ACTA ARITHMETICA
LV (1990)

Governing fields for the 2-classgroup of $Q(\sqrt{-q_1 q_2 p})$ and a related reciprocity law

by

PATRICK MORTON* (Wellesley, Mass.)

§1. Introduction. In his thesis [18] Stevenhagen has recently managed to prove one of the conjectures of Cohn and Lagarias [1] concerning the classgroup $\mathscr{C}(Dp)$ in the quadratic field $Q(\sqrt{Dp})$. His theorem can be stated as follows:

THEOREM 1 (Stevenhagen). *Let $D \not\equiv 2 \pmod 4$ be a nonzero integer and let K_D be the field generated over Q by all the square roots $\sqrt{q}$ for which $q|D$ and q is a prime fundamental discriminant. Then the isomorphism type of $\mathscr{C}(Dp)/\mathscr{C}(Dp)^8$ in the field $k = Q(\sqrt{Dp})$, for primes p for which $Dp \equiv 0, 1 \pmod 4$, only depends on the Frobenius class of p in the maximal abelian extension Ω_D of K_D that is unramified outside $2D\infty$ and has a Galois group of exponent 2 over K_D.*

The classgroup $\mathscr{C}(Dp)$ in this theorem is the restricted (or narrow) classgroup of the quadratic order of discriminant Dp in k. Recall that a fundamental discriminant Δ is a discriminant of a quadratic field (i.e. of the maximal order in such a field), and is a product of prime fundamental discriminants, integers of the form -4, 8, -8 or $q^* = (-1)^{(q-1)/2}q$, where q is an odd prime. Further, the Frobenius class of p in Ω_D, denoted $\left(\frac{\Omega_D/Q}{p}\right)$, is a conjugacy class in the Galois group of Ω_D/Q which is intimately related to the way in which p splits into prime ideals in Ω_D and its subfields.

This beautiful theorem (and its proof, which involves the idelic formulation of classfield theory) generalizes the qualitative results of [11]–[13]. If, in close agreement with Cohn and Lagarias [1], we define the *minimal governing field* $\Sigma_3(D)$ for the structure $\mathscr{C}/\mathscr{C}^8 = \mathscr{C}(Dp)/\mathscr{C}(Dp)^8$ in $k = Q(\sqrt{Dp})$ to be the smallest normal extension of Q (containing $Q(\sqrt{-1})$) with the property that the Frobenius class of p (for primes $p \not| 2D$ with $Dp \equiv 0, 1 \pmod 4$) in $\mathrm{Gal}(\Sigma_3(D)/Q)$ determines the isomorphism type of $\mathscr{C}/\mathscr{C}^8$, then Stevenhagen's result says that $\Sigma_3(D)$ is contained in the field Ω_D. ($\Sigma_3(D)$ is assumed to contain

* The author gratefully acknowledges the support of AT&T Bell Laboratories, Murray Hill, NJ, during the period this article was written.

$Q(\sqrt{-1})$ so that primes p for which $Dp \equiv 0, 1 \pmod 4$ can be sorted out using the Frobenius class $\left(\frac{\Sigma_3/Q}{p}\right)$. Note that Ω_D does contain $Q(\sqrt{-1})$.)

In more generality, and deviating only slightly from Cohn and Lagarias, we define $\Sigma_\nu(D)$, *if it exists*, to be the smallest normal extension of Q (containing $Q(\sqrt{-1})$) with the property that $\left(\frac{\Sigma_\nu/Q}{p}\right)$ determines the structure of $\mathscr{C}/\mathscr{C}^{2^\nu}$ in $Q(\sqrt{Dp})$. The uniqueness of $\Sigma_\nu(D)$ (see [1], appendix) implies

$$\Sigma_1(D) \subseteq \Sigma_2(D) \subseteq \ldots \subseteq \Sigma_\nu(D) \subseteq \ldots$$

The importance of the governing fields Σ_ν lies in the fact that they can be used to compute the density of the set of primes p for which $\mathscr{C}(Dp)/\mathscr{C}(Dp)^{2^\nu}$ has a given structure. See [11]–[13].

In this paper I take a look at a special case of this theorem, namely the case

$$(1) \qquad D = -q_1q_2, \quad \text{where} \quad q_1 \equiv q_2 \equiv 3 \pmod 4,$$

and the q_i are distinct primes. This case is interesting for several reasons. As stated in [1], the case $q_1 = 3$, $q_2 = 7$ is the simplest case to which the methods I used in [11] and [12] do not apply. The first step of the method used there depends on a trick that was thoroughly exploited by Rédei and is only valid for primes $q \equiv 1 \pmod 4$, the trick being that the Legendre symbol $\left(\frac{a}{q}\right)$ can be expressed as a 4th power residue symbol:

$$(2) \qquad \left(\frac{a}{q}\right) = \left(\frac{a^2}{q}\right)_4.$$

This is useful if a^2 is one term of a ternary quadratic equation that can be replaced by a combination of terms involving q. But it forced me to look at integers D which were products of primes $\equiv 1 \pmod 4$. (See also the final remarks in [4].)

In [1] the simplest $D = -21$ of (1) was considered. Based on extended numerical calculations, Cohn and Lagarias conjectured that the field $\Sigma_3(-21)$ is a subfield of

$$(3) \quad K = Q(\sqrt{-1}, \sqrt{3}, \sqrt{7}, \sqrt{-2(3+\sqrt{21})}, \sqrt{1+2\sqrt{7}}, \sqrt{2(7+\sqrt{21})}).$$

In [18] Stevenhagen shows that Ω_{-21} is a quadratic extension of K, but does not determine $\Sigma_3(-21)$.* The way in which K arises in [1] is of interest. There the following more explicit conjecture is stated. ($\boldsymbol{Z}_n$ is shorthand for the group $\boldsymbol{Z}/n\boldsymbol{Z}$.)

* Added in proof. While this article was in press, Stevenhagen [19] found a different method of determining $\Sigma_3(-21)$.

CONJECTURE (Cohn–Lagarias). *If* $p \equiv 3 \pmod 4$, *then*

$$\mathscr{C}(-21p)/\mathscr{C}(-21p)^8 \cong \boldsymbol{Z}_8 \times \boldsymbol{Z}_2$$

if and only if

(A) $\left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = +1$ *and* p *splits completely in*

$$K_A = Q(\sqrt{-3}, \sqrt{-7}, \sqrt{-2(3+\sqrt{21})});$$

(B) $\left(\frac{p}{3}\right) = +1$, $\left(\frac{p}{7}\right) = -1$ *and* p *splits completely in*

$$K_B = Q(\sqrt{-3}, \sqrt{7}, \sqrt{1+2\sqrt{7}}); \quad or$$

(C) $\left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = -1$ *and* p *splits completely in*

$$K_C = Q(\sqrt{3}, \sqrt{7}, \sqrt{2(7+\sqrt{21})}).$$

In this paper I prove this conjecture, along with the analogous result in the more general case (1). In particular, it follows that $\Sigma_3(-21)$ equals the field K of (3). In the proof I make essential use of the quadratic reciprocity law in quadratic fields, along with the smallest positive solution (a, b) in integers of the Diophantine equation

$$(4) \qquad a^2q_2 - b^2q_1 = 1 \qquad \left(\left(\frac{q_2}{q_1}\right) = +1\right).$$

(See § 3.) The use of quadratic reciprocity replaces (2). This leads me to believe that a more elementary proof of Stevenhagen's theorem can be given, if one uses a system of Rédei equations of type (4) (see [16], [11]), along with some form of quadratic reciprocity.

As a corollary of the proof one can easily compute the density of the set of primes p for which $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8$ has a given structure. These densities are given in the adjoining table:

$\mathscr{C}/\mathscr{C}^8 \cong$	Density of $p \equiv 3 \pmod 4$
$\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$	1/8
$\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$	3/16
$\boldsymbol{Z}_2 \times \boldsymbol{Z}_8$	3/16

In addition, the explicit nature of the results given here leads directly to a curious kind of 3-termed reciprocity law. Such a law arises from general considerations in the following way.

If the normal field $\Sigma_\nu(D)$ exists for all D (or all $D \not\equiv 2 \pmod 4$) then there must be a relationship between the Frobenius class of p in $\Sigma_\nu(D)$ and the Frobenius class of a prime divisor q of D in $\Sigma_\nu\left(\frac{D}{q}p\right)$, since both fields govern $\mathscr{C}(Dp)/\mathscr{C}(Dp)^{2^\nu}$. More explicitly, fix an isomorphism type T of $\mathscr{C}(Dp)/\mathscr{C}(Dp)^{2^\nu}$ and let $A_T(D)$ represent the union of the conjugacy classes in $\mathrm{Gal}(\Sigma_\nu(D)/\boldsymbol{Q})$ for which

$$\left(\frac{\Sigma_\nu(D)/\boldsymbol{Q}}{p}\right) \subseteq A_T(D) \Rightarrow \mathscr{C}(Dp)/\mathscr{C}(Dp)^{2^\nu} \cong T.$$

Then the above relationship takes the form of a reciprocity law:

$$\left(\frac{\Sigma_\nu(D)/\boldsymbol{Q}}{p}\right) \subseteq A_T(D) \quad \text{iff} \quad \left(\frac{\Sigma_\nu\left(\frac{D}{q}p\right)/\boldsymbol{Q}}{q}\right) \subseteq A_T\left(\frac{D}{q}p\right),$$

for any odd prime q dividing D.

In particular, Stevenhagen's Theorem 1 shows that such a result holds for $\nu = 3$ and for the field Ω_D in place of $\Sigma_3(D)$. To state a symmetrical result, let the odd prime divisors of $Dp = \Delta$ be $p_1, \ldots, p_r$, where we take the p_i to be distinct:

$$\Delta = \pm 2^a \prod_{i=1}^{r} p_i \equiv 0, 1 \pmod 4. \tag{5}$$

Then we have the

General Reciprocity Theorem. *Let Δ have the form* (5) *and write $D_i = \Delta/p_i$, $1 \leqslant i \leqslant r$. If T is any finite abelian 2-group and $A_T(D_i)$ represents the union of the conjugacy classes in* $\mathrm{Gal}(\Omega_{D_i}/\boldsymbol{Q})$ (Ω_{D_i} *as in Stevenhagen's theorem*) *for which*

$$\left(\frac{\Omega_{D_i}/\boldsymbol{Q}}{p}\right) \subseteq A_T(D_i) \Rightarrow \mathscr{C}(D_ip)/\mathscr{C}(D_ip)^8 \cong T,$$

then for $1 \leqslant i, j \leqslant r$, $i \neq j$ we have

$$\left(\frac{\Omega_{D_i}/\boldsymbol{Q}}{p_i}\right) \subseteq A_T(D_i) \quad \textit{iff} \quad \left(\frac{\Omega_{D_j}/\boldsymbol{Q}}{p_j}\right) \subseteq A_T(D_j). \tag{6}$$

Here I work out the form of the law (6) when $\Delta = -q_1q_2q_3$ and the primes q_i are $\equiv 3 \pmod 4$. In order to state it, let me first state the general result corresponding to the above conjecture of Cohn and Lagarias.

Theorem 2. ($D = -q_1q_2$) *If $q_1 \equiv q_2 \equiv 3 \pmod 4$ and $\left(\frac{q_2}{q_1}\right) = +1$, then $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8 \cong \boldsymbol{Z}_8 \times \boldsymbol{Z}_2$ if and only if*

(A) $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = +1$ *and p splits completely in $K_A(q_1, q_2)$;*

(B) $\left(\frac{p}{q_1}\right) = +1$, $\left(\frac{p}{q_2}\right) = -1$ *and p splits completely in $K_B(q_1, q_2)$; or*

(C) $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$ *and p splits completely in $K_C(q_1, q_2)$;*

where K_A, K_B and K_C are the fields

$$\begin{aligned} K_A(q_1, q_2) &= \boldsymbol{Q}(\sqrt{-q_1}, \sqrt{-q_2}, \sqrt{\pi_{12}}),\\ K_B(q_1, q_2) &= \boldsymbol{Q}(\sqrt{-q_1}, \sqrt{q_2}, \sqrt{\pi_1}),\\ K_C(q_1, q_2) &= \boldsymbol{Q}(\sqrt{q_1}, \sqrt{q_2}, \sqrt{-\varepsilon_2\sqrt{q_2}\pi_1}), \end{aligned} \tag{7}$$

and where

$$\begin{aligned} &\mathrm{Norm}\,\pi_{12} = -q_1 \textit{ in } k_{12} = \boldsymbol{Q}(\sqrt{q_1q_2}),\\ &\pi_{12} \equiv \left(\frac{2}{q_1}\right) \pmod 4; \end{aligned}$$

$$\begin{aligned} &\mathrm{Norm}\,\pi_1 = -q_1^{h_2} \textit{ in } k_2 = \boldsymbol{Q}(\sqrt{q_2}), \textit{ with}\\ &h_2 = \textit{classnumber of } k_2,\\ &\pi_1 \equiv 1 \pmod 2,\\ &\pi_1 < 0 \textit{ for the infinite prime of } k_2 \textit{ for which } \sqrt{q_2} > 0,\\ &(\pi_1, 1 - a\sqrt{q_2}) \neq 1, \textit{ where } a \textit{ is as in } (4); \end{aligned} \tag{8}$$

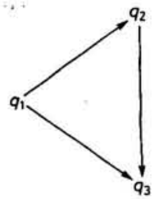
and

$$\varepsilon_2 > 1 \textit{ is the fundamental unit of } k_2.$$

If $\left(\frac{p}{q_1}\right) = -1$, $\left(\frac{p}{q_2}\right) = +1$, then $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8 \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$. If one of the Legendre symbol conditions in (A)–(C) *holds but p does not split completely in the corresponding field, then $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8 \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_4$.*

An "explicit" reciprocity theorem of the form (6) results from Theorem 2 by taking $T = \boldsymbol{Z}_8 \times \boldsymbol{Z}_2$ and replacing p by $q_3 \equiv 3 \pmod 4$. Its statement requires us to introduce a directed graph G on the vertices q_1, q_2, q_3, as follows. The directed edge (q_i, q_j) (from q_i to q_j) lies in G iff $\left(\frac{q_j}{q_i}\right) = +1$. (See [7] for a similar graph.) If G contains a cycle, the triple (q_1, q_2, q_3) will be called *cyclic*, otherwise the triple is noncyclic. (Cyclic triples correspond to primes for which $\mathscr{C}(-q_1q_2q_3)/\mathscr{C}(-q_1q_2q_3)^8 \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$.)

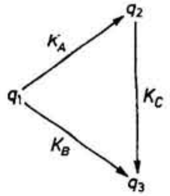
Special Reciprocity Theorem. ($\Delta = -q_1q_2q_3$) *If* (q_1, q_2, q_3) *is a non-cyclic triple of primes* $\equiv 3 \pmod 4$, *with directed graph*



then:

q_1 *splits completely in* $K_C(q_2, q_3)$ *iff*
q_2 *splits completely in* $K_B(q_1, q_3)$ *iff*
q_3 *splits completely in* $K_A(q_1, q_2)$.

The fields K_A, K_B, K_C *are thus naturally associated to edges of* G:



This theorem may be expressed in terms of Legendre symbols using the fact that q_i splits in an appropriate subfield of $K_*(q_j, q_k)$. From (8) we find that

$$\left(\frac{\pi_{12}}{q_3}\right) = \left(\frac{\pi_1}{q_2}\right) = \left(\frac{-\varepsilon_3\sqrt{q_3}\pi_2}{q_1}\right), \tag{9}$$

where:

Norm $\pi_{12} = -q_1$ in $k_{12} = Q(\sqrt{q_1q_2})$,
$\pi_{12} = \left(\frac{2}{q_1}\right) \pmod 4$;

Norm $\pi_1 = -q_1^{h_3}$ in $k_3 = Q(\sqrt{q_3})$, with
$h_3 =$ classnumber of k_3,
$\pi_1 \equiv 1 \pmod 2$,
$\pi_1 < 0$ when $\sqrt{q_3} > 0$,
$(\pi_1, 1-a\sqrt{q_3}) \neq 1$, where $a^2q_3 - b^2q_1 = 1$, $a > 0$;

$\varepsilon_3 > 1$ is the fundamental unit of k_3,
Norm $\pi_2 = -q_2^{h_3}$ in k_3,
$\pi_2 \equiv 1 \pmod 2$, $\pi_2 < 0$ when $\sqrt{q_3} > 0$,
$(\pi_2, 1-c\sqrt{q_3}) \neq 1$, where $c^2q_3 - d^2q_2 = 1$, $c > 0$;

also $\mathfrak{q}_3$, $\mathfrak{q}_2$, $\mathfrak{q}_1$ are prime ideals lying over q_3, q_2, q_1 respectively in k_{12}, k_3, k_3 and the Legendre symbols are taken in the same fields. Noting that

$$\left(\frac{\pi_1}{\mathfrak{q}_2}\right) = \left(\frac{\pi_1}{\pi_2}\right) = -\left(\frac{\pi_2}{\pi_1}\right) = -\left(\frac{\pi_2}{\mathfrak{q}_1}\right)$$

in k_3 (see § 4) shows that the last equality in (9) is equivalent to

$$\left(\frac{\varepsilon_3}{\pi_1}\right) = \left(\frac{\sqrt{q_3}}{\pi_1}\right) \tag{10}$$

in the field k_3.

Equations (9) and (10) can be viewed as the analogue for primes $\equiv 3 \pmod 4$ of a quartic reciprocity law due to E. Lehmer [8], [9]: let $p_1 \equiv p_2 \equiv 1 \pmod 4$ be primes for which $\left(\frac{p_1}{p_2}\right) = +1$, and let

$$\alpha_i = \frac{a_i + \sqrt{p_i}}{2}, \qquad a_i^2 + 4b_i^2 = p_i;$$

if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of $Q(\sqrt{p_2})$ and $Q(\sqrt{p_1})$ lying over p_1 and p_2, respectively, then for an appropriate choice of sign of a_i,

$$\left(\frac{\alpha_1}{\mathfrak{p}_2}\right) = \left(\frac{p_1}{p_2}\right)_4\left(\frac{p_2}{p_1}\right)_4 = \left(\frac{\alpha_2}{\mathfrak{p}_1}\right).$$

A proof of this result is given in [13] which is completely parallel to the proof we have given here for (9) and (10), and corresponds to the case $\Delta = p_1p_2$ of the general reciprocity theorem.

It is interesting to note that Lehmer's result concerns two primes $\equiv 1 \pmod 4$, while the corresponding statement (9) for primes $\equiv 3 \pmod 4$ requires three primes for its formulation. The role of the equations $p_i = a_i^2 + 4b_i^2$ is played here by the diophantine equations

$$a^2q_j - b^2q_i = 1, \quad (q_i, q_j) \in G.$$

Lehmer's result is closely related to a cyclic quartic extension of Q, while (9) and (10) come from extensions which are nonabelian (and dihedral) over Q.

The results presented here are also related to the prime decomposition symbols discussed by Rédei [15], Fröhlich [2] and Furuta [3]. See especially the "inversion law" in [3, p. 99] which concerns triples of primes, at least two of which are $\equiv 1 \pmod 4$. The reader is also referred to [6], which discusses results similar to (10) using classfield theory, in the case where at least one of the primes involved is $\equiv 1 \pmod 4$.

I take this opportunity to correct two misreferences in [10]. The first is a reference to Dirichlet in the introduction and § 3 and § 4 of that paper, references which should be to Dedekind. (See Dirichlet–Dedekind, *Vorlesungen* *über Zahlentheorie.*) The second occurs in footnote 2 of the introduction. There I mention an algorithm for computing the structure of the 2-classgroup of $\boldsymbol{Q}(\sqrt{d})$ which uses quadratic forms, in connection with Lagarias' determination of its computational complexity. The algorithm itself is due to D. Shanks [17].

§ 2. Preliminaries. In this section we set up notation and state several elementary lemmas. Sections 3–5 are devoted respectively to proving Cases (A)–(C) of Theorem 2. The last two sections of the paper use Theorem 2 to compute $\Sigma_3(-q_1q_2)$ and to derive the special reciprocity theorem as stated in the introduction.

We shall make use of the algorithm given in [10], which combines ideas of Rédei, Hasse and Bauer. The algorithm starts with the ramified primes in $k=\boldsymbol{Q}(\sqrt{-q_1q_2p})$, namely $\mathfrak{q}_1$, $\mathfrak{q}_2$ and $\mathfrak{p}$, where

$$\text{(11)}\qquad \mathfrak{q}_i^2=(q_i),\qquad \mathfrak{p}^2=(p),$$

and where we assume $\left(\frac{q_2}{q_1}\right)=+1$. The algorithm also makes use of the two independent quadratic characters on the classgroup $\mathscr{C}$ of k, defined for any ideal of k by the Hilbert symbol

$$\text{(12)}\qquad \chi_i(\mathfrak{a})=\left(\frac{\text{Norm }\mathfrak{a},-q_1q_2p}{q_i}\right)$$
$$=\left(\frac{\text{Norm }\mathfrak{a}}{q_i}\right),\qquad \text{if } (q_i,\ \text{Norm }\mathfrak{a})\ =1.$$

Using the ideals in (11) and the characters in (12) we form the matrix

$$\text{(13)}\qquad M=\begin{bmatrix}\chi_1(\mathfrak{q}_1) & \chi_2(\mathfrak{q}_1)\\ \chi_1(\mathfrak{q}_2) & \chi_2(\mathfrak{q}_2)\\ \chi_1(\mathfrak{p}) & \chi_2(\mathfrak{p})\end{bmatrix}=\begin{array}{c|cc} & \chi_1 & \chi_2\\ \hline q_1 & \left(\frac{p}{q_1}\right) & -1\\ q_2 & 1 & -\left(\frac{p}{q_2}\right)\\ p & \left(\frac{p}{q_1}\right) & \left(\frac{p}{q_2}\right)\end{array},$$

and think of the rows and columns of M as being indexed respectively by the ideals and characters in (11) and (12).

We put M into "reduced" form, obtaining a new matrix M' using elementary (multiplicative) row and column operations:

$$M'=\begin{bmatrix}D & +\\ + & +\end{bmatrix},$$

where D is a "diagonal" matrix with -1's on the diagonal and $+1$'s elsewhere. Further, the rows and columns of M' are indexed by the ideals and characters that arise when applying the operations that lead from M to M' to the indexing ideals and characters of M. Call these the *row ideals* and *column characters* of M and M'.

The purpose of reducing M is to find a basis for quadratic characters on $\mathscr{C}$ which have square roots in the character group of $\mathscr{C}$. Such a basis is provided by the column characters corresponding to columns of $+1$'s in M'. In addition, the row ideals corresponding to rows of $+1$'s in M' generate the classes of order 2 in $\mathscr{C}$ which have square roots. Call these characters and ideals the *square* (indexing) characters and ideals of M'.

Let e_{2^n} be the 2^n-rank of $\mathscr{C}$, i.e. the number of invariants of $\mathscr{C}$ which are divisible by 2^n. From (13) and the above remarks it is not hard to see that

$$e_4=2-r,$$

where r is the multiplicative rank of M, and that $e_4=0$ or 1. Further, if $e_4=1$, then either of the two square indexing ideals $\mathfrak{a}$ of M' generates the unique square class of order 2 in $\mathscr{C}$. Let χ be the square indexing character of M'. Then we have the rule:

$$e_8=1\quad\text{iff}\quad \chi(\mathfrak{z})=+1,\quad\text{where}\quad \mathfrak{z}^2\sim\mathfrak{a}.$$

(For proofs of these elementary facts see [11].) Character theory usually requires that $\chi(\mathfrak{z})=+1$ for all quadratic χ characters of $\mathscr{C}$, in order for $\mathfrak{z}$ to be a square. That it suffices to consider only the square (indexing) character of M' follows easily from the form of M' and cuts our work in half.

In every case e_4 depends on Legendre symbols in $\boldsymbol{Q}$. The problem is to show that e_8 depends on Legendre symbols in quadratic extensions of $\boldsymbol{Q}$. We divide the discussion into 4 cases.

In the first and easiest case

$$\text{(X)}\qquad \left(\frac{p}{q_1}\right)=-1,\qquad \left(\frac{p}{q_2}\right)=+1.$$

Here (13) gives

$$M=\begin{bmatrix}-1 & -1\\ 1 & -1\\ -1 & 1\end{bmatrix},$$

so

$$M'=\begin{bmatrix}-1 & 1\\ 1 & -1\\ 1 & 1\end{bmatrix},$$

implying that $e_4=e_8=0$ and $\mathscr{C}/\mathscr{C}^8\cong\boldsymbol{Z}_2\times\boldsymbol{Z}_2$.

We turn now to the three nontrivial cases, for which we need several lemmas.

Lemma 1. *If $\mathfrak{a}$ is a square indexing ideal of M' and (x, y, z) is a positive primitive solution of*

$$x^2+q_1q_2py^2-az^2=0, \qquad a = \text{Norm } \mathfrak{a},$$

then $\mathfrak{z}^2 \sim \mathfrak{a}$, where $\mathfrak{z}$ is an ideal for which

$$\text{Norm } \mathfrak{z} = \begin{cases} z, & z \text{ odd}, \\ z/2, & z \text{ even}. \end{cases}$$

The proof is given in [10] or [11] for the case that z is even, and is easily adapted to the case in which z is odd. This proof gives $\mathfrak{a}\mathfrak{z}^2 = (\gamma)$, where

$$\gamma = \begin{cases} x+y\sqrt{-q_1q_2p}, & \text{if } z \text{ is odd}, \\ \tfrac{1}{2}(x+y\sqrt{-q_1q_2p}), & \text{if } z \text{ is even}. \end{cases}$$

Lemma 2. (See [16], Lemma 1.) *Let $x = (u+v\sqrt{d})/2$, where $d \equiv 1 \pmod 4$ and u, v are odd integers. If α is relatively prime to 2, then $\alpha^3 \in \mathbf{Z}[\sqrt{d}]$.*

We omit the straightforward proof. (See also [13], Lemma 2.)

Lemma 3. *If q is a prime $\equiv 3 \pmod 4$, then a fundamental unit in $\mathbf{Q}(\sqrt{q})$ has the form*

$$\varepsilon = 2r+s\sqrt{q},$$

where $r, s \in \mathbf{Z}$ and s is odd.

Proof. If ε is not of this form, it must have the form $r+2s\sqrt{q}$, in which case all powers of ε have the same form and all solutions of $x^2-qy^2=1$ have $2|y$. Thus it suffices to show that

$$4x^2-qy^2=1$$

is solvable. Write this equation as

$$(2x-1)(2x+1)=qy^2.$$

It is well known that $m^2-n^2q=\pm 2$ is solvable according as $\left(\frac{\pm 2}{q}\right)=+1$. (A proof can easily be given using Rédei's theory [10], [16].) Set

$$2x-1=m^2, \quad 2x+1=m^2+2=n^2q \quad \text{in case } \left(\frac{-2}{q}\right)=+1,$$

$$2x-1=n^2q, \quad 2x+1=n^2q+2=m^2 \quad \text{in case } \left(\frac{2}{q}\right)=+1.$$

Since m, n are odd, $x \in \mathbf{Z}$. Setting $y = mn$ we have

$$4x^2-1=m^2n^2q=qy^2. \ \blacksquare$$

This lemma will find application in Cases B and C.

§ 3. **Case A:** $\left(\frac{p}{q_1}\right)=\left(\frac{p}{q_2}\right)=+1$. In this case

$$M = \begin{bmatrix} 1 & -1 \\ 1 & -1 \\ 1 & 1 \end{bmatrix}, \qquad M' = \begin{array}{c|cc} & \chi_2 & \chi_1 \\ \hline q_1 & -1 & 1 \\ q_1q_2 & 1 & 1 \\ .p & 1 & 1 \end{array}.$$

Hence $e_4 = 1$, and $e_8 = 1$ iff $\chi_1(\mathfrak{z}) = +1$, where $\mathfrak{z}^2 \sim \mathfrak{p}$. From (12) and Lemma 1,

$$\chi_i(\mathfrak{z}) = \left(\frac{z}{q_1}\right), \tag{14}$$

where (x, y, z) is a positive primitive solution of

$$x^2+q_1q_2py^2-4pz^2=0.$$

Putting $x = px_1$, this equation becomes

$$px_1^2 = 4z^2-q_1q_2y^2, \tag{15}$$

which begs to be considered in the field $k_{12} = \mathbf{Q}(\sqrt{q_1q_2})$.

To solve it recall that the absolute classnumber h_{12} of k_{12} is odd and the equation

$$q_2a^2-q_1b^2=1 \qquad \left(\text{recall } \left(\frac{q_2}{q_1}\right)=+1\right), \tag{16}$$

is solvable, giving

$$-q_1 = \text{Norm}(q_1b+a\sqrt{q_1q_2}) = \text{Norm } \pi_{12}$$

as the norm of the prime element $\pi_{12} = q_1b+a\sqrt{q_1q_2}$ in k_{12}. This may be seen by applying Rédei's theory [10], [16] to the field k_{12} using the matrix analogous to (13):

$$M_{12} = \begin{bmatrix} \bar{\chi}_1(\mathfrak{Q}_1) \\ \bar{\chi}_1(\mathfrak{Q}_2) \end{bmatrix} = \begin{bmatrix} -\left(\frac{q_2}{q_1}\right) \\ \left(\frac{q_2}{q_1}\right) \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \end{bmatrix};$$

here

$$\bar{\chi}_1(\mathfrak{a}) = \left(\frac{\operatorname{Norm}\mathfrak{a},\, q_1 q_2}{q_1}\right)$$

is the unique quadratic character on the restricted classgroup of k_{12} and $\mathfrak{Q}_i$ is the prime ideal of k_{12} lying over q_i. Since the rank of M_{12} is 1, the restricted classnumber $h_{12}^{+} = 2h_{12} \equiv 2 \pmod 4$, and so h_{12} is odd. Further, the form of M_{12} shows that $\mathfrak{Q}_2$ is principal (in the restricted sense), and hence that (16) is solvable. (See [10], § 4.) As is known (see [16], Lemmas 1 and 2), the smallest positive solution of (16) has the property that

$$(a\sqrt{q_2}+b\sqrt{q_1})^2 = \varepsilon_{12} \text{ or } \varepsilon_{12}^3,$$

where $\varepsilon_{12} > 1$ is the fundamental unit of k_{12}.

Now we solve (15). Since $\left(\frac{p}{q_1}\right) = +1$, a prime ideal $\mathfrak{P}$ of k_{12} lying over p is in the principal genus in k_{12}, i.e. is equivalent to an ideal square $\mathfrak{a}^2$ in k_{12} (in the restricted sense). Hence $\mathfrak{P}^{h_{12}} \sim \mathfrak{a}^{h_{12}^{+}} \sim 1$ is generated by an integer of k_{12} with positive norm. By cubing (see Lemma 2) and taking conjugates we may assume

$$(17) \qquad \mathfrak{P}^{3h_{12}} = (\eta), \quad \eta = 2z + y\sqrt{q_1 q_2}, \quad y, z > 0,$$
$$p^{3h_{12}} = 4z^2 - q_1 q_2 y^2;$$

note that η can be assumed to have the given form since $(\eta, 2) = 1$ and $p \equiv 3 \pmod 4$. This solves (15) with $x_1 = p^{(3h_{12}-1)/2}$.

Using (14) and computing

$$\chi_1(\mathfrak{z}) = \left(\frac{z}{q_1}\right) = \left(\frac{z}{\pi_{12}}\right)$$

in k_{12} gives, since $\eta \equiv 2z \pmod{\pi_{12}}$, that

$$\chi_1(\mathfrak{z}) = \left(\frac{2}{q_1}\right)\left(\frac{\eta}{\pi_{12}}\right).$$

To the last term in this expression we apply the quadratic reciprocity law in k_{12} (see [5], Part II):

$$(18) \qquad \left(\frac{\eta}{\pi_{12}}\right) = \left(\frac{\pi_{12}}{\eta}\right) \prod_{\mathfrak{p}_2 | 2} \left(\frac{\pi_{12}, \eta}{\mathfrak{p}_2}\right) \cdot \prod_{\mathfrak{p}_\infty | \infty} \left(\frac{\pi_{12}, \eta}{\mathfrak{p}_\infty}\right),$$

where $\mathfrak{p}_2$ and $\mathfrak{p}_\infty$ run respectively over the prime divisors of 2 and the infinite primes in k_{12}, and the symbols behind the product signs are norm residue symbols. Certainly the terms corresponding to the infinite primes are $+1$, since $\eta \gg 0$ by (17). I claim that the terms involving $\mathfrak{p}_2$ are $+1$ also.

To see this write $\pi_{12} = r + s\sqrt{q_1 q_2}$ with $r, s \in \mathbf{Z}$. The equation $-q_1 = r^2 - q_1 q_2 s^2$ shows that r is odd and s is even, since the left-hand side is $\equiv 1 \pmod 4$. If $4|s$, either π_{12} or $-\pi_{12}$ is $\equiv 1 \pmod 4$. If $2\|s$, then we still have

$$\pm\pi_{12} = 2u + 1 + 2v\sqrt{q_1 q_2} \qquad (u \text{ odd})$$
$$= 1 + 4\frac{u + v\sqrt{q_1 q_2}}{2} \equiv 1 \pmod 4.$$

It follows that the conductor of $k_{12}(\sqrt{\pm\pi_{12}})$ over k_{12} is prime to 2 (see [14], p. 200), so that the residue symbols in (18) involving 2 are $+1$. Replacing π_{12} by $-\pi_{12}$ if necessary, (18) gives

$$\chi_1(\mathfrak{z}) = \left(\frac{2}{q_1}\right)\left(\frac{\pi_{12}}{\eta}\right) = \left(\frac{2}{q_1}\right)\left(\frac{\pi_{12}}{\mathfrak{P}}\right), \quad \text{with} \quad p = \mathfrak{P}\mathfrak{P}' \text{ in } k_{12}.$$

Finally by replacing π_{12} by $-\pi_{12}$ in case $\left(\frac{2}{q_1}\right) = -1$ we can write

$$(19) \qquad \chi_1(\mathfrak{z}) = \left(\frac{\pi_{12}}{\mathfrak{P}}\right).$$

It is easy to see that the expression (19) does not depend on the choice of $\mathfrak{P}$. Further, in case A it is clear that p splits completely in $Q(\sqrt{-q_1}, \sqrt{-q_2})$, and therefore (19) shows that e_8 depends only on the splitting of p in the normal field

$$(20) \qquad K_A = Q(\sqrt{-q_1}, \sqrt{-q_2}, \sqrt{\pi_{12}}) \text{ where } \begin{cases} \operatorname{Norm}\pi_{12} = -q_1 \text{ in } k_{12} = Q(\sqrt{q_1 q_2}), \\ \pi_{12} \equiv \left(\frac{2}{q_1}\right) \pmod 4. \end{cases}$$

We have proven

Criterion A. *If* $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = +1$, $e_8 = 1$ *in* $Q(\sqrt{-q_1 q_2 p})$ *iff* p *splits completely in the field* K_A *defined by* (20).

In the special case $q_1 = 3$, $q_2 = 7$, the relation $2^2 \cdot 7 - 3^2 \cdot 3 = 1$ gives $\operatorname{Norm}(9 + 2\sqrt{21}) = -3$, and since $\left(\frac{2}{3}\right) = -1$ we take $\pi_{12} = 9 + 2\sqrt{21} \equiv -1 \pmod 4$. Also,

$$9 + 2\sqrt{21} = -\frac{3+\sqrt{21}}{2}\left(\frac{-5-\sqrt{21}}{2}\right) = -\frac{3+\sqrt{21}}{2}\left(\frac{\sqrt{-3}-\sqrt{-7}}{2}\right)^2,$$

so that

$$K_A = Q(\sqrt{-3}, \sqrt{-7}, \sqrt{9+2\sqrt{21}}) = Q(\sqrt{-3}, \sqrt{-7}, \sqrt{-2(3+\sqrt{21})})$$

is indeed the field conjectured by Cohn and Lagarias.

§ 4. Case B: $\left(\frac{p}{q_1}\right) = +1$, $\left(\frac{p}{q_2}\right) = -1$. Here

$$M = \begin{bmatrix} 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad M' = \begin{array}{c|cc} & \chi_2 & \chi_1 \\ \hline q_1 & -1 & 1 \\ q_2 & 1 & 1 \\ q_1p & 1 & 1 \end{array},$$

and again $e_4 = 1$, while $e_8 = 1$ iff $\chi_1(\mathfrak{z}) = 1$, where $\mathfrak{z}^2 \sim \mathfrak{q}_2$. To compute $\chi_1(\mathfrak{z})$ we are required to solve

$$x^2 + q_1q_2py^2 - q_2z^2 = 0,$$

or

(21) $$pq_1y^2 = z^2 - q_2x_1^2, \quad x = q_2x_1.$$

We will solve this with an odd value of z, so from Lemma 1 we have

(22) $$\chi_1(\mathfrak{z}) = \left(\frac{z}{q_1}\right).$$

In this case we work in the field $k_2 = Q(\sqrt{q_2})$. In k_2 the restricted classnumber is $h_2^+ = 2h_2$, where h_2 is the (odd) absolute classnumber of k_2. Since $\left(\frac{p}{q_2}\right) = -1$, $\left(\frac{q_2}{p}\right) = +1$ and for some prime ideal $\mathfrak{P}$ of k_2 and some $\eta \in k_2$

(23) $$\mathfrak{P}^{h_2} = (\eta), \quad \text{Norm}\,\eta = -p^{h_2}.$$

We set

(24) $$\eta = u + v\sqrt{q_2} \quad (u, v > 0).$$

Using the fundamental unit ε_2 of k_2 and the result of Lemma 3, we may assume that u is odd and v is even, since

$$\eta\varepsilon_2 = (u+v\sqrt{q_2})(2r+s\sqrt{q_2}) = 2ur + vsq_2 + (2vr+us)\sqrt{q_2}.$$

This allows us to assume $\eta \equiv 1 \pmod 2$. Also, since $\left(\frac{q_1}{q_2}\right) = -1$, there is an element π_1 in k_2 whose norm is $-q_1^{h_2}$. Let $\mathfrak{Q}$ be the prime ideal in k_2 lying over q_1; for which

(25) $$\pi_1 = (\mathfrak{Q})^{h_2}, \quad \text{Norm}\,\pi_1 = -q_1^{h_2}, \quad \pi_1 \equiv 1 \pmod 2.$$

(The last condition holds for π_1 or $\pi_1\varepsilon_2$, as above.)

From § 3 we use the positive solution (a, b) of equation (16), which we write here as

(26) $$-q_1b^2 = 1 - q_2a^2 \quad (2|a \text{ since } q_2 \equiv 3 \pmod 4).$$

Putting $\xi = 1 + a\sqrt{q_2}$, we assume $\mathfrak{Q}'|\xi$, where $\mathfrak{Q}'$ is the conjugate of the prime $\mathfrak{Q}$ in (25). We can certainly achieve this by a suitable choice of π_1. Hence we require

(27) $$(\pi_1, 1 - a\sqrt{q_2}) \neq 1.$$

Now compute

$$\eta\xi = (u+v\sqrt{q_2})(1+a\sqrt{q_2}) = u + avq_2 + (au+v)\sqrt{q_2}.$$

Taking norms in this equation and using (23) and (26) leads to

$$p^{h_2}q_1b^2 = \text{Norm}(\eta\xi) = (u+avq_2)^2 - q_2(au+v)^2;$$

this is a solution of (21) with

(28) $$x_1 = au+v, \quad y = bp^{(h_2-1)/2}, \quad z = u + avq_2 \equiv 1 \pmod 2.$$

Before continuing we check for the primitivity of this solution. If l is a prime dividing g.c.d. (x, y, z), then $l = p$ or $l|b$. If $l \neq p$, then $l|\eta\xi$ implies $l|\xi$, which is impossible since $\xi = 1 + a\sqrt{q_2}$. Thus $l = p$. But then $p|\eta\xi$ and $(\xi) = \mathfrak{Q}'\mathfrak{b}^2$ imply that the conjugate ideal $\mathfrak{P}'$ of $\mathfrak{P}$ in k_2 divides the ideal $\mathfrak{b}$ and hence p divides $\text{Norm}\,\mathfrak{b} = b$. We can therefore guarantee primitivity by requiring that $p \nmid b$. We make this assumption temporarily and show later how to proceed when $p|b$.

To compute $\chi_1(\mathfrak{z})$ we use the assumption (27) in the form

$$1 + a\sqrt{q_2} \equiv 0 \pmod{\mathfrak{Q}'}.$$

From (22) and (28) we have

(29) $$\chi_1(\mathfrak{z}) = \left(\frac{u+avq_2}{q_1}\right) = \left(\frac{u-v\sqrt{q_2}}{\mathfrak{Q}'}\right) = \left(\frac{\eta'}{\mathfrak{Q}'}\right) = \left(\frac{\eta'}{\mathfrak{Q}'}\right)^{h_2} = \left(\frac{\eta'}{\pi_1'}\right) = \left(\frac{\eta}{\pi_1}\right).$$

Appealing to quadratic reciprocity in k_2, we find

(30) $$\left(\frac{\eta}{\pi_1}\right) = \left(\frac{\pi_1}{\eta}\right)\left(\frac{\pi_1, \eta}{\mathfrak{p}_2}\right)\prod_{\mathfrak{p}_\infty|\infty}\left(\frac{\pi_1, \eta}{\mathfrak{p}_\infty}\right), \quad \mathfrak{p}_2^2 = (2) \text{ in } k_2.$$

If $\mathfrak{p}_\infty$ is the infinite prime for which $\sqrt{q_2} > 0$, then $\eta > 0$ for $\mathfrak{p}_\infty$ by (24). If we assume $\pi_1 < 0$ for $\mathfrak{p}_\infty$, then by (25), $\pi_1 > 0$ for $\mathfrak{p}'_\infty$ and the infinite terms in (30) drop out. (This can be achieved by taking $-\pi_1$ in place of π_1.) Finally, the fact that $\eta \equiv \pi_1 \equiv 1 \pmod 2$ implies $\left(\frac{\pi_1, \eta}{\mathfrak{p}_2}\right) = +1$, which is equivalent to η being a norm residue from the field $k_2(\sqrt{\pi_1})$. To see this, note that the 2-conductor of $k_2(\sqrt{\pi_1})/k_2$ divides 2, by Theorem 5.6 in [14]. The congruence

$$\eta \equiv 1 \pmod 2 \equiv \mathrm{Norm}_{k_2(\sqrt{\pi_1})} 1 \pmod 2$$

now makes the claim obvious. Hence (29) and (30) give

$$\chi_1(\mathfrak{z}) = \left(\frac{\pi_1}{\eta}\right) = \left(\frac{\pi_1}{\mathfrak{P}}\right),$$

at first with the restriction $p \nmid b$.

If $p|b$, then from above $\mathfrak{P}'|\mathrm{b}$ but $\mathfrak{P} \nmid \mathrm{b}$ since $\xi = 1 + a\sqrt{q_2}$ is primiti In this case replace $\mathfrak{P}'$ by $\mathfrak{P}$ and go through the above argument w $\eta' = u - v\sqrt{q_2}$ in place of η:

$$\eta'\xi = (u - v\sqrt{q_2})(1 + a\sqrt{q_2}) = u - avq_2 + (au - v)\sqrt{q_2}.$$

Note that $u^2 - a^2v^2q_2 \leqslant u^2 - v^2q_2 < 0$ since η has a negative norm, and her $u - avq_2 < 0$. This requires that we take $z = -u + avq_2 > 0$, and from (2

$$\chi_1(\mathfrak{z}) = \left(\frac{-u + avq_2}{q_1}\right) = \left(\frac{-u - v\sqrt{q_2}}{\mathfrak{Q}'}\right) = \left(\frac{-\eta}{\pi_1'}\right) = \left(\frac{-\eta'}{\pi_1}\right) = \left(\frac{\pi_1}{\eta'}\right) \tag{31}$$

by the same reasoning that follows (30), since $\eta' < 0$ for $\mathfrak{p}_\infty$, $-\eta' > 0$ for $\mathfrak{p}$ and $\pi_1 > 0$ for $\mathfrak{p}'_\infty$. Thus

$$\chi_1(\mathfrak{z}) = \left(\frac{\pi_1}{\eta'}\right) = \left(\frac{\pi_1'}{\eta}\right) = \left(\frac{\pi_1}{\eta}\right)\left(\frac{-q_1}{p}\right) = \left(\frac{\pi_1}{\eta}\right) = \left(\frac{\pi_1}{\mathfrak{P}}\right),$$

and the restriction $p \nmid b$ is unnecessary.

This proves

Criterion B. *If* $\left(\frac{p}{q_1}\right) = +1$, $\left(\frac{p}{q_2}\right) = -1$, *then* $e_8 = 1$ *in the fi* $\boldsymbol{Q}(\sqrt{-q_1q_2p})$ *if and only if p splits completely in the normal field*

$$K_B = \boldsymbol{Q}(\sqrt{-q_1}, \sqrt{q_2}, \sqrt{\pi_1}), \tag{32}$$

where

(33) Norm $\pi_1 = -q_1^{h_2}$ *in* $\boldsymbol{Q}(\sqrt{q_2})$,
$\pi_1 \equiv 1 \pmod 2$ *and* $\pi_1 < 0$ *for* $\mathfrak{p}_\infty$ (*when* $\sqrt{q_2} > 0$),
$(\pi_1, 1 - a\sqrt{q_2}) \neq 1$, *where* $a^2q_2 - b^2q_1 = 1$.

If $q_1 = 3$ and $q_2 = 7$, $\varepsilon_2 = 8 + 3\sqrt{7}$ and $2^2 \cdot 7 - 3^2 \cdot 3 = 1$ as in § 3. Hence π_1 must be chosen so that $(\pi_1, 1 - 2\sqrt{7}) \neq 1$. Since $h_2 = 1$, π_1 is principal and Norm $\pi_1 = -3$. The right choice for π_1 is $\pi_1 = -5 - 2\sqrt{7}$, since $\pi_1 | 1 - 2\sqrt{7}$, so

$$K_B = \boldsymbol{Q}(\sqrt{-3}, \sqrt{7}, \sqrt{-5 - 2\sqrt{7}}).$$

Note that $1 - 2\sqrt{7} = (2 + \sqrt{7})^2(-5 - 2\sqrt{7})$ and $(1 + 2\sqrt{7})(1 - 2\sqrt{7}) = -27 = (3\sqrt{-3})^2$, so

$$K_B = \boldsymbol{Q}(\sqrt{-3}, \sqrt{7}, \sqrt{1 + 2\sqrt{7}}),$$

the field Cohn and Lagarias conjecture in [1].

§ 5. Case C: $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$. In the last case

$$M = \begin{bmatrix} -1 & -1 \\ 1 & 1 \\ -1 & -1 \end{bmatrix}, \quad M' = \begin{array}{c|cc} & \chi_1 & \chi_1\chi_2 \\ \hline q_1 & -1 & 1 \\ q_2 & 1 & 1 \\ q_1p & 1 & 1 \end{array},$$

and e_8 depends on $\chi_1\chi_2(\mathfrak{z})$, where $\mathfrak{z}^2 \sim \mathfrak{q}_1\mathfrak{p} \sim \mathfrak{q}_2$. We are required to solve

$$x^2 + q_1q_2py^2 - q_2z^2 = 0,$$

or

$$q_1py^2 = z^2 - q_2x_1^2, \quad x = q_2x_1,$$

as in Case B.

If (16) holds and $p \nmid b$ then a primitive solution is given by (28). With the same notation we have

$$\chi_1\chi_2(\mathfrak{z}) = \left(\frac{u + avq_2}{q_1q_2}\right) \quad (\text{note } (u, q_2) = 1)$$

$$= \left(\frac{u}{q_2}\right)\left(\frac{u + avq_2}{q_1}\right) = \left(\frac{\eta}{\pi_2}\right)\left(\frac{\eta}{\pi_1}\right) = \left(\frac{\eta}{\pi_1\pi_2}\right)$$

where $\pi_2 = (\sqrt{q_2})$ in $k_2 = \boldsymbol{Q}(\sqrt{q_2})$.

In case $p|b$, using $z = -u + avq_2$ as in (31) leads to

$$\chi_1\chi_2(\mathfrak{z}) = \left(\frac{-u}{q_2}\right)\left(\frac{-u + avq_2}{q_1}\right)$$

$$= \left(\frac{-\eta'}{\pi_1\pi_2}\right) = \left(\frac{\eta}{\pi_1\pi_2}\right)\left(\frac{-p}{q_1q_2}\right) = \left(\frac{\eta}{\pi_1\pi_2}\right).$$

If we choose $\pi_2 \equiv 1 \pmod 2$ and $\pi_2 < 0$ for $\mathfrak{p}_\infty$, say $\pi_2 = -\sqrt{q_2}\varepsilon_2$, then $\pi_1\pi_2 \gg 0$ and quadratic reciprocity gives just as in § 4 that

$$\chi_1\chi_2(3) = \left(\frac{\pi_1\pi_2}{\mathfrak{P}}\right) = \left(\frac{-\varepsilon_2\sqrt{q_2}\pi_1}{\mathfrak{P}}\right).$$

CRITERION C. *If* $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$, *then* $e_8 = 1$ *in the field* $Q(\sqrt{-q_1q_2p})$ *if and only if p splits completely in the normal field*

$$K_C = Q(\sqrt{q_1}, \sqrt{q_2}, \sqrt{-\varepsilon_2\sqrt{q_2}\pi_1}), \tag{34}$$

with π_1 *defined as in* (33).

When $q_1 = 3$, $q_2 = 7$, the same choice of π_1 as in § 4 gives

$$\begin{aligned} -\varepsilon_2\sqrt{q_2}\pi_1 &= -(8+3\sqrt{7})\sqrt{7}(-5-2\sqrt{7}) \\ &= -(8+3\sqrt{7})^2\sqrt{7}(2-\sqrt{7}) = (8+3\sqrt{7})^2(7-2\sqrt{7}). \end{aligned}$$

Hence K_C is also generated over $Q(\sqrt{3}, \sqrt{7})$ by $\sqrt{7-2\sqrt{7}}$ or its conjugate $\sqrt{7+2\sqrt{7}}$. Finally,

$$7+2\sqrt{7} = \left(\frac{2-\sqrt{3}+\sqrt{7}}{2}\right)^2 \cdot \frac{7+\sqrt{21}}{2}$$

shows that K_C is the field conjectured by Cohn and Lagarias.

This completes the proof of Theorem 2 and the Cohn–Lagarias conjecture stated in the introduction.

§ 6. The governing field for $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8$. An immediate consequence of Theorem 2 is the following

DENSITY THEOREM. *If* q_1, q_2, p *are distinct primes* $\equiv 3 \pmod 4$, *the density of p for which the classgroup* $\mathscr{C}$ *in* $Q(\sqrt{-q_1q_2p})$ *satisfies*

$$\mathscr{C}/\mathscr{C}^8 \cong \begin{cases} Z_2 \times Z_2 \\ Z_4 \times Z_2 \\ Z_8 \times Z_2 \end{cases} \text{is} \begin{cases} 1/8 \\ 3/16 \\ 3/16. \end{cases}$$

Proof. Case X (in § 2) gives a set of primes of density 1/8 for which $\mathscr{C}/\mathscr{C}^8 \cong Z_2 \times Z_2$ (keep in mind that $p \equiv 3 \pmod 4$). On the other hand, each of the criteria A, B, C gives a set of primes of density 1/16 for which $\mathscr{C}/\mathscr{C}^8 \cong Z_8 \times Z_2$. (Use the Frobenius density theorem [5], II applied to the fields $K_A(\sqrt{-1})$, $K_B(\sqrt{-1})$, $K_C(\sqrt{-1})$.) These sets are clearly disjoint, since they correspond to primes p for which respectively

$$\left(\left(\frac{p}{q_1}\right), \left(\frac{p}{q_2}\right)\right) = (1, 1), (1, -1), (-1, -1).$$

The theorem follows.

We now show that the field $K = K_AK_BK_C$ is the exact governing field for the structure $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8$, i.e. that

$$\Sigma_3(-q_1q_2) = K_AK_BK_C.$$

We first prove that $[K: Q] = 64$. By Kummer theory it suffices to show that π_{12}, π_1 and $\varepsilon_2\sqrt{q_2}$ are square-independent over $F = Q(\sqrt{-1}, \sqrt{q_1}, \sqrt{q_2})$ (see (7)), i.e. that the relation

$$\pi_{12}^a\pi_1^b(\varepsilon_2\sqrt{q_2})^c = \eta^2, \quad \eta \in F, \tag{35}$$

implies $a \equiv b \equiv c \equiv 0 \pmod 2$.

First apply the automorphism

$$(\sqrt{q_1} \to -\sqrt{q_1}, \sqrt{q_2} \to \sqrt{q_2}, \sqrt{-1} \to \sqrt{-1})$$

of F to (35) and multiply the resulting equation by (35), i.e. take norms to $Q(\sqrt{-1}, \sqrt{q_2})$. This gives

$$(-q_1)^a = \eta_1^2, \quad \eta_1 \in Q(\sqrt{-1}, \sqrt{q_2}),$$

which is only possible if $2|a$. Now take norms in

$$\pi_1^b(\varepsilon_2\sqrt{q_2})^c = \eta^2, \quad \eta \in F,$$

to $Q(\sqrt{-1}, \sqrt{q_1})$. This gives

$$(-q_1)^{h_2b}(-q_2)^c = \eta_1^2, \quad \eta_1 = \operatorname{Norm}\eta \in Q(\sqrt{-1}, \sqrt{q_1}).$$

Since $-q_1$ is a square in $Q(\sqrt{-1}, \sqrt{q_1})$ this shows that $2|c$. Finally, if it were true that

$$\pi_1 = \eta^2, \quad \eta \in F,$$

the field $K_B = Q(\sqrt{-q_1}, \sqrt{q_2}, \sqrt{\pi_1})$ would be a subfield of the abelian field F, hence $Q(\sqrt{\pi_1})$ would be abelian, which it is *not*. (Note $\sqrt{\pi_1}\sqrt{\pi_1'} = (\sqrt{-q_1})^{h_2}$ does not lie in $Q(\sqrt{\pi_1})$, so this field is not even normal.)

This proves our claim that $[K: Q] = 64$ and also shows that K is the independent composition of $K_A(\sqrt{-1})$, $K_B(\sqrt{-1})$, $K_C(\sqrt{-1})$ over $F = Q(\sqrt{-1}\ \sqrt{q_1}, \sqrt{q_2})$. We now prove

THEOREM 3. *We have*

$$\Sigma_3(-q_1q_2) = K = K_AK_BK_C;$$

i.e. K is the smallest normal extension of Q which contains $Q(\sqrt{-1})$ and governs the structure $\mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8$.

Proof. Suppose $\Sigma_3(-q_1q_2) = L$. Then $L \subseteq K$ by Theorem 2 and $F \subseteq L$ since $F = \Sigma_2(-q_1q_2)$. (This follows from the Rédei–Reichardt theorem, or from our computations in § 2–§ 5.) For some $\sigma_L \in \mathrm{Gal}(L/Q)$, the following implication holds:

$$\left(\frac{L/Q}{p}\right) = \{\sigma_L\} \Rightarrow \mathscr{C}(-q_1q_2p)/\mathscr{C}(-q_1q_2p)^8 \cong Z_4\times Z_2, \tag{36}$$

where $\{\sigma_L\}$ is the conjugacy class of σ_L in $\mathrm{Gal}(L/Q)$, and $p \equiv 3 \pmod 4$. By Theorem 2 and the Frobenius density theorem there must be automorphisms σ_L satisfying (36) which fix any one of the quartic subfields $Q(\sqrt{-q_1}, \sqrt{-q_2})$, $Q(\sqrt{-q_1}, \sqrt{q_2})$, $Q(\sqrt{q_1}, \sqrt{q_2})$. Suppose that σ_L fixes the first of these fields. Then we claim $K_A \subseteq L$. If not,

$$L\cap K_A(\sqrt{-1}) = Q(\sqrt{-1}, \sqrt{-q_1}, \sqrt{-q_2}),$$

and by the Chebotarev density theorem there are primes $p \equiv 3 \pmod 4$ for which

$$\left(\frac{LK_A/Q}{p}\right) = \begin{cases}\{\sigma_L\} & \text{on } L,\\ 1 & \text{on } K_A.\end{cases}$$

But by Criterion A, $\mathscr{C}/\mathscr{C}^8 \cong Z_8\times Z_2$ for any such prime p, by virtue of $\left(\frac{K_A/Q}{p}\right) = 1$. This contradicts (36) and shows that $K_A \subseteq L$. In the same way K_B, $K_C \subseteq L$, and the theorem is proved.

§ 7. **A reciprocity theorem.** Since the primes q_1, q_2 and p are all $\equiv 3 \pmod 4$, the fact that $Q(\sqrt{-q_1q_2p})$ is symmetric in q_1, q_2 and p leads to some interesting relationships between the fields K_A, K_B and K_C. In order to derive them we replace p by q_3 and write $K_A(q_1, q_2)$ for K_A etc., to make the dependence on q_1 and q_2 explicit. Note that the order of q_1 and q_2 is important since we have assumed $\left(\frac{q_2}{q_1}\right) = +1$ in our discussion so far.

Criteria A, B, and C may be stated as follows. Here e_8 refers as always to the 8-rank in $Q(\sqrt{-q_1q_2q_3})$.

A: $\left(\frac{q_3}{q_1}\right) = +1 = \left(\frac{q_3}{q_2}\right) \quad \Rightarrow e_8 = 1$ iff q_3 splits in $K_A(q_1, q_2)$

B: $\left(\frac{q_3}{q_1}\right) = +1, \left(\frac{q_3}{q_2}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_3 splits in $K_B(q_1, q_2)$

C: $\left(\frac{q_3}{q_1}\right) = -1, \left(\frac{q_3}{q_2}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_3 splits in $K_C(q_1, q_2)$

($\left(\frac{q_2}{q_1}\right) = +1$).

Rewriting the Legendre symbol conditions in these statements in terms of the prime q_2 and referring to the appropriate field gives the following statements:

A: $\left(\frac{q_2}{q_1}\right) = +1, \left(\frac{q_2}{q_3}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_2 splits in $K_B(q_1, q_3)$

B: $\left(\frac{q_2}{q_1}\right) = +1, \left(\frac{q_2}{q_3}\right) = +1 \quad \Rightarrow e_8 = 1$ iff q_2 splits in $K_A(q_1, q_3)$

C: $\left(\frac{q_2}{q_3}\right) = +1, \left(\frac{q_2}{q_1}\right) = +1 \quad \Rightarrow e_8 = 1$ iff q_2 splits in $K_A(q_3, q_1)$

(Note $\left(\frac{q_3}{q_1}\right) = +1$ in A and B while $\left(\frac{q_1}{q_3}\right) = +1$ in C.)

In the same way, taking q_1 to be the featured prime gives the respective statements:

A: $\left(\frac{q_1}{q_2}\right) = -1, \left(\frac{q_1}{q_3}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_1 splits in $K_C(q_2, q_3)$

B: $\left(\frac{q_1}{q_3}\right) = -1, \left(\frac{q_1}{q_2}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_1 splits in $K_C(q_3, q_2)$

C: $\left(\frac{q_1}{q_3}\right) = +1, \left(\frac{q_1}{q_2}\right) = -1 \quad \Rightarrow e_8 = 1$ iff q_1 splits in $K_B(q_3, q_2)$

($\left(\frac{q_3}{q_2}\right) = +1$ in A, while $\left(\frac{q_2}{q_3}\right) = +1$ in B and C.)

Each of the formulations of Case A are equivalent, as are the formulations of Cases B and C. Collecting the equivalent forms of A, B and C together, we have:

CASE A: *If* $\left(\frac{q_2}{q_1}\right) = +1$, $\left(\frac{q_3}{q_1}\right) = +1$, $\left(\frac{q_3}{q_2}\right) = +1$, *then*

q_3 splits in $K_A(q_1, q_2)$ iff
q_2 splits in $K_B(q_1, q_3)$ iff
q_1 splits in $K_C(q_2, q_3)$.

Case B: *If* $\left(\frac{q_2}{q_1}\right) = +1,\ \left(\frac{q_3}{q_1}\right) = +1,\ \left(\frac{q_3}{q_2}\right) = -1,$ *then*

q_3 splits in $K_B(q_1, q_2)$ iff
q_2 splits in $K_A(q_1, q_3)$ iff
q_1 splits in $K_C(q_3, q_2)$.

Case C: *If* $\left(\frac{q_2}{q_1}\right) = +1,\ \left(\frac{q_3}{q_1}\right) = -1,\ \left(\frac{q_3}{q_2}\right) = -1,$ *then*

q_3 splits in $K_C(q_1, q_2)$ iff
q_2 splits in $K_A(q_3, q_1)$ iff
q_1 splits in $K_B(q_3, q_2)$.

It is easy to see that Cases B and C arise from Case A by renaming the primes q_i. The one combination of Legendre symbols which does not occur in these formulations is the one for which $e_4 = 0$, i.e.

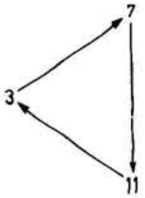
$$\left(\frac{q_2}{q_1}\right) = +1,\quad \left(\frac{q_3}{q_1}\right) = -1,\quad \left(\frac{q_3}{q_2}\right) = +1.$$

Rewriting this as

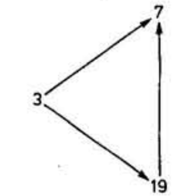
$$(37)\qquad \left(\frac{q_1}{q_3}\right) = +1,\quad \left(\frac{q_3}{q_2}\right) = +1,\quad \left(\frac{q_2}{q_1}\right) = +1$$

shows that this case represents a *cyclic* combination of q_1, q_2 and q_3. Define a triple of primes ($\equiv 3 \pmod 4$) to be a *quadratic cyclic triple* if (37) holds for some ordering of the primes, and *noncyclic* if (37) holds for *no* ordering of the primes.

This can be put in graph-theoretic terms using the graph G defined in the introduction: the directed edges of G are (q_i, q_j) (from q_i to q_j), where $\left(\frac{q_j}{q_i}\right) = +1$. For example, the triple (3, 7, 11) has the graph



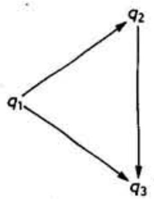
and is therefore a cyclic triple, while (3, 7, 19) has the graph



and is noncyclic. Thus (q_1, q_2, q_3) is cyclic iff G has a cycle.

The above formulation of Case A may now be stated as the

Reciprocity Theorem. *If (q_1, q_2, q_3) is a noncyclic triple of primes* $\equiv 3 \pmod 4$), *with graph*



then:

q_3 splits completely in the field $K_A(q_1, q_2)$ iff
q_2 splits completely in $K_B(q_1, q_3)$ iff
q_1 splits completely in $K_C(q_2, q_3)$,

where the respective fields are defined in equation (7) (*or in* (20), (32) *and* (34)).

This is the special reciprocity theorem as stated in the introduction.

References

[1] H. Cohn and J. C. Lagarias, *On the existence of fields governing the 2-invariants of the classgroup of $Q(\sqrt{dp})$ as p varies*, Math. Comp. 41 (1983), 711–730.

[2] A. Fröhlich, *A prime decomposition symbol for certain non Abelian number fields*, Acta Sci. Math. (Szeged) 21 (1960), 229–246.

[3] Y. Furuta, *A prime decomposition symbol for a non-abelian central extension which is abelian over a bicyclic biquadratic field*, Nagoya Math. J. 79 (1980), 79–109.

[4] F. Gerth, *Counting certain number fields with prescribed l-class numbers*, J. Reine Angew. Math. 337 (1982), 195–207.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Dritte Auflage, Physica-Verlag, Würzburg–Wien 1970.

[6] K. Kramer, *Residue properties of certain quadratic units*, J. Number Theory 21 (1985), 204–213.

[7] J. C. Lagarias, *On determining the 4-rank of the ideal class group of a quadratic field*, ibid. 12 (1980), 191–196.

[8] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), 42–48.

[9] — *On some special quartic reciprocity laws*, Acta Arith. 21 (1972), 367–377.

[10] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. 307/308 (1979), 373–398.

[11] — *Density results for the 2-classgroups of imaginary quadratic fields*, ibid. 332 (1982), 156–187.

[12] — *Density results for the 2-classgroups and fundamental units of real quadratic fields*, Studia Sci. Math. Hungar. 17 (1982), 21–43.

[13] — *The quadratic number fields with cyclic 2-classgroups*, Pacific J. Math. 108 (1983), 165–175.

[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN–Polish Scientific Publishers, Warszawa 1973.

[15] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I*, J. Reine Angew. Math. 180 (1939), 1–43.

[16] — *Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Acad. Sci. Hungar. 4 (1953), 31–87.

[17] D. Shanks, *Gauss's ternary form reduction and the 2-Sylow subgroup*, Math. Comp. 25 (1971), 837–853.

[18] P. Stevenhagen, *Class groups and governing fields*, Ph.D. thesis, Univ. of California at Berkeley, 1988.

[19] — *Ray class groups and governing fields*, Academisch proefschrift, Universiteit van Amsterdam, 1989.

DEPARTMENT OF MATHEMATICS
WELLESLEY COLLEGE
Wellesley, Massachusetts, U.S.A.

Received on 4.11.1988 (1882)

ACTA ARITHMETICA
LV (1990)

Explicit reciprocity laws on relative Lubin–Tate groups

by

YUTAKA SUEYOSHI (Fukuoka)

§ 1. **Introduction.** In [6], E. de Shalit proved an explicit reciprocity law conjectured by R. F. Coleman [3, 4]. It gives an explicit formula for the norm residue symbol on fields generated by division points of Lubin–Tate formal groups, and generalizes the explicit reciprocity laws of Artin–Hasse, Iwasawa, Kudo and Wiles [1, 9, 12, 17]. In the present paper, we extend it to *relative Lubin–Tate formal groups* and give a refinement of the explicit formulas of Iwasawa, Kudo and Wiles.

Let p be a prime number, $k/\boldsymbol{Q}_p$ a finite extension, and q the number of elements in the residue field of k. Let d be a positive integer, k' the unramified extension of k of degree d, and φ the Frobenius automorphism of k'/k. Let $\mathfrak{o}$ and $\mathfrak{o}'$ denote the integer rings of k and k', respectively, and $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. Let $v\colon k^\times \to \boldsymbol{Z}$ denote the normalized valuation of k, and let x be an element of k such that $v(x) = d$. Let $\pi \in k'$ be such that $N_{k'/k}\pi = x$, and take a power series $f \in \mathfrak{o}'[[X]]$ satisfying $f(X) \equiv \pi X \bmod \deg 2$ and $f(X) \equiv X^q \bmod \pi$. There exists a unique one-dimensional commutative formal group law (called a *relative Lubin–Tate formal group* [5]) $F_f \in \mathfrak{o}'[[X, Y]]$ such that $f \in \operatorname{Hom}(F_f, F_f^\varphi)$. We write $\underset{f}{+}$ for its addition. For $a \in \mathfrak{o}$ we denote by $[a]_f \in X\mathfrak{o}'[[X]]$ the endomorphism of F_f such that $[a]_f(X) \equiv aX \bmod \deg 2$ and $[a]_f^\varphi \circ f = f \circ [a]_f$.

Let Ω denote the completion of the algebraic closure of k, and $\mathfrak{p}_\Omega$ the maximal ideal of the integer ring of Ω. Let W_f^i denote the set of all $\mathfrak{p}^i$-division points of $F_f(\mathfrak{p}_\Omega)$. The field $k_{x,i} = k'(W_f^i)$, $i \geqslant 1$, does not depend on the choices of π and f, and is an abelian extension over k with norm group $\langle x \rangle \times (1 + \mathfrak{p}^i)$. Any element of $\tilde{W}_f^i = W_f^i - W_f^{i-1}$ is a prime element of $k_{x,i}$. The *Tate module*

$$W_f = \varprojlim_i W^i_{\varphi^{-i}(f)}$$

(the limit is taken with respect to the maps $\varphi^{-i}(f)$) of F_f is a free $\mathfrak{o}$-module of rank 1 by $[a]_f(\gamma) = ([a]_{\varphi^{-i}(f)}(\gamma_i))_i$ for $a \in \mathfrak{o}$ and $\gamma = (\gamma_i)_i \in W_f$, and