MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 171
JULY 1985, PAGES 233-242

The Construction of Unramified Cyclic Quartic Extensions of $Q(\sqrt{m})$

By Theresa P. Vaughan

Abstract. We give an elementary general method for constructing fields K satisfying $[K: Q] = 8$, the Galois group of K over Q is dihedral, and K is unramified over one of its quadratic subfields. Given an integer m, we describe all such fields K which contain $Q(\sqrt{m})$. The description is specific and is given in terms of the arithmetic of the quadratic subfields of K.

0. Introduction. In this paper we give an elementary general method for constructing fields K which have the following properties: $[K: Q] = 8$, the Galois group of K over Q is dihedral, and K is unramified over one of its quadratic subfields. Our procedure is from the ground up, so to speak: Given a quadratic field $Q(\sqrt{m})$ we describe those fields K (as above) which contain $Q(\sqrt{m})$. The description is specific and entirely in terms of the arithmetic behavior of the quadratic subfields of K.

One application of this work is in finding, for a fixed $Q(\sqrt{m})$, all of its cyclic unramified extensions of degree 4.

Results of this nature are already known for special values of m, n, and with extensions of higher degree than 4; see, e.g., [1], [3], [5]. We feel that our method is more precise and better adapted for use as an actual construction. In addition, we require no restrictions on m.

An advantage of our intrinsic construction is that it can easily be used in different ways. Thus, given m, we can describe the (infinitely many) square-free integers n such that $(m, n) = 1$ and $Q(\sqrt{nm})$ has a cyclic unramified extension of degree 4 containing $Q(\sqrt{m})$. The conditions which n must satisfy are just the necessary and sufficient conditions for the construction described in Section 2.

In Section 3 we give some assorted examples of the use of the construction.

1. Notation and Preliminaries. The notation given here will be used throughout.

Let $m \in Z$ and put $F_m = Q(\sqrt{m})$. Let $\alpha \in F_m$, with its conjugate α', and put $\alpha\alpha' = nk^2$, where n is a square-free integer.

Suppose that $n \neq 1, m$. Then $F_m(\sqrt{\alpha})$ is a field of degree 4 which is not normal over Q. Its normal closure is $K = Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{\alpha'}) = Q(\sqrt{m}, \sqrt{n}, \sqrt{\alpha})$, which has degree 8 and is normal over Q with dihedral Galois group. K contains three quadratic fields, F_m, F_n, F_{nm}, and the quartic field $J = Q(\sqrt{m}, \sqrt{n})$.

It is known [4] that the discriminant of J, $\operatorname{disc} J$, is the product of the discriminants of its three quadratic subfields. The following lemma is an immediate

Received June 7, 1984.
1980 *Mathematics Subject Classification*. Primary 12A05, 12A50.

consequence of this. (We use the notation $p^j \| t$ if $p^j \mid t$ and $p^{j+1} \nmid t$, for an integer t and a prime p.)

1.1. LEMMA. *Suppose that* $(m, n) = 1$. *Then* $\operatorname{disc} J = 2^j t^2$, *where t is an odd integer, and j is given by*

$$\begin{aligned} j = 0 &\quad \textit{iff } \{m, n, mn\} \equiv \{1,1,1\} \pmod 4, \\ j = 4 &\quad \textit{iff } \{m, n, mn\} \equiv \{1,3,3\} \pmod 4, \\ j = 6 &\quad \textit{iff } \{m, n, mn\} \equiv \{1,2,2\} \pmod 4, \\ j = 8 &\quad \textit{iff } \{m, n, mn\} \equiv \{3,2,2\} \pmod 4. \end{aligned}$$

From this it is easy to state some weak necessary conditions for our dihedral K to be unramified over one of its quadratic subfields.

1.2. LEMMA. *If K is given as above, and if K is unramified over one of its quadratic subfields, then*

(a) *K is unramified over J, that is,* $\operatorname{disc} K = (\operatorname{disc} J)^2$;

(b) *if p is an odd prime and* $p \mid \operatorname{disc} K$, *then* $p^2 \| \operatorname{disc} J$ *and* $p^4 \| \operatorname{disc} K$;

(c) *if* $2^j \| \operatorname{disc} K$, *then* $j \in \{0, 8, 12\}$.

Proof. Since $\operatorname{disc} J$ is the product of the discriminants of the three quadratic subfields, and $\operatorname{disc} K$ must be the fourth power of one of these, we have (a), and then (b) also follows. If $2^8 \| \operatorname{disc} J$, then $2^{16} \mid \operatorname{disc} K$, and this cannot be the fourth power of any quadratic discriminant. Then (c) follows from (a). □

We assume throughout that α is an integer in F_m.

The principal ideal (α) factors into prime ideals in F_m:

$$(\alpha) = P_{i_1} P_{i_2} \cdots P_{i_r} (P_{j_1} P_{j_2} \cdots P_{j_s})^2.$$

Define the ideal $S = S(\alpha)$ by $S = P_{i_1} P_{i_2} \cdots P_{i_r}$; we say that S is the square-free part of (α). Let $N(S)$ be the norm of this ideal. If p_{i_t} is the norm of P_{i_t}, then $N(S)$ is the product of these integers. If $r = 0$, then put $N(S) = 1$.

We say that α satisfies *condition* (U) if

(i) none of the p_{i_t} is an inert prime in $Q(\sqrt{m})$;

(ii) none of the p_{i_t} is ramified in $Q(\sqrt{m})$;

(iii) the p_{i_t} are all distinct.

Evidently, if α satisfies (U), then $N(S)$ is square-free and $(N(S), D_m) = 1$ (where $D_m = \operatorname{disc} F_m$).

In [8] it is shown how to find $\operatorname{disc} F_m(\sqrt{\alpha})$ in detail. We shall require some material from [8], and we shall make use of Table V from [8].

Say that α is reduced relative to a prime p if (α) is not divisible by the square of any prime divisor of the ideal (p). If β is an integer which is not reduced relative to p, then there is a reduced α and integers x, y so that $x^2\alpha = y^2\beta$; then $F_m(\sqrt{\alpha}) = F_m(\sqrt{\beta})$. We assume throughout, without loss of generality, that α is reduced relative to 2. For such α, Table V of [8] gives the integer t such that $2^t \| \operatorname{disc} F_m(\sqrt{\alpha})$. For the convenience of the reader, this table is given in Appendix 1, where it is called Table I.

1.3. LEMMA. *If we write* $\operatorname{disc} F_m(\sqrt{\alpha}) = D_m^2 D_\alpha$, *then for odd primes p one has* $p^t \| D_\alpha$ *if and only if* $p^t \| N(S)$. □

(I believe this is due to Hilbert.) Thus for any specific α the computation of our discriminant is not difficult.

It will be convenient to have a special name for a field K which has all the following properties: $[K:Q]=8$; K is normal over Q, and the Galois group of K is dihedral; K is unramified over one of its quadratic subfields. We shall say that such a K is *of Type* U.

The following list may be convenient:

$\alpha \in Q(\sqrt{m})$, α an integer;
$(\alpha) = P_{i_1}P_{i_2} \cdots P_{i_r}(P_{j_1} \cdots P_{j_s})^2$ (P_{i_t} distinct);
$N(\alpha) = nk^2$, n square-free, $n \neq 1, m$;
$J = Q(\sqrt{m}, \sqrt{n})$;
$K =$ normal closure of $Q(\sqrt{m}, \sqrt{\alpha})$;
$D_m = \operatorname{disc} Q(\sqrt{m})$;
$D_\alpha =$ relative discriminant of $Q(\sqrt{m}, \sqrt{\alpha})$ over $Q(\sqrt{m})$;
$F_m = Q(\sqrt{m})$.

2. Necessary and Sufficient Conditions. We show first that condition (U) is necessary for K to be of Type U. In a general sense, condition (U) guarantees the good behavior of all odd primes. It gives some restrictions on 2 also, but not enough.

2.1. THEOREM. *Each of the following four conditions implies that K is not of Type* U.

(a) *$N(\alpha)$ is a square in F_m;*
(b) *$N(S)$ is divisible by an inert prime p;*
(c) *$N(S)$ is divisible by a ramified prime p;*
(d) *S is divisible by both factors of a splitting prime p.*

Proof. (a) If $N(\alpha)$ is square in F_m, then $K = F_m(\sqrt{\alpha})$ is normal of degree 4.

(b) First let p be odd. Then $p^2 \| D_\alpha$, and $p \mid \operatorname{disc} K$. On the other hand, if $N(\alpha) = nk^2$, n square-free, then $p \nmid n$ and so $p \nmid \operatorname{disc} J$. By Lemma 1.2(a), K is not of Type U.

Now let $p = 2$ (then it must be that $m \equiv 5 \pmod 8$). We are assuming α reduced relative to 2, so $\alpha = 2\beta$ where $2 \nmid N(\beta)$. From Table I we have $2^6 \| \operatorname{disc} F_m(\sqrt{\alpha})$ and $2^{12} \mid \operatorname{disc} K$. But since n is odd in this case, and m is odd, $2^6 \nmid \operatorname{disc} J$ by Lemma 1.1. Then by Lemma 1.2(a), K is not of Type U.

(c) First let p be odd. Then we have $p \| D_\alpha$ and $p^3 \| \operatorname{disc} F_m(\sqrt{\alpha})$. Then $p^6 \mid \operatorname{disc} K$ and K is not of Type U by Lemma 1.2(b).

If $p = 2$, then $m \equiv 2, 3 \pmod 4$. Using Table I, we find that if $m \equiv 2 \pmod 4$, then $2^{11} \| \operatorname{disc} F_m(\sqrt{\alpha})$ and $2^{22} \mid \operatorname{disc} K$; if $m \equiv 3 \pmod 4$, then $2^9 \| \operatorname{disc} F_m(\sqrt{\alpha})$ and $2^{18} \mid \operatorname{disc} K$. In either case, K is not of Type U by Lemma 1.2(c).

(d) If p is odd, then as in (b) we find $p \nmid \operatorname{disc} J$, but $p \mid \operatorname{disc} K$.

If $p = 2$, then $m \equiv 1 \pmod 8$, and we can assume $\alpha = 2\beta$, where $N(\beta)$ is odd. Then $N(\alpha) = nk^2$, where n is odd, and, by Lemma 1.1, $2^6 \nmid \operatorname{disc} J$. But, from Table I, $2^6 \| \operatorname{disc} F_m(\sqrt{\alpha})$ and $2^{12} \mid \operatorname{disc} K$. Thus, K is not of Type U by Lemma 1.2(a). □

In view of Theorem 2.1(a), we may assume from now on that $N(\alpha)$ is not square in F_m, so that $F_m(\sqrt{\alpha}, \sqrt{\alpha'})$ always has degree 8. For $N(\alpha) = nk^2$, this assumption implies $n \neq 1$, $n \neq m$.

The necessity of condition (U) has been established. We shall see that if α satisfies (U) and $N(\alpha) = nk^2$ with n square-free, then $(n, D_m) = 1$, and if K is to be of Type

U, it must be unramified over F_{mn}. The first order of business is to show that the odd primes behave properly when α satisfies (U).

2.2. THEOREM. *Let α satisfy* (U) *with $N(\alpha) = nk^2$, n square-free. If p is any odd prime divisor of mn, then $p^2 \| \operatorname{disc} J$ and $p^4 \| \operatorname{disc} K$.*

Proof. First suppose that $p \mid n$. Then $(p) = P_1 P_2$ in F_m, $P_1 \neq P_2$, since p is a splitting prime in F_m by (U). Certainly $p \nmid m$, and we have $p \| N(S)$. Letting $L = F_m(\sqrt{\alpha})$, we have $p \| \operatorname{disc} L$ by Lemma 1.3.

In L the ideal P becomes a square, and the ideal P' remains prime. In L the norm of P' is p^2. In F_m we have $(\alpha, p) = P$ and $(\alpha', p) = P'$ (where α' is the conjugate of α), and so in L the square-free part of (α') is divisible by P'. Then the relative discriminant D of $K = L(\sqrt{\alpha'})$ over L is divisible by precisely p^2; $p^2 \| D$. Now $\operatorname{disc} K = (\operatorname{disc} L)^2 D$, so we have $p^4 \| \operatorname{disc} K$.

Since $(N(S), D_m) = 1$, then for every odd prime divisor q of m we have $q^2 \| \operatorname{disc} L$ and $q^4 \| \operatorname{disc} K$. Now the same is true for every odd prime divisor of mn. □

The behavior of 2 is considerably more complicated, particularly in case 2 is a splitting prime.

2.3. THEOREM. *Suppose that $m \equiv 2, 3 \pmod 4$ or $m \equiv 5 \pmod 8$. Then a necessary condition for K to be of Type* U *is that for some integer β in F_m, we have $\alpha \equiv \beta^2 \pmod 4$, and $N(\alpha)$ is odd.*

Proof. We use Table I extensively. Put $L = F_m(\sqrt{\alpha})$, and let D_α be the relative discriminant of L over F_m. First let $N(\alpha)$ be odd and $\alpha \equiv \beta^2 \pmod 4$. It is shown in [8] that, in this situation, D_α is odd.

Since $\alpha' \equiv (\beta')^2 \pmod 4$, then also the relative discriminant of $L(\sqrt{\alpha'})$ over L is odd. Then for $m \equiv 2 \pmod 4$, we have $2^{12} \| \operatorname{disc} K$; for $m \equiv 3 \pmod 4$, $2^8 \| \operatorname{disc} K$; and for $m \equiv 5 \pmod 8$, $\operatorname{disc} K$ is odd.

Now let $m \equiv 2 \pmod 4$ and $\alpha \not\equiv \beta^2 \pmod 4$. Write $\alpha = a + b\sqrt{m}$. If a is odd, b is even, and $a + b \equiv 1 \pmod 4$, then $\alpha \equiv \beta^2 \pmod 4$; otherwise, not. If a is odd, b is even, and $a + b \equiv 3 \pmod 4$, then $2^8 \| \operatorname{disc} L$ and $2^{16} \mid \operatorname{disc} K$. If a and b are odd, then $2^{10} \| \operatorname{disc} L$ and $2^{20} \mid \operatorname{disc} K$. In both cases, K is not of Type U by Lemma 1.2(c). If a is even, b odd, then K is not of Type U by Theorem 2.1(c). (If a, b are even, then α is not reduced relative to 2.)

Let $m \equiv 3 \pmod 4$ and write $\alpha = a + b\sqrt{m}$. If a is odd and $b \equiv 0 \pmod 4$, then $\alpha \equiv \beta^2 \pmod 4$; otherwise, not. Say that $2^j \| D_\alpha$. If a is odd and $b \equiv 2 \pmod 4$, then $j = 6$. If a is even, b odd, then $j = 8$. In both cases, $N(\alpha) \equiv 1 \pmod 4$ and $2^4 \| \operatorname{disc} J$. Thus, by Lemma 1.2(a), K is not of Type U. If a and b are both odd and α is reduced relative to 2, then K is not of Type U by Theorem 2.1(c).

Let $m \equiv 5 \pmod 8$ and write $\alpha = a + b\Delta$, where $\Delta = (1 + \sqrt{m})/2$. If $N(\alpha) \equiv 1 \pmod 4$ but $\alpha \not\equiv \beta^2 \pmod 4$, then we have $\operatorname{disc} L$ is even, while $\operatorname{disc} J$ is odd; then K is not of Type U. Suppose $N(\alpha) \equiv 3 \pmod 4$, so that $2^4 \| \operatorname{disc} J$. From Table I we have $2^4 \| \operatorname{disc} L$. Since $K = J(\sqrt{\alpha})$, the relative discriminant of K over J will be even *unless* $\alpha \equiv \gamma^2 \pmod 4$ for some $\gamma \in J$. A square in J can be written as (recall $N(\alpha) = nk^2$)

$$(u + v\sqrt{n})^2 = u^2 + nv^2 + 2uv\sqrt{n}$$

where $u, v \in F_m$. In order that $\alpha \equiv (u + v\sqrt{n})^2 \pmod 4$ in J, either u or v must be a multiple of 2, since 2 is prime in F_m. Then either $\alpha \equiv u^2 \pmod 4$ or $\alpha \equiv nv^2 \equiv -v^2 \pmod 4$ in F_m. But $\alpha \not\equiv u^2 \pmod 4$ in F_m, and if $\alpha \equiv -v^2 \pmod 4$ in F_m, then $N(\alpha) \equiv 1 \pmod 4$, contradicting $N(\alpha) \equiv 3 \pmod 4$. Then $\operatorname{disc}(K/J)$ is even; $2^9 \mid \operatorname{disc} K$, and K is not of Type U by Lemma 1.2(a). □

2.4. THEOREM. *Let $m \equiv 2, 3 \pmod 4$ or $m \equiv 5 \pmod 8$. Then K is of Type* U *if and only if α satisfies condition* (U) *and $\alpha \equiv \beta^2 \pmod 4$ in F_m. If K is of Type* U, *then it is unramified over F_{mn} and not over F_m or F_n.*

Proof. The necessity has already been shown, so let α satisfy (U) and $\alpha \equiv \beta^2 \pmod 4$. Then $N(\alpha) \equiv 1 \pmod 4$; $n \equiv 1 \pmod 4$. By assumption, $N(\alpha) = nk^2$ is not a perfect square, so n must have prime divisors and also $(n, D_m) = 1$ (by (U)). Then K must ramify over F_m. If $m \equiv 2, 3 \pmod 4$ then $\operatorname{disc} K$ is even, and K ramifies over F_n. If $m \equiv 5 \pmod 8$, then m has prime divisors, and since $(n, D_m) = 1$, then K must ramify over F_n.

The previous results allow the computation of $\operatorname{disc} K$, and we now compare this with D_{mn}^4. In view of Theorem 2.2, we only have to check the powers of 2. If $m \equiv 2 \pmod 4$, then $nm \equiv 2 \pmod 4$ and $2^{12} \parallel D_{nm}^4$. From the proof of Theorem 2.3, $2^{12} \parallel \operatorname{disc} K$. We also have $\operatorname{disc} J = D_{nm}^2$, and the relative discriminant of K over J is one (it certainly cannot be -1); thus $\operatorname{disc} K = (D_{nm})^4$. If $m \equiv 3 \pmod 4$, then $nm \equiv 3 \pmod 4$ and $2^8 \parallel D_{nm}^4$; $2^8 \parallel \operatorname{disc} K$, and again $\operatorname{disc} K = D_{nm}^4$. If $m \equiv 5 \pmod 8$, then all our discriminants are odd and $\operatorname{disc} K = D_{nm}^4$. □

If $m \equiv 1 \pmod 8$, then 2 is a splitting prime, and there are more possibilities for α. Write $\alpha = a + b\Delta$, where $\Delta = (1 + \sqrt{m})/2$.

2.5. THEOREM. *Let $m \equiv 1 \pmod 8$. Then K is of Type* U *if and only if α satisfies condition* (U) *and one of the following*:

(a) $\alpha \equiv \beta^2 \pmod 4$ (*i.e.*, $a \equiv 1, b \equiv 0 \pmod 4$);

(b) $N(\alpha) \equiv 3 \pmod 4$ (*i.e.*, $(a, b) \equiv (1,2)$ *or* $(3,2) \pmod 4$);

(c) $N(\alpha) \equiv 2 \pmod 4$, *and the equation $r^2 - \alpha s^2 \equiv 0 \pmod 4$ is solvable for some $r, s \in F_m$, with $r \equiv 0 \pmod 2$* (*i.e.*, *for $m \equiv 9 \pmod{16}$, $(a, b) \equiv (0,3)$ or $(3,1) \pmod 4$; for $m \equiv 1 \pmod{16}$, $(a, b) \equiv (2,3)$ or $(1,1) \pmod 4$*).

Proof. We use Table I. (a) If $N(\alpha) \equiv 1 \pmod 4$, then $\operatorname{disc} J$ is odd, and a necessary condition for K to be of Type U is $\alpha \equiv \beta^2 \pmod 4$. Since $N(\alpha)$ is not square, then $n \neq 1$. Then both m and n have prime divisors; since $(m, n) = 1$, K ramifies over both F_m and F_n. As in Theorem 2.4, when $N(\alpha) \equiv 1 \pmod 4$, then K is of Type U if and only if α satisfies (U) and $\alpha \equiv \beta^2 \pmod 4$; then $\operatorname{disc} K = (D_{mn})^4$.

(b) Let $N(\alpha) \equiv 3 \pmod 4$, so $n \equiv 3 \pmod 4$ and $2^4 \parallel \operatorname{disc} J$. In J we have the congruences

$$1 + 2\Delta \equiv (1 + \Delta + \Delta\sqrt{n})^2 \pmod 4,$$

$$3 + 2\Delta \equiv (\Delta + n + \Delta\sqrt{n})^2 \pmod 4.$$

If $N(\alpha) \equiv 3 \pmod 4$, then $\alpha = a + b\Delta$, with $(a, b) \equiv (1,2)$ or $(3,2) \pmod 4$, and there is a γ in J so that $\alpha \equiv \gamma^2 \pmod 4$. $N(\alpha)$ is odd, so the relative discriminant of

$J(\sqrt{\alpha})$ over J is odd. Hence, $2^8 \| \operatorname{disc} K$. Evidently K ramifies over F_m and, since $(m, n) = 1$, over F_n also. As before, we find $\operatorname{disc} K = (D_{mn})^4$, and K unramified over F_{nm}, when α satisfies (U).

(c) Let $N(\alpha) \equiv 2 \pmod 4$ and write $(2) = PP'$, where $P \| (\alpha)$ and $P' \| (\alpha')$. If $r^2 - \alpha s^2 \equiv 0 \pmod 4$ is only solvable with $r \equiv 0 \pmod 2$, then $2^5 \| \operatorname{disc} F_m(\sqrt{\alpha})$. Put $L = F_m(\sqrt{\alpha})$. Then P' remains prime in L, and the equation $u^2 - \alpha' v^2 \equiv 0 \pmod 4$ requires at least $P' \mid (u)$. Then the relative discriminant of $L(\sqrt{\alpha'})$ will be divisible by at least the power of 2 dividing $N(P')N(\alpha')$, where these are norms in L; this number is 2^6. Then at least $(2^5)^2 \cdot (2^6)$ divides $\operatorname{disc} K$, and K is not of Type U.

On the other hand, if $N(\alpha) \equiv 2 \pmod 4$, and if the equation $r^2 - \alpha s^2 \equiv 0 \pmod 4$ is solvable with some $r \not\equiv 0 \pmod 2$, then it is solvable with some $r \in P - P^2$, $r \notin P'$ (see [8] for details). In this case, $2^3 \| \operatorname{disc} L$. In L we have $(r')^2 - \alpha'(s')^2 \equiv 0 \pmod 4$, where $r' \in P' - P'^2$, $r' \notin P$. Now the power of 2 dividing the relative discriminant of $L(\sqrt{\alpha'})$ over L cannot exceed the power of 2 dividing $N(P'^2)N(\alpha')$, which is 2^6 (the norms are in L). The power of 2 dividing $\operatorname{disc} K$ is no more than $(2^3)^2(2^6) = 2^{12}$. We also have $2^6 \| \operatorname{disc} J$, and then $2^{12} \| \operatorname{disc} K$. As before, if, in addition, α satisfies (U), then K ramifies over F_m and F_n and is unramified over F_{nm}. □

3. Applications. Using the construction directly, it is simple to churn out theorems like the following:

3.1. THEOREM. *Let $m \equiv 2 \pmod 4$ and suppose $a^2 - mb^2 = nk^2 \equiv 1 \pmod 4$ (where n is square-free). If $(n, m) = 1$, then $Q(\sqrt{nm})$ has a cyclic unramified extension of degree 4 over $Q(\sqrt{nm})$, containing $Q(\sqrt{m})$.*

Proof. If $a^2 - mb^2 \equiv 1 \pmod 4$, then a is odd and b is even. Thus one of $a + b$, $-a - b$ is $\equiv 1 \pmod 4$, so one of $a + b\sqrt{m}$, $-a - b\sqrt{m}$ is a square (mod 4), and the result follows. □

Examples. Let $m = 2$. Since $1 - 2 \cdot 4^2 = -31$, $Q(\sqrt{-62})$ has a cyclic unramified extension of degree 4 (and 4 divides the class number). The same thing is true for $Q(\sqrt{-14})$ $(-7 = (-1)^2 - 2 \cdot 2^2)$, $Q(\sqrt{-46})$ $(-23 = 9 - 2 \cdot 16)$, $Q(\sqrt{-254})$ $(1 - 2 \cdot 64 = -127)$ and so on.

3.2. THEOREM. *If $a^2 - 3b^2 = n \equiv 1 \pmod{12}$ with a odd, $b \equiv 0 \pmod 4$, then $Q(\sqrt{3n})$ has a cyclic unramified extension of degree 4 containing $\sqrt{3}$. Then $Q(\sqrt{3n})$ has an unramified abelian extension of degree 16.*

Proof. The first statement follows from Section 2. Since we have a cyclic unramified extension of degree 4 containing $\sqrt{3}$, then we can adjoin $\sqrt{n}$ without any further ramifying, which produces a field of degree 8. We can also adjoin $\sqrt{-3}$ without ramifying, and so we get a field of degree 16.

The reverse question is also interesting. For which square-free integers k is there a field K of degree 8, normal over Q, with dihedral Galois group, and K unramified over $Q(\sqrt{k})$? Evidently, it is necessary and sufficient that $k = mn$, where m, n "fit" into the theorems of Section 2, but this is rather complicated. The following necessary condition is easy to see and to use.

3.3. THEOREM. *Let $k \in Z$ be square-free. If there is a K as described in the previous paragraph, then it must be that*

(a) $k = mn$, $m \neq 1$, $n \neq 1$, and $m \equiv 1$ (4) for some integers m, n;

(b) every prime factor of n is a splitting prime in $Q(\sqrt{m})$ (and vice versa).

Proof. If (a) does not hold, then $Q(\sqrt{k})$ does not even have an unramified quadratic extension. If (b) does not hold, then no $\alpha \in Q(\sqrt{m})$ can satisfy condition (U). □

Example. Let $k = \pm 330 = \pm 2 \times 3 \times 5 \times 11$. The factors congruent to 1 (mod 4) are 5, −3, −11, $3 \cdot 5 \cdot 11$, $-5 \cdot 11$, $3 \cdot 11$, $-3 \cdot 5$. It is easy to check that with each of these choices of m, the corresponding factor n does not satisfy (b), so there is no K of Type U unramified over $Q(\sqrt{330})$ (or $Q(\sqrt{-330})$).

In the next example we show how to find K, if it exists.

Let $k = \pm 5 \times 11 \times 19$. The divisors congruent to 1 (mod 4) are (a) −11, (b) -11×5, (c) 5, (d) -19×5, (e) −19, (f) 11×19, (g) $5 \times 11 \times 19$, and we consider each in turn.

For $m \equiv 1$ (mod 4), put $w = (1 + \sqrt{m})/2$.

(a) In $Q(\sqrt{-11})$, 19 does not split.

(b) In $Q(\sqrt{-11 \times 5})$, 19 does not split.

(c) In $Q(\sqrt{5})$, 11 and 19 split; $N(3 + w) = 11$, $N(1 + 5w) = -19$, $N(4 + w) = 19$, $N(1 + 4w) = -11$. We find

$$\begin{aligned}(3 + w)(4 + w) &= 13 + 8w \equiv 1 \ (4),\\ (3 + w)(4 + w') &= 14 + w,\\ (1 + 4w)(4 + w) &= 8 + 21w,\\ (1 + 4w)(4 + w') &= 1 + 15w.\end{aligned}$$

Since $5 \equiv 5$ (16), then $\alpha = a + bw$ is congruent to an odd square (mod 4) if and only if $(a, b) \equiv (1,0),(1,1),(2,3)$ (mod 4). Then we have

$$Q(\sqrt{5}, \sqrt{13 + 8w}, \sqrt{13 + 8w'})$$

is a K of Type U, unramified over $Q(\sqrt{5 \times 11 \times 19})$; $Q(\sqrt{-5 \times 11 \times 19})$ has no such K *containing* $\sqrt{5}$.

(d) If $m = -19 \times 5$, then 11 splits, and $N(1 + 2w) = 11 \times 9 \equiv 3$ (4). Here, $m \equiv 1$ (8), and so $Q(\sqrt{-19 \times 5}, \sqrt{1 + 2w}, \sqrt{1 + 2w'})$ is a K of Type U, containing $\sqrt{-19 \times 5}$, unramified over $Q(\sqrt{-5 \times 11 \times 19})$. Since all norms in $Q(\sqrt{m})$ are nonnegative, there is no such K containing $Q(\sqrt{19 \times 5})$ and unramified over $Q(\sqrt{5 \times 11 \times 19})$.

(e) In $Q(\sqrt{-19})$, $N(2 + w) = 11$ and $N(w) = 5$. Since $-19 \equiv 13$ (mod 16), the odd squares (mod 4) are $a + bw \equiv 1, 3 + w, 3w$ (mod 4). We find

$$w(2 + w) = -5 + 3w, \qquad w'(2 + w) = 7 - 2w.$$

So none of these or their conjugates is congruent to a square mod 4. Then $Q(\sqrt{-19})$ (which has class number one) has no elements of norm 55 and congruent to a square mod 4; there is *no* K of Type U containing $Q(\sqrt{-19})$ and unramified over $Q(\sqrt{-19 \times 11 \times 5})$, or over $Q(\sqrt{19 \times 11 \times 5})$ either (since $Q(\sqrt{-19})$ has no elements of negative norm).

(f) If $m = 11 \times 19$, we already know what happens if $n = 5$. We check $n = -5$. Fortunately, $Q(\sqrt{209})$ has class number 1. We find $5 = N(27 + 4w)$. The fundamental unit has norm $+1$; it is $\zeta = 43331 + 6440w \equiv 3$ (4), so $\zeta \cdot (27 + 4w) \equiv 1$ (4), and

$$K = Q\left(\sqrt{11 \times 19}, \sqrt{\zeta \cdot (27 + 4w)}, \sqrt{\zeta' \cdot (27 + 4w')}\right)$$

is of Type U, unramified over $Q(\sqrt{5 \times 11 \times 19})$ and contains $Q(\sqrt{11 \times 19})$. Since $Q(\sqrt{209})$ contains no numbers of norm -5 there is no such K unramified over $Q(\sqrt{-5 \times 11 \times 19})$.

(g) Since $11 \equiv 3 \pmod 4$ we cannot solve the equation $-x^2 = y^2 - 1045z^2$ in integers. Then there is no K of Type U, unramified over $Q(\sqrt{-5 \times 11 \times 19})$ and containing $Q(\sqrt{-1})$.

In conclusion, $L_1 = Q(\sqrt{5 \times 11 \times 19})$ has just one cyclic unramified extension K_1 of degree 4, and $\sqrt{5} \in K_1$. $L_2 = Q(\sqrt{-5 \times 11 \times 19})$ also has just one, K_2, and $\sqrt{11} \in K_2$.

The unramified quadratic extensions of L_1 are $L_1(\sqrt{5})$, $L_1(\sqrt{-11})$, $L_1(\sqrt{-19})$, and so $K_1(\sqrt{-11})$ is an abelian unramified extension of L_1 of degree 8, with Galois group $C(2) \times C(4)$.

Appendix 1. Let Z be a square-free integer. Let $w = \sqrt{Z}$ if $Z \equiv 2,3 \pmod 4$ and $w = (1 + \sqrt{Z})/2$ if $Z \equiv 1 \pmod 4$. Then $\{1, w\}$ is an integral basis for $Q(\sqrt{Z})$. Let $\alpha = n + mw$ and let S be the ring of integers of the field $Q(\sqrt{\alpha})$. Assume that α is reduced relative to 2, that is, the principal ideal (α) is not divisible by the square of any prime factor of (2). The discriminant of S, disc S, is the absolute discriminant (over Q).

TABLE I

(a) $Z \equiv 2 \pmod 4$

n	m		Exact power of 2 dividing disc S
odd	even	$n + m \equiv 1 \pmod 4$	2^6
odd	even	$n + m \equiv 3 \pmod 4$	2^8
odd	odd		2^{10}
even	odd		2^{11}

(b) $Z \equiv 3 \pmod 4$

n	m	Exact power of 2 dividing disc S
odd	$4j$	2^4
odd	$4j + 2$	2^6
even	odd	2^8
odd	odd	2^9

(c) $Z \equiv 5 \pmod{16}$

n	m	Exact power of 2 dividing disc S
$4k+1$	$4j$	
$4k+1$	$4j+1$	$2 \nmid$ disc S
$4k+2$	$4j+3$	
all others with n, m not both even		2^4
$2k$	$2j$ (j,k not both even)	2^6

(d) $Z \equiv 13 \pmod{16}$

n	m	Exact power of 2 dividing disc S
$4k+1$	$4j$	
$4k+3$	$4j+1$	$2 \nmid$ disc S
$4k$	$4j+3$	
all others with n,m not both even		2^4
$2k$	$2j$ (j,k not both even)	2^6

(e) $Z \equiv 8y+1$

n	m	Exact power of 2 dividing disc S
$4k+1$	$4j$	$2 \nmid$ disc S
$4k+3$	$4j+2$	2^2
$4k+1$	$4j+2$	2^2
$4k+3$	$4j$	2^4
$2k$	$4j+1$ ($k-y$ odd)	2^5
$2k+1$	$4j+3$ ($k-y$ odd)	2^5
All others with $2 \| N(n+mw)$		2^3
$4k+2$	$4j$	2^6

Department of Mathematics
University of North Carolina at Greensboro
Greensboro, North Carolina 27412

1. HARVEY COHN, "Cyclic-sixteen class fields for $Q(-p)^{1/2}$ by modular arithmetic," *Math. Comp.*, v. 33, 1979, pp. 1307–1316.

2. HARVEY COHN, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York, 1978.

3. HARVEY COHN, "The explicit Hilbert 2-cyclic class field for $Q(\sqrt{-p})$," *J. Reine Angew. Math.*, v. 321, 1981, pp. 64–77.

4. DANIEL A. MARCUS, *Number Fields*, Springer-Verlag, New York, 1977.

5. L. RÉDEI & H. REICHARDT, "Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers," *J. Reine Angew. Math.*, v. 170, 1934, pp. 69–74.

6. A. SCHOLZ, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *J. Reine Angew. Math.*, v. 166, 1932, pp. 201–203.

7. B. L. VAN DER WAERDEN, *Modern Algebra*, Ungar, New York, 1953.

8. THERESA P. VAUGHAN, "The discriminant of a quadratic extension of an algebraic field," *Math. Comp.*, v. 40, 1983, pp. 685–707.