a cyclic normal subgroup N such that P/N is cyclic. This important property is preserved by Res : $\mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$ in the following sense.

Proposition 3. *If the class $[D]$ lies in the image of* Res : $\mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$, *and if D is a crossed product algebra for a group G, then G is Sylow-*

metacyclic.

Proof. Let $L/Q(i)$ be maximal subfield of D, assume $L/Q(i)$ is Galois, and let P be a Sylow p-subgroup of $\mathrm{Gal}(L/Q(i))$. We claim P is contained in a decomposition group of $L/Q(i)$ at a prime of $Q(i)$ not dividing p. This will imply P is metacyclic by Theorem 1. By [**Sch1**, Prop. 2.6], P is contained in $\mathrm{Gal}(L_{\wp}/Q(i)_{\wp})$ for at least two primes $\wp$ of $Q(i)$. If $p = 2$ or $p \equiv 3 \pmod 4$, the claim follows from the fact that p has a unique extension to $Q(i)$. If $p \equiv 1 \pmod 4$ and $\wp$ divides p, then $\mathrm{inv}_{\wp}(D) = \mathrm{inv}_{\bar{\wp}}(D)$. Since 2 is prime to p, the element $\mathrm{inv}_{\wp}(D) + \mathrm{inv}_{\bar{\wp}}(D)$ of Q/Z has order a multiple of $|P|$. Then $\sum \mathrm{inv}_{\wp}(D) = 0$ implies $|P|$ divides the local index of D at some prime v other than $\wp, \bar{\wp}$. This implies that a copy of P is contained in $\mathrm{Gal}(L_v/Q(i)_v)$ as desired. □

Proposition 3 reflects the statement above about Q-division rings as crossed products. However the proposition is easily false if $Q(i)$ is replaced by an arbitrary number field. For instance, let p be an odd prime, let K/Q be a cyclic extension of degree p^3 in which p splits completely. Let D be the unique K-division ring whose invariants are $1/p^3$ at each of the p^3 divisors of p in K, and 0 elsewhere. Let G be the nonabelian group of order p^3 and exponent p. Since G is generated by two elements, it follows easily from [**Sh**] and [**Neu2**, Main Thm.] that D has a G-Galois maximal subfield L/K. This D lies in the image of the restriction map. For if Δ is the Q-division ring whose invariants are $1/p^3$ at p, $-1/p^3$ at some prime of degree p^3, and 0 elsewhere, then $K \otimes_Q \Delta \cong D$.

We have used the fact that a class $[D]$ in the image of $\mathrm{Res} : \mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$ has equal invariants at conjugate primes. This property actually characterizes the image in the present case. We omit the easy proof of the following proposition, which uses only the fact that $\mathrm{Gal}(Q(i)/Q)$ is cyclic. The case of a finite Galois extension is slightly more complicated, and is treated in [**Mac**, p. 330].

Proposition 4. *The image of* $\mathrm{Res} : \mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$ *consists of those classes* $[D]$ *such that* $\mathrm{inv}_{\wp}(D) = \mathrm{inv}_{\bar{\wp}}(D)$ *whenever* $\wp$ *is conjugate to* $\bar{\wp}$ *over* Q.

With Proposition 4 we describe those $Q(i)$-division rings which may be defined over Q:

Proposition 5. *Let* D *be a* $Q(i)$*-division ring of index* $2^t \cdot m$, m *odd. Then*

there exists a Q-division ring Δ such that $D \cong Q(i) \otimes_Q \Delta$ if and only if

(i) $\mathrm{inv}_{\wp}(D) = \mathrm{inv}_{\bar{\wp}}(D)$ *for all primes $\wp, \bar{\wp}$ conjugate over Q, and*

(ii) *if $t \geq 1$, then 2^t divides $\mathrm{ind}_{\wp}(D)$ only if $\wp$ divides a rational prime $p \equiv 1 \pmod 4$.*

Proof. If $D = Q(i) \otimes_Q \Delta$ is a division ring, then the invariants of D are equal at conjugate primes, and 2^t is the highest power of 2 dividing $\mathrm{ind}(\Delta)$, so 2^t divides $\mathrm{ind}_p(\Delta)$ for some prime p. If $t \geq 1$, then (ii) follows from the fact that $[Q(i)_{\wp} : Q_p] = 2$ unless $p \equiv 1 \pmod 4$. Conversely, if (i) holds then there is a Q-division ring Δ such that $[Q(i) \otimes_Q \Delta] = [D]$ by Proposition 4, and $\mathrm{ind}(\Delta) \geq \mathrm{ind}(D)$. If (ii) is assumed, then the 2-part of $\mathrm{ind}_p(\Delta)$ is at most 2^t for all rational primes p. Therefore $\mathrm{ind}(\Delta) = 2^t \cdot m = \mathrm{ind}(D)$ and $Q(i) \otimes_Q \Delta \cong D$. □

We begin our study of maximal subfields of $Q(i)$-division rings with a determination of those division rings having a maximal subfield which is a cyclic extension of Q. Suppose D has index $2^t \cdot m$, m odd, and assume D has such a maximal subfield. Then $t = 0$ according to the fact that $Q(i)/Q$ cannot be embedded a cyclic extension of degree 4. We show that conversely, a $Q(i)$-division ring of odd index has a maximal subfield which is cyclic over Q. This is immediate from:

Proposition 6 ([**Alb**, Thm. 24]). *Let K and F be number fields with $[K : F] = q$, and assume K/F is Galois. If D is a K-division ring of index n prime to q, then there is a cyclic extension E/F of degree n such that EK is a maximal subfield of D.*

Proof. Let S be the set of primes of F which lie under primes of K where $\mathrm{ind}_{\wp}(D) > 1$. By the Grunwald-Wang theorem ([**A-T**, Chap. 10]), there is a cyclic extension E/F of degree n such that $[E_{\wp} : F_{\wp}] = \mathrm{ind}_{\wp}(D)$ for all $\wp \in S$. Then $[EK : K] = n$. Since K/F is Galois, the degrees $[K_{\wp} : F_{\wp}]$ are divisors of q. Therefore $K_{\wp}$ and $E_{\wp}$ are disjoint over $F_{\wp}$ and $[(EK)_{\wp} : K_{\wp}] = \mathrm{ind}_{\wp}(D)$ for all $\wp$ such that $\mathrm{ind}_{\wp}(D) > 1$. This shows that EK splits D, and is a maximal subfield of D. □

Remarks. 1. The assumption that K/F be Galois was omitted in [**Alb**], but is shown to be necessary by the following example. We take $F = Q$. Since the 3-adic field Q_3 contains no primitive 5-th root of unity, the only cyclic extension of Q_3 of degree 5 is unramified. Let L/Q be a Galois extension with group S_7 such that $L_{\wp}$ is unramified of degree 5 at a divisor of 3. Let $\alpha \in L$ be such that $[Q(\alpha) : Q] = 7$ and L is generated by the conjugates of

α over Q. We may assume α is chosen so that $L_\wp = Q_3(\alpha)$. Let $K = Q(\alpha)$ and let D be a K-division ring of index 5 such that $\mathrm{ind}_p(D) = 5$, where p lies under the prime $\wp$ of L. Then $K_p = L_\wp$ is unramified of degree 5 over Q_3. Any cyclic extension E/Q of degree 5 such that EK splits D must have the property that $[E_p : Q_3] = 5$ at the unique divisor of 3 in E, and $[(EK)_p : K_p] = 5$ at the unique divisor of p in EK. But then E_p/Q_3 is unramified, hence $(EK)_p = K_p$, and EK cannot split D.

2. The following related question is considered in [**Sch2**]. If D is a K-division ring, K a number field, it is well known that D has a cyclotomic splitting field $L \subseteq K(\mu_n)$ for some n (see [**A-T**, p. 57]). Thus $[D] = [(L/K, f)]$ for a cyclotomic extension L of K. It had been conjectured that L could be chosen to be a maximal subfield of D, so that similarity could be strengthened to an isomorphism $D \cong (L/K, f)$. This conjecture is disproved in [**Sch2**] (counterexamples over $Q(i)$ are given below). It was stated in [**Sch2**, Thm. 2] that this conjecture is true if K/Q has degree q prime to $n = \mathrm{ind}(D)$. The proof given there is valid if K/Q is Galois, but the K-division ring D of the preceding remark is a counterexample to the conjecture, hence also to [**Sch2**, Thm. 2]. Indeed, if $L \subseteq K(\mu_n)$ is a maximal subfield of D, then $K \cap Q(\mu_n) = Q$ implies L has the form EK, where $E \subseteq Q(\mu_n)$ is cyclic of degree 5 over Q. By Remark 1, D has no such subfield.

According to Proposition 6, if $\mathrm{ind}(D) = m$ is odd, there is a cyclic extension E/Q of degree m such that $E(i)$ is a maximal subfield of D, and $E(i)/Q$ is clearly cyclic. We have proved

Theorem 7. *A $Q(i)$-division ring D has maximal subfields which are cyclic over Q if and only if* $\mathrm{ind}(D)$ *is odd.*

Next we determine the $Q(i)$-division rings having maximal subfields which are abelian over Q. The problem is easily reduced to the case of 2-power index as follows. According to [**Hers**, Thm. 4.4.6], let $D = D_1 \otimes_{Q(i)} D_2$, where $\mathrm{ind}(D_1) = m$ is odd, and $\mathrm{ind}(D_2) = 2^t$. If D_1 and D_2 have maximal subfields L_1 and L_2, respectively, then the composite $L_1L_2 \cong L_1 \otimes_{Q(i)} L_2$ is a maximal subfield of D. If L_1 and L_2 are abelian over Q, then so is L_1L_2. Conversely, if D has a maximal subfield L abelian over Q, let M be the fixed field of the Sylow 2-subgroup H of $\mathrm{Gal}(L/Q)$, and let K be the fixed field of the complement of H. Then $M(i)$ splits D_1, K splits D_2, and these are abelian over Q.

According to the above decomposition of D, we define four sets of primes as follows:

S' = the finite set of primes $\wp$ of $Q(i)$ such that $\mathrm{ind}_{\wp}(D_2) > 1$,
S = the restrictions to Q of primes in S',
S_3 = primes $p \in S$ such that $p \equiv 3 \pmod 4$,
T = primes in S_3 such that $\mathrm{ind}_{\wp}(D_2) = 2^t$, $\wp$ a divisor of p.

Theorem 8. *Let D be a $Q(i)$-division ring of index $2^t \cdot m$, m odd. If $t = 1$, then D has maximal subfields which are abelian over Q. If $t \geq 2$, then D has maximal subfields which are abelian over Q if and only if $T = \emptyset$.*

Proof. As shown above, we may assume D has 2-power index. Assume $t = 1$. By the approximation theorem, let E/Q be a quadratic extension such that $[E_{\wp} : Q_p] = 2$ for each $p \in S$, and $\sqrt{-1} \notin E_{\wp}$ if $p = 2$ or $p \equiv 3 \pmod 4$. Then $[E(i)_{\wp} : Q(i)_{\wp}] = 2$ for each $\wp \in S'$, so $E(i)$ splits D.

Next assume $t \geq 2$ and that D has a maximal subfield L abelian over Q. Then $[L : Q] = 2^{t+1}$. Let σ denote complex conjugation restricted to L. Then $\sqrt{-1} \in L$ implies σ has order 2, and we let M denote the fixed field of σ, $[M : Q] = 2^t$. If $\mathrm{ind}_{\wp}(D) = 2^t$, and $\wp$ divides a rational prime $p \equiv 3 \pmod 4$, then $[L_{\wp} : Q(i)_{\wp}] = 2^t$, $L_{\wp} = M(i)_{\wp}$, and $M_{\wp} \cap Q(i)_{\wp} = Q_p$, with $[M_{\wp} : Q_p] = 2^t$. The unramified quadratic extension of Q_p is $Q(i)_{\wp}$, so $M_{\wp}/Q_p$ is totally and tamely ramified. Therefore $M_{\wp} = Q_p(\alpha)$, α a root of $X^{2^t} - \pi$ for some prime element π of Q_p. Then $M_{\wp}/Q_p$ is Galois, so $\mu_{2^t} \subseteq Q_p$, which contradicts $\sqrt{-1} \notin Q_p$.

Conversely, assume $\mathrm{ind}(D) = 2^t$, $t \geq 2$, and $T = \emptyset$. By the Grunwald-Wang theorem ([**A-T**, Chap. 10, Thm. 5]) let E/Q be a cyclic extension of degree 2^t with the following properties:

(i) $L_2 = Q_2(\zeta + \zeta^{-1})$, ζ a primitive 2^{t+2}-th root of unity, and

(ii) $L_{\wp}/Q_p$ is unramified of degree 2^t for odd primes $p \in S$.

Though we are in the special case of the Grunwald-Wang theorem [**A-T**, Thm. 5, Chap. 10] if $t \geq 3$, this choice of L_2 permits its use by [**A-T**, Lemma 8, p. 104]. Then $E(i)/Q(i)$ has degree 2^t, has local degree 2^{t-1} at divisors of primes in S congruent to 3 (mod 4), and has local degree 2^t over all other primes in S. So $E(i)$ is a maximal subfield of D and $\mathrm{Gal}(E(i)/Q)$ is abelian. □

Example. If D is the $Q(i)$-division ring of index 4 with invariant 0 at all primes except $\mathrm{inv}_p(D) = 1/4$, $\mathrm{inv}_q(D) = -1/4$, where p and q are the divisors of 3 and 7 in $Q(i)$, then D has no maximal subfield abelian over Q. In

particular, no maximal subfield of D is contained in a cyclotomic extension of $Q(i)$. Thus we have additional counterexamples to the conjecture considered in [**Sch2**].

As a corollary to the proof of Theorem 8, we answer the rationality question for $Q(i)/Q$ stated in the introduction.

Corollary 9. *A $Q(i)$-division ring of index n has maximal subfields of the form $E(i)$, where E/Q is cyclic of degree n, if and only if D has maximal subfields which are abelian over Q.*

We now consider maximal subfields which are Galois over Q. As in the abelian case, the existence of such subfields depends only on the local indices of the 2-component of $D_1 \otimes_{Q(i)} D_2$ at divisors of rational primes congruent to 3 (mod 4). We are now at a disadvantage in that if $L \supseteq Q(i) \supseteq Q$ is Galois, a Sylow 2-subgroup of $\mathrm{Gal}(L/Q)$ need not be a normal subgroup, and there need not exist a complementary subgroup of order m. It will turn out that some choice of L/Q yields a Galois group with these properties.

In order to show that the existence of maximal subfields of D Galois over Q does not depend on $\mathrm{ind}_{\wp}(D)$ at the prime divisor of 2, we are required to solve certain 2-adic embedding problems. We define the following groups:

$$\begin{aligned} D_{2^{t+1}} &= \langle x, y \,|\, x^{2^t} = 1,\ y^2 = 1,\ y^{-1}xy = x^{-1} \rangle,\ t \geq 1 \\ Q_{2^{t+1}} &= \langle x, y \,|\, x^{2^t} = 1,\ y^2 = x^{2^{t-1}},\ y^{-1}xy = x^{-1} \rangle,\ t \geq 2 \\ SD_{2^{t+1}} &= \langle x, y \,|\, x^{2^t} = 1,\ y^2 = 1,\ y^{-1}xy = x^{-1+2^{t-1}} \rangle,\ t \geq 3. \end{aligned}$$

The presentations of the dihedral and quaternion groups as metacyclic groups are unique, but the relation $y^2 = 1$ in the presentation for the semidihedral group may be replaced by $y^2 = x^{2^{t-1}}$. We let X denote the subgroup generated by x, and similarly $Y = \langle y \rangle$.

Lemma 10. *For $t \geq 1$, $Q_2(i)/Q_2$ has an embedding in a dihedral extension of degree 2^{t+1}. For $t \geq 3$, $Q_2(i)/Q_2$ has an embedding in a semidihedral extension of degree 2^{t+1}.*

Proof. Let K denote $Q_2(i)$. Then K has the prime element $\pi = 1 - i$. For $j \geq 1$, let U^j denote the group of units of K which are congruent to 1 modulo π^j. In the direct decomposition

$$K^* = \langle \pi \rangle \times U^1,$$

U^1 is invariant under automorphisms from $Y = \mathrm{Gal}(K/Q_2)$ and is therefore a right multiplicative module for the group ring $Z_2[Y]$ of Y over the 2-adic

integers. We claim U^1 has a normal basis, i.e., that there is a 1-unit θ such that every 1-unit has a unique expression of the form $i^a\theta^b\theta^{cy}$, where $0 \le a \le 3$ and $b, c \in Z_2$. Let $\theta = 1 - 2i$, $\theta^y = 1 + 2i$. To prove the claim it suffices to show that the 1-units $i, 1 - 2i, 1 + 2i$ generate a set of representatives of each of the quotients U^j/U^{j+1}, for then they generate U^1 itself and the module structure is completely determined. Since K/Q_2 is totally ramified, each U^j/U^{j+1} has order 2, so it is enough to produce a nontrivial element of each level. In fact:

$$\begin{aligned} i &= 1 - \pi \text{ generates } U^1/U^2, \\ -1 &= 1 - i\pi^2 \text{ generates } U^2/U^3, \\ -1(1 - 2i) &= 1 + i\pi^3 \text{ generates } U^3/U^4, \\ 5 &= N(1 - 2i) = 1 - \pi^4 \text{ generates } U^4/U^5. \end{aligned}$$

It follows from [**Has**, Chap. 15, §5] that $(1 + i\pi^3)^{2^v}$ generates level $3 + 2v$, and $(1 - \pi^4)^{2^v}$ generates level $4 + 2v$. This proves the claim.

The relations $\pi^y = 1 + i = i\pi$ show that the subgroup of K^* generated by π, i is Y-invariant, with the submodule generated by θ as Y-invariant complement. Therefore if we let Γ be the subgroup of K^* generated by $(K^*)^{2^t}, \pi, i$, then K^*/Γ is Y-isomorphic to the group ring $Z_{2^t}[Y]$ of Y over $Z/2^tZ$.

By local class field theory there is a unique abelian extension $\tilde{L}/K$ such that $N_{\tilde{L}/K}(\tilde{L}^*) = \Gamma$, and one has the reciprocity isomorphism

$$r_{\tilde{L}/K} : K^*/\Gamma \xrightarrow{\sim} \mathrm{Gal}(\tilde{L}/K).$$

The Y-invariance of Γ implies that $\tilde{L}/Q_2$ is a Galois extension. Here Y acts on K^*/Γ on the right via the Galois action and Y acts on $\mathrm{Gal}(\tilde{L}/K)$ via the conjugation $\sigma \to \tau^{-1}\sigma\tau$, τ a lift of y to G_{Q_2}, and the map $r_{\tilde{L}/K}$ commutes with these actions ([**Neu3**, Prop. 2.8]). This makes $r_{\tilde{L}/K} : Z_{2^t}[Y] \to \mathrm{Gal}(\tilde{L}/K)$ an isomorphism of Y-modules. The exact sequence $0 \to Z_{2^t}[Y] \to \mathrm{Gal}(\tilde{L}/Q_2) \to Y \to 1$ is therefore split.

In the dihedral case, the conjugation $y^{-1}xy = x^{-1}$ makes X a $Z_{2^t}[Y]$-module. It is a quotient of the free module $Z_{2^t}[Y]$ by the map which sends $1 \mapsto x$. Let $L \subseteq \tilde{L}$ be the fixed field of the kernel of this map. Then $1 \to X \to \mathrm{Gal}(L/Q_2) \to \mathrm{Gal}(K/Q_2) \to 1$ is split exact, and L/Q_2 is a dihedral extension of K/Q_2. In the same way, $\tilde{L}$ contains a semidihedral extension of K/Q_2. □

We next consider cyclic extensions $L/Q(i)$ of degree 2^t for which L/Q is Galois and $\mathrm{Gal}(L/Q) = G$ is dihedral or semidihedral. These groups have

unique cyclic subgroups of index 2, and we identify $\mathrm{Gal}(Q(i)/Q)$ with G/X. Let $G_\wp = \mathrm{Gal}(L_\wp/Q_p)$ be the decomposition group of G over a rational prime $p \equiv 3 \pmod 4$. Then $\sqrt{-1} \notin Q_p$ implies that the restriction to $G_\wp$ of the canonical map $G \to G/X$ is surjective, i.e., $G_\wp$ and X generate G. This puts some restriction on the isomorphism types of subgroups which may occur as decomposition groups at such primes. We now determine these. The same remarks apply to extensions of the form $L/M(i)/M$, where $\wp$ is a divisor of p such that $\sqrt{-1} \notin M_\wp$.

Lemma 11. *For $t \geq 2$, a subgroup H of $D_{2^{t+1}}$ for which $HX = D_{2^{t+1}}$ is isomorphic to one of $D_{2^{t+1}}, D_{2^t}, \ldots, D_4$, or C_2. For $t \geq 3$, a subgroup H of $SD_{2^{t+1}}$ for which $HX = SD_{2^{t+1}}$ is isomorphic to one of $SD_{2^{t+1}}, D_{2^t}, \ldots, D_4$, $Q_{2^t}, \ldots, Q_8, C_4$, or C_2.*

Proof. Let H be generated by x^{2^i} and a preimage $x^j y$ of σ in the exact sequence

$$1 \to X \cap H \to H \to \langle \sigma \rangle \to 1,$$

where σ has order 2. If $i = 0$ then $H = D_{2^{t+1}}$ or $SD_{2^{t+1}}$. We assume $i \geq 1$, then $x^j y$ sends x^{2^i} to x^{-2^i} by conjugation. In $D_{2^{t+1}}$, $x^j y$ has order 2, so H is dihedral of order $2|X \cap H|$, unless $H \cap X = (1)$ and $H = C_2$. In $SD_{2^{t+1}}$, $(x^j y)^2 = x^{j2^{t-1}}$, so $x^j y$ has order ≤ 4, with equality if and only if j is odd. If j is odd then $(x^j y)^2 = x^{2^{t-1}}$ and H is quaternion of order $2|X \cap H|$, unless $|X \cap H| = 2$ and $H = C_4$. If j is even then $x^j y$ has order 2, and H is dihedral of order $2|X \cap H|$, unless $X \cap H = (1)$ and $H = C_2$. □

Definition. For a prime $p \equiv 3 \pmod 4$, we denote by d_p the greatest integer d such that $p \equiv -1 \pmod{2^d}$.

One has $2 \leq d_p < \infty$. For $p \equiv 3 \pmod 4$, Theorem 1 implies $D_{2^{t+1}}$ occurs as a Galois group over Q_p iff $p \equiv -1 \pmod{2^t}$ iff $t \leq d_p$, and $SD_{2^{t+1}}$ occurs iff $p \equiv -1 + 2^{t-1} \pmod{2^t}$ iff $t = d_p + 1$. For $t \geq 3$, we will refer to the following conditions on the sets of primes S_3 and T defined prior to Theorem 8, and the indices $\mathrm{ind}_\wp(D_2)$:

(a) each prime in T is congruent to $-1 \pmod{2^t}$. If $p \in S_3$ then

$$\mathrm{ind}_\wp(D_2) \leq 2^{d_p}.$$

(b) each prime in T is congruent to $-1 + 2^{t-1} \pmod{2^t}$. If $p \in S_3$, then
$p \equiv -1 \pmod{2^t} \Rightarrow \mathrm{ind}_\wp(D_2) \leq 2^{t-1}$;
$p \not\equiv -1 \pmod{2^t}$ and $p \not\equiv -1 + 2^{t-1} \pmod{2^t} \Rightarrow \mathrm{ind}_\wp(D_2) \leq 2^{d_p}$.

We now prove our main theorem.

Theorem 12. *Let D be a $Q(i)$-division ring of index $2^t \cdot m$, where $t \geq 0$ and m is odd. Then the following statements hold:*

(i) *D has maximal subfields cyclic over Q if and only if $t = 0$.*

(ii) *D has maximal subfields abelian over Q if and only if $t \leq 1$ or $T = \emptyset$.*

(iii) *D has maximal subfields Galois over Q if and only if $t \leq 2$ or $T = \emptyset$, or $T \neq \emptyset$ and condition* (a) *or* (b) *is satisfied.*

Proof. Assume D has a maximal subfield L Galois over Q, and assume $t \geq 3$. Let σ denote complex conjugation restricted to L, let H be a Sylow 2-subgroup of $G = \mathrm{Gal}(L/Q)$ containing σ, and let $M \subseteq L$ be the fixed field of H. Then $[M : Q] = m = [M(i) : Q(i)]$ and $\mathrm{Gal}(L/M(i))$ is a Sylow 2-subgroup of $\mathrm{Gal}(L/Q(i))$. If $p \in T$ then $G_\wp = \mathrm{Gal}(L_\wp/Q_p)$ contains H, where $\wp$ is some divisor of p in L, and σ is identified with an element of $H = H_\wp = \mathrm{Gal}(L_\wp/M_\wp)$. In addition, $[L_\wp : M(i)_\wp] = 2^t$ shows $M(i) \otimes_{Q(i)} D_2$ is an $M(i)$-division ring of index 2^t having L as a maximal subfield.

The unramified quadratic extension of $M_\wp$ is $M(i)_\wp$. Therefore $L_\wp^\sigma$, the subfield of $L_\wp$ fixed by σ, is a totally and tamely ramified extension of $M_\wp$ of degree 2^t. It follows that $L_\wp^\sigma = M_\wp(\alpha)$, α a root of $X^{2^t} - \pi$, π a prime element of $M_\wp$. The normal closure of $L_\wp^\sigma/M_\wp$ contains μ_{2^t}, and $t \geq 3$, so $L_\wp^\sigma/M_\wp$ is not normal. But $\mu_{2^t} \subseteq L_\wp$ and $M_\wp(\mu_{2^t})/M_\wp$ is unramified, so $\mu_{2^t} \subseteq M(i)_\wp$. If q denotes the number of elements of the residue field of $M_\wp$, it follows that 2 equals the least positive integer f such that $q^f \equiv 1 \pmod{2^t}$. Since q equals p raised to the odd power $f(M_\wp/Q_p) =$ residue degree of $M_\wp/Q_p$, we have $p \equiv q \pmod{2^t}$, and $p \equiv -1$ or $-1 + 2^{t-1} \pmod{2^t}$. Theorem 1 shows $H_\wp$ has a presentation $\langle x, y \mid x^{2^t} = 1, y^2 = x^j, y^{-1}xy = x^p \rangle$, where $j = 2^t$ or 2^{t-1}. But $\sigma \in H_\wp$ restricts to a generator of $\mathrm{Gal}(M(i)_\wp/M_\wp)$, so we take y to have order 2, $j = 2^t$. Then $H = D_{2^{t+1}}$ or $H = SD_{2^{t+1}}$ according as each prime in T is congruent to -1 or $-1 + 2^{t-1} \pmod{2^t}$.

Suppose $p \equiv -1 \pmod{2^t}$ for all $p \in T$, so that $\mathrm{Gal}(L/Q)$ has a Sylow 2-subgroup $H = \langle x, y \mid x^{2^t} = 1, y^2 = 1, y^{-1}xy = x^{-1} \rangle$. We show that condition (a) is satisfied by the indices $\mathrm{ind}_\wp(M(i) \otimes_{Q(i)} D_2) = \mathrm{ind}_\wp(D_2)$. Let $p \in S_3$, $\wp$ a divisor of p in L such that $H_\wp = H \cap G_\wp$ is a Sylow 2-subgroup of $G_\wp$, and $H_\wp$ has fixed field $M_\wp$. Then $Q(i)_\wp/Q_p$ is proper, so $H_\wp \not\subseteq \mathrm{Gal}(L_\wp/Q(i)_\wp)$. In particular, $H_\wp \not\subseteq \mathrm{Gal}(L_\wp/M(i)_\wp)$, so $\sqrt{-1} \notin M_\wp$, and H is generated by $H_\wp$ and X. Then $H_\wp$ is among the groups listed in Lemma 11. In particular, $H_\wp$ has order at most 2^{d_p+1} by Theorem 1, which implies $\mathrm{ind}_\wp(M(i) \otimes_{Q(i)} D_2) \leq 2^{d_p}$. This proves that (a) is satisfied. If $p \equiv -1 + 2^{t-1} \pmod{2^t}$ for all $p \in T$, then $H = \langle x, y \mid x^{2^t} = 1, y^2 = 1, y^{-1}xy = x^{-1+2^{t-1}} \rangle$. If $p \equiv -1 \pmod{2^t}$ and $p \in S$, then Lemma 11 and Theorem 1 show $H_\wp$ may be dihedral (or quaternion) of order at most 2^t, so that $\mathrm{ind}_\wp(D_2) \leq 2^{t-1}$. If p is congruent to neither -1 nor $-1 + 2^{t-1} \pmod{2^t}$ then similarly $\mathrm{ind}_\wp(D_2) \leq 2^{d_p}$. This

proves that (b) is satisfied.

Conversely, let $D = D_1 \otimes_{Q(i)} D_2$ as usual. Suppose L_1 is a maximal subfield of D_1 which is cyclic over Q according to Theorem 7. If L_2 is a maximal subfield of D_2 which is Galois over Q, then $L_1 L_2$ is a maximal subfield of D which is Galois over Q. So we assume $D = D_2$ has index 2^t, and $t \geq 2$ by Theorem 8.

Suppose first that $t = 2$. If $p_1, \ldots, p_s$ are the rational primes in S, then the splitting field L of $f(X) = X^4 - p_1 \cdots p_s$ has Galois group D_8 over Q, $L/Q(i)$ is cyclic of degree 4, and $[L(i)_\wp : Q(i)_\wp] = 4$ at the critical primes, so L is a maximal subfield of D which is Galois over Q.

Now let $t \geq 3$ and assume a nonempty set T which satisfies condition (a). We embed $Q(i)/Q$ in a $D_{2^{t+1}}$-extension L with prescribed behavior at the primes $p \in S$ as follows. By Lemma 10, there is an embedding of $Q_2(i)/Q_2$ in a dihedral extension L_2 of degree 2^{t+1}. If $p \in T$, the splitting field $L_\wp$ of $f(X) = X^{2^t} - p$ is a $D_{2^{t+1}}$-extension of $Q(i)_\wp/Q_p$ by Theorem 1. More generally, if $p \in S_3$ then $Q(i)_\wp/Q_p$ embeds in a dihedral extension $L_\wp/Q_p$ of degree 2^r, where $r = \min(d_p + 1, t + 1)$. If $p \in S$ and $p \equiv 1 \pmod 4$, let $L_\wp/Q_p$ be unramified of degree 2^t. These local prescriptions are consistent by Lemma 11.

If the nonempty set T satisfies (b), we embed $Q(i)/Q$ in an $SD_{2^{t+1}}$-extension L/Q with the following localizations. By Lemma 10, there is an embedding of $Q_2(i)/Q_2$ in a semidihedral extension L_2 of degree 2^{t+1}. If $p \in T$, the splitting field $L_\wp$ of $f(X) = X^{2^t} - p$ is an $SD_{2^{t+1}}$-extension of $Q(i)_\wp/Q_p$ by Theorem 1. If $p \in S$ and $p \equiv -1 \pmod{2^t}$, then $Q(i)_\wp/Q_p$ embeds in a dihedral extension $L_\wp$ of degree 2^t. For all other $p \in S_3$, $Q(i)_\wp/Q_p$ embeds in a dihedral extension $L_\wp$ of degree 2^{d_p+1}. If $p \in S$ and $p \equiv 1 \pmod 4$, let $L_\wp/Q_p$ be unramified of degree 2^t. These local prescriptions are consistent by Lemma 11.

We now solve the embedding problem, with prescribed local solutions, given by the exact sequence $1 \to X \to G \xrightarrow{j} Y \to 1$, where $Y = \mathrm{Gal}(Q(i)/Q)$ and $G = D_{2^{t+1}}$ or $G = SD_{2^{t+1}}$. Let G_Q denote the absolute Galois group of Q, and let $\phi : G_Q \to \mathrm{Gal}(Q(i)/Q)$ be the canonical map. Observe that the group extension is split for either choice of G. It follows that there is trivially a weak solution to the embedding problem, i.e., a (not surjective) homomorphism $\psi : G_Q \to G$ such that $j \circ \psi = \phi$. For $q = -1$ or $-1 + 2^{t-1}$, the conjugation $y^{-1}xy = x^q$ makes X a G_Q-module. Also G_Q acts on $X' = \mathrm{Hom}(X, \mu_{2^t})$ by $f^z(x) = f(x^{z^{-1}})^z$, $x \in X$, $z \in G_Q$. Let T' denote the fixed field of the kernel of this action. If σ_q, for q odd, denotes the automorphism of $Q(\mu_{2^t})$ defined by sending a primitive 2^t-th root of unity to its q-th power, then one may easily check that T' equals the fixed field of σ_{-1} in the dihedral case , and T' equals the fixed field of $\sigma_{-1+2^{t-1}}$ in the semidihedral case. These

fixed fields are cyclic extensions of Q. If G' denotes the Galois group of T'/Q, then G' is cyclic, in particular the decomposition groups G'_p for $p \in S$ are cyclic. It follows from [**Neu1**, Kor. 2.5, Kor. 6.4(b)] that there is a G-Galois extension L of $Q(i)/Q$ such that the completions of L at divisors of primes $p \in S$ coincide with the given fields $L_{\wp}$.

Since $[L_{\wp} : Q(i)_{\wp}]$ is a multiple of $\mathrm{ind}_{\wp}(D)$ for each $\wp \in S'$, we have shown that L is a splitting field of D, and is a maximal subfield of D which is a Galois extension of Q. □

We have two corollaries from the proof of Theorem 12.

Corollary 13. *Assume D has maximal subfields L Galois over Q, but no maximal subfields abelian over Q. Then the Sylow 2-subgroups of the Galois groups* $\mathrm{Gal}(L/Q)$ *are all dihedral or all semidihedral. In this case, L may be chosen to be the composite of a cyclic m-extension of Q with a dihedral or semidihedral extension of $Q(i)/Q$.*

Corollary 14. *Let $D = D_1 \otimes_{Q(i)} D_2$, where* $\mathrm{ind}(D_1)$ *is odd,* $\mathrm{ind}(D_2) = 2^t$. *Then D has maximal subfields cyclic, abelian, or Galois over Q if and only if the same is true for D_2.*

Examples. 1. If D is the $Q(i)$-division ring of index 8 with invariant 0 at all primes except $\mathrm{inv}_p(D) = 1/8$, $\mathrm{inv}_q(D) = -1/8$, where p and q are the divisors of 3 and 7 in $Q(i)$, then D has no maximal subfield Galois over Q. By Proposition 4, $[D]$ belongs to the image of $\mathrm{Res} : \mathrm{Br}(Q) \to \mathrm{Br}(Q(i))$. For instance, the Q-division ring Δ with invariant 0 at all primes except $\mathrm{inv}_3(\Delta) = 1/16$ and $\mathrm{inv}_7(\Delta) = -1/16$ satisfies $Q(i) \otimes_Q \Delta \cong M_2(D)$.

2. Let p_1, p_2, p_3 be distinct primes of $Q(i)$ which divide rational primes congruent to $-1 \pmod{16}$ and let p be the divisor of 3 in $Q(i)$. Let D be the $Q(i)$-division ring of index 16 having invariant 0 at all primes except $\mathrm{inv}_p(D) = 1/8$, $\mathrm{inv}_{p_j}(D) = -1/8, 1/16$, and $-1/16$ for $j = 1, 2, 3$. Then $d_3 = 2$ and $\mathrm{ind}_p(D) > 4$ show that condition (a) is not satisfied, and D has no maximal subfield Galois over Q. In terms of the proof of Theorem 12, if L/Q is any D_{32}-extension of $Q(i)/Q$, then $[L_{\wp} : Q_3(i)] \leq 4$, so $\mathrm{ind}_p(D) \leq 4$ would be implied by the existence of such a subfield.

References

[Alb] A.A. Albert, *On p-adic fields and rational division algebras*, Ann. of Math., **41** (1940), 674-693.

[A-T] E. Artin and J. Tate, *Class Field Theory*, Addison-Wesley, Reading, 1990.

[Has] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, 1980.

[Hers] I.N. Herstein, *Noncommutative Rings*, Carus Monograph, **15**, Math. Assoc. Amer., 1968.

[Mac] S. MacLane, *Symmetry of algebras over a number field*, Bull. Amer. Math. Soc., **54** (1948), 328-333.

[Neu1] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math., **21** (1973), 59-116.

[Neu2] ———, *On solvable number fields*, Invent. Math., **53** (1979), 135-164.

[Neu3] ———, *Class Field Theory*, Springer-Verlag, Berlin, 1986.

[Rein] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[Sch1] M. Schacher, *Subfields of division rings*, I, J. Algebra, **9** (1968), 451-477.

[Sch2] ———, *Cyclotomic splitting fields*, Proc. Amer. Math. Soc., **25** (1970), 630-633.

[Sh] I. Shafarevich, *On p-extensions*, Mat. Sb., **20** (1947), 351-363; Amer. Math. Soc. Transl., (Ser. 2), **4** (1956), 59-72.

Received April 29, 1994. The author is grateful for support from a Fulbright Research Fellowship from the U.S. - Israel Educational Foundation.

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY
32000 HAIFA
ISRAEL

Current address:
UNIVERSITY OF NOTRE DAME
NOTRE DAME, IN 46556