ACTA ARITHMETICA
XXX (1976)

Parametric form of an eight class field

by

HARVEY COHN* (New York, N. Y.)
and GEORGE COOKE** (Ithaca, N. Y.)

1. Introduction. Let p be a positive prime, $p\equiv 1 \pmod 8$. Earlier work by Barrucand and Cohn [1], [2] dealt with $h(-p)$ the class number of the field[1]

$$k_2 = \boldsymbol{Q}(\sqrt{-p}). \tag{1.1}$$

It was shown that the representation

$$p = x_0^2+8y_0^2 \tag{1.2}$$

determines whether $h(-p)\equiv 0$ or $h(-p)\equiv 4 \pmod 8$, according as y_0 is even or odd. Nevertheless no natural way emerged for constructing the eight class field (i.e., the class field whose ideal group consists of classes which are eighth powers).

The two class field (the genus field) and the four class field are classically known to be ([9], [2])

$$k_4 = k_2(i), \qquad k_8 = k_4(\sqrt{\varepsilon}) \tag{1.3}$$

where ε denotes the fundamental unit of $\boldsymbol{Q}(\sqrt{p})$ $(\varepsilon\varepsilon' = -1)$. In this paper we construct the eight class field of k_2, namely

$$k_{16} = k_8\left(\sqrt{(f+\sqrt{-p})\,(1-i)\sqrt{\varepsilon}}\right) \tag{1.4}$$

where e and f are integral solutions of

$$-p = f^2-2e^2; \qquad e>0, \qquad f\equiv -1 \pmod 4). \tag{1.5}$$

Historically the first such class field was found by Weber [13] using complex multiplication, for the prime $p = 41\ (= 3^2+8\cdot 2^2)$. Here $h(-p) = 8$ and (ignoring minor misprints in [13]) the value of the Weber function

* Supported in part by NSF Research Grant GP-33910.

** Supported in part by NSF Research Grant GP-33960X. Second author currently at Mathematics Department, University of Maryland, College Park, Md., U.S.A.

[1] Subscripts indicate the degree of the field over $\boldsymbol{Q}$.

appears as $f(\sqrt{-41})^2 = \sqrt{2}\lambda$, where

$$\lambda + 1/\lambda = \tfrac{1}{2}(\zeta + \sqrt{\zeta}), \qquad \zeta = (5+\sqrt{41})/2. \tag{1.6}$$

Thus λ is of degree 8 and, alternatively, $k_{16} = k_2(\lambda)$. Although the method of complex multiplication is still being pursued (see [12]), subsequent collections of examples (see [7], [14]) have not included further cases for such primes by any method. The class field construction in this paper was first given for $p = 41$ in lecture notes of Cooke [3].

We actually find k_{16} in the form

$$k_{16} = k_4(\sqrt[4]{\beta}), \qquad \beta = [(f+\sqrt{-p})/(1+i)]^2\varepsilon' \tag{1.7}$$

and the adjunction of a 4-th root to k_4 is the key method. The fact that k_4 contains i but not $\sqrt{i}$ indicates a limitation in attempting to cope with (say) the sixteen class field. Regardless, we note that the succession $k_2 - k_4 - k_8 - k_{16}$ is accomplished by parameters from various quadratic fields, hence the phrase "parametric form".

Finally, we determine the fundamental unit $\varepsilon = S + T\sqrt{p}$ of $\boldsymbol{Q}(\sqrt{p})$ modulo 8, as follows:

$$S \equiv h(-p) \pmod 8, \tag{1.8}$$

$$T \equiv \frac{p+1}{2} \pmod 8, \tag{1.9}$$

when S and T are chosen positively (see Theorem 4.8). For this we require the result that $T \equiv 1 \pmod 4$, due to J. C. Lagarias [10] which constitutes part of Proposition 3.4. We conclude with a traditional illustrative interpretation of the eight class field in terms of quadratic forms.

2. Ideal class groups.

In this section we start with a general theorem concerning class structure in unramified extensions of certain number fields. We apply it to the field $\boldsymbol{Q}(\sqrt{-p})$; we obtain thereby a general result about the tower of unramified 2-primary extensions of $\boldsymbol{Q}(\sqrt{-p})$ (Proposition 2.14) and a specific result about the eight class field, when it exists (Proposition 2.27). We originally proved the theorem for the prime 2; Olga Taussky communicated to us the proof given here, which is a simplification of our original proof and applies for general l.

Notation. If K is a number field, and l is a prime, $H_l(K)$ denotes the l-primary class field, i.e., the maximal unramified abelian extension of K whose degree over K is a power of l. The Galois group of $H_l(K)/K$ is just the l-primary component of the ideal class group of K, and is denoted $\mathrm{Cl}_l(K)$.

(2.1) THEOREM. *Let K be a number field, and assume $\mathrm{Cl}_l(K)$ is cyclic. Then*

$$H_l(H_l(K)) = H_l(K). \tag{2.2}$$

Proof. Let $K_1 = H_l(K)$, $K_2 = H_l(K_1)$, and consider the tower of fields $K - K_1 - K_2$. The Galois groups satisfy:

$$\mathrm{Gal}\,K_1/K \text{ is cyclic}, \qquad (\mathrm{Gal}\,K_2/K)^{ab} \approx \mathrm{Gal}\,K_1/K. \tag{2.3}$$

Therefore $\mathrm{Gal}\,K_2/K$ is a p-group which when abelianized is cyclic. By direct argument or reference to the Burnside basis theorem [4], p. 176, $\mathrm{Gal}\,K_2/K$ is cyclic. Therefore $K_2 = K_1$. ∎

Suppose K is a field such that $\mathrm{Cl}_l(K)$ is cyclic of order l^r. Consider the tower of cyclic unramified lth degree extensions.

$$K = K^{(0)} - K^{(1)} - \ldots - K^{(r)} = H_l(K). \tag{2.4}$$

Ideal extension and norm define maps

$$\mathrm{Cl}_l(K) \underset{N}{\overset{j}{\rightleftarrows}} \mathrm{Cl}_l(K^{(i)}). \tag{2.5}$$

The composition $N \circ j$ "multiplies" by l^i (see [11]). Therefore $\ker j$ has order $\leqslant l^i$. On the other hand, by Theorem 2.1, $H_l(K^{(i)}) = H_l(K)$ and so $\mathrm{Cl}_l(K^{(i)})$ has order l^{r-i}. Therefore

(2.6) COROLLARY. *The map j in (2.5) is onto with kernel $\boldsymbol{Z}/l^i$.*

We now specialize to the case where $l = 2$. Each successive field $K^{(i+1)}$ is obtained by a square-root adjunction:

$$K^{(i+1)} = K^{(i)}(\sqrt{\alpha_i}), \qquad 0 \leqslant i \leqslant r-1. \tag{2.7}$$

Since $K^{(i+1)}/K^{(i)}$ is unramified, (α_i) is an ideal square. Write

$$(\alpha_i) = \mathfrak{a}_i^2. \tag{2.8}$$

The ideal class of $\mathfrak{a}_i$ is well-defined. It must be trivial or of order 2 in $\mathrm{Cl}_2(K^{(i)})$. Suppose $i = \sqrt{-1} \in K$. Then each extension $K^{(i+2)}/K^{(i)}$ is obtainable as a 4th-root extension:

$$K^{(i+2)} = K^{(i)}(\sqrt[4]{\beta_i}), \qquad 0 \leqslant i \leqslant r-2. \tag{2.9}$$

Now, since $K^{(i+2)}/K^{(i)}$ is unramified, (β_i) is an ideal fourth power. Write

$$(\beta_i) = \mathfrak{b}_i^4. \tag{2.10}$$

The ideal class of $\mathfrak{b}_i$ is well-defined.

Since $K^{(i+1)} = K^{(i)}(\sqrt{\alpha_i}) = K^{(i)}(\sqrt{\beta_i})$, we have

$$\mathfrak{a}_i \sim \mathfrak{b}_i^2. \tag{2.11}$$

Since $K^{(i+2)} = K^{(i+1)}(\sqrt{\alpha_{i+1}}) = K^{(i+1)}(\sqrt{\sqrt{\beta_i}})$, we have

$$\mathfrak{a}_{i+1} \sim \mathfrak{b}_i \mathfrak{O}_{K^{(i+1)}}. \tag{2.12}$$

The following is an immediate consequence of (2.11), (2.12), and Corollary (2.6).

(2.13) PROPOSITION. *Assume $i \in K$. Either $\mathfrak{a}_i$ is principal for $i \geqslant 0$ or $\mathfrak{a}$ has class of order 2 for $i \geqslant 0$.*

Specialize to the case $K = k_2 = \boldsymbol{Q}(\sqrt{-p})$. The 2-primary part of the ideal class group is cyclic of order divisible by 4. As remarked in § 1, $i \in k_4 = K^{(1)}$, and $K^{(2)} = k_8 = k_4(\sqrt{\varepsilon})$. Apply Proposition (2.13) and (2.11) to k_4 to deduce the following:

(2.14) PROPOSITION. *In the case $K = k_2 = \boldsymbol{Q}(\sqrt{-p})$, each field in the tower (2.4) ($l = 2$) is obtained from the preceding one by adjoining the square root of a unit. For $i \geqslant 1$, we have $K^{(i+2)} = K^{(i)}(\sqrt[4]{\beta_i})$ where*

$$(\beta_i) = \mathfrak{b}_i^4 \tag{2.15}$$

and $\mathfrak{b}_i$ is principal or has class of order 2.

We now study the initial portion of the tower: $k_2 - k_4 - k_8 - k_{16}$. We are going to assume that k_{16} exists and see what form it must take.

(2.16) Notation. Let $\mathfrak{O}_n$ denote the integer ring and $\mathfrak{O}_n^*$ the unit group of k_n.

The field k_{16}, if it exists, is $k_4(\sqrt[4]{\beta_1})$, and since $k_8 = k_4(\sqrt{\varepsilon})$, we have

$$\beta_1 = \theta^2 \varepsilon \quad \text{for some } \theta \in k_4, \tag{2.17}$$

$$(\beta_1) = \mathfrak{b}_1^4 \quad \text{where} \quad \mathfrak{b}_1^2 \sim 1. \tag{2.18}$$

There are thus two possibilities for the ideal class of $\mathfrak{b}_1$.

Case 1. $\mathfrak{b}_1 \sim 1$. In this case $k_{16} = k_4(\sqrt[4]{\mu})$ for some unit μ. The units of k_4 are given (see [6]) by

$$\mathfrak{O}_4^* \approx \boldsymbol{Z}/4 \times \boldsymbol{Z} = \langle i \rangle \times \langle \varepsilon \rangle. \tag{2.19}$$

By (2.17), $\mu = \theta^2 \varepsilon$ for some unit θ. Therefore we need only consider the fields $k_4(\sqrt[4]{\varepsilon})$, $k_4(\sqrt[4]{-\varepsilon})$. But $k_4(\sqrt[4]{\varepsilon})$ is not Galois over k_2, because the conjugate of ε relative to k_2 is $-\varepsilon^{-1}$ and

$$\sqrt[4]{-\varepsilon^{-1}} \notin k_4(\sqrt[4]{\varepsilon}). \tag{2.20}$$

The same holds for $k_4(\sqrt[4]{-\varepsilon})$. Therefore Case 1 never occurs.

Case 2. $\mathfrak{b}_1$ has ideal class of order 2. By considering ideal extension j: $\mathrm{Cl}_2(k_2) \to \mathrm{Cl}_2(k_4)$ and applying Corollary 2.6 we see that the ideal class of $\mathfrak{b}_1$ comes from an ideal class of order 4 in $\mathrm{Cl}_2(k_2)$. There is a parametric representation of such an ideal, obtained as follows: Since $p \equiv 1 \pmod{8}$, p splits completely in $\boldsymbol{Q}(\sqrt{2})$. The latter has class number 1 and fundamental unit of norm -1. It follows that $-p$ is a norm from $\boldsymbol{Q}(\sqrt{2})$. Let e and f be solutions of (1.5). Then

$$2e^2 = f^2 + p = (f + \sqrt{-p})(f - \sqrt{-p}). \tag{2.21}$$

Since 2 is ramified in $k_2/\boldsymbol{Q}$, we let $\mathfrak{2}_1$ denote the unique prime of k_2 over 2. The class of $\mathfrak{2}_1$ is of order 2. From (2.21) we can write

$$\mathfrak{2}_1 \mathfrak{a} = (f + \sqrt{-p}), \qquad N\mathfrak{a} = e^2. \tag{2.22}$$

It follows that $\mathfrak{a}$ is the square of an odd integral ideal $\mathfrak{b}$ whose class is of order 4 in $\mathfrak{O}_2$. Therefore we can take

$$\mathfrak{b}_1 = \mathfrak{b}\mathfrak{O}_4. \tag{2.23}$$

Applying (2.18), we find

$$(\beta_1) = \mathfrak{b}_1^4 = \mathfrak{b}^4 \mathfrak{O}_4 = \mathfrak{a}^2 \mathfrak{O}_4. \tag{2.24}$$

Now $\mathfrak{2}_1$ becomes principal when extended to k_4, by Corollary (2.6). In fact, by considering the subfield $\boldsymbol{Q}(i)$ of k_4, we have

$$\mathfrak{2}_1 \mathfrak{O}_4 = (1 + i). \tag{2.25}$$

Therefore, applying (2.22), (2.24), (2.25)

$$(\beta_1) = (f + \sqrt{-p})^2 (1 + i)^{-2}. \tag{2.26}$$

Applying (2.17), we get

(2.27) PROPOSITION. *Assume $8 | h(-p)$. Then the eight class field of $k_2 = \boldsymbol{Q}(\sqrt{-p})$ is obtained by adjoining $\sqrt[4]{\beta_1}$ to k_4, where β_1 is of the form*

$$\mu^2 (f + \sqrt{-p})^2 (1 + i)^{-2} \varepsilon, \qquad \mu \in \mathfrak{O}_4^*. \tag{2.28}$$

This is as far as we wish to proceed before studying congruence properties in k_4 and k_8 in § 3.

(2.29) Remark. Since 2 is split in the subfield $\boldsymbol{Q}(\sqrt{p})$ of k_4, we can write

$$(1 + i) = \mathfrak{p}_1 \mathfrak{p}_2 \quad \text{in} \quad \mathfrak{O}_4. \tag{2.30}$$

The ideal factors $\mathfrak{p}_1$, $\mathfrak{p}_2$ of $(1+i)$ in k_4 split or are inert in k_8 according as whether or not $h(-p) \equiv 0 \pmod{8}$. For the ideal $\mathfrak{2}_1$, which has ideal class of order 2, must split completely in k_8 (the four class field of k_2) exactly when its class is a fourth power in k_2. Apply (2.17) and (2.18).

3. Congruence properties in k_4 and k_8. We let (small or large) roman letters denote elements of $\boldsymbol{Z}$ while small (and large) greek letters denote elements of $\mathfrak{O}_4$ (and $\mathfrak{O}_8$ respectively). Then the integral bases of $\boldsymbol{Z}[i]$, $\mathfrak{O}_4, \mathfrak{O}_8$ are denoted by the succession

$$(3.1)\qquad [1, i], \quad [1, i]\times[1, \omega], \quad [1, i]\times[1, \omega]\times[1, \Omega]$$

where

$$(3.2)\qquad \omega = \frac{1+\sqrt{p}}{2}, \quad \Omega = \frac{\sigma+\sqrt{\varepsilon}}{2}$$

where σ is any solution of

$$(3.3)\qquad \sigma^2 \equiv \varepsilon \ (\mathrm{mod}\ 4).$$

The choice of σ is related to the following information about ε.

(3.4) PROPOSITION. *When $p \equiv 1 \ (\mathrm{mod}\ 8)$ the fundamental unit ε of $\boldsymbol{Q}(\sqrt{p})$ satisfies $\varepsilon = S+T\sqrt{p}$, with S, $T > 0$, and $\varepsilon \equiv \sqrt{p} \ (\mathrm{mod}\ 4)$.*

Proof. The fact that $\varepsilon = S+T\sqrt{p}$, S, $T \in \boldsymbol{Z}$, is an immediate consequence of the splitting of 2 in $\boldsymbol{Q}(\sqrt{p})$. Since ε is the fundamental unit, we must have $S > 0$, $T > 0$. Since $p \equiv 1 \ (\mathrm{mod}\ 8)$, $N\varepsilon = -1$, and it follows that $S \equiv 0 \ (\mathrm{mod}\ 4)$. The fact that $T \equiv 1 \ (\mathrm{mod}\ 4)$ is due to Lagarias [10]. For completeness we present the following argument, based on an idea communicated to us by Harold Stark, due to J. Lagarias.

Proof that $T \equiv 1 \ (\mathrm{mod}\ 4)$. Noting that

$$(3.5)\qquad \varepsilon\sqrt{p} = Tp+S\sqrt{p} \equiv T \ (\mathrm{mod}\ 4),$$

there exists a unique choice of sign so that if $L = \boldsymbol{Q}(\sqrt{p})\big(\sqrt{\pm\varepsilon\sqrt{p}}\big)$, then $L/\boldsymbol{Q}(\sqrt{p})$ is unramified at even primes. Since the conjugate of $\varepsilon\sqrt{p}$ is $\frac{1}{\varepsilon}\sqrt{p}$, L is Galois over $\boldsymbol{Q}$. Since $L/\boldsymbol{Q}$ is abelian, Kronecker's theorem asserts that $L \subset \boldsymbol{Q}(\zeta_n)$ for some n where $\zeta_n = \exp(2\pi i/n)$. By construction, $L/\boldsymbol{Q}$ is ramified only at p (and perhaps at ∞). Since $[L:\boldsymbol{Q}] = 4$, we see that $L \subset \boldsymbol{Q}(\zeta_p)$. Therefore L is the field fixed by the unique subgroup H of index 4 in $\mathrm{Gal}\big(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}\big) \approx (\boldsymbol{Z}/p)^*$. Since $p \equiv 1 \ (\mathrm{mod}\ 8)$, $-1 \in H$ and so L is real. It follows that the plus sign is the correct sign in the definition of L and so $T \equiv 1 \ (\mathrm{mod}\ 4)$. ■

Since $k_8 = k_4(\sqrt{\varepsilon})$ and k_8/k_4 is unramified, an integral bases for $\mathfrak{O}_8$ is given by (3.2), (3.3).

(3.6) LEMMA. $\sigma \equiv i\big(1+(1+i)\omega\big) \ (\mathrm{mod}\ 2)$.

Proof. First note that if $\lambda \in \mathfrak{O}_4$ and λ is odd, then, in $\mathfrak{O}_4$,

$$(3.7)\qquad \lambda^2 \equiv \pm 1, \ \pm(2\omega-1) \ (\mathrm{mod}\ 4),$$

$$(3.8)\qquad \lambda^4 \equiv 1 \ (\mathrm{mod}\ 8).$$

These are obtained by observing that the odd residue classes (mod 2) in $\mathfrak{O}_4$ are

$$(3.9)\qquad \{1, i\}\times\{1, 1+(1+i)\omega\}$$

and that if $\lambda_1 \equiv \lambda_2 \ (\mathrm{mod}\ 2)$, then $\lambda_1^2 \equiv \lambda_2^2 \ (\mathrm{mod}\ 4)$, $\lambda_1^4 \equiv \lambda_2^4 \ (\mathrm{mod}\ 8)$, etc. Since $\varepsilon = S+T\sqrt{p} \equiv +2\omega-1 \ (\mathrm{mod}\ 4)$, one sees that Lemma (3.6) is the only possibility by squaring the residue classes (3.9). ■

According to Remark (2.29), $8 \mid h(-p)$ if and only if the even primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathfrak{O}_4$ split in k_8/k_4. The Hilbert condition for splitting [9] in this case is solvability of the congruence

$$(3.10)\qquad \varepsilon \equiv \sigma^2 \ \mathrm{mod}\ 4(1+i), \quad \sigma \in \mathfrak{O}_4.$$

(3.11) LEMMA. *The congruence* (3.10) *is solvable if and only if*

$$(3.12)\qquad S-T+\frac{p+1}{2} \equiv 0 \ (\mathrm{mod}\ 8).$$

Proof. To determine solvability of (3.10), we consider the aggregate of odd residue classes modulo $2(1+i)$, namely

$$(3.13)\qquad \{\pm 1, \pm i\}\times\{1, 1+(1+i)\omega, 1+(1-i)\omega, 1+2\omega\}.$$

A solution of (3.10) is in particular a solution of (3.3). Therefore, by Lemma (3.6), referring also to (3.13), we have that if σ solves (3.10) then

$$(3.14)\qquad \sigma \equiv \pm i\big(1+(1\pm i)\omega\big) \ \mathrm{mod}\ 2(1+i).$$

Squaring,

$$(3.15)\qquad \sigma^2 \equiv -\frac{p+1}{2}+2\omega \ \mathrm{mod}\ 4(1+i).$$

Therefore σ^2, as well as ε, lies in $\boldsymbol{Q}(\sqrt{p})$ modulo $4(1+i)$. But since 2 is unramified in that field, the modulus escalates from $4(1+i)$ in (3.15) to 8; and (3.10) is solvable if and only if

$$(3.16)\qquad \varepsilon \equiv -\frac{p+1}{2}+2\omega \ \mathrm{mod}\ 8.$$

This leads to (3.12) upon equating coefficients of the basis $[1, \omega]$ for $\boldsymbol{Q}(\sqrt{p})$. ■

Finally we have a lemma concerning solvability of a congruence in $\mathfrak{O}_8$.

(3.17) LEMMA. *If $h(-p) \equiv 0 \ (\mathrm{mod}\ 8)$, then the congruence*

$$(3.18)\qquad \Xi^4 \equiv \gamma \ \big(\mathrm{mod}\ 4(1+i)\big)$$

is solvable for odd $\gamma \in \mathfrak{O}_4$ (and $\Xi \in \mathfrak{O}_8$) only when $\gamma \equiv 1 \ \big(\mathrm{mod}\ 4(1+i)\big)$.

Proof. First of all, assume $\Gamma^2 \equiv \gamma \pmod{4(1+i)}$ is solvable, $\Gamma \in \mathfrak{O}_8$. Writting $\Gamma = \alpha_1+\beta_1\Omega$, compute

$$\Gamma^2 = \alpha_1^2+\beta_1^2\left(\frac{\varepsilon-\sigma^2}{4}\right)+(2\alpha_1\beta_1+\beta_1^2\sigma)\,\Omega .$$

Since $\gamma \in \mathfrak{O}_4$, the congruence mod $4(1+i)$ implies

$$(3.19) \qquad 2\alpha_1\beta_1+\beta_1^2\sigma \equiv 0 \pmod{4}.$$

Since σ is odd, it follows from (3.19) that

$$(3.20) \qquad 2\,|\,\beta_1 .$$

Now assume (3.18) is solvable, and set

$$(3.21) \qquad \Xi^2 = \Gamma .$$

Write $\Xi = \alpha_2+\beta_2\Omega$, and equate coefficients of Ω in (3.21). It follows that

$$(3.22) \qquad 2\alpha_2\beta_2+\beta_2^2\sigma = \beta_1 .$$

Now apply (3.20) and deduce that $2\,|\,\beta_2^2\sigma$. Since σ is odd, this forces

$$(3.23) \qquad (1+i)\,|\,\beta_2, \quad \Xi = \alpha_2+\beta_2'(1+i)\,\Omega .$$

Since γ is assumed odd, so is Ξ, so α_2 is odd. Compute Ξ^4, and obtain

$$(3.24) \qquad \gamma \equiv \Xi^4 \equiv \alpha_2^4 \equiv 1 \pmod{4}$$

applying (3.23) and (3.8).

Assume, contrary to our desired conclusion, that in (3.18), $\gamma \not\equiv 1 \bmod 4(1+i)$. Write $\Xi^4-\alpha_2^4 = 4\Lambda$ (use (3.24)); then, since (3.8) has modulus 8, $\Lambda \not\equiv 0 \bmod (1+i)$. Expanding Ξ^4, and reducing mod $4(1+i)$, we find, using (3.23),

$$(3.25) \qquad \Lambda \equiv \alpha_2^2\beta_2'^2\Omega^2+\beta_2'^4\Omega^4 \not\equiv 0 \bmod (1+i),$$

so β_2' is also odd. Now in k_8, $(1+i)$ has 4 prime factors (by Remark (2.29), and our assumption $h(-p) \equiv 0 \pmod{8}$), each of degree 1. For one of them, (say) $\mathfrak{P}$, $\Lambda \equiv 1 \pmod{\mathfrak{P}}$. Then, from (3.25),

$$(3.26) \qquad 1 \equiv \Omega^2+\Omega^4 \pmod{\mathfrak{P}}$$

a clear contradiction in the field $\mathfrak{O}_8/\mathfrak{P}$ of two elements! ■

4. Main results. We shall show that when $8\,|\,h(-p)$ the eight class field is given by (1.7), while the criterion (1.8) emerges incidentally (see Theorem (4.11)).

(4.1) LEMMA. *If an eight class field exists for k_2, then it must be given by* (1.7).

Proof. We start from the result of Proposition (2.27): The field k_{16} must be $k_4(\sqrt[4]{\beta})$, where, rewriting (2.28) slightly,

$$(4.2) \qquad \beta = \mu^2(f+\sqrt{-p})^2(1+i)^{-2}\varepsilon', \quad \mu \in \mathfrak{O}_4^* .$$

Now computation with (1.5) demonstrates that

$$(4.3) \qquad (f+\sqrt{-p})^2(1+i)^{-2} \equiv f\sqrt{p} \pmod{8}.$$

Furthermore, since e is odd in (1.5), $p \equiv f^2 \pmod{16}$. Since $\varepsilon = S+T\sqrt{p}$ has norm -1, and $4\,|\,S$, $p \equiv T^2 \pmod{16}$. Therefore $f^2 \equiv T^2 \pmod{16}$. Apply Lemma (3.4) and our choice of f in (1.5) to deduce

$$(4.4) \qquad f \equiv -T \pmod{8}.$$

Now combine (4.2), (4.3), (4.4):

$$(4.5) \qquad \beta \equiv -\mu^2T\sqrt{p}\,\varepsilon' \pmod{8} \equiv \mu^2(1+S\sqrt{p}) \pmod{8}$$

since $S \equiv 0 \pmod{4}$. The effect of μ^2 in (4.5) is only to introduce a ± sign, since the units of $\mathfrak{O}_4$ are generated by $\{i, \varepsilon\}$, (2.19) and $\varepsilon^2 \equiv 1 \pmod{8}$.

Now, since $k_{16} = k_8(\sqrt{\sqrt{\beta}})$ is unramified over k_8 we must have

$$(4.6) \qquad \Xi^2 \equiv \sqrt{\beta} \pmod{4}$$

is solvable in $\mathfrak{O}_8$. Squaring, we find

$$4.7) \qquad \Xi^4 \equiv \beta \pmod{8}.$$

Apply Lemma (3.17). It follows that $\beta \equiv 1 \bmod 4(1+i)$. Therefore, in (4.5), $\mu^2 = +1$ and $S \equiv 0 \pmod{8}$. This proves that if $8\,|\,h(-p)$, then the eight class field is $k_4(\sqrt[4]{\beta})$ where β is given by (4.2) with $\mu^2 = 1$. ■

Furthermore we proved that if $8\,|\,h(-p)$, then $8\,|\,S$. Conversely, assume $8\,|\,S$; then, taking $\mu = 1$ in (4.2), direct computation shows that (4.6) is solvable in $\mathfrak{O}_8$. Alternatively, note that $\beta \equiv 1 \pmod{8}$, and apply the general nonramification criterion for a 4th-root extension given in Hasse [5]. In any event it follows that $k_4(\sqrt[4]{\beta})$ is unramified cyclic over k_4. It is indeed cyclic over k_2. This may be proved by direct computation. Or apply Theorem (2.1) to deduce $H_2(k_2) = H_2(k_4)$ (compare [8]). Therefore $k_4(\sqrt[4]{\beta})$, which is unramified abelian over k_4, must be likewise over k_2. Therefore $8\,|\,h(-p)$. This proves (1.8).

We conclude this section by collecting information on ε, $h(-p)$.

(4.8) THEOREM. *Assume $p \equiv 1 \pmod 8$, let $\varepsilon = S + T\sqrt{p}$ denote as usual the fundamental unit of $\mathbf{Q}(\sqrt{p})$. Then*

$$S \equiv h(-p) \pmod 8, \tag{4.9}$$

$$T \equiv \frac{p+1}{2} \pmod 8. \tag{4.10}$$

Proof. We have already demonstrated (4.9). As to (4.10), the result of Lemma (3.11) may be restated as

$$S - T + \frac{p+1}{2} \equiv h(-p) \pmod 8. \tag{4.11}$$

Apply (4.9). ■

5. Congruential criteria. To illustrate the main theorem in terms of quadratic forms, take $p = 41$, where there are $h(-41) = 8$ inequivalent forms of discriminant $-4\cdot 41$. Let P be a prime $(\neq 2\cdot 41)$

$$P = \begin{Bmatrix} 3x^2 \pm 2xy + 14y^2, & (\text{e.g., } 3) \\ 6x^2 \pm 2xy + 7y^2, & (\text{e.g., } 7) \end{Bmatrix} \Leftrightarrow A \text{ true, } B \text{ false,} \tag{5.1a}$$

$$P = 5x^2 \pm 4xy + 9y^2, \ (\text{e.g., } 5) \Leftrightarrow A, B \text{ true, } C \text{ false,} \tag{5.1b}$$

$$P = 2x^2 + 2xy + 21y^2, \ (\text{e.g., } 61) \Leftrightarrow A, B, C \text{ true, } D \text{ false,} \tag{5.1c}$$

$$P = x^2 + 41y^2, \ (\text{e.g., } 173) \Leftrightarrow A, B, C, D \text{ true,} \tag{5.1d}$$

where A, B, C, D refer to the rational solvability of the congruences

$$A\colon\ x_1^2 + 41 \equiv 0 \pmod P, \tag{5.2a}$$

$$B\colon\ x_2^2 + 1 \equiv 0 \pmod P, \tag{5.2b}$$

$$C\colon\ x_3^2 \equiv 32 + 5x_1x_2 \pmod P, \tag{5.2c}$$

$$D\colon\ x_4^2 \equiv (3 + x_1)(1 + x_2)x_3 \pmod P. \tag{5.2d}$$

We should recognize in (5.2bcd) the adjunctions shown in (1.3) and (1.4) as they affect the splitting primes in (5.2a). (Note $\varepsilon = 32 + 5\sqrt{41}$ and $2\cdot 5^2 = 41 + 3^2$). The forms in (5.1a) correspond to ideal classes $\mathfrak{m}^{\pm 1}$ and $\mathfrak{m}^{\pm 3}$, while those of (5.1b) correspond to $\mathfrak{m}^{\pm 2}$ and those of (5.1c) to $\mathfrak{m}^4$ and (5.1d) to $\mathfrak{m}^8 \sim 1$, where (say) $\mathfrak{m} = (3, 1 + \sqrt{-41})$ in k_2.

The problem of "congruentially" distinguishing the forms in (5.1a) is still unfathomable.

References

[1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, Journ. Reine Angew. Math. 238 (1969), pp. 67–70.

[2] — — *On some class fields related to primes of type $x^2 + 32y^2$*, Journ. Reine Angew. Math. 262/3 (1973), pp. 400–414.

[3] G. Cooke, *Construction of Hilbert class field extension of $K = \mathbf{Q}(\sqrt{-41})$*, (informal) Lecture Notes, Cornell Univ. Ithaca, N. Y. 1974.

[4] M. Hall, *The Theory of Groups*, Macmillan Company, New York 1959.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, Physica Verlag, Würzburg–Wien 1965, pp. 45–47.

[6] — *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952.

[7] C. S. Herz, *Construction of class fields*, Chapter VII, *Seminar on Complex Multiplication*, Lecture Notes No. 21, Springer-Verlag, Berlin 1957–8.

[8] D. Hilbert, *Über die Dirichletschen biquadratischen Zahlkörper*, Math. Ann. 45 (1894), § 10.

[9] — *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Ann. 51 (1899), § 4.

[10] J. C. Lagarias (Dissertation, M. I. T. unpublished).

[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa 1974, p. 140.

[12] R. Schertz (unpublished work).

[13] H. Weber, *Elliptische Funktionen und algebraische Zahlen*, Fr. Vieweg und Sohn, Braunschweig 1891 (Anhang).

[14] H. Zimmer, *Computational Problems, Methods, and Results in Algebraic Number Theory*, Lecture Notes No. 262, Springer-Verlag, Berlin 1972.

[15] P. Kaplan, *Unités de norme -1 de $\mathbf{Q}(\sqrt{p})$ et corps de classes de degré 8 de $\mathbf{Q}(\sqrt{-p})$ où p est un nombre premier congru à 1 modulo 8* (to appear).

MATHEMATICS DEPARTMENT
CITY COLLEGE OF NEW YORK
New York, N. Y.

MATHEMATICS DEPARTMENT
CORNELL UNIVERSITY
Ithaca, N. Y.

Received on 20. 12. 1974 (651)