Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 345–411

On the Decomposition Laws of Rational Primes in Certain Class 2 Extensions

Susumu Shirai

Introduction

By '*class* 2 *extension*' we understand throughout this paper Galois extension whose group is a finite nilpotent group of class 2.

The investigation of non-Abelian laws of prime decomposition in certain class 2 extensions over the rational number field Q has been made by a number of writers. The first results connecting this subject matter were obtained by Rédei [36]. He defined a symbol $\{a_1, a_2, a_3\}$ with $a_i \equiv 1 \pmod 4$ which expresses the prime decomposition in a certain non-Abelian Galois extension containing $Q(\sqrt{a_1}, \sqrt{a_2})$ of degree 8 over Q, and found the multiplication and inversion properties of the symbol. Kuroda [32] proved a reciprocity of the biquadratic residue symbol, and first discovered the decomposition laws of rational primes in certain non-Abelian Galois extensions containing $Q(\sqrt{-1})$ of degree 8 over Q in terms of biquadratic residue symbols. Furuta [10] generalized the reciprocity of Kuroda to the case of 2^n-th power residue symbol. Fröhlich [7] gave a general theory of the restricted biquadratic residue symbol, and discussed again Kuroda's results with deeper properties of the symbol. Fröhlich [9] defined a new symbol $[a_1, a_2, a]_c$ which coincides with Rédei's one for a certain fixed value of c, where $c \in H^2(G(K/Q), \{\pm 1\})$ and $K = Q(\sqrt{a_1}, \sqrt{a_2})$, and which expresses the prime decomposition in a certain non-Abelian Galois extension $\hat{K}$ containing K of degree 8 over Q associated with c. This symbol is essentially the same as the Artin symbol $\left(\frac{\hat{K}/K}{\mathfrak{A}}\right)$, $\mathfrak{A}$ being an ideal of K whose norm to Q is equal to (a). Under the restriction of $a_1 \equiv a_2 \equiv 1 \pmod 4$, he proved the decomposition theorems, the uniqueness theorems, the inversion laws and the multiplication laws for the symbol, and furthermore, stated without proof the explicit form for the symbol in terms of rational quadratic characters associated with certain rational ternary quadratic forms. Recently Furuta [13] defined a simpler symbol $[a_1, a_2, a]$ via a sufficiently large ray class field of $Q(\sqrt{a_1}, \sqrt{a_2})$, which is the same as

Received July 5, 1986.

Fröhlich's one up to a part associated with Abelian extensions over Q, and made things more transparent. He gave the explicit expressions for the symbol, and proved the inversion laws with a supplementary conjecture which was verified by Akagawa [0] and Suzuki [47].

We are now in a position to state the purpose of this paper.

Let m be a natural number, K be the m-th cyclotomic field over Q, and let $\hat{K}_{\tilde{m}}$ be the central class field mod $\tilde{m}$ of K/Q in the sense of [40, § 3], where $\tilde{m}=mp_\infty$ and p_∞ stands for the real prime divisor of Q. Then $\hat{K}_{\tilde{m}}/Q$ is a class 2 extension, and conversely any class 2 extension over Q is contained in some $\hat{K}_{\tilde{m}}$ with suitable m. One answer to the problem of finding the decomposition laws of rational primes in $\hat{K}_{\tilde{m}}$ can be deduced from [40, Lemma 28]:

Lemma. *Let H be the group of total norm residues of K/Q, $S(\tilde{m})=\{a \in Q^\times \mid a\equiv 1 \pmod{\tilde{m}}\}$, $\mathfrak{g}_{K/Q}(\tilde{m})=\prod(1-\zeta_q)$, where q ranges over the prime factors of m and ζ_q denotes a primitive q-th root of unity, $N_{K/Q}$ be the norm map for K/Q, and let $S_K(\mathfrak{g}_{K/Q}(\tilde{m}))=\{\alpha \in K^\times \mid \alpha\equiv 1 \pmod{\mathfrak{g}_{K/Q}(\tilde{m})}\}$. Then*

$$G(\hat{K}_{\tilde{m}}/K)\cong H\cap S(\tilde{m})/N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m}))).$$

For $a \in H\cap S(\tilde{m})$, let $\mathfrak{A}$ be an ideal of K prime to $\tilde{m}$ such that $N_{K/Q}\mathfrak{A}=(a)$. Then the isomorphism is given in such a way that the Artin symbol $\left(\frac{\hat{K}_{\tilde{m}}/K}{\mathfrak{A}}\right)$ corresponds to a mod $N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))$.

Hence we have

Proposition. *Let p be a rational prime not dividing m, $\mathrm{Ord}\,(m,p)$ be the order of p mod m, and let f_p be the order of the class of $p^{\mathrm{Ord}\,(m,p)}$ in $H\cap S(\tilde{m})/N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))$. Then p is unramified in $\hat{K}_{\tilde{m}}$ and factors in $\hat{K}_{\tilde{m}}$ into the product of distinct prime ideals of degree $\mathrm{Ord}\,(m,p)f_p$.*

We can surely describe the groups

$$H\cap S(\tilde{m}) \quad \text{and} \quad H\cap S(\tilde{m})/N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))$$

in purely rational terms: namely, $H\cap S(\tilde{m})$ is the free Abelian group generated by the set of rational primes $\{p^{\mathrm{Ord}\,(m,p)} \mid p\nmid m\}$ and $H\cap S(\tilde{m})/N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))\cong H^{-3}(G(K/Q), Z)$, the Schur multiplicator of $G(K/Q)$. Nevertheless the proposition is unsatisfactory, because we do not know anything about the denominator $N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))$. In order to get a rational criterion for $p^{\mathrm{Ord}\,(m,p)}$ to be in $N_{K/Q}(S_K(\mathfrak{g}_{K/Q}(\tilde{m})))$, the author thinks that we must give deeper consideration to the problem.

Our goal in this paper is to determine the decomposition laws of rational primes p in all the class 2 extensions $\hat{K}_{\tilde{m}}$ whose relative groups $G(\hat{K}_{\tilde{m}}/K)$ are of exponent 2 in connection with representations of p or a certain power of p by binary quadratic forms, and the results obtained here are in a prolonged line of the papers mentioned above.

The present paper gives a full detail of the abstract [44] which was written in 1981. Since then the works in this field were done by several authors. For them, the author hopes that the reader notices especially Akagawa [0], Furuta [14], [15], [16], Furuta and Kaplan [17], Gurak [19], [20], Kaplan and Williams [28], Halter-Koch, Kaplan and Williams [29], and Suzuki [47].

The author lectured on this paper at the University of Köln in Sommersemester of 1984 and consequently could improve it in many points. He wishes to express his deep appreciation to Professor Jehne for having given him the opportunities.

Notation. Throughout this paper the following basic notation will be used.

Z	the ring of rational integers on which a finite group acts trivially.
Q	the field of rational numbers.
$\phi(n)$	the Euler function, that is, the number of positive integers $\leqq n$ which are relatively prime to n.
$\mathrm{Ord}\,(m, p)$	the order of p mod m.
$\left(\frac{h}{p}\right)$	the Legendre symbol with $\left(\frac{0}{p}\right)=0$.
(m, n)	the G.C.D. of m and n if m, n are rational integers.
p_∞	the real prime divisor of Q.
$\tilde{m}$	the product of a rational integer m and p_∞.
ζ_m	a primitive m-th root of unity.
(α)	the principal ideal generated by a number α.
$\lvert S\rvert$	the number of elements of a set S.
$\langle S\rangle$	the subgroup generated by S if S is a subset in a group.
(x, y)	the commutator $xyx^{-1}y^{-1}$ of x and y if x, y are elements in a group.
$SL_2(F)$	the special linear group of degree 2 over a field F.
$N_{K/k}$	the norm map for an extension K/k.
$G(K/k)$	the Galois group of a Galois extension K/k.
$\left(\frac{K/k}{\mathfrak{a}}\right)$	the Artin symbol.

$\left(\frac{\alpha, K/k}{\mathfrak{p}}\right)$ the Hasse norm residue symbol.

§ 1. Preliminaries I

Let K be a finite Galois extension of a finite number field k, $\mathfrak{p}$ be a prime divisor of k, $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in K, $V_{\mathfrak{P}}(i)$ be the i-th ramification group of $\mathfrak{P}$ over k, and let $\psi_{\mathfrak{P}}(i)$ be the Hasse function of $\mathfrak{P}$ with respect to K/k. We denote by $\mu(\mathfrak{p})$ the least integer i such that $V_{\mathfrak{P}}(\psi_{\mathfrak{P}}(i-1)+1)=1$, which does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$. We set

$$\mathfrak{f}(K/k)=\prod_{\mathfrak{p}} \mathfrak{p}^{\mu(\mathfrak{p})},$$

where $\mathfrak{p}$ ranges over all the finite and infinite prime divisors of k, and call this the *Galois conductor* of K/k (see [40, § 2]). By the well-known formula of Hasse [23] concerning the conductor, the Galois conductor coincides with the ordinary one if K/k is Abelian. For a module $\mathfrak{m}=\prod_{\mathfrak{p}} \mathfrak{p}^{i_{\mathfrak{p}}}$ of k, let

$$\mathfrak{g}_{K/k}(\mathfrak{m})=\prod_{\mathfrak{P}} \mathfrak{P}^{\psi_{\mathfrak{P}}(i_{\mathfrak{p}}-1)+1},$$

in which $\mathfrak{P}$ runs through all the finite and infinite prime divisors of K and $\mathfrak{p}$ is the restriction of $\mathfrak{P}$ to k. Since $i_{\mathfrak{p}}=0$ for almost all $\mathfrak{p}$, $\mathfrak{g}_{K/k}(\mathfrak{m})$ is a module of K. Put $\mathfrak{F}(K/k)=\mathfrak{g}_{K/k}(\mathfrak{f}(K/k))$, which is equal to the Geschlechtermodul when K/k is Abelian. For the Geschlechtermodul, see Iyanaga [25]. It holds from [40, Proposition 18] that if $\mathfrak{D}(K/k)$ is the different of K/k, then $\mathfrak{f}(K/k)=\mathfrak{D}(K/k)\mathfrak{F}(K/k)$. Moreover by [40, Lemmas 19, 20 and 21], we have the following three lemmas.

Lemma 1.1. *Let $L\supset K\supset k$ be a tower of Galois extensions, and let $\mathfrak{f}(K/k)\,|\,\mathfrak{m}$. Then*:

(i) $\mathfrak{f}(K/k)\,|\,\mathfrak{f}(L/k)$.

(ii) *If $\mathfrak{f}(L/K)\,|\,\mathfrak{g}_{K/k}(\mathfrak{m})$, then $\mathfrak{f}(L/k)\,|\,\mathfrak{m}$. In particular, if $\mathfrak{f}(L/K)\,|\,\mathfrak{F}(K/k)$, then $\mathfrak{f}(L/k)=\mathfrak{f}(K/k)$.*

Lemma 1.2. *Let $L\supset K\supset k$ be a tower of Galois extensions, L/K be Abelian, and let $\mathfrak{f}(K/k)\,|\,\mathfrak{m}$. Then*:

(i) $\mathfrak{f}(L/K)\,|\,\mathfrak{g}_{K/k}(\mathfrak{f}(L/k))$.

(ii) *If $\mathfrak{f}(L/k)\,|\,\mathfrak{m}$, then $\mathfrak{f}(L/K)\,|\,\mathfrak{g}_{K/k}(\mathfrak{m})$. In particular, if $\mathfrak{f}(L/k)=\mathfrak{f}(K/k)$, then $\mathfrak{f}(L/K)\,|\,\mathfrak{F}(K/k)$.*

Lemma 1.3 *Let K/k be a Galois extension, and let k'/k be an Abelian extension. If $\mathfrak{f}(k'/k)\,|\,\mathfrak{m}$, then $\mathfrak{f}(Kk'/K)\,|\,\mathfrak{g}_{K/k}(\mathfrak{m})$.*

Let $L \supset K \supset k$ be a tower of Galois extensions. Then L is called a central extension of K/k if $G(L/K)$ is contained in the center of $G(L/k)$, and is said to be a genus extension of K/k if it is obtained from K by composing an Abelian extension over k. Let $\mathfrak{m}$ be a module of k, and let K/k be a Galois extension with $\mathfrak{f}(K/k)\,|\,\mathfrak{m}$. Then we denote by $\hat{K}_{\mathfrak{m}}$ (resp. $K_{\mathfrak{m}}^{*}$) the maximal central (resp. genus) extension L with $\mathfrak{f}(L/k)\,|\,\mathfrak{m}$ of K/k, which is equal to the maximal central (resp. genus) extension of K/k contained in the ray class field mod $\mathfrak{g}_{K/k}(\mathfrak{m})$ of K by Lemmas 1.1 and 1.2, and call it the central class field (resp. the genus field) mod $\mathfrak{m}$ of K/k. For the structure of $G(\hat{K}_{\mathfrak{m}}/K_{\mathfrak{m}}^{*})$, see Heider [24] who completed a general theory of central extensions, Scholz [37] and [40, Theorem 29].

From now on we treat the case where the base field k is the rational number field Q and K the m-th cyclotomic field over Q. In this case, the central class field $\hat{K}_{\tilde{m}}$ mod $\tilde{m}$ of K/Q is a class 2 extension over Q by definition. We obtain from [40, Theorem 32]

Theorem 1.4. *Let m be a natural number such that $(m, 16) \neq 8$, and let K be the m-th cyclotomic field over Q. Then*

$$G(\hat{K}_{\tilde{m}}/K) \cong H^{-3}(G(K/Q), Z).$$

This is a generalization of Fröhlich [6, Theorem 3] to a cyclotomic field over Q. Hence by [42, Theorem A] and [43, Lemma 1], we have

Theorem 1.5. *Let $m = 2^{\nu} q_1^{\nu_1} \cdots q_r^{\nu_r}$ be the factorization of m into rational prime factors, and let K be the m-th cyclotomic field over Q. If $\nu \neq 3$, then $\hat{K}_{\tilde{m}}/Q$ is a class 2 extension of degree $\phi(m) \prod (\phi(q_i^{\nu_i}), \phi(q_j^{\nu_j}))$, where i, j range over the integers such that $1 \leqq i < j \leqq r$ or $-1 \leqq i < j \leqq r$ according as $\nu \leqq 1$ or $\nu \geqq 2$ under the conventions of $\phi(q_{-1}^{\nu_{-1}}) = 2^{\nu-2}$ and $\phi(q_0^{\nu_0}) = 2$. Conversely every class 2 extension over Q is contained in some $\hat{K}_{\tilde{m}}$ with suitable m.*

Let m be a natural number as in Theorem 1.5, and let g_j be a fixed primitive root mod $q_j^{\nu_j}$. Then we define the symbols $[j, i]$, $[0, i]^*$ and $[0, i]$ by putting

$$
(1.1)\qquad
\begin{aligned}
&q_i \equiv g_j^{[j,i]} \pmod{q_j^{\nu_j}},\ i = 0, 1, \cdots, r,\ j = 1, \cdots, r,\ i \neq j,\\
&q_i \equiv (-1)^{[0,i]^*}\, 5^{[0,i]} \pmod{2^{\nu}},\ i = 1, \cdots, r,\\
&[i, i] = 0,\ i = 1, \cdots, r,
\end{aligned}
$$

where $q_0 = 2$. In other words, $[j, i]$ is the index of q_i mod $q_j^{\nu_j}$ relative to the primitive root g_j, and $[0, i]^*$, $[0, i]$ are the indices of q_i mod 2^ν relative to the basis $\{-1, 5\}$. The next theorem is [42, Theorem 6], which is a generalization of Fröhlich [6, Theorem 4].

Theorem 1.6. *Let $m=2^\nu q_1^{\nu_1}\cdots q_r^{\nu_r}$, and let K be the m-th cyclotomic field over Q. Then:*

(i) $\nu=0, 1$. *The Galois group $G(\hat{K}_{\tilde{m}}/Q)$ is generated by r elements $x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j), \qquad \textit{all } i, j, k,$$

$$x_i^{\phi(q_i^{\nu_i})} = \left(\prod_{j=1}^{r}(x_i, x_j)^{-[j,i]}\right)^{q_i^{\nu_i-1}}, \qquad i=1, \cdots, r.$$

(ii) $\nu=2$. *$G(\hat{K}_{\tilde{m}}/Q)$ is generated by $r+1$ elements $x_0, x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j), \qquad \textit{all } i, j, k,$$

$$x_0^2 = 1,$$

$$x_i^{\phi(q_i^{\nu_i})} = \left((x_i, x_0)^{-[0,i]^*}\prod_{j=1}^{r}(x_i, x_j)^{-[j,i]}\right)^{q_i^{\nu_i-1}}, \qquad i=1, \cdots, r.$$

(iii) $\nu\geqq 4$. *$G(\hat{K}_{\tilde{m}}/Q)$ is generated by $r+2$ elements $x_{-1}, x_0, x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j), \qquad \textit{all } i, j, k,$$

$$x_{-1}^{2^{\nu-2}} = 1,$$

$$x_0^2 = \prod_{j=1}^{r}(x_{-1}, x_j)^{-[j,0]},$$

$$x_i^{\phi(q_i^{\nu_i})} = \left((x_i, x_{-1})^{-[0,i]}(x_i, x_0)^{-[0,i]^*}\prod_{j=1}^{r}(x_i, x_j)^{-[j,i]}\right)^{q_i^{\nu_i-1}},$$
$$i=1, \cdots, r.$$

In any case, $(x, y)=xyx^{-1}y^{-1}$, the commutator of x and y, and x_{-1}, x_0, x_i are suitable extensions of the norm residue symbols

$$\tau=\left(\frac{5, K/Q}{2}\right), \quad \tau^*=\left(\frac{-1, K/Q}{2}\right) \quad \textit{and}$$
$$\tag{1.2} \tau_i=\left(\frac{g_i, K/Q}{q_i}\right) \qquad \textit{for } i=1, \cdots, r,$$

to $\hat{K}_{\tilde{m}}$, respectively.

Moreover from Theorem 1.4 and [43, Lemma 2] follows

Theorem 1.7. *Let the hypotheses and notation be as in Theorem* 1.6. *Then*:

(i) $\nu=0, 1$. *The Galois group* $G(\hat{K}_{\tilde{m}}/K)$ *is generated by* $\binom{r}{2}$ *elements* x_{ij}, $1\leqq i<j\leqq r$, *and completely determined by the relations*

$$\begin{aligned} &x_{ij}x_{kl}=x_{kl}x_{ij}, && \text{all } i, j, k, l, \\ &x_{ij}^{(\phi(q_i^{\nu_i}),\phi(q_j^{\nu_j}))}=1, && 1\leqq i<j\leqq r. \end{aligned}$$

(ii) $\nu=2$. $G(\hat{K}_{\tilde{m}}/K)$ *is generated by* $\binom{r+1}{2}$ *elements* x_{ij}, $0\leqq i<j\leqq r$, *and completely determined by the relations*

$$\begin{aligned} &x_{ij}x_{kl}=x_{kl}x_{ij}, && \text{all } i, j, k, l, \\ &x_{0i}^2=1, && i=1, \cdots, r, \\ &x_{ij}^{(\phi(q_i^{\nu_i}),\phi(q_j^{\nu_j}))}=1, && 1\leqq i<j\leqq r. \end{aligned}$$

(iii) $\nu\geqq 4$. $G(\hat{K}_{\tilde{m}}/K)$ *is generated by* $\binom{r+2}{2}$ *elements* x_{ij}, $-1\leqq i<j\leqq r$, *and completely determined by the relations*

$$\begin{aligned} &x_{ij}x_{kl}=x_{kl}x_{ij}, && \text{all } i, j, k, l, \\ &x_{-10}^2=1, && \\ &x_{-1i}^{(2^{\nu-2},\phi(q_i^{\nu_i}))}=1, && i=1, \cdots, r, \\ &x_{0i}^2=1, && i=1, \cdots, r, \\ &x_{ij}^{(\phi(q_i^{\nu_i}),\phi(q_j^{\nu_j}))}=1, && 1\leqq i<j\leqq r. \end{aligned}$$

In any case, $x_{ij}=(x_i, x_j)$, x_i *being as in Theorem* 1.6.

We next treat the last case of $\nu=3$. As regard this case, see the footnotes on pages 242 and 247 of Fröhlich [6]. We use the results and notation of [40] and [42].

Let K be a finite Galois extension of a $\mathfrak{p}$-adic number field k, $U_K^{(i)}$ be the i-th unit group of K, and let T be the inertia field of K/k. We denote by $\psi_{K/k}(i)$ the Hasse function for K/k, and by $\mu(K/k)$ the $\mathfrak{p}$-exponent of the local Galois conductor of K/k in the sense of [40, § 1]. Notice that $\mu(K/k)$ is equal to $\mu(\mathfrak{p})$ defined at the first part of this section.

Lemma 1.8. *Let* $Z(n)$ *denotes the cyclic group of order* n. *If* $G(K/T)\cong Z(n_1)\times Z(n_2)\times\cdots\times Z(n_r)$ (*direct product*), *then*

$$|1^*(H^{-1}(G(K/k), U_K^{(\psi_{K/k}(i-1)+1)}))|\leqq\prod_{1\leqq i<j\leqq r}(n_i, n_j)$$

for $i\geqq\mu(K/k)$, *where* $1: U_K^{(\psi_{K/k}(i-1)+1)}\to K^\times$ *denotes the inclusion map and* 1^* *the corresponding cohomology map.*

Proof. We have the following commutative diagram in which the first row is exact by [40, Lemma 8]:

$$\begin{array}{ccccc} H^{-1}(G(K/T), U_K^{(\psi_{K/k}(i-1)+1)}) & \xrightarrow{\mathrm{Inj}} & H^{-1}(G(K/k), U_K^{(\psi_{K/k}(i-1)+1)}) & \longrightarrow & 0 \\ \downarrow{\scriptstyle 1^*} & & \downarrow{\scriptstyle 1^*} & & \\ H^{-1}(G(K/T), K^\times) & \xrightarrow{\mathrm{Inj}} & H^{-1}(G(K/k), K^\times), & & \end{array}$$

here Inj mean the injection maps. By local class field theory,

$$H^{-1}(G(K/T), K^\times)$$

is isomorphic to the Schur multiplicator $H^{-3}(G(K/T), Z)$, and

$$|H^{-3}(G(K/T), Z)|=\prod_{1\leqq i<j\leqq r}(n_i, n_j)$$

(see [43, Lemma 1], for example). This completes the proof.

Theorem 1.9. *Let the situation be as in Theorem* 1.6, *and suppose* $\nu=3$. *Then* $(x_{-1}, x_0)=1$, *and the Galois group* $G(\hat{K}_{\tilde{m}}/K)$ *with* $\nu=3$ *is isomorphic to the factor group of* $H^{-3}(G(K/Q), Z)$ *modulo the subgroup of order* 2, *and hence it is generated by* $\binom{r+2}{2}-1$ *elements* $x_{ij}=(x_i, x_j)$, $-1\leqq i<j\leqq r$, $(i,j)\neq(-1, 0)$, *and completely determined by the relations*

$$\begin{aligned} &x_{ij}x_{kl}=x_{kl}x_{ij}, && \textit{all } i, j, k, l,\\ &x_{-1i}^2=1, && i=1, \cdots, r,\\ &x_{0i}^2=1, && i=1, \cdots, r,\\ &x_{ij}^{(\phi(q_i^{\nu_i}),\phi(q_j^{\nu_j}))}=1, && 1\leqq i<j\leqq r. \end{aligned}$$

Proof. Let Q_2 be the 2-adic number field, T/Q_2 be a finite unramified extension, ζ be a primitive 2^3-th root of unity, and let $K_2=T(\zeta)$. Let further

$$\tau^*=(-1, K_2/Q_2), \qquad \tau=(5, K_2/Q_2),$$

where $(, K/k)$ denotes the local norm residue symbol for K/k, and let $\hat{K}_2$ be any central extension of K_2/Q_2 such that $\mu(K_2/Q_2)\leqq 3$. Since $1+2\sqrt{-1}\in U_{Q_2(\sqrt{-1})}^{(2)}$, and since $T(\sqrt{-1})/Q_2(\sqrt{-1})$ is unramified, there exists $\alpha\in U_{T(\sqrt{-1})}^{(2)}$ such that $N_{T(\sqrt{-1})/Q_2(\sqrt{-1})}\alpha=1+2\sqrt{-1}$, $N_{K/k}$ being the norm map for K/k. Thus we have

$$\tau=(1+2\sqrt{-1},\ K_2/Q_2(\sqrt{-1}))=(\alpha,\ K_2/T(\sqrt{-1})),$$

because of $N_{Q_2(\sqrt{-1})/Q_2}(1+2\sqrt{-1})=5$. Noticing that $\hat{K}_2/T(\sqrt{-1})$ is Abelian, we put

$$\tilde{\tau}=(\alpha,\ \hat{K}_2/T(\sqrt{-1})).$$

Then it follows from [42, Lemma 3] that $\tilde{\tau}^2=1$. Therefore for any extension $\tilde{\tau}^*$ of τ^* to $\hat{K}_2$,

$$\begin{aligned}(\tilde{\tau},\ \tilde{\tau}^*)&=\tilde{\tau}\tilde{\tau}^*\tilde{\tau}^{-1}\tilde{\tau}^{*-1}=\tilde{\tau}\tilde{\tau}^*\tilde{\tau}\tilde{\tau}^{*-1}\\&=(\alpha,\ \hat{K}_2/T(\sqrt{-1}))(\alpha^{\tau^*},\ \hat{K}_2/T(\sqrt{-1}))\\&=(N_{T(\sqrt{-1})/T}\alpha,\ \hat{K}_2/T(\sqrt{-1})),\end{aligned}$$

because the restriction of τ^* to $T(\sqrt{-1})$ is the generator of $G(T(\sqrt{-1})/T)$. The Hasse function for $T(\sqrt{-1})/T$ is given by $\psi(i-1)+1=2(i-1)$ for $i\geqq 2$, and hence

$$N_{T(\sqrt{-1})/T}\alpha \in N_{T(\sqrt{-1})/T}U^{(2)}_{T(\sqrt{-1})}=U^{(2)}_T\subset U^{(4)}_{T(\sqrt{-1})}$$

(see for example [40, Lemma 6]). On the other hand, since $\mu(\hat{K}_2/Q_2)\leqq 3$, it follows from [40, Lemma 4] that $\mu(\hat{K}_2/T(\sqrt{-1}))\leqq 4$, which implies $(\tilde{\tau},\ \tilde{\tau}^*)=1$. According to [42, § 3], it is now clear that we can choose the extensions x_{-1}, x_0 of τ and τ^* to $\hat{K}_{\tilde{m}}$, respectively, such that $(x_{-1},\ x_0)=1$ and $x_{-1}^2=1$.

Since $G(\hat{K}_{\tilde{m}}/Q)$ is of class 2, and since $G(\hat{K}_{\tilde{m}}/K)$ is the commutator subgroup of $G(\hat{K}_{\tilde{m}}/Q)$, the elements x_{ij}, $-1\leqq i<j\leqq r$, generate $G(\hat{K}_{\tilde{m}}/K)$, and satisfy the relations described in the theorem and $x_{-10}^2=1$. But $x_{-10}=(x_{-1},\ x_0)=1$, hence

$$|G(\hat{K}_{\tilde{m}}/K)|\leqq 2^{2r}\prod_{1\leqq i<j\leqq r}(\phi(q_i^{\nu_i}),\ \phi(q_j^{\nu_j})).$$

We remark that the right side is equal to the half of the order of $H^{-3}(G(K/Q),\ Z)$. On the other hand, it follows from [40, Theorem 29] that

$$H^{-3}(G(K/Q),\ Z)/F(K/Q)_{\tilde{m}}\cong G(\hat{K}_{\tilde{m}}/K),$$

where

$$F(K/Q)_{\tilde{m}}=\sum_{\mathfrak{P}|\tilde{m}}\mathrm{Inj}_{\mathfrak{P}}\ \iota_{\mathfrak{P}}^{-1}1^*(H^{-1}(G_{\mathfrak{P}},\ U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})})),$$

$\mu_{\mathfrak{P}}=\psi_{K_{\mathfrak{P}}/Q_{q_i}}(\nu_i-1)+1$, $i=0, 1, \cdots, r+1$, if $\mathfrak{P}\,|\,q_i$ with the convention that $q_0=2$, $\nu_0=3$ and $q_{r+1}=p_\infty$, $\nu_\infty=1$,

$U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})}$	the $\mu_{\mathfrak{P}}$-th unit group of the completion $K_{\mathfrak{P}}$,
$G_{\mathfrak{P}}$	the decomposition group of $\mathfrak{P}$ over Q,
1^*	the cohomology map induced by the inclusion map $1: U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})} \longrightarrow K_{\mathfrak{P}}^{\times}$,
$\iota_{\mathfrak{P}}$	the Tate isomorphism of $H^{-3}(G_{\mathfrak{P}}, Z)$ to $H^{-1}(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times})$,
$\mathrm{Inj}_{\mathfrak{P}}$	the injection map of $H^{-3}(G_{\mathfrak{P}}, Z)$ to $H^{-3}(G(K/Q), Z)$,

and the sum runs over non-conjugate prime factors of $\tilde{m}$ in K. By Lemma 1.8, we see $|F(K/Q)_{\tilde{m}}| \leqq 2$, because the inertia group of a prime factor of 2 in K is of type (2, 2), and the others are cyclic. Hence $|F(K/Q)_{\tilde{m}}|=2$, and $G(\hat{K}_{\tilde{m}}/K)$ is completely described by the relations given in the theorem.

Theorem 1.10. *Let the situation be as in Theorem* 1.6, *and suppose* $\nu=3$. *Then the Galois group* $G(\hat{K}_{\tilde{m}}/Q)$ *is generated by* $r+2$ *elements* x_{-1}, $x_0, x_1, \cdots, x_r$, *and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j), \qquad \text{all } i, j, k,$$

$$(x_{-1}, x_0)=1,$$

$$x_{-1}^2=1,$$

$$x_0^2=\prod_{j=1}^{r}(x_{-1}, x_j)^{-[j,0]},$$

$$x_i^{\phi(q_i^{\nu_i})}=((x_i, x_{-1})^{-[0,i]}(x_i, x_0)^{-[0,i]^*}\prod_{j=1}^{r}(x_i, x_j)^{-[j,i]})^{q_i^{\nu_i-1}},$$
$$i=1, \cdots, r,$$

where x_{-1}, x_0, x_i *are suitable extensions of the norm residue symbols* (1.2) *to* $\hat{K}_{\tilde{m}}$, *respectively.*

Proof. Since $G(K/Q)$ is generated by (1.2), it is clear that $G(\hat{K}_{\tilde{m}}/Q)$ is generated by the elements x_i, and in the proof of Theorem 1.9, we already understood the second and third relations. The other relations follows from Theorem 1.6, (iii), because $\hat{K}_{\tilde{m}}$ with $\nu=3$ is contained in $\hat{K}_{\tilde{m}}$ with $\nu \geqq 4$ (see the footnote on page 126 of [42]). To show the converse, let G be the abstract group generated by $r+2$ elements x_i with the above defining relations except $(x_{-1}, x_0)=1$, and let $G'=G/\langle(x_{-1}, x_0)\rangle$. Then G is one of the representation groups of $G(K/Q)$, and $G(\hat{K}_{\tilde{m}}/Q)$ is a homomorphic image of G'. Since $(x_{-1}, x_0)^2=(x_{-1}^2, x_0)=1$,

$$|G'|=|G(K/Q)|\cdot|H^{-3}(G(K/Q), Z)|/2.$$

By Theorem 1.9, we know that $G(\hat{K}_{\tilde{m}}/Q)$ has the same order. Hence

$G(\hat{K}_{\tilde{m}}/Q)\cong G'$, which implies that $G(\hat{K}_{\tilde{m}}/Q)$ is completely determined by the relations given in the theorem.

§ 2. Reduction

Let $m=q_1^{\nu_1}\cdots q_r^{\nu_r}$, $q_1,\cdots,q_r$ distinct odd primes, K be the m-th cyclotomic field over Q, and let $\hat{K}_{\tilde{m}}$ be the central class field mod $\tilde{m}$ of K/Q. We denote by K_{ij} the $q_i^{\nu_i}q_j^{\nu_j}$-th cyclotomic field over Q, and by $\hat{K}_{ij}$ the central class field mod $q_i^{\nu_i}q_j^{\nu_j}p_\infty$ of K_{ij}/Q for the sake of simplicity.

Lemma 2.1. *The central class field* mod $\tilde{m}$ *of* K_{12}/Q *is equal to* $\hat{K}_{12}K$.

Proof. Let L be the central class field mod $\tilde{m}$ of K_{12}/Q. Since the genus field mod $\tilde{m}$ of K_{12}/Q is K by [40, Lemma 27], it follows from [40, Theorem 29] that $[L:K]=|H^{-3}(G(K_{12}/Q),Z)|$. On the other hand, since the genus field mod $q_1^{\nu_1}q_2^{\nu_2}p_\infty$ of K_{12}/Q is K_{12} itself, $\hat{K}_{12}\cap K=K_{12}$, and hence $[\hat{K}_{12}K:K]=[\hat{K}_{12}:K_{12}]=|H^{-3}(G(K_{12}/Q),Z)|$ by Theorem 1.4. Thus it suffices to show $L\supset\hat{K}_{12}K$. Since the Abelian extension $\hat{K}_{12}K/K_{12}$ is defined mod $\mathfrak{g}_{K_{12}/Q}(\tilde{m})$ by the definition of $\hat{K}_{12}$ and Lemma 1.2, the Galois conductor of $\hat{K}_{12}K/Q$ divides $\tilde{m}$ by Lemma 1.1. It is clear that $\hat{K}_{12}K$ is a central extension of K_{12}/Q. Hence $L\supset\hat{K}_{12}K$.

According to Theorem 1.7, $G(\hat{K}_{\tilde{m}}/K)$ is generated by $\binom{r}{2}$ elements $x_{ij}=(x_i,x_j)$, $1\leqq i<j\leqq r$, and completely determined by the relations

$$x_{ij}x_{kl}=x_{kl}x_{ij},\qquad \text{all } i,j,k,l,$$
$$x_{ij}^{(\phi(q_i^{\nu_i}),\phi(q_j^{\nu_j}))}=1,\qquad 1\leqq i<j\leqq r.$$

Lemma 2.2. *Let* $H=\langle\{x_{ij}\,|\,1\leqq i<j\leqq r,\ (i,j)\neq(1,2)\}\rangle$. *Then* $\hat{K}_{12}K$ *is the subfield of* $\hat{K}_{\tilde{m}}$ *corresponding to* H.

Proof. Let M be the fixed subfield of $\hat{K}_{\tilde{m}}$ under H. Then $[M:K]$ $(\phi(q_1^{\nu_1}),\phi(q_2^{\nu_2}))=|H^{-3}(G(K_{12}/Q),Z)|=[\hat{K}_{12}K:K]$. We show $\hat{K}_{12}K\supset M$. By Theorem 1.6, $G(M/Q)$ is completely described by the relations

$$(\bar{x}_1,\bar{x}_2)\bar{x}_k=\bar{x}_k(\bar{x}_1,\bar{x}_2),\qquad k=1,\cdots,r,$$
$$\bar{x}_i\bar{x}_j=\bar{x}_j\bar{x}_i,\quad 1\leqq i<j\leqq r,\quad (i,j)\neq(1,2),$$
$$\bar{x}_1^{\phi(q_1^{\nu_1})}=(\bar{x}_1,\bar{x}_2)^{-[2,1]q_1^{\nu_1-1}},$$
$$\bar{x}_2^{\phi(q_2^{\nu_2})}=(\bar{x}_1,\bar{x}_2)^{[1,2]q_2^{\nu_2-1}},$$
$$\bar{x}_i^{\phi(q_i^{\nu_i})}=1,\qquad i=3,\cdots,r,$$

where $\bar{x}_i$ denotes the restriction of x_i to M. Since the restrictions of $\bar{x}_3,\cdots,\bar{x}_r$ and $(\bar{x}_1,\bar{x}_2)$ to K_{12} are trivial by (1.2), $G(M/K_{12})\supset\langle(\bar{x}_1,\bar{x}_2),$

$\bar{x}_3, \cdots, \bar{x}_r\rangle$, but they have the same order $(\phi(q_1^{\nu_1}), \phi(q_2^{\nu_2}))\times\phi(q_3^{\nu_3}\cdots q_r^{\nu_r})$ and hence coincide. We see that $G(M/K_{12})$ is contained in the center of $G(M/Q)$. By the definition of $\hat{K}_{\tilde{m}}$ and Lemma 1.1, it is trivial that the Galois conductor of M/Q divides $\tilde{m}$. We get $\hat{K}_{12}K\supset M$, because of Lemma 2.1.

Theorem 2.3. *Let $m=2^\nu q_1^{\nu_1}\cdots q_r^{\nu_r}$, $q_1, \cdots, q_r$ be distinct odd primes, K be the m-th cyclotomic field over Q, and let $\hat{K}_{\tilde{m}}$ be the central class field* mod $\tilde{m}$ *of K/Q. Let further K_i be the $q_i^{\nu_i}$-th cyclotomic field over Q for $i=1, \cdots, r$, $K_0=Q(\sqrt{-1})$ if $\nu\geqq 2$, and let K_{-1} be the maximal real subfield of the 2^ν-th cyclotomic field over Q if $\nu\geqq 3$. Set $K_{ij}=K_iK_j$ for $-1\leqq i<j\leqq r$, and denote by $\hat{K}_{ij}$ the central class field* mod $q_i^{\nu_i}q_j^{\nu_j}p_\infty$ *of K_{ij}/Q for $1\leqq i<j\leqq r$, by $\hat{K}_{0j}$ the central class field* mod $2^2q_j^{\nu_j}p_\infty$ *of K_{0j}/Q for $j=1, \cdots, r$, by $\hat{K}_{-10}$ the central class field* mod $2^\nu p_\infty$ *of K_{-10}/Q, and by $\hat{K}_{-1j}$ the central class field* mod $2^\nu q_j^{\nu_j}p_\infty$ *of K_{-1j}/Q for $j=1, \cdots, r$. Then:*

(i) $\nu=0, 1$.

$$\hat{K}_{\tilde{m}}=\prod_{1\leqq i<j\leqq r}\hat{K}_{ij}.$$

(ii) $\nu=2$.

$$\hat{K}_{\tilde{m}}=\prod_{0\leqq i<j\leqq r}\hat{K}_{ij}.$$

(iii) $\nu=3$.

$$\hat{K}_{\tilde{m}}=\prod_{\substack{-1\leqq i<j\leqq r\\(i,j)\neq(-1,0)}}\hat{K}_{ij}.$$

(iv) $\nu\geqq 4$.

$$\hat{K}_{\tilde{m}}=\prod_{-1\leqq i<j\leqq r}\hat{K}_{ij}.$$

Proof. (i) By Lemma 2.2, we obtain

$$\hat{K}_{\tilde{m}}=\prod_{1\leqq i<j\leqq r}\hat{K}_{ij}K=\Big(\prod_{1\leqq i<j\leqq r}\hat{K}_{ij}\Big)K=\prod_{1\leqq i<j\leqq r}\hat{K}_{ij}.$$

The arguments of the same type ensure the other cases. We must notice that if $\nu=3$, then $\hat{K}_{-10}=K_{-10}$ by Theorem 1.9, and in the cases (iii) and (iv), the genus field mod $2^\nu q_j^{\nu_j}p_\infty$ of K_{-1j}/Q is not K_{-1j} but $K_{-10}K_j$ which is the $2^\nu q_j^{\nu_j}$-th cyclotomic field over Q, because of $\mathfrak{f}(K_{-1j}/Q)=2^\nu q_j^{\nu_j}p_\infty$ and [40, Lemma 27].

The next lemma is well-known and can be easily verified.

Lemma 2.4. *Let K_i be a Galois extension of a finite number field k*

for $i=1, \cdots, r$, $L=K_1 \cdots K_r$, $\mathfrak{P}$ be a prime ideal of L, and let $\mathfrak{P}_i$ be the restriction of $\mathfrak{P}$ to K_i. Denote by $f(\mathfrak{P}), f(\mathfrak{P}_i)$ the degrees of $\mathfrak{P}$ and $\mathfrak{P}_i$ over k, respectively. Then if $\mathfrak{P}$ is unramified over k, $f(\mathfrak{P})=\{f(\mathfrak{P}_1), \cdots, f(\mathfrak{P}_r)\}$, the least common multiple.

From Theorem 2.3 and Lemma 2.4, we may conclude that the investigation of the decomposition laws of rational primes in $\hat{K}_{\tilde{m}}$ can be reduced to that in the following four types of class 2 extensions:

$$(\alpha) \quad \hat{K}_{12}, \quad [\hat{K}_{12}: K_{12}]=(\phi(q_1^{\nu_1}), \phi(q_2^{\nu_2})), \quad m=q_1^{\nu_1}q_2^{\nu_2}.$$

$$(\beta) \quad \hat{K}_{01}, \quad [\hat{K}_{01}: K_{01}]=2, \quad m=2^2 q_1^{\nu_1}.$$

$$(\gamma) \quad \hat{K}_{-10}, \quad [\hat{K}_{-10}: K_{-10}]=2, \quad m=2^{\nu} \quad \text{with} \quad \nu \geqq 4.$$

$$(\delta) \quad \hat{K}_{-11}, \quad [\hat{K}_{-11}: K_{-10}K_1]=(2^{\nu-2}, \phi(q_1^{\nu_1})) \text{ with } \nu \geqq 3.$$

Here we study the decomposition laws of rational primes with certain conditions in the class 2 extensions of these four types.

For any rational prime $p \neq q_1, q_2$, let

$$p \equiv g_1^{\mathrm{ind}_1 p} \pmod{q_1^{\nu_1}} \quad \text{and} \quad p \equiv g_2^{\mathrm{ind}_2 p} \pmod{q_2^{\nu_2}},$$

where g_1, g_2 are as in (1.1), and for any odd prime p, let

$$p \equiv (-1)^{\mathrm{ind}_0^* p}\, 5^{\mathrm{ind}_0 p} \pmod{2^{\nu}}.$$

Theorem 2.5. *Let $m=q_1^{\nu_1}q_2^{\nu_2}$, and let $d_{12}=(\phi(q_1^{\nu_1}), \phi(q_2^{\nu_2}))$. If p is a rational prime not dividing m, then it is unramified in $\hat{K}_{12}$. Moreover, if* Ord $(m, p) \equiv 0$ (mod d_{12}), *and if $\mathfrak{P}$ is a prime factor of p in K_{12}, then*

$$\left(\frac{\hat{K}_{12}/K_{12}}{\mathfrak{P}}\right)=(x_1, x_2)^{\{[1,2]\,\mathrm{ind}_2 p/(q_2-1)-[2,1]\,\mathrm{ind}_1 p/(q_1-1)+\frac{1}{2}\mathrm{ind}_1 p\, \mathrm{ind}_2 p\}\, \mathrm{Ord}(m,p)}$$

$$=(x_1, x_2),$$

and hence p is decomposed in $\hat{K}_{12}$ as

$$(p)=\mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_g,$$

$$N_{\hat{K}_{12}/Q}\mathfrak{Q}_i=p^{\mathrm{Ord}(m,p)f_p}, \qquad \mathrm{Ord}\,(m, p)f_p g=\phi(m)d_{12},$$

where

$$f_p=d_{12}\Big/\left(d_{12}, \left\{[1, 2]\frac{\mathrm{ind}_2 p}{q_2-1}-[2, 1]\frac{\mathrm{ind}_1 p}{q_1-1}+\frac{1}{2}\,\mathrm{ind}_1 p\, \mathrm{ind}_2 p\right\} \times \mathrm{Ord}\,(m, p)\right),$$

and $\{x_1, x_2\}$ *is the system of generators of* $G(\hat{K}_{12}/Q)$ *as in Theorem* 1.6.

Proof. Since the Galois conductor of $\hat{K}_{12}/Q$ is $\tilde{m}=q_1^{\nu_1}q_2^{\nu_2}p_\infty$, p is unramified in $\hat{K}_{12}$. By Theorem 1.6, $G(\hat{K}_{12}/Q)$ is generated by x_1, x_2, and completely determined by the relations

$$(2.1)\qquad \begin{aligned} &(x_1, x_2)x_k=x_k(x_1, x_2), \qquad k=1, 2,\\ &x_1^{\phi(q_1^{\nu_1})}=(x_1, x_2)^{-[2,1]q_1^{\nu_1-1}},\\ &x_2^{\phi(q_2^{\nu_2})}=(x_1, x_2)^{[1,2]q_2^{\nu_2-1}}, \end{aligned}$$

here x_1, x_2 are extensions of the norm residue symbols

$$\tau_1=\left(\frac{g_1, K_{12}/Q}{q_1}\right) \quad\text{and}\quad \tau_2=\left(\frac{g_2, K_{12}/Q}{q_2}\right)$$

to $\hat{K}_{12}$, respectively. Now let $\mathfrak{Q}$ be any prime factor of p in $\hat{K}_{12}$, and let $\left[\frac{\hat{K}_{12}}{\mathfrak{Q}}\right]$ denote the Frobenius automorphism of $\mathfrak{Q}$ over Q. Since $\hat{K}_{12}$ is a central extension of K_{12}/Q, the value of the Artin symbol $\left(\frac{\hat{K}_{12}/K_{12}}{\mathfrak{P}}\right)$ does not depend on the choice of $\mathfrak{P}$ over p, and hence

$$\left[\frac{\hat{K}_{12}}{\mathfrak{Q}}\right]^{\mathrm{Ord}\,(m,p)}=\left(\frac{\hat{K}_{12}/K_{12}}{\mathfrak{P}}\right).$$

Using the product formula of Hasse for the norm residue symbol (see [21]), we have

$$\left(\frac{p, K_{12}/Q}{p}\right)\left(\frac{p, K_{12}/Q}{q_1}\right)\left(\frac{p, K_{12}/Q}{q_2}\right)=1,$$

which implies

$$\left(\frac{K_{12}/Q}{p}\right)=\tau_1^{\mathrm{ind}_1 p}\tau_2^{\mathrm{ind}_2 p}.$$

The restriction of $\left[\frac{\hat{K}_{12}}{\mathfrak{Q}}\right]$ to K_{12} is equal to the left side of this equality, and hence we may write

$$\left[\frac{\hat{K}_{12}}{\mathfrak{Q}}\right]=x_1^{\mathrm{ind}_1 p}x_2^{\mathrm{ind}_2 p}\varepsilon \qquad \text{for some } \varepsilon\in G(\hat{K}_{12}/K_{12}).$$

Since $G(\hat{K}_{12}/K_{12})$ is contained in the center of $G(\hat{K}_{12}/Q)$, and since by assumption $\mathrm{Ord}(m, p)$ is divisible by $d_{12}=|G(\hat{K}_{12}/K_{12})|$, we get

$$\left(\frac{\hat{K}_{12}/K_{12}}{\mathfrak{P}}\right)=(x_1^{\mathrm{ind}_1 p}x_2^{\mathrm{ind}_2 p})^{\mathrm{Ord}(m,p)}$$

$$=x_1^{\mathrm{Ord}(m,p)\mathrm{ind}_1 p}x_2^{\mathrm{Ord}(m,p)\mathrm{ind}_2 p}$$

$$\cdot(x_1, x_2)^{-\frac{1}{2}\mathrm{Ord}(m,p)(\mathrm{Ord}(m,p)-1)\mathrm{ind}_1 p\ \mathrm{ind}_2 p},$$

because as is well-known, if x, y are elements in a group of class 2, then for $n\geqq 1$

$$(xy)^n=x^n y^n(x, y)^{-\frac{1}{2}n(n-1)}.$$

Since $(\mathrm{ind}_i\, p, \phi(q_i^{\nu_i}))=\phi(q_i^{\nu_i})/\mathrm{Ord}(q_i^{\nu_i}, p)$, $\mathrm{Ord}(m, p)\,\mathrm{ind}_i\, p$ is divisible by $\phi(q_i^{\nu_i})$, and hence by (2.1) we obtain the formula for $\left(\frac{\hat{K}_{12}/K_{12}}{\mathfrak{P}}\right)$ given in the theorem. The latter half now follows immediately, because (x_1, x_2) is a generator of the cyclic group $G(\hat{K}_{12}/K_{12})$ of order d_{12} by Theorem 1.7.

Theorem 2.6. *Let* $m=2^2q_1^{\nu_1}$. *If p is a rational prime not dividing m, then it is unramified in* $\hat{K}_{01}$. *Moreover, if* $p\equiv 1 \pmod 4$ *and* $\mathrm{Ord}(m, p)\equiv 0 \pmod 2$, *then p factors in* $\hat{K}_{01}$ *into the product of distinct prime ideals of degree* $\mathrm{Ord}(m, p)$ *or* $2\,\mathrm{Ord}(m, p)$, *according as* $q_1\equiv 1$ *or* $3 \pmod 4$. *If* $p\equiv 3 \pmod 4$, *then p factors in* $\hat{K}_{01}$ *into the product of distinct prime ideals of degree* $\mathrm{Ord}(m, p)$.

Proof. Since $\mathfrak{f}(\hat{K}_{01}/Q)=mp_\infty$, p is unramified in $\hat{K}_{01}$. By Theorem 1.6, $G(\hat{K}_{01}/Q)$ is generated by two elements x_0, x_1, and completely determined by the relations

$$(2.2)\qquad \begin{aligned} &(x_0, x_1)x_k=x_k(x_0, x_1), \qquad k=0, 1,\\ &x_0^2=1, \qquad x_1^{\phi(q_1^{\nu_1})}=(x_0, x_1)^{[0,1]*q_1^{\nu_1}-1}, \end{aligned}$$

where x_0, x_1 are extensions of the norm residue symbols

$$\tau^*=\left(\frac{-1, K_{01}/Q}{2}\right) \quad\text{and}\quad \tau_1=\left(\frac{g_1, K_{01}/Q}{q_1}\right)$$

to $\hat{K}_{01}$, respectively. Applying the Hasse product formula for K_{01}/Q to p, we get

$$\left(\frac{K_{01}/Q}{p}\right)=\tau^{*\mathrm{ind}_0^* p}\tau_1^{\mathrm{ind}_1 p}.$$

Thus the Frobenius automorphism $\left[\frac{\hat{K}_{01}}{\mathfrak{Q}}\right]$ of a prime factor $\mathfrak{Q}$ of p in $\hat{K}_{01}$

can be written in the form

$$\left[\frac{\hat{K}_{01}}{\mathfrak{Q}}\right]=x_0^{\mathrm{ind}_0^* p}x_1^{\mathrm{ind}_1 p}\varepsilon, \qquad \varepsilon\in G(\hat{K}_{01}/K_{01}).$$

Let $\mathfrak{P}$ be any prime factor of p in K_{01}, and let $\mathrm{Ord}\,(m, p)\equiv 0 \pmod 2$. Since $|G(\hat{K}_{01}/K_{01})|=2$ and $G(\hat{K}_{01}/K_{01})$ is contained in the center of $G(\hat{K}_{01}/Q)$, we have

$$\begin{aligned}\left(\frac{\hat{K}_{01}/K_{01}}{\mathfrak{P}}\right)&=x_0^{\mathrm{Ord}(m,p)\mathrm{ind}_0^* p}x_1^{\mathrm{Ord}(m,p)\mathrm{ind}_1 p}\\&\quad\cdot(x_0, x_1)^{-\frac{1}{2}\mathrm{Ord}(m,p)(\mathrm{Ord}(m,p)-1)\mathrm{ind}_0^* p\ \mathrm{ind}_1 p}\\&=(x_0, x_1)^{\frac{1}{2}\mathrm{Ord}(m,p)\{1-(\mathrm{Ord}(m,p)-1)\mathrm{ind}_0^* p\}\mathrm{ind}_1 p},\end{aligned}$$

in which the second sign of equality follows from (2.2), because of

$$\phi(q_1^{\nu_1})\,|\,\mathrm{Ord}\,(m, p)\ \mathrm{ind}_1 p \quad\text{and of}\quad [0, 1]^*\equiv\frac{q_1-1}{2} \pmod 2.$$

Suppose $p\equiv 1 \pmod 4$. Then $\mathrm{ind}_0^* p\equiv 0 \pmod 2$ and $\mathrm{Ord}\,(m, p)=\mathrm{Ord}\,(q_1^{\nu_1}, p)$. Thus the power exponent of (x_0, x_1) becomes $\frac{1}{2}\mathrm{Ord}\,(q_1^{\nu_1}, p)\ \mathrm{ind}_1 p$. Let $\mathrm{Ord}\,(q_1^{\nu_1}, p)\ \mathrm{ind}_1 p=\phi(q_1^{\nu_1})d$. Since $(\mathrm{ind}_1 p, \phi(q_1^{\nu_1}))=\phi(q_1^{\nu_1})/\mathrm{Ord}\,(q_1^{\nu_1}, p)$,

$$(d, \mathrm{Ord}\,(q_1^{\nu_1}, p))=1,$$

and hence d is odd by assumption. Hence

$$\frac{1}{2}\,\mathrm{Ord}\,(q_1^{\nu_1}, p)\ \mathrm{ind}_1 p\equiv\frac{1}{2}\phi(q_1^{\nu_1})d\equiv\frac{q_1-1}{2} \pmod 2,$$

from which follows

$$\left(\frac{\hat{K}_{01}/K_{01}}{\mathfrak{P}}\right)=(x_0, x_1)^{(q_1-1)/2}.$$

This completes the proof of the first half.

Next assume $p\equiv 3 \pmod 4$. Then $\mathrm{Ord}\,(m, p)$ is even, and $\mathrm{ind}_0^* p\equiv 1 \pmod 2$, which imply that the power exponent of (x_0, x_1) is even. Thus we obtain

$$\left(\frac{\hat{K}_{01}/K_{01}}{\mathfrak{P}}\right)=1$$

which is the desired result.

The same procedure yields the following two theorems:

Theorem 2.7. *Let $m=2^\nu$ with $\nu\geqq 4$. If p is an odd prime, then it is unramified in $\hat{K}_{-10}$. Moreover, if $p\not\equiv 1 \pmod{2^\nu}$, then p factors in $\hat{K}_{-10}$ into the product of distinct prime ideals of degree* $\mathrm{Ord}(m, p)$.

Theorem 2.8. *Let $\nu\geqq 3$, and let $d_{-11}=(2^{\nu-2}, \phi(q_1^{\nu_1}))$. If p is an odd prime different from q_1, then it is unramified in $\hat{K}_{-11}$. Moreover, if*

$$\mathrm{Ord}(2^\nu q_1^{\nu_1}, p)\equiv 0 \pmod{d_{-11}},$$

then p factors in $\hat{K}_{-11}$ into the product of distinct prime ideals of degree $\mathrm{Ord}(2^\nu q_1^{\nu_1}, p)f_p$, *where*

$$f_p=d_{-11}\Big/\left(d_{-11}, \left\{[0,1]\frac{\mathrm{ind}_1 p}{q_1-1}-[1,0]\frac{\mathrm{ind}_0^* p}{2}+\frac{1}{2}\,\mathrm{ind}_0 p\,\mathrm{ind}_1 p\right\}\right.$$
$$\left.\times\,\mathrm{Ord}(2^\nu q_1^{\nu_1}, p)\right),$$

where $[0, 1]$, $[1, 0]$ *are the indices defined by* (1.1).

Remark. We can describe the Artin classes of rational primes with some conditions in $G(\hat{K}_{ij}/Q)$. By purely group-theoretical consideration, it can be checked that the coset $x_1^{\mathrm{ind}_1 p}x_2^{\mathrm{ind}_2 p}G(\hat{K}_{12}/K_{12})$ of $G(\hat{K}_{12}/K_{12})$ comprises $(\mathrm{ind}_1 p, \mathrm{ind}_2 p, d_{12})$ conjugate classes. Hence, if $(\phi(q_1^{\nu_1})/\mathrm{Ord}(q_1^{\nu_1}, p)$, $\phi(q_2^{\nu_2})/\mathrm{Ord}(q_2^{\nu_2}, p))=(\mathrm{ind}_1 p, \mathrm{ind}_2 p, d_{12})=1$, then the Artin class $\left[\frac{\hat{K}_{12}}{p}\right]$ of p in $G(\hat{K}_{12}/Q)$ is given by

$$\left[\frac{\hat{K}_{12}}{p}\right]=x_1^{\mathrm{ind}_1 p}x_2^{\mathrm{ind}_2 p}G(\hat{K}_{12}/K_{12}).$$

Similarly, if $(2/\mathrm{Ord}(2^2, p), \phi(q_1^{\nu_1})/\mathrm{Ord}(q_1^{\nu_1}, p))=1$, then

$$\left[\frac{\hat{K}_{01}}{p}\right]=x_0^{\mathrm{ind}_0^* p}x_1^{\mathrm{ind}_1 p}G(\hat{K}_{01}/K_{01}),$$

and if $(2/\mathrm{Ord}(2^\nu, (-1)^{\mathrm{ind}_0^* p}), 2^{\nu-2}/\mathrm{Ord}(2^\nu, 5^{\mathrm{ind}_0 p}))=1$, then

$$\left[\frac{\hat{K}_{-10}}{p}\right]=x_{-1}^{\mathrm{ind}_0 p}x_0^{\mathrm{ind}_0^* p}G(\hat{K}_{-10}/K_{-10}).$$

Finally, if $(2^{\nu-2}/\mathrm{Ord}(2^\nu, 5^{\mathrm{ind}_0 p}), \phi(q_1^{\nu_1})/\mathrm{Ord}(q_1^{\nu_1}, p))=1$, then

$$\left[\frac{\hat{K}_{-11}}{p}\right]=\bar{x}_{-1}^{\mathrm{ind}_0 p}\bar{x}_0^{\mathrm{ind}_0^* p}\bar{x}_1^{\mathrm{ind}_1 p}G(\hat{K}_{-11}/K_{-10}K_1),$$

where $\{x_{-1}, x_0, x_1\}$ is the system of generators of $G(\hat{K}_{\bar{m}}/Q)$ with $m=2^\nu q_1^{\nu_1}$, $\nu\geqq 3$, given in Theorems 1.6 or 1.10, and $\bar{x}_i$ means the restriction of x_i to $\hat{K}_{-11}$ for $i=-1, 0, 1$.

Now let us return to the theme of this section. It is obvious that any class 2 extension $\hat{K}_{\bar{m}}$ with exponent $G(\hat{K}_{\bar{m}}/K)=2$ is composed of a finite number of class 2 extensions of the following four types:

(α') $\hat{K}_{12}$, $m=q_1^{\nu_1}q_2^{\nu_2}$ with $(\phi(q_1^{\nu_1}), \phi(q_2^{\nu_2}))=2$.

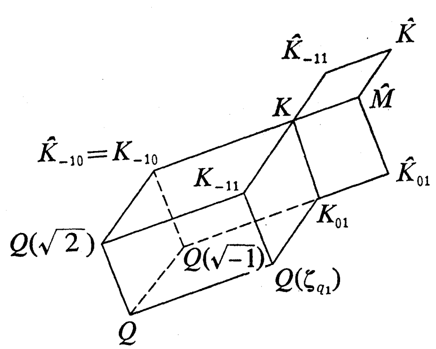
(β') $\hat{K}_{01}$, $m=2^2 q_1^{\nu_1}$.

(γ') $\hat{K}_{-10}$, $m=2^\nu$ with $\nu\geqq 4$.

(δ') $\hat{K}_{-11}$, $(2^{\nu-2}, \phi(q_1^{\nu_1}))=2$ with $\nu\geqq 3$.

But in the case (α') for example, $(\phi(q_1^{\nu_1}), \phi(q_2^{\nu_2}))=2$ implies $(\phi(q_1), \phi(q_2))=2$. Thus denoting by $\hat{K}'_{12}$ the class 2 extension $\hat{K}_{12}$ with $m=q_1q_2$, we have $\hat{K}_{12}=K\hat{K}'_{12}$, and hence the problem of finding the decomposition laws in $\hat{K}_{12}$ can be reduced to that in the case of $\hat{K}'_{12}$, because of Lemma 2.4. The same holds for the cases (β') with $\nu_1=1$ and (γ') with $\nu=4$, and though it is true also for the case (δ') with $\nu=3$ and $\nu_1=1$, we choose another class 2 extension in this case, because we wish to use the well-known quadratic decomposition of primes (see § 5).

Suppose $\nu=3$ and $\nu_1=1$ in the case (δ'). Then $K_{-10}=Q(\sqrt{2}, \sqrt{-1})$, $K_{-11}=Q(\sqrt{2}, \zeta_{q_1})$, $K_{01}=Q(\sqrt{-1}, \zeta_{q_1})$, and the genus field mod $2^3q_1p_\infty$ of K_{-11}/Q is $K=Q(\sqrt{2}, \sqrt{-1}, \zeta_{q_1})$. Let $\hat{K}$, $\hat{M}$ be the central class fields mod $2^3q_1p_\infty$ of K/Q and K_{01}/Q, respectively. By Theorem 1.9, $G(\hat{K}/K)$ is generated by two elements (x_{-1}, x_1), (x_0, x_1), where x_{-1}, x_0, x_1 are suitable extensions of (1.2) to $\hat{K}$. $G(\hat{K}/K)$ is of type (2, 2), whereas $H^{-3}(G(K/Q), \boldsymbol{Z})$ is of type (2, 2, 2). The fact comes from $\hat{K}_{-10}=K_{-10}$, or the same thing $(x_{-1}, x_0)=1$. We show that $\hat{K}_{-11}$ is the fixed subfield of $\hat{K}$ under $\langle(x_0, x_1)\rangle$. Let x'_i be the restriction of x_i to $\hat{K}_{-11}$ for $i=0, 1$. Since the restriction of x'_0 to K_{-11} is equal to $\left(\dfrac{-1, K_{-11}/Q}{2}\right)=1$, $x'_0\in G(\hat{K}_{-11}/K_{-11})$, and hence $(x'_0, x'_1)=1$, i.e. $(x_0, x_1)\in G(\hat{K}/\hat{K}_{-11})$, because $G(\hat{K}_{-11}/K_{-11})$ is contained in the center of $G(\hat{K}_{-11}/Q)$. Since the order of (x_0, x_1) is two, and since $[\hat{K}_{-11}: K]=2$, we have $G(\hat{K}/\hat{K}_{-11})=\langle(x_0, x_1)\rangle$. In a similar manner, we may show that $\hat{M}$ corresponds to $\langle(x_{-1}, x_1)\rangle$. The relation among fields can be described by the following diagram:



We notice that $\hat{M}=K\hat{K}_{01}$, because the genus field mod $2^3q_1p_\infty$ of K_{01}/Q is equal to K.

Lemma 2.9. *Let $L=Q(\sqrt{-2}, \zeta_{q_1})$, and let $\hat{L}$ be the central class field mod $2^3q_1p_\infty$ of L/Q. Then $\hat{L}$ is the subfield of $\hat{K}$ corresponding to $\langle(x_{-1}x_0, x_1)\rangle$.*

Proof. Let x'_i denote the restriction of x_i to $\hat{L}$ for $i=-1, 0, 1$. Since $\mathfrak{f}(Q(\sqrt{-2})/Q)=2^3p_\infty$ and $-5\equiv 3 \pmod{2^3}$, we have

$$\left(\frac{-5, Q(\sqrt{-2})/Q}{2}\right)=\left(\frac{3, Q(\sqrt{-2})/Q}{2}\right)=1,$$

because of $N_{Q(\sqrt{-2})/Q}(1+\sqrt{-2})=3$, and in addition

$$\left(\frac{-5, Q(\zeta_{q_1})/Q}{2}\right)=1,$$

because 2 is unramified in $Q(\zeta_{q_1})$. Thus the restriction of $x'_{-1}x'_0$ to L is trivial. We have as before $(x'_{-1}x'_0, x'_1)=1$, namely $G(\hat{K}/\hat{L})=\langle(x_{-1}x_0, x_1)\rangle$.

It is now clear that $\hat{K}=\hat{L}\hat{M}=\hat{L}\hat{K}_{01}$. Therefore the problem of finding the decomposition laws of rational primes in $\hat{K}_{-11}$ can be reduced to that in the case of $\hat{L}$ provided that we succeed in the case (β'), because of Lemma 2.4 and of $\hat{K}\supset\hat{K}_{-11}$.

We conclude that the investigation of the decomposition laws of rational primes in the class 2 extensions $\hat{K}_{\tilde{m}}$ with exponent $G(\hat{K}_{\tilde{m}}/K)=2$ can be reduced to that in the following four types of class 2 extensions:

(A) $\hat{K}_{12}$, $m=q_1q_2$ with $(q_1-1, q_2-1)=2$.
(B) $\hat{K}_{01}$, $m=2^2q_1$.
(C) $\hat{K}_{-10}$, $m=2^4$.
(D) $\hat{L}$, the central class field mod $2^3q_1p_\infty$ of $L=Q(\sqrt{-2}, \zeta_{q_1})/Q$.

In Sections 3–7, we determine the decomposition laws of all the rational primes in these class 2 extensions in connection with representations of primes or powers of primes by binary quadratic forms and in any case, we always regard the Galois group of order two as $\{\pm 1\}$.

§ 3. The case (B)

Throughout this section, let $q=q_1$ be an odd prime, $k=K_0=Q(\sqrt{-1})$, $K=K_{01}=Q(\sqrt{-1}, \zeta_q)$, and let $\hat{K}=\hat{K}_{01}$ be the central class field mod 2^2qp_∞ of K/Q. We denote by $\mathfrak{P}_p$ any prime factor of a rational prime p in K. Then if $\mathfrak{P}_p$ is unramified in $\hat{K}$, the value of the Artin symbol $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)$ does not depend on the choice of $\mathfrak{P}_p$ over p, because $\hat{K}$ is a central extension of K/Q.

The Galois conductor of $\hat{K}/Q$ is $\mathfrak{f}(\hat{K}/Q) =2^2qp_\infty$ by the definition of $\hat{K}$. Since $G(K/k)$ is cyclic, $G(\hat{K}/k)$ is Abelian, and since the Hasse function $\psi(i)$ of $(1-\sqrt{-1})$ with respect to k/Q is $\psi(i)=2i-1$ for $i\geqq 1$ and q is unramified in k, we have $\mathfrak{g}_{k/Q}(2^2qp_\infty)=2q\mathfrak{p}_\infty$, where $\mathfrak{p}_\infty$ stands for the complex prime divisor of k, and hence by Lemma 1.2,

$$\mathfrak{f}(\hat{K}/k)\,|\,2q\mathfrak{p}_\infty. \tag{3.1}$$

Let p be any odd prime different from q. If $p\equiv 3 \pmod 4$, then by Theorem 2.6, $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$. So we may assume $p\equiv 1 \pmod 4$. Then p can be written in the form

$$p=a^2+b^2, \qquad a \text{ odd, } b \text{ even.}$$

Remark. Jacobsthal [27] proved that if $p=a^2+b^2$ is a prime, then $a=\Phi_2(r)/2$, $b=\Phi_2(s)/2$, where $\Phi_e(n)$ is the Jacobsthal sum defined by

$$\Phi_e(n)=\sum_{h=1}^{p-1}\left(\frac{h}{p}\right)\left(\frac{h^e+n}{p}\right), \tag{3.2}$$

r is any quadratic residue mod p and s any non-residue. But in the following, we use only the property that a is odd and b even except the proof of Theorem 3.8.

Now set

$$\lambda(p)=a+b\sqrt{-1}.$$

Then $\lambda(p)$ is a prime number of k. Applying the Hasse product formula for $\hat{K}/k$ to $\lambda(p)$, we get

$$\prod_{\mathfrak{p}}\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{p}}\right)=1,$$

where $\mathfrak{p}$ ranges over all the prime divisors of k, which implies

$$\left(\frac{\hat{K}/k}{\lambda(p)}\right)=\prod_{\mathfrak{p}|q}\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{p}}\right), \tag{3.3}$$

because of (3.1) and of $\lambda(p)\equiv 1 \pmod 2$. Since the degree of $\mathfrak{P}_p$ over k is $\mathrm{Ord}\,(q, p)$, we have

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left\{\prod_{\mathfrak{p}|q}\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}\,(q,p)} \tag{3.4}$$

We first assume $q\equiv 1 \pmod 4$. It follows from Theorem 1.6 that the Galois group $G(\hat{K}/Q)$ is generated by two elements x_0, x_1, and completely determined by the relations

$$\begin{aligned} &(x_0, x_1)x_i=x_i(x_0, x_1), \qquad i=0, 1,\\ &x_0^2=1, \qquad x_1^{q-1}=1, \end{aligned} \tag{3.5}$$

where x_0, x_1 are extensions of the norm residue symbols

$$\tau^*=\left(\frac{-1,\, K/Q}{2}\right) \quad \text{and} \quad \tau_1=\left(\frac{g_1,\, K/Q}{q}\right) \tag{3.6}$$

to $\hat{K}$, respectively, and g_1 is the primitive root mod $q=q_1$ as in (1,1). Since $\sqrt{-1}^{x_0}=\sqrt{-1}^{-1}=-\sqrt{-1}$ and q is splits completely in k, we put

$$(q)=\mathfrak{q}\mathfrak{q}^{x_0}.$$

From

$$\begin{aligned} \prod_{\mathfrak{p}|q}\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{p}}\right)&=\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{q}}\right)\left(\frac{\lambda(p),\, \hat{K}/k}{\mathfrak{q}^{x_0}}\right)\\ &=\left(\frac{p,\, \hat{K}/k}{\mathfrak{q}}\right)\left(x_0,\ \left(\frac{\lambda(p)^{x_0},\, \hat{K}/k}{\mathfrak{q}}\right)\right), \end{aligned} \tag{3.7}$$

we obtain

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(x_0,\ \left(\frac{\lambda(p)^{x_0},\, \hat{K}/k}{\mathfrak{q}}\right)\right)^{\mathrm{Ord}\,(q,p)},$$

because of $p^{\mathrm{Ord}\,(q,p)}\equiv 1 \pmod q$ and of (3.1). Since $\left(\frac{-1}{q}\right)=1$, there exists a rational integer r such that

$$r^2 \equiv -1 \pmod{q} \quad \text{or} \quad r \equiv \pm\sqrt{-1} \pmod{\mathfrak{q}}.$$

Then

$$\lambda(p)^{x_0} = a - b\sqrt{-1} \equiv a \pm br \equiv g_1^{\mathrm{ind}\,(a\pm br)} \pmod{\mathfrak{q}},$$

where ind $(a \pm br)$ means the index of $a \pm br$ mod q with respect to g_1, and so

$$(3.8) \qquad \left(\frac{\lambda(p)^{x_0},\, K/k}{\mathfrak{q}}\right) = \left(\frac{g_1,\, K/k}{\mathfrak{q}}\right)^{\mathrm{ind}\,(a\pm br)} = \tau_1^{\mathrm{ind}\,(a\pm br)},$$

which implies that $\left(\frac{\lambda(p)^{x_0},\, \hat{K}/k}{\mathfrak{q}}\right) = x_1^{\mathrm{ind}\,(a\pm br)}\varepsilon$ for some ε in $G(\hat{K}/K)$ and hence in the center of $G(\hat{K}/Q)$. Thus

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = (x_0, x_1)^{\mathrm{Ord}\,(q,p)\,\mathrm{ind}\,(a\pm br)}.$$

The Galois group $G(\hat{K}/K)$ is generated by (x_0, x_1) and of order two. So if Ord (q, p) is even, then always $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = 1$, which follows also from Theorem 2.6. Suppose that Ord (q, p) is odd. Then

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = 1 \quad \text{iff} \quad \mathrm{ind}\,(a \pm br) \equiv 0 \pmod{2},$$

i.e.

$$\left(\frac{a \pm br}{q}\right) = 1.$$

But since

$$(a+br)^{\mathrm{Ord}\,(q,p)}(a-br)^{\mathrm{Ord}\,(q,p)} \equiv p^{\mathrm{Ord}\,(q,p)} \equiv 1 \pmod{q},$$

we have

$$\left(\frac{a+br}{q}\right) = \left(\frac{a-br}{q}\right).$$

Hence we have proved

Theorem 3.1. *Let* $q \equiv 1 \pmod{4}$, *and let* $p = a^2 + b^2$, *a odd, b even, be* *a rational prime different from* 2 *and* q. *Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{a+br}{q}\right)^{\mathrm{Ord}\,(q,p)},$$

where r *is a rational integer such that* $r^2\equiv -1 \pmod{q}$.

Remark. Kuroda [32] determined the decomposition laws of rational primes in certain Galois extensions containing $Q(\sqrt{-1})$ of degree 8 over Q. The class of fields covered by Kuroda was discussed again in an article by Fröhlich [7]. We state here a relation between $\hat{K}$ with $q\equiv 1 \pmod 4$ and the field considered by Kuroda and Fröhlich.

Let the notation be as before, and let $F=Q(\sqrt{-1}, \sqrt{q})$. Then $K\supset F$ and $[F:Q]=4$. Moreover, since $G(\hat{K}/F)=\langle x_1^2, (x_0, x_1)\rangle$, $(x_0, x_1^2)=(x_0, x_1)^2=1$ and $\mathfrak{f}(\hat{K}/Q)=2^2qp_\infty=\mathfrak{f}(F/Q)$, $\hat{K}$ is the central class field mod 2^2qp_∞ of F/Q and K the genus field mod 2^2qp_∞ of F/Q (cf. [40, Theorem 29]). Let further E be the subfield of $\hat{K}$ corresponding to the subgroup $\langle x_1^2\rangle$. Then E/Q is a Galois extension, $K\cap E=F$ and $\hat{K}=KE$, because $\langle (x_0, x_1)\rangle \cap \langle x_1^2\rangle=1$ by (3.5), which implies that E/Q is non-Abelian. Thus E/Q is a non-Abelian Galois extension containing $Q(\sqrt{-1})$ of degree 8. Let $p=a^2+b^2$, a odd, b even, be a rational prime such that $\left(\frac{p}{q}\right)=1$, and let $\mathfrak{P}_p'$ denote the restriction of $\mathfrak{P}_p$ to F. Since p splits completely in F, we have by (3.3), (3.7) and (3.8)

$$\left(\frac{\hat{K}/F}{\mathfrak{P}'}\right)=\left(\frac{p, \hat{K}/k}{\mathfrak{q}}\right)(x_0, x_1)^{\mathrm{ind}\,(a\pm br)}.$$

There exists a rational integer s such that $s^2\equiv p \pmod{q}$. So by (3.1),

$$\left(\frac{p, \hat{K}/k}{\mathfrak{q}}\right)=\left(\frac{s, \hat{K}/k}{\mathfrak{q}}\right)^2, \quad \text{and} \quad \left(\frac{s, \hat{K}/k}{\mathfrak{q}}\right)\in G(\hat{K}/F),$$

because the restriction of $\left(\frac{s, \hat{K}/k}{\mathfrak{q}}\right)$ to F is equal to

$$\left(\frac{s, F/k}{\mathfrak{q}}\right)=\left(\frac{s, F/Q}{\mathfrak{q}}\right)^2=1.$$

Denoting by x_i' the restriction of x_i to E and restricting the above equality to E, we obtain

$$\left(\frac{E/F}{\mathfrak{P}'}\right)=(x_0', x_1')^{\mathrm{ind}\,(a\pm br)}=\left(\frac{a+br}{q}\right), \tag{3.9}$$

because $G(E/F)=\langle(x_0', x_1')\rangle$ is of order two and

$$\left(\frac{a+br}{q}\right)\left(\frac{a-br}{q}\right)=\left(\frac{p}{q}\right)=1.$$

Let $q=c^2+d^2$, c odd, d even, and let $\gamma^2=(c+\sqrt{q})/2$. Then by Fröhlich [7, Lemma 3.1], $F(\gamma)/Q$ is a non-Abelian Galois extension of degree 8, and moreover, it follows from Kuroda [32, Satz 1] or Fröhlich [7, Theorem 6] that

$$\left(\frac{F(\gamma)/F}{\mathfrak{P}'}\right)=\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4, \tag{3.10}$$

where $\left(\frac{}{—}\right)_4$ stands for the forth power residue symbol in Q. According to Fröhlich [7, Theorem 7], this right side is equal to that of (3.9). Hence by the well-known theorem of Bauer [2] (see also Hasse [22, § 25]), we conclude

$$E=F(\gamma).$$

Furuta [12, p. 179, (20)] also proved (3.10), and gave another direct proof in [13, Theorem 5.4, (i)].

We notice that the methods used by Kuroda and Fröhlich to obtain the decomposition laws in $F(\gamma)$ need the generating element γ, but our methods do not.

We next treat the case of $q\equiv 3 \pmod 4$. In this case, the Galois group $G(\hat{K}/Q)$ is generated by x_0, x_1, and completely determined by the relations

$$\begin{aligned} &(x_0, x_1)x_i=x_i(x_0, x_1), \qquad i=0, 1, \\ &x_0^2=1, \qquad x_1^{q-1}=(x_0, x_1), \end{aligned} \tag{3.11}$$

where x_0, x_1 are extensions of (3.6) to $\hat{K}$. Since q remains prime in k, we have by (3.4)

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{\lambda(p)^{\mathrm{Ord}\,(q,p)},\ \hat{K}/k}{q}\right). \tag{3.12}$$

Let G be a generator of the group of reduced residue classes mod q in k such that

$$N_{k/Q}G\equiv g_1 \pmod q, \tag{3.13}$$

and put $\lambda(p)^{\mathrm{Ord}\,(q,p)}\equiv G^e \pmod q$. Multipling the both sides by their conjugates, we get $g_1^e \equiv p^{\mathrm{Ord}(q,p)} \equiv 1 \pmod{q}$ and hence $q-1 \mid e$. Write $e=(q-1)e'$, then

$$\lambda(p)^{\mathrm{Ord}(q,p)} \equiv G^{(q-1)e'} \pmod{q}. \tag{3.14}$$

Thus by (3.1), we have

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{G,\ \hat{K}/k}{q}\right)^{(q-1)e'}.$$

The restriction of $\left(\frac{G,\ \hat{K}/k}{q}\right)$ to K is

$$\left(\frac{G,\ K/k}{q}\right)=\left(\frac{g_1,\ K/Q}{q}\right)=\tau_1$$

by (3.13), and so we may write $\left(\frac{G,\ \hat{K}/k}{q}\right)=x_1\varepsilon$, $\varepsilon \in G(\hat{K}/K)$. Since $G(\hat{K}/K)$ is contained in the center of $G(\hat{K}/Q)$ and of order two, we obtain from (3.11)

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=(x_0,\ x_1)^{e'},$$

which means that $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $2 \mid e'$. (This is equivalent to the condition that $\lambda(p)^{\mathrm{Ord}(q,p)}$ is a forth power residue mod q in k, because of (3.14) and of $q \equiv 3 \pmod{4}$.)

To get a rational expression of this condition, we employ the regular representation f of k with respect to the basis $\{1, \sqrt{-1}\}$ as an algebra over Q. f is given by

$$f(u+v\sqrt{-1})=\begin{bmatrix} u & -v \\ v & u \end{bmatrix}$$

for any $u, v \in Q$. Let

$$R=\left\{\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \middle| \alpha, \beta \in Z/qZ\right\},$$

and let

$$S(q)=R \cap SL_2(Z/qZ).$$

Then f induces the isomorphism $\tilde{f}$ of the residue class field mod q in k to R. Since the sequence

$$1 \longrightarrow S(q) \longrightarrow R^{\times} \xrightarrow{\det} (Z/qZ)^{\times} \longrightarrow 1$$

is exact, $S(q)$ is a cyclic group of order $q+1$, here $R^{\times}$ denotes the group of non-zero elements in R. By (3.14), in $R^{\times}$

$$\tilde{f}(\lambda(p))^{\mathrm{Ord}\,(q,p)} = \tilde{f}(G)^{(q-1)e'}.$$

Since $\tilde{f}(G)$ is a generator of $R^{\times}$, $\tilde{f}(G)^{(q-1)}$ becomes a generator of $S(q)$. Hence

$$\text{(3.15)} \qquad \left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = 1 \quad \text{iff} \quad \tilde{f}(\lambda(p))^{\mathrm{Ord}\,(q,p)} \in S(q)^2,$$

where

$$\tilde{f}(\lambda(p)) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad (\text{mod } q).$$

Further we study this last condition. Let

$$X = \{(\alpha, \beta) \in Z/qZ \times Z/qZ \mid \alpha^2 + \beta^2 = 1\},$$

which has $q+1$ elements, because for $\begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix} \in R$, $\begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix} \in S(q)$ iff $\alpha^2 + \beta^2 = 1$. The fact follows also from Dickson [4, (19) and Theorem 2]. It is trivial that $(0, \pm 1)$, $(\pm 1, 0) \in X$ and if $(\alpha, \beta) \neq (0, \pm 1)$, $(\pm 1, 0)$ is contained in X, then $(\pm\alpha, \pm\beta) \in X$. Therefore the number of the set

$$Y = \{(\alpha^2 - \beta^2, 2\alpha\beta) \mid (\alpha, \beta) \in X\}$$

is $\dfrac{q+1}{2}$. For example:

$q=3$, $\quad Y = \{(\pm 1, 0)\}$.

$q=7$, $\quad Y = \{(\pm 1, 0), (0, \pm 1)\}$.

$q=11$, $\quad Y = \{(\pm 1, 0), (\pm 5, \pm 8)\}$.

$q=19$, $\quad Y = \{(\pm 1, 0), (\pm 2, \pm 4), (\pm 12, \pm 3)\}$.

$q=23$, $\quad Y = \{(\pm 1, 0), (0, \pm 1), (\pm 11, \pm 15), (\pm 15, \pm 11)\}$, etc.

It can be checked that if $q \equiv 7 \pmod 8$, then $(\gamma, \delta) \in Y$ iff $(\delta, \gamma) \in Y$, because of $\left(\dfrac{2}{q}\right) = 1$. Let

$$Z=\{(\gamma^2, \delta^2) \mid (\gamma, \delta) \in Y\}.$$

The number n_q of elements of Z is $\frac{q+5}{8}$ or $\frac{q+9}{8}$, according as $q\equiv 3$ or 7 (mod 8). Let $\Gamma_q(x)$ be the polynomial of degree n_q defined by

$$\Gamma_q(x)=\prod_{(\eta,\theta)\in Z}(x-\theta), \tag{3.16}$$

which is uniquely determined only by q. Let $p=a^2+b^2$, a odd, b even, and let

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{\mathrm{Ord}\,(q,p)} \equiv \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \pmod q.$$

Then

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1 \quad \text{iff} \quad \Gamma_q(B^2)\equiv 0 \pmod q.$$

Proof. Let $\Gamma_q(B^2)\equiv 0 \pmod q$, then there exists $(\alpha^2-\beta^2, 2\alpha\beta) \in Y$ such that $B^2\equiv 4\alpha^2\beta^2 \pmod q$, from which follows that

$$A^2\equiv 1-B^2\equiv(\alpha^2+\beta^2)^2-4\alpha^2\beta^2\equiv(\alpha^2-\beta^2)^2 \pmod q.$$

Thus

$$\begin{bmatrix} A & -B \\ B & A \end{bmatrix} \equiv \begin{bmatrix} \alpha & -(\pm\beta) \\ \pm\beta & \alpha \end{bmatrix}^2 \quad \text{or} \quad \begin{bmatrix} \beta & -(\pm\alpha) \\ \pm\alpha & \beta \end{bmatrix}^2 \pmod q,$$

according as $(A, B)\equiv(\alpha^2-\beta^2, \pm 2\alpha\beta)$ or $(\beta^2-\alpha^2, \pm 2\alpha\beta) \pmod q$ with corresponding sings. Hence by (3.15), $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$. The converse is obvious.

Furthermore, suppose $q\equiv 7 \pmod 8$. Then $(\eta, \theta) \in Z$ iff $(\theta, \eta) \in Z$. Therefore $\Gamma_q(x)$ is divisible by $(x-\eta)(x-\theta)=x(x-1)+\eta\theta$, because of $\eta+\theta=1$, and then $(B^2-\eta)(B^2-\theta)\equiv -\{(AB)^2-\eta\theta\} \pmod q$. We set

$$\Delta_q(x)^2=\prod_{(\eta,\theta)\in Z}(x-\eta\theta). \tag{3.17}$$

It is now trivial that if $q\equiv 7 \pmod 8$, then

$$(3.18)\qquad \left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1 \quad \text{iff} \quad \Delta_q((AB)^2)\equiv 0 \pmod q.$$

In the first part of this section, we used the property that a is odd and b even to drive (3.3). But in the case of $q\equiv 7 \pmod 8$, we see from Lemma 3.6 below that the prime factor of 2 in k is unramified in $\hat{K}$, and hence the conductor of $\hat{K}/k$ is $\mathfrak{f}(\hat{K}/k)=q$. Thus we have (3.3) without the restriction on a and b. This is the reason why the condition (3.18) has symmetry on A and B.

We have proved

Theorem 3.2. *Let $q\equiv 3 \pmod 4$, $p=a^2+b^2$, a odd and b even, be a rational prime different from q, and let*

$$\begin{bmatrix} A & -B \\ B & A \end{bmatrix}\equiv\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{\operatorname{Ord}(q,p)} \pmod q.$$

Let further $\Gamma_q(x)$, $\Delta_q(x)$ denote the polynomials defined by (3.16) *and* (3.17), *respectively. Then $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $\Gamma_q(B^2)\equiv 0 \pmod q$. In particular, if $q\equiv 7 \pmod 8$, then this condition can be replaced by $\Delta_q((AB)^2)\equiv 0 \pmod q$.*

Another expression of Theorem 3.2 is given as follows:

Convention 3.3. *For any (non-Abelian) group G, we put*

$$[G]^2=\{x^2 \mid x\in G\}, \quad \text{the subset of } G.$$

The next can be easily checked.

Lemma 3.4. *For $X\in S(q)$, $X\in S(q)^2$ iff $X\in[SL_2(Z/qZ)]^2$.*

Hence by (3.15),

Theorem 3.5. *Let the hypotheses and notation be as in Theorem 3.2. Then $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{\operatorname{Ord}(q,p)} \pmod q \in [SL_2(Z/qZ)]^2$.*

Remark. Lehmer [33, p. 24] gave a criterion for the forth power residue symbol $\left(\frac{q}{p}\right)_4$. Since it can be checked that $\hat{K}$ contains $k(\sqrt[4]{-q})$, we may give an analogous criterion for $\left(\frac{q}{p}\right)_4$ with $q\equiv 3 \pmod 4$, but we omit here the details.

We finally determine the decomposition laws of 2 and q in $\hat{K}$. Needless to say, these primes are ramified in K. First we give the necessary and sufficient conditions for $\mathfrak{P}_2$ and $\mathfrak{P}_q$ to be unramified in $\hat{K}$. According to [43, §§ 2 and 3], the inertia groups of $\mathfrak{P}_2$, $\mathfrak{P}_q$ with respect to $\hat{K}/K$ are generated by $(x_0, x_1)^{[1,0]}$ and $(x_0, x_1)^{-[1,0]^*}$, respectively. Since $2 \equiv g_1^{[1,0]} \pmod{q = q_1}$ and $q \equiv (-1)^{[0,1]^*} \pmod 4$, and since $G(\hat{K}/K) = \langle (x_0, x_1) \rangle$ is of order two, we obtain

Lemma 3.6. (i) *$\mathfrak{P}_2$ is unramified in $\hat{K}$ iff*

$$\left(\frac{2}{q}\right) = 1, \quad \text{i.e.} \quad q \equiv 1, 7 \pmod 8.$$

(ii) *$\mathfrak{P}_q$ is unramified in $\hat{K}$ iff* $q \equiv 1 \pmod 4$.

As a side result, we have that if $q \equiv 1 \pmod 8$, then the central class number of the 2^2q-th cyclotomic field K is even. For the central class number which is a divisor of the class number of a Galois extension, see Furuta [11].

Let $q \equiv 1, 7 \pmod 8$. Since the prime factor $1+\sqrt{-1}$ of 2 in k is unramified in $\hat{K}$, we get by the Hasse product formula

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_2}\right) = \left\{ \prod_{\mathfrak{p} \mid q} \left(\frac{1+\sqrt{-1},\ \hat{K}/k}{\mathfrak{p}}\right) \right\}^{\mathrm{Ord}(q,2)}.$$

So by the same procedure for $\lambda(p)$, that is, by putting $a=b=1$ in $\lambda(p)$, we may assert

Theorem 3.7. (i) *If* $q \equiv 1 \pmod 8$, *then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_2}\right) = \left(\frac{1+r}{q}\right)^{\mathrm{Ord}(q,2)},$$

where r is a rational integer such that $r^2 \equiv -1 \pmod q$.

(ii) *If* $q \equiv 7 \pmod 8$, *then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_2}\right) = 1 \quad \textit{iff} \quad \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{\mathrm{Ord}(q,2)} \pmod q \in [SL_2(Z/qZ)]^2.$$

It follows from Fröhlich [7, Theorem 7] that

$$\left(\frac{2}{q}\right)_4 \left(\frac{q}{2}\right)_4 = \left(\frac{1+r}{q}\right).$$

Thus Theorem 3.7, (i) corresponds to the result of Furuta [13, Theorem 5.4, (ii)].

Next assume $q\equiv 1 \pmod 4$. Following Jacobsthal [27], let

$$q=a^2+b^2, \quad a=\Phi_2(1)/2, \quad b=\Phi_2(g_1)/2, \tag{3.19}$$

where $\Phi_e(*)$ is the Jacobsthal sum defined by (3.2) and g_1 the primitive root mod $q=q_1$ as in (1.1). Then $a\equiv -1 \pmod 4$, and so b is even. Moreover

$$2a\equiv -c \pmod q, \qquad c=\binom{\frac{q-1}{2}}{\frac{q-1}{4}}, \tag{3.20}$$

c being the binomial coefficient, which is a result of Gauss [18] (see Whiteman [51, p. 95]). As before, let $\lambda(q)=a+b\sqrt{-1}$, and let $\mathfrak{q}=(\lambda(q))$ in k. Then $(q)=\mathfrak{q}\mathfrak{q}^{x_0}$. Let T be the inertia field for a prime factor in $\hat{K}$ of $\mathfrak{q}$ over Q, which does not depend on the choice of a prime factor of $\mathfrak{q}$ in $\hat{K}$, because $\hat{K}/k$ is Abelian. Since $\mathfrak{q}$ is totally ramified in K, and since $\mathfrak{P}_q$ is unramified in $\hat{K}$, we have $K\cap T=k$, $[T\colon k]=2$ and $\hat{K}=KT$. Thus

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_q}\right)=\left(\frac{T/K}{\mathfrak{q}}\right), \tag{3.21}$$

because the degree of $\mathfrak{P}_q$ over k is one. Using (3.1) and $\lambda(q)\equiv 1 \pmod 2$, it follows from the Hasse product formula for $\hat{K}/k$ that

$$\left(\frac{\lambda(q),\, \hat{K}/k}{\mathfrak{q}}\right)\left(\frac{\lambda(q),\, \hat{K}/k}{\mathfrak{q}^{x_0}}\right)$$
$$=\left(\frac{q,\, \hat{K}/k}{\mathfrak{q}}\right)\left(x_0, \left(\frac{\lambda(q)^{x_0},\, \hat{K}/k}{\mathfrak{q}}\right)\right)=1.$$

Since $\lambda(q)^{x_0}=a-b\sqrt{-1}\equiv 2a\equiv g^{\operatorname{ind} 2a} \pmod{\mathfrak{q}}$,

$$\left(\frac{\lambda(q)^{x_0},\, K/k}{\mathfrak{q}}\right)=\left(\frac{g_1,\, K/k}{\mathfrak{q}}\right)^{\operatorname{ind} 2a}=\tau_1^{\operatorname{ind} 2a},$$

and hence

$$\left(\frac{q,\, \hat{K}/k}{\mathfrak{q}}\right)^{-1}=(x_0, x_1)^{\operatorname{ind} 2a}.$$

Restricting the both sides to T and using (3.21),

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_q}\right)=(x_0', x_1')^{\operatorname{ind} 2a}=\left(\frac{2a}{q}\right)=\left(\frac{c}{q}\right),$$

where x_i' denotes the restriction of x_i to T, because (x_0', x_1') is a generator of $G(T/k)$ of order two. The third equality sign follows from (3.20) and $q\equiv 1 \pmod 4$. Hence

Theorem 3.8. *Let* $q\equiv 1 \pmod 4$. *Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_q}\right)=\left(\frac{2a}{q}\right)=\left(\frac{c}{q}\right),$$

where a, c *are the integer and the binomial coefficient defined by* (3.19) *and* (3.20), *respectively.*

EXAMPLE 3.9. Let $q=3$. Then $\hat{K}/Q$ is a class 2 extension of degree $2\phi(2^2\cdot 3)=8$, and the Galois group $G(\hat{K}/Q)=\langle x_0, x_1\rangle$ is completely determined by the relations

$$(x_0, x_1)x_i=x_i(x_0, x_1), \quad i=0, 1, \quad x_0^2=1, \quad x_1^2=(x_0, x_1),$$

which imply

$$x_0^2=x_1^4=1, \qquad x_0x_1^3=x_1x_0.$$

Thus $G(\hat{K}/Q)$ is a dihedral group of order 8.

(i) Let $p\equiv 7, 11 \pmod{12}$. Then $p\equiv 3 \pmod 4$ and $\mathrm{Ord}(12, p)=2$. Hence by Theorem 2.6, p factors in $\hat{K}$ into the product of four distinct prime ideals of degree 2.

(ii) Let $p\equiv 5 \pmod{12}$. Then $p\equiv 1 \pmod 4$ and $\mathrm{Ord}(12, p)=2$. Hence by Theorem 2.6, p factors in $\hat{K}$ into the product of two distinct prime ideals of degree 4.

(iii) Let $p\equiv 1 \pmod{12}$, and let $p=a^2+b^2$, a odd, b even. In this case, $\Gamma_3(x)$ defined by (3.16) becomes $\Gamma_3(x)=x$. Hence by Theorem 3.2, $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $3\mid b$. Consequently, it follows from the density theorem (see [22, § 24]) that the sets of rational primes

$$\{p\equiv 1 \pmod{12} \mid p=a^2+b^2,\ 6\mid b\}$$

and

$$\{p\equiv 1 \pmod{12} \mid p=a^2+b^2,\ 6\nmid b\}$$

have density 1/8 each.

(iv) By Lemma 3.6, $\mathfrak{P}_2$, $\mathfrak{P}_3$ are ramified in $\hat{K}$.

EXAMPLE 3.10. Let $q=7$. Then $\hat{K}/Q$ is a class 2 extension of degree

$2\phi(2^2 \cdot 7)=24$. Let $p\equiv 1 \pmod{28}$, and let $p=a^2+b^2$. In this case, $\Delta_7(x)$ defined by (3.17) is given by $\Delta_7(x)=x$. Hence by Theorem 3.2, p splits completely in $\hat{K}$ iff $7\,|\,ab$. Consequently, the sets of rational primes

$$\{p\equiv 1 \pmod{28}\,|\,p=a^2+b^2,\, 7\,|\,ab\}$$

and

$$\{p\equiv 1 \pmod{28}\,|\,p=a^2+b^2,\, 7\nmid ab\}$$

have density 1/24 each.

By Lemma 3.6, $\mathfrak{P}_7$ is ramified in $\hat{K}$, whereas $\mathfrak{P}_2$ is unramified in $\hat{K}$ and $\left(\frac{\hat{K}/K}{\mathfrak{P}_2}\right)=-1$ by Theorem 3.7, because of

$$\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}^3 \notin [SL_2(Z/7Z)]^2.$$

§ 4. The case (C)

Throughout this section, let $k=K_0=Q(\sqrt{-1})$, $K=K_{-10}=Q(\zeta_{24})$, and let $\hat{K}=\hat{K}_{-10}$ be the central class field mod 2^4p_∞ of K/Q. We denote by $\mathfrak{P}_p$ any prime factor of a rational prime p in K.

Since $G(K/k)$ is cyclic, $G(\hat{K}/k)$ is Abelian. The Galois conductor of $\hat{K}/Q$ is $\mathfrak{f}(\hat{K}/Q)=2^4p_\infty$, and as stated in Section 3, the Hasse function of $(1-\sqrt{-1})$ with respect to k/Q is $\psi(i)=2i-1$ for $i\geqq 1$. Therefore $\mathfrak{g}_{k/Q}(2^4p_\infty)=2^3\mathfrak{p}_\infty$, $\mathfrak{p}_\infty$ being the complex prime divisor of k. It follows from Lemma 1.2 that $\hat{K}/k$ is an Abelian extension defined mod $2^3\mathfrak{p}_\infty$.

Let $p\not\equiv 1 \pmod{2^4}$. Then we have $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ by Theorem 2.7. Thus we may assume $p\equiv 1 \pmod{2^4}$ in the following. Let $p=a^2+b^2$, a odd b even, and let $\lambda(p)=a+b\sqrt{-1}$ as before. Applying the Hasse product formula for $\hat{K}/k$ to $\lambda(p)$ and using $\mathfrak{f}(\hat{K}/k)\,|\,2^3p_\infty$ and the property that the degree of $\mathfrak{P}_p$ over k is one, we get

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{\hat{K}/k}{(\lambda(p))}\right)=\left(\frac{\lambda(p),\,\hat{K}/k}{(1-\sqrt{-1})}\right).$$

It can be easily checked that the group of reduced residue classes mod 2^3 in k is an Abelian group of type (2, 4, 4), and that $\{5,\, 1+2\sqrt{-1},\, \sqrt{-1}\}$ is a basis for it. Let

$$\lambda(p)\equiv 5^l(1+2\sqrt{-1})^m\sqrt{-1}^n \pmod{2^3}.$$

We have $1\equiv\sqrt{-1}^n \pmod 2$, so n is even. Write $n=2n'$. Then

$$(4.1)\qquad \left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{5,\hat{K}/k}{(1-\sqrt{-1})}\right)^l\left(\frac{1+2\sqrt{-1},\hat{K}/k}{(1-\sqrt{-1})}\right)^m\left(\frac{-1,\hat{K}/k}{(1-\sqrt{-1})}\right)^{n'},$$

because of $\mathfrak{f}(\hat{K}/k)\,|\,2^3\mathfrak{p}_\infty$.

By Theorem 1.6, the Galois group $G(\hat{K}/Q)$ is generated by x_{-1}, x_0, and completely determined by the relations

$$(x_{-1}, x_0)x_i=x_i(x_{-1}, x_0),\quad i=-1, 0,\quad x_{-1}^4=x_0^2=1,$$

where x_{-1}, x_0 are suitable extensions of

$$\tau=\left(\frac{5, K/Q}{2}\right)\quad\text{and}\quad \tau^*=\left(\frac{-1, K/Q}{2}\right),$$

respectively. In fact, we took in [42, §§ 2 and 3]

$$x_{-1}=\left(\frac{1+2\sqrt{-1},\hat{K}/k}{(1-\sqrt{-1})}\right),\qquad x_0=\left(\frac{\theta^2+\theta-1,\hat{K}/R}{\mathfrak{P}_2'}\right),$$

where $\theta=\zeta_{2^4}+\zeta_{2^4}^{-1}$, $R=Q(\theta)$, and $\mathfrak{P}_2'$ means the unique prime factor of 2 in R. Notice that $N_{k/Q}(1+2\sqrt{-1})=5$ and $N_{R/Q}(\theta^2+\theta-1)=-1$. Thus

$$1=x_0^2=\left(\frac{\theta^2+\theta-1,\hat{K}/K}{\mathfrak{P}_2}\right)=\left(\frac{N_{K/k}(\theta^2+\theta-1),\hat{K}/k}{(1-\sqrt{-1})}\right)=\left(\frac{-1,\hat{K}/k}{(1-\sqrt{-1})}\right),$$

because of $[K\colon R]=2$, so by (4.1),

$$\begin{aligned}\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)&=\left(\frac{1-2\sqrt{-1},\hat{K}/k}{(1-\sqrt{-1})}\right)^l\left(\frac{1+2\sqrt{-1},\hat{K}/k}{(1-\sqrt{-1})}\right)^{l+m}\\&=(x_0x_{-1}x_0^{-1})^l x_{-1}^{l+m}=(x_0, x_{-1})^l x_{-1}^{2l+m},\end{aligned}$$

because of $\sqrt{-1}^{x_0}=-\sqrt{-1}$. Restricting this to K, we get $\tau^{2l+m}=1$, and so $4\,|\,2l+m$. Hence

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=(x_0, x_1)^l.$$

Since $G(\hat{K}/K)=\langle(x_{-1}, x_0)\rangle$ is of order two, $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $2\,|\,l$, thus $4\,|\,m$, which is equivalent to $\lambda(p)=a+b\sqrt{-1}\equiv(-1)^{n'}\pmod{2^3}$, so $8\,|\,b$. Conversely, when $p\equiv1\pmod{2^4}$, $8\,|\,b$ implies $\lambda(p)\equiv\pm1\pmod{2^3}$. It is obvious that if $p\equiv1\pmod 8$, then always $4\,|\,b$. Hence we have proved

Theorem 4.1. *Let* $p\equiv1\pmod{2^4}$, *and let* $p=a^2+b^2$, *a odd, b even. Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=(-1)^{b/4}.$$

We notice that if we choose the sign of a so that $a\equiv 1 \pmod 4$ from the start, then the above proof becomes a bit transparent, because in that case we have $4\,|\,n$.

According to [43, Lemma 3 and § 3], the inertia group of $\mathfrak{P}_2$ with respect to $\hat{K}/K$ is $\langle (x_{-1}, x_0)\rangle$. Thus

Theorem 4.2. *2 is totally ramified in* $\hat{K}$.

Remark. It can be checked that $k(\sqrt[4]{2})$ is contained in $\hat{K}$ and that it is the subfield corresponding to $\langle x_{-1}^2(x_0, x_{-1})\rangle$. Let $F=Q(\sqrt{2}, \sqrt{-1})$, $E=F(\sqrt[4]{2})$, $p=a^2+b^2\equiv 1 \pmod 8$, b even, and let $\mathfrak{P}'_p$ be the restriction of $\mathfrak{P}_p$ to F. Then by the same procedure as in the proof of Theorem 4.1, we obtain

$$\left(\frac{2}{p}\right)_4=\left(\frac{E/F}{\mathfrak{P}'_p}\right)=(-1)^{b/4}.$$

This is the theorem of Gauss [18, p. 89]. He proved this by means of the theory of cyclotomy. It is now clear that this result of Gauss implies Theorem 4.1, because of $\hat{K}=K(\sqrt[4]{2})$.

§ 5. The case (D)

Throughout this section, let $q=q_1$ be an odd prime, $k=Q(\sqrt{-2})$, $L=Q(\sqrt{-2}, \zeta_q)$, $K=Q(\zeta_{2^3q})=Q(\sqrt{2}, \sqrt{-1}, \zeta_q)$, and let $\hat{L}, \hat{K}$ be the central class fields mod 2^3qp_∞ of L/Q and K/Q, respectively. In this case, K is the genus field mod 2^3qp_∞ of L/Q. We denote by $\mathfrak{P}_p$ any prime factor of a rational prime p in K. The purpose of the present section is to characterize the value of the Artin symbol $\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)$.

Since $G(L/K)$ is cyclic, $G(\hat{L}/k)$ is Abelian. The Hasse function of $(\sqrt{-2})$ with respect to k/Q is given by $\psi(i)=2(i-1)$ for $i\geqq 2$, and $\mathfrak{f}(\hat{L}/Q)=2^3qp_\infty$. It follows from Lemma 1.2 that $\hat{L}/k$ is an Abelian extension defined mod $2\sqrt{-2}q\mathfrak{p}_\infty$, where $\mathfrak{p}_\infty$ stands for the complex prime divisor of k.

Let p be a rational prime such that $p\not\equiv 1 \pmod{2^3}$ and $p\neq 2, q$. Since $\mathrm{Ord}\,(2^3q, p)$ is even, we have by Theorem 2.8 with $\nu=3$ and $\nu_1=1$ $\left(\frac{\hat{K}_{-11}/K}{\mathfrak{P}_p}\right)=(-1)^{f_p-1}$, where $K_{-11}=Q(\sqrt{2}, \zeta_q)$, and f_p is the degree of $\mathfrak{P}_p$

with respect to $\hat{K}_{-11}/K$ given in Theorem 2.8. On the other hand, by using the case (B), we can find the value of $\left(\frac{\hat{M}/K}{\mathfrak{P}_p}\right)$, here $\hat{M}=K\hat{K}_{01}$ is the field in the diagram of Section 2. Hence by Lemma 2.4, we can obtain the decomposition law of $\mathfrak{P}_p$ in $\hat{K}$ and so in $\hat{L}$.

We assume $p\equiv 1 \pmod{2^3}$ in the following. Then as is well-known, p can be written in the form

$$p=a^2+2b^2.$$

To get the simpler results, we choose the sign of a so that

$$a\equiv 1 \pmod{4}.$$

Put

$$\lambda(p)=a+b\sqrt{-2}.$$

which is a prime number of k. Since

$$\mathfrak{f}(\hat{L}/k)\,|\,2\sqrt{-2}q\mathfrak{p}_\infty, \quad \lambda(p)\equiv 1 \pmod{2\sqrt{-2}}$$

and the degree of $\mathfrak{P}_p$ over k is $\mathrm{Ord}\,(q,p)$, it follows from the Hasse product formula applied to $\lambda(p)$ that

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=\left\{\prod_{\mathfrak{p}|q}\left(\frac{\lambda(p),\,\hat{L}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}\,(q,p)}. \tag{5.1}$$

By Theorem 1.10, $G(\hat{K}/Q)$ is generated by x_{-1}, x_0, x_1, and completely determined by the relations

$$\begin{aligned} &(x_i, x_j)x_k=x_k(x_i, x_j), \qquad \text{all } i, j, k,\\ &x_{-1}x_0=x_0x_{-1}, \quad x_{-1}^2=1, \quad x_0^2=(x_{-1}, x_0)^{-[1,0]},\\ &x_1^{q-1}=(x_{-1}, x_1)^{[0,1]}(x_0, x_1)^{[0,1]^*}, \end{aligned} \tag{5.2}$$

where x_{-1}, x_0, x_1 are suitable extensions of

$$\tau=\left(\frac{5,\,K/Q}{2}\right), \quad \tau^*=\left(\frac{-1,\,K/Q}{2}\right) \quad \text{and} \quad \tau_1=\left(\frac{g_1,\,K/Q}{q}\right)$$

to $\hat{K}$, respectively, and [0, 1], [0, 1]*, [1, 0] the indices defined by

$$q\equiv(-1)^{[0,1]^*}5^{[0,1]} \pmod{2^3}, \qquad 2\equiv g_1^{[1,0]} \pmod{q}, \tag{5.3}$$

g_1 being a fixed primitive root mod $q=q_1$. We note that $\sqrt{-2}^{x_0}=-\sqrt{-2}$, because if we take $\zeta_{2^3}=\dfrac{1+\sqrt{-1}}{\sqrt{2}}$ for example, then $\sqrt{-2}=\zeta_{2^3}-\zeta_{2^3}^{-1}$ and hence $\sqrt{-2}^{\tau^*}=\zeta_{2^3}^{-1}-\zeta_{2^3}=-\sqrt{-2}$.

Now we first suppose $\left(\dfrac{-2}{q}\right)=1$, i.e. $q\equiv 1, 3 \pmod{2^3}$. In this case, q splits completely in k. Set $(q)=\mathfrak{q}\mathfrak{q}^{x_0}$ in k. Then by (5.1), we have

$$\begin{aligned}\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)&=\left\{\left(\frac{\lambda(p),\ \hat{L}/k}{\mathfrak{q}}\right)x_0'\left(\frac{\lambda(p)^{x_0},\ \hat{L}/k}{\mathfrak{q}}\right)x_0'^{-1}\right\}^{\mathrm{Ord}\,(q,p)}\\&=\left(\frac{p^{\mathrm{Ord}\,(q,p)},\ \hat{L}/k}{\mathfrak{q}}\right)\left(x_0',\left(\frac{\lambda(p)^{x_0},\ \hat{L}/k}{\mathfrak{q}}\right)\right)^{\mathrm{Ord}\,(q,p)}\\&=\left(x_0',\left(\frac{\lambda(p)^{x_0},\ \hat{L}/k}{\mathfrak{q}}\right)\right)^{\mathrm{Ord}\,(q,p)},\end{aligned}$$

here x_i' denotes the restriction of x_i to $\hat{L}$, because of $\mathfrak{f}(\hat{L}/k)\,|\,2\sqrt{-2}q\mathfrak{p}_\infty$ and $p^{\mathrm{Ord}\,(q,p)}\equiv 1 \pmod{q}$. There exists a rational integer r such that $r^2\equiv -2 \pmod{q}$. Then $\lambda(p)^{x_0}\equiv a\pm br \pmod{\mathfrak{q}}$. Since

$$\left(\frac{\lambda(p)^{x_0},\ K/k}{\mathfrak{q}}\right)=\left(\frac{a\pm br,\ K/k}{\mathfrak{q}}\right)=\tau_1^{\mathrm{ind}\,(a\pm br)}$$

with $a\pm br\equiv g_1^{\mathrm{ind}\,(a\pm br)} \pmod{q}$, we get

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=(x_0',\ x_1')^{\mathrm{Ord}(q,p)\ \mathrm{ind}(a\pm br)},$$

in which $(x_0', x_1')=(x_{-1}', x_1')$ is a generator of $G(\hat{L}/K)$ of order two by Lemma 2.9. Let Ord (q, p) be odd. Then

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=1 \quad \text{iff} \quad \left(\frac{a\pm br}{q}\right)=1.$$

It is clear that

$$\left(\frac{a+br}{q}\right)=\left(\frac{a-br}{q}\right).$$

We obtain

Theorem 5.1. *Let* $q\equiv 1, 3 \pmod{2^3}$, *and let* $p=a^2+2b^2$, $a\equiv 1 \pmod{4}$. *Then*

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=\left(\frac{a+br}{q}\right)^{\mathrm{Ord}\,(q,p)},$$

where $r^2 \equiv -2 \pmod q$.

We next suppose $\left(\frac{-2}{q}\right)=-1$, i.e. $q\equiv 5, 7 \pmod{2^3}$. In this case, q remains prime in k. Thus by (5.1),

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=\left(\frac{\lambda(p)^{\mathrm{Ord}\,(q,p)},\ \hat{L}/k}{q}\right).$$

Let G be a generator of the group of reduced residue classes mod q in k such that $N_{k/Q}G\equiv g_1 \pmod q$, and set $\lambda(p)^{\mathrm{Ord}\,(q,p)}\equiv G^e \pmod q$. Then $q-1\,|\,e$. Writing $e=(q-1)e'$, we have

$$\lambda(p)^{\mathrm{Ord}\,(q,p)}\equiv G^{(q-1)e'} \pmod q, \tag{5.4}$$

from which follows

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=\left(\frac{G,\ \hat{L}/k}{q}\right)^{(q-1)e'},$$

because of $\mathfrak{f}(\hat{L}/k)\,|\,2\sqrt{-2}q\mathfrak{p}_\infty$. The restriction of

$$\left(\frac{G,\ \hat{L}/k}{q}\right) \quad \text{to } K \text{ is} \quad \left(\frac{G,\ K/k}{q}\right)=\left(\frac{g_1,\ K/Q}{q}\right)=\tau_1,$$

and $G(\hat{L}/K)$ is contained in the center of $G(\hat{L}/Q)$. Thus by (5.2),

$$\begin{aligned}\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)&=x_1'^{(q-1)e'}=\{(x'_{-1},\ x'_1)^{[0,1]}(x'_0,\ x'_1)^{[0,1]^*}\}^{e'}\\ &=(x'_0,\ x'_1)^{([0,1]+[0,1]^*)e'}=(x'_0,\ x'_1)^{e'},\end{aligned}$$

because $[0, 1]+[0, 1]^*$ is odd provided that $q\equiv 5, 7 \pmod{2^3}$, which implies

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=(-1)^{e'}. \tag{5.5}$$

To get a rational expression of this, let f be the regular representation of k with respect to the basis $\{1, \sqrt{-2}\}$ as an algebra over Q. Then for any $u, v \in Q$, $f(u+v\sqrt{-2})=\begin{bmatrix} u & -2v \\ v & u\end{bmatrix}$. Let

$$R=\left\{\begin{bmatrix}\alpha & -2\beta\\ \beta & \alpha\end{bmatrix}\,\middle|\,\alpha,\ \beta\in Z/qZ\right\},$$

and let

$$S(q)=R\cap SL_2(Z/qZ). \tag{5.6}$$

Then f induces the isomorphism $\tilde{f}$ of the residue class field mod q in k to R. Since the sequence

$$1\longrightarrow S(q)\longrightarrow R^{\times}\xrightarrow{\det}(Z/qZ)^{\times}\longrightarrow 1$$

is exact, $S(q)$ is a cyclic group of order $q+1$, and hence $\tilde{f}(G)^{(q-1)}$ is a generator of $S(q)$. Because $\tilde{f}(\lambda(p))^{\mathrm{Ord}(q,p)}=\tilde{f}(G)^{(q-1)e'}$ by (5.4), we get from (5.5)

Theorem 5.2. *Let $q\equiv 5, 7 \pmod{2^3}$, and let $p=a^2+2b^2$, $a\equiv 1 \pmod 4$, be a rational prime. Then $\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=1$ iff $\begin{bmatrix} a & -2b \\ b & a \end{bmatrix}^{\mathrm{Ord}(q,p)} \pmod q \in S(q)^2$, where $S(q)$ is the cyclic group of order $q+1$ defined by* (5.6)

The next lemma with Convention 3.3 can be verified in an elementary way.

Lemma 5.3. *Let $X\in S(q)$.*
(i) *If $q\equiv 7 \pmod{2^3}$, then $X\in S(q)^2$ iff $X\in [SL_2(Z/qZ)]^2$.*
(ii) *If $q\equiv 5 \pmod{2^3}$, then $X\in S(q)^2$ iff $X\in [SL_2(Z/qZ)]^2$ and*

$$X\neq -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We obtain another expression of Theorem 5.2, namely,

Theorem 5.4. *Let the hypotheses and notation be as in Theorem 5.2. Then*

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_p}\right)=1 \quad \textit{iff} \quad \begin{bmatrix} a & -2b \\ b & a \end{bmatrix} \pmod q \in [SL_2(Z/qZ)]^2$$

or

$$\begin{bmatrix} a & -2b \\ b & a \end{bmatrix} \pmod q \in [SL_2(Z/qZ)]^2$$

and

$$\begin{bmatrix} a & -2b \\ b & a \end{bmatrix}\not\equiv -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod q,$$

according as $q\equiv 7$ or $5 \pmod{2^3}$.

For the rest, we determine the decomposition laws of 2 and q in $\hat{L}$. It follows from [43, Lemmas 3, 4 and § 3] that the inertia group of $\mathfrak{P}_2$ with respect to $\hat{K}/K$ is generated by three elements (x_{-1}, x_0), $(x_{-1}, x_1)^{[1,0]}$, $(x_0, x_1)^{[1,0]}$ and that of $\mathfrak{P}_q$ by $(x_0, x_1)^{-[0,1]^*}(x_{-1}, x_1)^{-[0,1]}$. But $(x_{-1}, x_0)=1$ by Theorem 1.9 when $\nu=3$ and $(x'_{-1}, x'_1)=(x'_0, x'_1)$ by Lemma 2.9. Thus the inertia group of $\mathfrak{P}_2$ in $\hat{L}$ is $\langle(x'_0, x'_1)^{[1,0]}\rangle$ and that of $\mathfrak{P}_q$ $\langle(x'_0, x'_1)^{[0,1]^*+[0,1]}\rangle$. Since (x'_0, x'_1) is of order two, we have by (5.3)

Lemma 5.5. (i) *$\mathfrak{P}_2$ is unramified in $\hat{L}$ iff* $\left(\frac{2}{q}\right)=1$, *i.e.* $q\equiv 1, 7$ (mod 2^3).

(ii) *$\mathfrak{P}_q$ is unramified in $\hat{L}$ iff* $q\equiv 1, 3$ (mod 2^3).

Let $q\equiv 1, 7$ (mod 2^3), and let T be the inertia field of $(\sqrt{-2})$ with respect to $\hat{L}/k$. Since $T\supset L$, and since $\mathfrak{P}_2$ is totally ramified over L, we have $K\cap T=L$. The ramification index of $(\sqrt{-2})$ with respect to $\hat{L}/k$ is two, so $[T\colon k]=[\hat{L}\colon k]/2=2(q-1)$, thus $[T\colon L]=2$. We get $\hat{L}=KT$, and hence $\left(\frac{\hat{L}/K}{\mathfrak{P}_2}\right)=\left(\frac{T/L}{\mathfrak{P}'_2}\right)$, where $\mathfrak{P}'_2$ means the restriction of $\mathfrak{P}_2$ to L. Now applying the Hasse product formula to $\sqrt{-2}$ and raising the both sides to the Ord $(q, 2)$ power, we have

$$\left(\frac{\sqrt{-2}, \hat{L}/k}{(\sqrt{-2})}\right)^{-\mathrm{Ord}\,(q,2)}=\left\{\prod_{\mathfrak{p}|q}\left(\frac{\sqrt{-2}, \hat{L}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}\,(q,2)},$$

whose right side is just equal to that of (5.1) if we regard as $\lambda(2)=0+1\sqrt{-2}=\sqrt{-2}$. Therefore by the same procedure as before, we get that if $q\equiv 1$ (mod 2^3), then

$$\left(\frac{\sqrt{-2}, \hat{L}/k}{(\sqrt{-2})}\right)^{-\mathrm{Ord}\,(q,2)}=(x'_0, x'_1)^{\mathrm{Ord}\,(q,2)\ \mathrm{ind}\,(\pm r)},$$

where $r^2\equiv -2$ (mod q). Restricting this to T and denoting by x''_i the restriction of x'_i to T,

$$\left(\frac{T/L}{\mathfrak{P}'_2}\right)=(x''_0, x''_1)^{\mathrm{Ord}\,(q,2)\ \mathrm{ind}\,(\pm r)},$$

because $(\sqrt{-2})$ is unramified in T and the degree of $\mathfrak{P}'_2$ over k is Ord $(q, 2)$. Since (x''_0, x''_1) is a generator of $G(T/L)$, and since

$$\left(\frac{r}{q}\right)\left(\frac{-r}{q}\right)=\left(\frac{2}{q}\right)=1,$$

we conclude

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_2}\right)=\left(\frac{r}{q}\right)^{\mathrm{Ord}\,(q,2)}.$$

On the other hand, if $q\equiv 7 \pmod{2^3}$, then by putting $\lambda(2)^{\mathrm{Ord}\,(q,2)}\equiv G^{(q-1)e'}$ $\pmod{q}$ in k, we have

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_2}\right)=(x_0'', x_1'')^{e'}.$$

Thus we obtain

Theorem 5.6. (i) *If* $q\equiv 1 \pmod{2^3}$, *then*

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_2}\right)=\left(\frac{r}{q}\right)^{\mathrm{Ord}\,(q,2)}=\left(\frac{-2}{q}\right)_4^{\mathrm{Ord}\,(q,2)},$$

where

$$r^2\equiv -2 \pmod{q} \quad \textit{and} \quad \left(\frac{}{-}\right)_4$$

stands for the forth power residue symbol in Q.

(ii) *If* $q\equiv 7 \pmod{2^3}$, *then*

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_2}\right)=1 \quad \textit{iff} \quad \begin{bmatrix}0 & -2\\ 1 & 0\end{bmatrix}^{\mathrm{Ord}\,(q,2)} \pmod{q} \in [SL_2(Z/qZ)]^2.$$

Next assume $q\equiv 1, 3 \pmod{2^3}$. Then q splits completely in k: $(q)=\mathfrak{q}\mathfrak{q}^{x_0}$. Let T be the inertia field of $\mathfrak{q}$ with respect to $\hat{L}/k$. It is easy to see that $T\cap K=Q(\zeta_{23})$ and $\hat{L}=TK$. Thus $\left(\frac{\hat{L}/K}{\mathfrak{P}_q}\right)=\left(\frac{T/Q(\zeta_{23})}{\mathfrak{P}_q'}\right)$, $\mathfrak{P}_q'$ being the restriction of $\mathfrak{P}_q$ to $Q(\zeta_{23})$, because the degree of $\mathfrak{P}_q$ over $\mathfrak{P}_q'$ is one. We first treat the case of $q\equiv 3 \pmod{2^3}$. From the Hasse product formula

$$\left(\frac{q, \hat{L}/k}{(\sqrt{-2})}\right)\left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)\left(\frac{q, \hat{L}/k}{\mathfrak{q}^{x_0}}\right)=1,$$

we have

$$\left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)^{-2}=\left(\frac{q, \hat{L}/k}{(\sqrt{-2})}\right)\left(x_0', \left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)\right). \tag{5.7}$$

Apply the Hasse product formula for K/Q to q, then

$$\left(\frac{q, K/k}{\mathfrak{q}}\right)=\left(\frac{q, K/Q}{q}\right)=(\tau^{*[0,1]*}\tau^{[0,1]})^{-1}=(\tau^{*}\tau)^{-1}$$

and hence

$$\left(x_0', \left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)\right)=(x_0', x_0'x_{-1}')^{-1}=(x_0', x_{-1}')^{-1}=1,$$

because of $(x_0, x_{-1})=1$ when $\nu=3$. Since $q\equiv -1 \pmod 4$ and $\mathfrak{f}(\hat{L}/k)|2\sqrt{-2}q\mathfrak{p}_\infty$, $\left(\frac{q, \hat{L}/k}{(\sqrt{-2})}\right)=\left(\frac{-1, \hat{L}/k}{(\sqrt{-2})}\right)$. Let $\sigma=\left(\frac{2, K/Q}{2}\right)^{-1}$. Then it follows from [42, p. 126, lines 6 and 7] that there exists an extension $\tilde{\sigma}$ of σ to $\hat{K}$ such that

$$\left(\frac{-\zeta_{23}, \hat{K}/Q(\zeta_{23})}{(1-\zeta_{23})}\right)=(x_0, \tilde{\sigma})=(x_0, x_1)^{[1,0]},$$

in which the second sign of equality follows from applying the Hasse product formula for K/Q to 2. Thus

$$\left(\frac{-1, \hat{L}/k}{(\sqrt{-2})}\right)=\left(\frac{-\zeta_{23}, \hat{L}/Q(\zeta_{23})}{(1-\zeta_{23})}\right)=(x_0', x_1')^{[1,0]}=(x_0', x_1'), \tag{5.8}$$

because of $N_{Q(\zeta_{23})/k}(-\zeta_{23})=-1$. So by (5.7),

$$\left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)^{-2}=(x_0', x_1').$$

Restricting the both sides to T, we obtain

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_q}\right)=\left(\frac{T/Q(\zeta_{23})}{\mathfrak{P}_q'}\right)=(x_0'', x_1''),$$

where x_i'' denotes the restriction of x_i' to T, because the degree of $\mathfrak{P}_q'$ over k is $\mathrm{Ord}\,(2^3, q)=2$. Hence $\mathfrak{P}_q$ remains prime in $\hat{L}$.

Next suppose $q\equiv 1 \pmod{2^3}$. In this case, q can be written in the form $q=a^2+2b^2$. Put $\lambda(q)=a+b\sqrt{-2}$, on which we do not make the assumption on the sign of a like $a\equiv 1 \pmod 4$. By the Hasse product formula, it holds that

$$\left(\frac{-1, \hat{L}/k}{(\sqrt{-2})}\right)^e\left(\frac{\lambda(q), \hat{L}/k}{\mathfrak{q}}\right)\left(\frac{\lambda(q), \hat{L}/k}{\mathfrak{q}^{x_0}}\right)=1$$

in which $e=0$ or 1, according as $a\equiv 1$ or $-1 \pmod 4$, and $\mathfrak{q}=(\lambda(q))$. Since $[1, 0]$ is even, we see from (5.8) $\left(\frac{-1, \hat{L}/k}{(\sqrt{-2})}\right)=1$, and hence

$$\left(\frac{q, \hat{L}/k}{\mathfrak{q}}\right)^{-1}=\left(x_0', \left(\frac{\lambda(q)^{x_0}, \hat{L}/k}{\mathfrak{q}}\right)\right)=(x_0', x_1')^{\operatorname{ind} 2a},$$

because $\lambda(q)^{x_0}=a-b\sqrt{-2}\equiv 2a \pmod{\mathfrak{q}}$ and

$$\left(\frac{\lambda(q)^{x_0}, K/k}{\mathfrak{q}}\right)=\left(\frac{2a, K/k}{q}\right)=\tau_1^{\operatorname{ind} 2a},$$

where $2a\equiv g_1^{\operatorname{ind} 2a} \pmod q$. The degree of $\mathfrak{P}_q'$ over k is one, and so restricting the above equality to T, we have

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_q}\right)=\left(\frac{T/Q(\zeta_{2^3})}{\mathfrak{P}_q'}\right)=(x_0'', x_1'')^{\operatorname{ind} 2a},$$

from which it follows that $\left(\frac{\hat{L}/K}{\mathfrak{P}_q}\right)=1$ iff $\left(\frac{2a}{q}\right)=1$.

According to Whiteman [50, § 5] or [51, § 8], one value of a can be expressed in the form $a=\Phi_4(1)/4$, where $\Phi_e(n)$ is the Jacobsthal sum defined by (3.2). Then

$$\text{(5.9)} \qquad 2a\equiv -c \pmod q, \qquad c=\begin{pmatrix} \frac{q-1}{2} \\ \frac{q-1}{8} \end{pmatrix},$$

c being the binomial coefficient, which is a result of Stern [45] (see also Whiteman [51, p. 97, (8.4)]), and hence $\left(\frac{2a}{q}\right)=\left(\frac{c}{q}\right)$.

Summarizing these results, we have

Theorem 5.7. (i) *If $q\equiv 1 \pmod{2^3}$, and if $q=a^2+2b^2$, then*

$$\left(\frac{\hat{L}/K}{\mathfrak{P}_q}\right)=\left(\frac{a}{q}\right)=\left(\frac{c}{q}\right),$$

where $a=\Phi_4(1)/4$ and c is the binomial coefficient as in (5.9).

(ii) *If $q\equiv 3 \pmod{2^3}$, then $\mathfrak{P}_q$ remains prime in $\hat{L}$.*

Example 5.8. Let $q=7$. Then $\hat{L}/Q$ is a class 2 extension of degree $2\phi(2^3\cdot 7)=48$. Let $p\equiv 1 \pmod{2^3\cdot 7}$, and let $p=a^2+2b^2$. Since

$$S(7)^2=\left\{\pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \pm 2\begin{bmatrix}0 & -2\\ 1 & 0\end{bmatrix}\right\},$$

we see by Theorem 5.2 that p splits completely in $\hat{L}$ iff $7\mid ab$. In this case, $[1, 0]$ is even, because of $\left(\frac{2}{7}\right)=1$, and hence by (5.8), $\left(\frac{-1, \hat{L}/k}{(\sqrt{-2})}\right)=1$. Thus we can obtain (5.1) without the assumption of $a\equiv 1 \pmod 4$. This is the reason why the decomposition criterion in this case does not depend on the choice of the sign of a such that $a\equiv 1 \pmod 4$. In general, the corresponding criteria will be independent of the condition $a\equiv 1 \pmod 4$ when $q\equiv 7 \pmod{2^3}$.

By the above, we conclude that the sets of rational primes

$$\{p\equiv 1 \pmod{56}\mid p=a^2+2b^2,\ 7\mid ab\}$$

and

$$\{p\equiv 1 \pmod{56}\mid p=a^2+2b^2,\ 7\nmid ab\}$$

have density 1/48 each.

§ 6. Preliminaries II

Let q be an odd prime, $\zeta=\exp(2\pi i/q)$, $\mathfrak{P}$ be any prime ideal in $Q(\zeta)$ not dividing q whose norm to Q is p^f, and let g be a primitive root mod $\mathfrak{P}$ such that $g^{(p^f-1)/q}\equiv\zeta \pmod{\mathfrak{P}}$. For every integer v, we define the generalized Jacobi-Kummer cyclotomic function $\Psi_v(\zeta)$ by

$$\Psi_v(\zeta)=\sum_h \zeta^{vh+\operatorname{ind}(g^h+1)},$$

where $\alpha\equiv g^{\operatorname{ind}\alpha} \pmod{\mathfrak{P}}$, and h ranges over the values $0, 1, \cdots, p^f-2$ with the exception of $(p^f-1)/2$ if p is odd and 0 if $p=2$ (see Kummer [31, p. 109]). This definition including the case of $p=2$ was given by Mitchell [34] who defined the function for the case where q is composite. Cf. also Vandiver [48, p. 403].

The most important property of the function $\Psi_v(\zeta)$ is the formula

$$\Psi_v(\zeta)\Psi_v(\zeta^{-1})=p^f \tag{6.1}$$

provided that $v\not\equiv 0, -1 \pmod q$ (see [31, p. 111] and [34, p. 168, (5)]).

We need the following simple

Lemma 6.1. *Let* $\pi=1-\zeta$. *Then* $\Psi_v(\zeta)\equiv -1 \pmod\pi$.

Proof. $\Psi_v(\zeta)\equiv\sum_h 1\equiv p^f-2\equiv -1 \pmod\pi$.

Remark. Schwering [39] proved that if $q>3$ and $f=1$, then $\Psi_v(\zeta) \equiv -1 \pmod{\pi^3}$. Mitchell [34, p. 196, (10)] generalized this result to the case where q is the power of a prime>3. See also Kronecker [30, p. 342, (J̄.)]. Dickson [5, Theorem 1] also extended this to the case in which q is an integer prime to 6 and $f=1$ in terms of coefficients of $\Psi_v(\zeta)$. Cf. also Parnami, Agrawal and Rajwade [35].

When $f=1$, i.e. $p\equiv 1 \pmod q$, the function can be written in the form

$$\Psi_v(\zeta)=\sum_{s+t\equiv 1 (\mathrm{mod}\, p)} \zeta^{v\,\mathrm{ind}\, s+\mathrm{ind}\, t},$$

where s, t run over all pairs of integers in the range $1\leqq u, v\leqq p-1$ satisfying the summation condition. Therefore we obtain the following expansion of $\Psi_v(\zeta)$ into a finite Fourier series:

$$\Psi_v(\zeta)=\sum_{i=0}^{q-1} B(i, v)\zeta^i. \tag{6.2}$$

The coefficients $B(i, v)$ are the so-called Dickson-Hurwitz sums defined by

$$B(i, v)=\sum_{h=0}^{q-1} ((h, i-vh)),$$

where $((h, k))$ stands for the cyclotomic number with respect to mod p. For the definition of $((h, k))$, see Dickson [4] for example, and for the above, see Whiteman [52, p. 47] and Dickson [5, p. 364].

Whiteman [50] employed cyclotomy to drive a number of theorems of the Jacobsthal type (cf. [27], [38], etc.) for the primes p with a very important theorem which expresses the Dickson-Hurwitz sum $B(i, 1)$ in terms of Jacobsthal sums. It states

$$qB(i, 1)=p-1+\Phi_q(4g^i), \tag{6.3}$$

where $\Phi_q(n)$ is the Jacobsthal sum defined by (3.2). See [50, Theorem 1] and [51, p. 95, (5.8)].

Lemma 6.2. *Let* $q\equiv 3 \pmod 4$, *and let p be a rational prime different from q. Then there exist rational integers A and B such that*

$$4p^{\frac{q-1}{2}f}=(2A+B)^2+qB^2 \tag{6.4}$$

and

(6.5) $$A+B\frac{1+\sqrt{-q}}{2}\equiv 1 \pmod{\mathfrak{q}},$$

here $f=\mathrm{Ord}\,(q,p)$ *and* $\mathfrak{q}=(\sqrt{-q})$.

Proof. Let $K_1=Q(\zeta)$ and $k=Q(\sqrt{-q})$. Since $N_{K_1/k}(-\Psi_1(\zeta))$ is an integer of k, we may write

$$N_{K_1/k}(-\Psi_1(\zeta))=A+B\frac{1+\sqrt{-q}}{2}$$

with some rational integers A, B. The lemma then follows from (6.1) and Lemma 6.1.

The equality (6.4) with $f=1$ is known. We find it on p. 287 of Bachmann [53].

We next study to express the values of A and B in Lemma 6.2 in terms of Jacobsthal sums when $f=1$, i.e. $p\equiv 1 \pmod q$.

Let $q\equiv 3 \pmod 4$, $p\equiv 1 \pmod q$, and let K_1, k be as in the proof of Lemma 3.7. Then the Galois group $G(K_1/k)$ is given by

$$G(K_1/k)=\left\{\zeta\to\zeta^{j^2}\,|\,j=1,\cdots,2,\frac{q-1}{2}\right\},$$

and so by (6.2),

$$N_{K_1/k}(-\Psi_1(\zeta))=-\prod_{j=1}^{\frac{q-1}{2}}\left(\sum_{i=0}^{q-1}B(i,1)\zeta^{ij^2}\right),$$

Therefore if we put

(6.6) $$N_{K_1/k}(-\Psi_1(\zeta))=a_0+a_1\zeta+\cdots+a_{q-1}\zeta^{q-1}$$

with some rational integers a_i, then for $i=0,1,\cdots,q-1$, we can take one of the values of a_i as

(6.7) $$a_i=-\sum B(i_1,1)B(i_2,1)\cdots B(i_{\frac{q-1}{2}},1),$$

where $i_1, i_2, \cdots, i_{\frac{q-1}{2}}$ run over all pairs of integers in the range $0\leqq i_1$, $i_2,\cdots, i_{\frac{q-1}{2}}\leqq q-1$ satisfying the condition

(6.8) $$i_1+2^2i_2+\cdots+\left(\frac{q-1}{2}\right)^2 i_{\frac{q-1}{2}}\equiv i \pmod q.$$

Substituting the Gauss sum

$$\sqrt{-q}=\zeta+\left(\frac{2}{q}\right)\zeta^2+\cdots+\left(\frac{q-1}{q}\right)\zeta^{q-1} \tag{6.9}$$

for $\sqrt{-q}$ in $N_{K_1/k}(-\Psi_1(\zeta))=A+B\frac{1+\sqrt{-q}}{2}$ and comparing with (6.6), we obtain

$$A=a_0-a_1 \quad \text{and} \quad B=a_1-a_{q-1}.$$

Hence by (6.3) and (6.7), A, B can be expressed in terms of Jacobstal sums, For example, let $q=3$. Then for $i=0, 1, 2,$

$$a_i=-B(i, 1)=-\tfrac{1}{3}(p-1+\Phi_3(4g^i)).$$

Since $\Phi_3(4)+\Phi_3(4g)+\Phi_3(4g^2)=-3$ (see Whiteman [51, p. 92, (4.1)]),

$$2A+B=2a_0-a_1-a_2=-\tfrac{1}{3}(1+\Phi_3(4)),$$
$$B=a_1-a_2=-\tfrac{1}{3}(\Phi_3(4g)-\Phi_3(4g^2))$$

which satisfy

$$4p=(2A+B)^2+3B^2.$$

This is the theorem of von Schrutka [38]. Cf. also Whitemen [50, § 6] and [51, § 7].

Theorem 6.3. *Let* $q\equiv 3 \pmod 4$ *and let* $p\equiv 1 \pmod q$. *Then one solution of the diophantine equation* (6.4) *with* (6.5) *is given by*

$$A=a_0-a_1, \qquad B=a_1-a_{q-1},$$

where a_i *are the integers defined by* (6.7). *Moreover, if* $p\equiv 1 \pmod{q_2}$ *for a prime* $q_2\neq q$, *then*

$$a_i\equiv-\frac{1}{q^{(q-1)/2}}\sum\Phi_q(4g^{i_1})\Phi_q(4g^{i_2})\cdots\Phi_q(4g^{i_{\frac{q-1}{2}}}) \pmod{q_2},$$

where $i_1, i_2, \cdots, i_{\frac{q-1}{2}}$ *run over all pairs of integers in the range* $0\leq i_1, i_2, \cdots, i_{\frac{q-1}{2}}\leq q-1$ *satisfying the condition* (6.8).

Proof. The congruence follows immediately from (6.3) and (6.7).

§ 7. The case (A)

Throughout this section, let q_1, q_2 be distinct odd primes such that

$(q_1-1, q_2-1)=2$, $\zeta_1=\exp(2\pi i/q_1)$, $K_1=Q(\zeta_1)$, $K=K_{12}$ be the q_1q_2-th cyclotomic field over Q, and let $\hat{K}=\hat{K}_{12}$ be the central class field mod $q_1q_2p_\infty$ of K/Q. Since q_1 or q_2 is of type $\equiv 3 \pmod 4$, we assume throughout

$$q_1 \equiv 3 \pmod 4.$$

Let $k=Q(\sqrt{-q_1})$. Then $K_1 \supset k$. Since $\left(\frac{q_1-1}{2}, q_2-1\right)=1$, $G(K/k)$ is cyclic, and hence $G(\hat{K}/k)$ is Abelian. Let $\mathfrak{q}_1=(\sqrt{-q_1})$. The Hasse function of $\mathfrak{q}_1$ with respect to k/Q is given by $\psi(i)=2i$ for $i \geqq 0$, or q_1 is tamely ramified in k, and so $\mathfrak{g}_{k/Q}(q_1q_2p_\infty)=\mathfrak{q}_1q_2\mathfrak{p}_\infty$, where $\mathfrak{p}_\infty$ stands for the complex prime divisor of k. Since $\mathfrak{f}(\hat{K}/Q)=q_1q_2p_\infty$, we get by Lemma 1.2

$$\mathfrak{f}(\hat{K}/k) \mid \mathfrak{q}_1q_2\mathfrak{p}_\infty. \tag{7.1}$$

We denote by $\mathfrak{P}_p$ any prime factor of a rational prime p in K. Let $p \neq q_1, q_2$. If $\operatorname{Ord}(q_1, p)$ is even, then we can completely describe the value of the Artin symbol $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)$ using Theorem 2.5. Thus in the following we suppose that $\operatorname{Ord}(q_1, p)$ is odd. Let A, B be the rational integers satisfying (6.4) with (6.5) in Lemma 6.2 for $q=q_1$, and let

$$\lambda(p)=A+B\frac{1+\sqrt{-q_1}}{2} \equiv 1 \pmod{\mathfrak{q}_1}. \tag{7.2}$$

Then $N_{k/Q}\lambda(p)=p^{\frac{q_1-1}{2}\operatorname{Ord}(q_1,p)}$ by Lemma 6.2. Thus we obtain from the Hasse product formula, (7.1) and (7.2) that

$$\prod_{\mathfrak{p}\mid p}\left(\frac{\lambda(p), \hat{K}/k}{\mathfrak{p}}\right)\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p), \hat{K}/k}{\mathfrak{p}}\right)=1. \tag{7.3}$$

Since $\operatorname{Ord}(q_1, p)$ is odd, $p^{\frac{q_1-1}{2}} \equiv 1 \pmod{q_1}$, namely, $\left(\frac{p}{q_1}\right)=1$, and hence by reciprocity law, $\left(\frac{-q_1}{p}\right)=1$ when p is odd, which implies that p splits completely in k. On the other hand, if $p=2$, then $q_1 \equiv 7 \pmod 8$, because of $q_1 \equiv 3 \pmod 4$. The discriminant of k is $-q_1$ which is congruent to 1 mod 8, and hence 2 also splits completely in k. Let $(p)=\mathfrak{p}_p\bar{\mathfrak{p}}_p$ and $(\lambda(p))=\mathfrak{p}_p^{e_1}\bar{\mathfrak{p}}_p^{e_2}$ be the factorizations of p and $\lambda(p)$ into prime factors in k, where $\bar{\mathfrak{p}}_p$ means the conjugate ideal of $\mathfrak{p}_p$. Then (7.3) yields

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)^{e_1}\left(\frac{\hat{K}/K}{\bar{\mathfrak{P}}_p}\right)^{e_2}=\left\{\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p), \hat{K}/k}{\mathfrak{p}}\right)\right\}^{\operatorname{Ord}(q_1q_2,p)},$$

here $\mathfrak{P}_p$, $\overline{\mathfrak{P}}_p$ denote prime factors of $\mathfrak{p}_p$ and $\bar{\mathfrak{p}}_p$ in K, respectively, because the degrees of $\mathfrak{P}_p$ and $\overline{\mathfrak{P}}_p$ over k are $\mathrm{Ord}(q_1q_2, p)$. Since $\hat{K}$ is a central extension of K/Q, the value of the Artin symbol $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)$ does not depend on the choice of $\mathfrak{P}_p$ over p. In addition $[\hat{K}: K]=2$ and by Lemma 6.2, $e_1+e_2=\frac{q_1-1}{2}\mathrm{Ord}(q_1, p)$ which is odd by assumption. Therefore,

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left\{\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p),\hat{K}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}(q_1q_2,p)}.$$

Moreover we show that the power exponent of the right side can be replaced by $\mathrm{Ord}(q_2, p)$. Restricting (7.3) to K and raising to the $\mathrm{Ord}(q_2, p)$-th power, we have

$$\left\{\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p), K/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}(q_2,p)}=\left(\frac{K/k}{\mathfrak{p}_p}\right)^{\frac{q_1-1}{2}\mathrm{Ord}(q_1,p)\mathrm{Ord}(q_2,p)}=1,$$

because $G(K/Q)$ is Abelian, which implies that

$$\left\{\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p),\hat{K}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}(q_2,p)}$$

belongs to $G(\hat{K}/K)$. Since $\mathrm{Ord}(q_1q_2, p)$ is the least common multiple of $\mathrm{Ord}(q_1, p)$ and $\mathrm{Ord}(q_2, p)$, it follows from the assumption on $\mathrm{Ord}(q_1, p)$ that $\mathrm{Ord}(q_1q_2, p)/\mathrm{Ord}(q_2, p)$ is odd. Hence we obtain

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left\{\prod_{\mathfrak{p}\mid q_2}\left(\frac{\lambda(p),\hat{K}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}(q_2,p)}. \tag{7.4}$$

The Galois group $G(\hat{K}/Q)$ is generated by two elements x_1, x_2 which are extensions of

$$\tau_1=\left(\frac{g_1, K/Q}{q_1}\right) \quad\text{and}\quad \tau_2=\left(\frac{g_2, K/Q}{q_2}\right) \tag{7.5}$$

to $\hat{K}$, respectively, where g_i is a fixed primitive root mod q_i, $i=1, 2$ as in (1.1). By the definition of the norm residue symbol τ_1, we see

$$\zeta_1^{\tau_1^{\frac{q_1-1}{2}}}=\zeta_1^{g_1^{\frac{q_1-1}{2}}}=\zeta_1^{-1}$$

and hence by (6.9),

$$\sqrt{-q_1}^{\tau_1^{\frac{q_1-1}{2}}}=-\sqrt{-q_1}. \tag{7.6}$$

We first investigate the case of $\left(\frac{q_2}{q_1}\right)=1$. By reciprocity law, $\left(\frac{-q_1}{q_2}\right)=1$, so q_2 splits completely in k. By (7.6), we may write the factorization of (q_2) in k as

$$(q_2)=\mathfrak{q}_2\mathfrak{q}_2^y,$$

here

$$y=x_1^{\frac{q_1-1}{2}}. \tag{7.7}$$

Then (7.4) becomes

$$\begin{aligned}\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)&=\left(\frac{p^{\mathrm{Ord}(q_1,p)\,\mathrm{Ord}(q_2,p)\frac{q_1-1}{2}},\ \hat{K}/k}{\mathfrak{q}_2}\right)\left(y,\left(\frac{\lambda(p)^y,\ \hat{K}/k}{\mathfrak{q}_2}\right)\right)^{\mathrm{Ord}\,(q_2,p)}\\&=\left(y,\left(\frac{\lambda(p)^y,\ \hat{K}/k}{\mathfrak{q}_2}\right)\right)^{\mathrm{Ord}\,(q_2,p)},\end{aligned}$$

because of (7.1) and of $p^{\mathrm{Ord}\,(q_2,p)}\equiv 1 \pmod{q_2}$. Let r be a rational integer such that $(2r-1)^2\equiv -q_1 \pmod{q_2}$. Since $\left(\frac{-q_1}{q_2}\right)=1$, such an integer always exists. Then $2r-1\equiv\pm\sqrt{-q_1} \pmod{\mathfrak{q}_2}$. So if $2r-1+\sqrt{-q_1}\equiv 0 \pmod{\mathfrak{q}_2}$, then

$$\lambda(p)^y=A+B\frac{1-\sqrt{-q_1}}{2}\equiv A+Br \pmod{\mathfrak{q}_2},$$

and hence

$$\left(\frac{\lambda(p)^y,\ K/k}{\mathfrak{q}_2}\right)=\left(\frac{g_2,\ K/Q}{q_2}\right)^{\mathrm{ind}\,(A+Br)}=\tau_2^{\mathrm{ind}\,(A+Br)},$$

where $\mathrm{ind}\,(A+Br)$ means the index of $A+Br \bmod q_2$ relative to the primitive root g_2. We have by (7.7)

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=(x_1,\ x_2)^{\frac{q_1-1}{2}\mathrm{Ord}(q_2,p)\,\mathrm{ind}(A+Br)}.$$

Since $G(\hat{K}/K)=\langle(x_1,x_2)\rangle$ is of order two, and since $\frac{q_1-1}{2}$ is odd, we get that $\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1$ iff $\mathrm{Ord}\,(q_2,p)\,\mathrm{ind}\,(A+Br)\equiv 0 \pmod 2$, which implies

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{A+Br}{q_2}\right)^{\mathrm{Ord}\,(q_2,p)}.$$

If $2r-1-\sqrt{-q_1}\equiv 0 \pmod{q_2}$, then by the same procedure as above, we obtain

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{A+B(1-r)}{q_2}\right)^{\mathrm{Ord}\,(q_2,p)}.$$

But by (6.4),

$$\begin{aligned}&(A+Br)^{\mathrm{Ord}\,(q_2,p)}(A+B(1-r))^{\mathrm{Ord}\,(q_2,p)}\\ &\equiv p^{\frac{q_1-1}{2}\mathrm{Ord}\,(q_1,p)\,\mathrm{Ord}\,(q_2,p)}\equiv 1 \pmod{q_2}.\end{aligned}$$

Theorem 7.1. *Let* $\left(\frac{q_2}{q_1}\right)=1$, *$p$ be a rational prime such that* Ord (q_1, p) *is odd, and let A, B be rational integers as in Lemma* 6.2. *Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{A+Br}{q_2}\right)^{\mathrm{Ord}\,(q_2,p)},$$

where r is a rational integer such that $(2r-1)^2\equiv -q_1 \pmod{q_2}$.

We next assume $\left(\frac{q_2}{q_1}\right)=-1$. In this case, q_2 remains prime in k. Thus by (7.4),

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=\left(\frac{\lambda(p)^{\mathrm{Ord}\,(q_2,p)},\ \hat{K}/k}{q_2}\right). \tag{7.8}$$

The Galois group $G(\hat{K}/Q)$ is generated by two elements x_1, x_2 which are extensions of (7.5) to $\hat{K}$, respectively, and completely determined by the relations

$$\begin{aligned}&(x_1, x_2)x_i=x_i(x_1, x_2), && i=1, 2,\\ &x_1^{q_1-1}=(x_1, x_2)^{-[2,1]}, && x_2^{q_2-1}=(x_1, x_2)^{[1,2]},\end{aligned}$$

where

$$q_1\equiv g_2^{[2,1]} \pmod{q_2}, \qquad q_2\equiv g_1^{[1,2]} \pmod{q_1}.$$

Since $\left(\frac{q_2}{q_1}\right)=-1$, $[1, 2]$ is odd, so

$$x_2^{q_2-1}=(x_1, x_2). \tag{7.9}$$

Let G be a generator of the group of reduced residue classes mod q_2 in k such that $N_{k/Q}G \equiv g_2 \pmod{q_2}$, and let $\lambda(p)^{\mathrm{Ord}\,(q_2,p)} \equiv G^e \pmod{q_2}$. We see $q_2 - 1 \mid e$ by multipling the both sides by their conjugates. Let $e = (q_2-1)e'$, then

$$\lambda(p)^{\mathrm{Ord}\,(q_2,p)} \equiv G^{(q_2-1)e'} \pmod{q_2}. \tag{7.10}$$

From (7.1), (7.8), (7.9) and (7.10), we have

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = \left(\frac{G,\, \hat{K}/k}{q_2}\right)^{(q_2-1)e'} = x_2^{(q_2-1)e'} = (x_1, x_2)^{e'},$$

because the restriction of $\left(\frac{G,\, \hat{K}/k}{q_2}\right)$ to K is $\left(\frac{G,\, K/k}{q_2}\right) = \left(\frac{g_2,\, K/Q}{q_2}\right) = \tau_2$ and so $\left(\frac{G,\, \hat{K}/k}{q_2}\right)x_2^{-1}$ is contained in $G(\hat{K}/K)$ and hence in the center of $G(\hat{K}/Q)$. Therefore

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right) = (-1)^{e'}. \tag{7.11}$$

To get a rational expression of (7.11), let f be the regular representation of k with respect to the basis $\left\{1, \frac{1+\sqrt{-q_1}}{2}\right\}$ as an algebra over Q. Then for any $u, v \in Q$, $f\left(a + b\frac{1+\sqrt{-q_1}}{2}\right) = \begin{bmatrix} u & -(q_1+1)v/4 \\ v & u+v \end{bmatrix}$. Let

$$R = \left\{ \begin{bmatrix} \alpha & -(q_1+1)\beta/4 \\ \beta & \alpha+\beta \end{bmatrix} \,\middle|\, \alpha, \beta \in Z/q_2Z \right\},$$

and let

$$S(q_2) = R \cap SL_2(Z/q_2Z). \tag{7.12}$$

It is clear that f induces the isomorphism $\tilde{f}$ of the residue class field mod q_2 in k to R. Since the sequence

$$1 \longrightarrow S(q_2) \longrightarrow R^{\times} \xrightarrow{\det} (Z/q_2Z)^{\times} \longrightarrow 1$$

is exact, $S(q_2)$ is a cyclic group of order q_2+1, so $\tilde{f}(G)^{q_2-1}$ is a generator of $S(q_2)$. By (7.10) and (7.11), we conclude

Theorem 7.2. *Let* $\left(\frac{q_2}{q_1}\right) = -1$, *$p$ be a rational prime such that*

Ord (q_1, p) *is odd, and let* A, B *be rational integers as in Lemma* 6.2. *Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1 \quad \textit{iff} \quad \begin{bmatrix} A & -(q_1+1)B/4 \\ B & A+B \end{bmatrix}^{\operatorname{Ord}(q_2,p)} \pmod{q_2} \in S(q_2)^2,$$

where $S(q_2)$ *is the subgroup of* $SL_2(Z/q_2Z)$ *defined by* (7.12).

Another expression of the above theorem is given as follows: We have, after some calculations, the next with Convention 3.3.

Lemma 7.3. *Let* $X \in S(q_2)$.
(i) *If* $q_2 \equiv 3 \pmod 4$, *then* $X \in S(q_2)^2$ *iff* $X \in [SL_2(Z/q_2Z)]^2$.
(ii) *If* $q_2 \equiv 1 \pmod 4$, *then* $X \in S(q_2)^2$ *iff* $X \in [SL_2(Z/q_2Z)]^2$ *and*

$$X \neq -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence

Theorem 7.4. *Let the situation and notation be as in Theorem* 7.2. *If* $q_2 \equiv 3 \pmod 4$, *then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1 \quad \textit{iff} \quad \begin{bmatrix} A & -(q_1+1)B/4 \\ B & A+B \end{bmatrix}^{\operatorname{Ord}(q_2,p)} \pmod{q_2} \in [SL_2(Z/q_2Z)]^2.$$

If $q_2 \equiv 1 \pmod 4$, *then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_p}\right)=1 \quad \textit{iff} \quad \begin{bmatrix} A & -(q_1+1)B/4 \\ B & A+B \end{bmatrix}^{\operatorname{Ord}(q_2,p)} \pmod{q_2} \in [SL_2(Z/q_2Z)]^2$$

and

$$\not\equiv -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{q_2}.$$

Finally we determine the decomposition laws of q_1 and q_2 in $\hat{K}$. For a while, let q_1, q_2 be any distinct odd primes, and let $d=(q_1-1, q_2-1)$. It follows from [43] that the inertia groups of $\mathfrak{P}_{q_1}$ and $\mathfrak{P}_{q_2}$ in $\hat{K}$ are generated by $(x_1, x_2)^{[2,1]}$ and $(x_1, x_2)^{-[1,2]}$, respectively. Since $q_1 \equiv g_2^{[2,1]} \pmod{q_2}$, $q_2 \equiv g_1^{[1,2]} \pmod{q_1}$, and since $G(\hat{K}/K)=\langle (x_1, x_2)\rangle$ is of order d, we obtain

Lemma 7.5. (i) $\mathfrak{P}_{q_1}$ *is unramified in* $\hat{K}$ *iff* q_1 *is a d-th power residue* mod q_2.
(ii) $\mathfrak{P}_{q_2}$ *is unramified in* $\hat{K}$ *iff* q_2 *is a d-th power residue* mod q_1.

Furthermore we have

Theorem 7.6. *Let n be a divisor of (q_1-1, q_2-1). If q_1 is an n-th power residue* mod q_2 *and q_2 an n-th power residue* mod q_1, *then the central class number of the q_1q_2-th cyclotomic field is divisible by n.*

Proof. By assumption, $[2, 1]\equiv[1, 2]\equiv 0 \pmod n$. Thus the inertia groups of $\mathfrak{P}_{q_1}$ and $\mathfrak{P}_{q_2}$ are contained in $G(\hat{K}/K)^n$. Let L be the subfield of $\hat{K}$ corresponding to $G(\hat{K}/K)^n$. Then L/K is an unramified extension of degree n, which implies that the central class number of K is divisible by n. Notice that the inertia groups of the cojugates ideals of $\mathfrak{P}_{q_i}$ in $\hat{K}$ coincide with that of $\mathfrak{P}_{q_i}$, because $\hat{K}$ is a central extension of K/Q.

Corollary 7.7. *Let q_1, q_2 be odd primes such that*

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

Then the central class number of the q_1q_2-th cyclotomic field is even.

Now let $q_1\equiv 3 \pmod 4$, $(q_1-1, q_2-1)=2$, as before. Then Lemma 7.5 states that

$$\mathfrak{P}_{q_1} \text{ is unramified in } \hat{K} \text{ iff } \left(\frac{q_1}{q_2}\right)=1,$$

$$\mathfrak{P}_{q_2} \text{ is unramified in } \hat{K} \text{ iff } \left(\frac{q_2}{q_1}\right)=1.$$

We first suppose $\left(\frac{q_1}{q_2}\right)=1$. The factorization of q_1 in k is $(q_1)=\mathfrak{q}_1^2$. Let T be the inertia field of $\mathfrak{q}_1$ in $\hat{K}$. Then $T\cap K_1=k$, because $\mathfrak{q}_1$ is totally ramified in K_1. We show $\hat{K}=TK_1$. Since the prime factor of $\mathfrak{q}_1$ in K_1 is unramified in $\hat{K}$, the ramification index of $\mathfrak{q}_1$ with respect to $\hat{K}/k$ is $[K_1: k]=(q_1-1)/2$, and hence $[T: k]=[\hat{K}: k]/[K_1: k]=2(q_2-1)$, so $[TK_1: k]=(q_1-1)(q_2-1)=[\hat{K}: k]$. Thus $\hat{K}=TK_1$. Let $K'=k(\zeta_{q_2})$, and let $\mathfrak{P}'_{q_1}$ be the restriction of $\mathfrak{P}_{q_1}$ to K'. Since the degree of $\mathfrak{P}_{q_1}$ over $\mathfrak{P}'_{q_1}$ is one and $T\cap K=K'$,

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_1}}\right)=\left(\frac{T/K'}{\mathfrak{P}'_{q_1}}\right).$$

We apply the Hasse product formula to $\sqrt{-q_1}$ using (7.1), and then obtain

$$\left(\frac{\sqrt{-q_1},\, \hat{K}/k}{\mathfrak{q}_1}\right)^{-\mathrm{Ord}\,(q_2,q_1)}=\left\{\prod_{\mathfrak{p}|q_2}\left(\frac{\sqrt{-q_1},\, \hat{K}/k}{\mathfrak{p}}\right)\right\}^{\mathrm{Ord}\,(q_2,q_1)}.$$

The right side of this equation is just equal to that of (7.4) if we regard $\sqrt{-q_1}$ as

$$\lambda(q_1) = -1 + 2\frac{1+\sqrt{-q_1}}{2} = \sqrt{-q_1}.$$

If $q_2 \equiv 1 \pmod 4$, then

$$\left(\frac{q_2}{q_1}\right) = (-1)^{\frac{q_2-1}{2}} = 1.$$

So by the same procedure as before, we have

$$\left(\frac{\sqrt{-q_1},\ \hat{K}/k}{\mathfrak{q}_1}\right)^{-\mathrm{Ord}\,(q_2,q_1)} = (x_1,\ x_2)^{\mathrm{Ord}\,(q_2,q_1)\ \mathrm{ind}\ \pm(1-2r)}$$

where $(2r-1)^2 \equiv -q_1 \pmod{q_2}$. Restricting the both sides to T, we get

$$\left(\frac{T/K'}{\mathfrak{P}'_{q_1}}\right) = (x'_1,\ x'_2)^{\mathrm{Ord}\,(q_2,q_1)\ \mathrm{ind}\ \pm(1-2r)},$$

x'_i being the restriction of x_i to T. Hence

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_1}}\right) = \left(\frac{1-2r}{q_2}\right)^{\mathrm{Ord}\,(q_2,q_1)},$$

because of

$$\left(\frac{1-2r}{q_2}\right)\left(\frac{-(1-2r)}{q_2}\right) = \left(\frac{-1}{q_2}\right) = 1.$$

On the other hand, if $q_2 \equiv 3 \pmod 4$, then $\left(\frac{q_2}{q_1}\right) = -1$. So if we put $\lambda(q_1)^{\mathrm{Ord}\,(q_2,q_1)} \equiv G^e \pmod{q_2}$ in k and $e = (q_2-1)e'$, then we see $\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_1}}\right) = (-1)^{e'}$, and so on.

Thus we have proved

Theorem 7.8. *Let* $\left(\frac{q_1}{q_2}\right) = 1$. *Then* $\mathfrak{P}_{q_1}$ *is unramified in* $\hat{K}$.

(i) *If* $q_2 \equiv 1 \pmod 4$, *then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_1}}\right) = \left(\frac{1-2r}{q_2}\right)^{\mathrm{Ord}\,(q_2,q_1)} = \left(\frac{-q_1}{q_2}\right)_4^{\mathrm{Ord}\,(q_2,q_1)},$$

where r *is a rational integer such that* $(2r-1)^2 \equiv -q_1 \pmod{q_2}$, *and* $\left(\frac{}{-}\right)_4$ *means the forth power residue symbol in* Q.

(ii) *If* $q_2 \equiv 3 \pmod 4$, *then* $\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_1}}\right)=1$ *iff*

$$\begin{bmatrix} -1 & -(q_1+1)/2 \\ 2 & 1 \end{bmatrix}^{\mathrm{Ord}\,(q_2, q_1)} \pmod{q_2} \in [SL_2(Z/q_2Z)]^2.$$

At last assume $\left(\frac{q_2}{q_1}\right)=1$, and let

$$\lambda(q_2)=A+B\frac{1+\sqrt{-q_1}}{2} \equiv 1 \quad (\mathrm{mod}\ \mathfrak{q}_1),$$

here A, B are integers for $p=q_2$ given in Lemma 6.2. q_2 splits completely in k: $(q_2)=\mathfrak{q}_2\mathfrak{q}_2^y$. Then by (7.1) and the Hasse product formula,

$$\left(\frac{\lambda(q_2),\ \hat{K}/k}{\mathfrak{q}_2}\right)\left(\frac{\lambda(q_2),\ \hat{K}/k}{\mathfrak{q}_2^y}\right)=1. \tag{7.13}$$

The factorization of $\lambda(q_2)$ in k is of the form

$$(\lambda(q_2))=\mathfrak{q}_2^{e_1}(\mathfrak{q}_2^y)^{e_2}, \qquad e_1+e_2=\frac{q_1-1}{2}\ \mathrm{Ord}\,(q_1, q_2). \tag{7.14}$$

Thus if $e_1=e_2$, then Ord (q_1, q_2) is even, which is a contradiction, because of $q_2^{\frac{q_1-1}{2}} \equiv 1 \pmod{q_1}$ and of $q_1 \equiv 3 \pmod 4$. Let $e_1 > e_2$, then

$$(\lambda(q_2))=(q_2)^{e_2}\mathfrak{q}_2^{e_1-e_2}.$$

By Lemma 6.2, (7.13) yields

$$\left(\frac{q_2,\ \hat{K}/k}{\mathfrak{q}_2}\right)^{-\frac{q_1-1}{2}\mathrm{Ord}\,(q_1, q_2)}=\left(y,\ \left(\frac{\lambda(q_2)^y,\ \hat{K}/k}{\mathfrak{q}_2}\right)\right). \tag{7.15}$$

Write

$$\lambda(q_2)=q_2^{e_2}\left(C+D\frac{1+\sqrt{-q_1}}{2}\right)$$

with some rational integers C, D. Notice that $q_2^{e_2}$ is the q_2-component of the G.C.D. of A and B. Then

$$\lambda(q_2)^y = q_2^{e_2}\left(C+D\frac{1-\sqrt{-q_1}}{2}\right),$$

and $C+D\dfrac{1-\sqrt{-q_1}}{2}$ is prime to $\mathfrak{q}_2$. Since $C+D\dfrac{1+\sqrt{-q_1}}{2}\equiv 0$ (mod $\mathfrak{q}_2$),

$$C+D\frac{1-\sqrt{-q_1}}{2}\equiv 2C+D \pmod{\mathfrak{q}_2},$$

and hence the right side of (7.15) becomes

$$\left(y, \left(\frac{q_2, \hat{K}/k}{\mathfrak{q}_2}\right)\right)^{e_2}\left(y, \left(\frac{2C+D, \hat{K}/k}{\mathfrak{q}_2}\right)\right)$$

by (7.1). Applying the Hasse product formula for K/Q to q_2, we have

$$\left(\frac{q_2, K/k}{\mathfrak{q}_2}\right)=\left(\frac{q_2, K/Q}{q_2}\right)=\tau_1^{-[1,2]},$$

and clearly

$$\left(\frac{2C+D, K/k}{\mathfrak{q}_2}\right)=\left(\frac{2C+D, K/Q}{q_2}\right)=\tau_2^{\operatorname{ind}(2C+D)},$$

here ind means the index mod q_2 with respect to the primitive root g_2. Therefore

$$\left(\frac{q_2, \hat{K}/k}{\mathfrak{q}_2}\right)^{-\frac{q_1-1}{2}\operatorname{Ord}(q_1,q_2)}=(x_1, x_2)^{\frac{q_1-1}{2}\operatorname{ind}(2C+D)}, \tag{7.16}$$

because of (7.7). Let T be the inertia field of $\mathfrak{q}_2$ in $\hat{K}$. It is easy to see that $K\cap T=K_1$, $[T:K_1]=2$ and hence $\hat{K}=KT$. Let $\mathfrak{P}'_{q_2}$ denote the restriction of $\mathfrak{P}_{q_2}$ to K_1. Then the degree of $\mathfrak{P}_{q_2}$ over K_1 is one and that of $\mathfrak{P}'_{q_2}$ over k Ord (q_1, q_2). Thus restricting the both sides of (7.16) to T, we obtain

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_2}}\right)=\left(\frac{T/K_1}{\mathfrak{P}'_{q_2}}\right)=(x'_1, x'_2)^{\operatorname{ind}(2C+D)}=\left(\frac{2C+D}{q_2}\right),$$

where x'_i is the restriction of x_i to T.

Let $e_1<e_2$, then we obtain from (7.13), (7.14)

$$\left(\frac{q_2,\ \hat{K}/k}{\mathfrak{q}_2^y}\right)^{-\frac{q_1-1}{2}\operatorname{Ord}(q_1,q_2)}=\left(y,\left(\frac{\lambda(q_2)^y,\ \hat{K}/k}{\mathfrak{q}_2^y}\right)\right)$$

and

$$(\lambda(q_2))=(q_2)^{e_1}(\mathfrak{q}_2^y)^{e_2-e_1},$$

respectively, and so forth. We get the same result. Summarizing these, we have

Theorem 7.9. *Let* $\left(\frac{q_2}{q_1}\right)=1$. *Then* $\mathfrak{P}_{q_2}$ *is unramified in* $\hat{K}$. *Let* A, B *be rational integers for* $p=q_2$ *described in Lemma* 6.2, q_2^e *be the* q_2-*component of the* G.C.D. *of* A *and* B, *and let* $A=q_2^eC$, $B=q_2^eD$. *Then*

$$\left(\frac{\hat{K}/K}{\mathfrak{P}_{q_2}}\right)=\left(\frac{2C+D}{q_2}\right).$$

We conclude this paper with a remark: As stated in Section 2, the decomposition laws in the cases $(\beta)=(\beta')$, $(\gamma)=(\gamma')$ can be deduced from the cases (B) and (C), respectively. By the theorem of Weber [49, p. 244, C], it is clear that the class number of $K_{-1}=Q(\zeta_{2^\nu}+\zeta_{2^\nu}^{-1})$ is odd. Hence some *odd* power of a rational prime can be expressed by the norm form from K_{-1} and in addition $[\hat{K}_{-11}: K_{-10}K_1]=(2^{\nu-2}, \phi(q_1^{\nu_1}))$. Thus the methods used in this paper will be applicable to get the decomposition laws in the case (δ). But it seems that the problem of finding the decomposition laws in the case (α) is still challengingly open.

Appendix

Here we test the examples of this paper by computer.

Let K/k be a Galois extension of algebraic number fields with group G, C be a conjugacy class in G, and let $\pi(x, C)$ be the number of prime ideals $\mathfrak{p}$ of k belonging to C such that $N_{k/Q}\mathfrak{p}\leq x$. Under the assumption of the general reciprocity law, Artin [1, Satz 4] proved that

$$(\,!\,)\qquad \pi(x, C)=\frac{|C|}{[K:k]}\operatorname{Li}(x)+O(x\cdot e^{-\alpha\sqrt{\log x}}),$$

where $\operatorname{Li}(x)$ is the logarithmic integral

$$\operatorname{Li}(x)=\int_2^x\frac{dt}{\log t},$$

and the number $\alpha > 0$ and the constant implied in the O-symbol depend only on the extension K/k (see also Suetuna [46, p. 235]).

(I) Let the situation be as in Example 3.9. Then the two sets of rational primes in (iii) belong to the conjugacy classes $\{1\}$ and $\{-1\}$ in $G(\hat{K}/Q)$, respectively. Therefore if we put

$$U(x) = |\{p \equiv 1 \pmod{12} \mid p = a^2 + b^2 \leqq x,\ 6 \mid b\}|,$$
$$V(x) = |\{p \equiv 1 \pmod{12} \mid p = a^2 + b^2 \leqq x,\ 6 \nmid b\}|,$$

then it follows from (!) that

$$U(x) \sim V(x) \sim \mathrm{Li}\,(x)/8 \qquad \text{as } x \to \infty.$$

The following table gives the values of $U(x)$, $V(x)$, $\mathrm{Li}\,(x)/8$, $\mathrm{Li}\,(x)/8U(x)$ and $\mathrm{Li}\,(x)/8V(x)$ for $x = 10000\,n$, $1 \leqq n \leqq 100$.

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/8$	$\mathrm{Li}(x)/8U(x)$	$\mathrm{Li}(x)/8V(x)$
10000	147	153	155.6	1.0588	1.0172
20000	277	278	285.9	1.0323	1.0286
30000	385	407	409.5	1.0636	1.0061
40000	507	526	529.0	1.0434	1.0057
50000	628	636	645.7	1.0282	1.0152
60000	744	757	760.2	1.0218	1.0043
70000	855	858	873.0	1.0211	1.0175
80000	966	967	984.4	1.0190	1.0180
90000	1067	1089	1094.5	1.0258	1.0051
100000	1186	1188	1203.6	1.0148	1.0131
110000	1297	1291	1311.7	1.0114	1.0161
120000	1387	1406	1419.0	1.0231	1.0092
130000	1493	1512	1525.5	1.0218	1.0089
140000	1604	1611	1631.3	1.0170	1.0126
150000	1705	1726	1736.5	1.0185	1.0061
160000	1816	1823	1841.1	1.0138	1.0099
170000	1914	1930	1945.1	1.0163	1.0079
180000	2022	2032	2048.7	1.0132	1.0082
190000	2125	2133	2151.8	1.0126	1.0088
200000	2229	2243	2254.4	1.0114	1.0051
210000	2328	2345	2356.6	1.0123	1.0049
220000	2436	2438	2458.4	1.0092	1.0084
230000	2527	2550	2559.8	1.0130	1.0039
240000	2623	2641	2660.9	1.0144	1.0075
250000	2729	2741	2761.6	1.0120	1.0075
260000	2826	2845	2862.0	1.0128	1.0060
270000	2924	2951	2962.1	1.0130	1.0038

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/8$	$\mathrm{Li}(x)/8U(x)$	$\mathrm{Li}(x)/8V(x)$
280000	3021	3047	3061.9	1.0136	1.0049
290000	3121	3146	3161.5	1.0130	1.0049
300000	3219	3248	3260.7	1.0130	1.0039
310000	3307	3363	3359.7	1.0159	0.9990
320000	3406	3458	3458.4	1.0154	1.0001
330000	3515	3553	3556.9	1.0119	1.0011
340000	3605	3654	3655.2	1.0139	1.0003
350000	3700	3748	3753.2	1.0144	1.0014
360000	3793	3852	3851.0	1.0153	0.9997
370000	3900	3945	3948.6	1.0125	1.0009
380000	3992	4047	4046.0	1.0135	0.9998
390000	4076	4155	4143.2	1.0165	0.9972
400000	4182	4237	4240.2	1.0139	1.0008
410000	4279	4329	4337.0	1.0136	1.0019
420000	4369	4427	4433.6	1.0148	1.0015
430000	4483	4512	4530.1	1.0105	1.0040
440000	4583	4614	4626.4	1.0095	1.0027
450000	4678	4708	4722.5	1.0095	1.0031
460000	4777	4798	4818.4	1.0087	1.0043
470000	4875	4900	4914.2	1.0080	1.0029
480000	4964	4998	5009.8	1.0092	1.0024
490000	5056	5089	5105.3	1.0098	1.0032
500000	5142	5187	5200.7	1.0114	1.0026
510000	5241	5276	5295.8	1.0105	1.0038
520000	5349	5369	5390.9	1.0078	1.0041
530000	5446	5473	5485.8	1.0073	1.0023
540000	5537	5571	5580.6	1.0079	1.0017
550000	5630	5654	5675.2	1.0080	1.0038
560000	5714	5751	5769.7	1.0098	1.0033
570000	5793	5858	5864.1	1.0123	1.0010
580000	5889	5951	5958.3	1.0118	1.0012
590000	5985	6058	6052.5	1.0113	0.9991
600000	6077	6146	6146.5	1.0114	1.0001
610000	6184	6236	6240.4	1.0091	1.0007
620000	6277	6326	6334.1	1.0091	1.0013
630000	6366	6421	6427.8	1.0097	1.0011
640000	6451	6514	6521.4	1.0109	1.0011
650000	6538	6612	6614.8	1.0118	1.0004
660000	6629	6706	6708.1	1.0119	1.0003
670000	6727	6802	6801.4	1.0111	0.9999
680000	6818	6882	6894.5	1.0112	1.0018
690000	6915	6979	6987.5	1.0105	1.0012
700000	7014	7068	7080.5	1.0095	1.0018
710000	7104	7168	7173.3	1.0098	1.0007
720000	7194	7252	7266.0	1.0100	1.0019
730000	7276	7351	7358.6	1.0114	1.0010

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/8$	$\mathrm{Li}(x)/8U(x)$	$\mathrm{Li}(x)/8V(x)$
740000	7361	7450	7451.2	1.0123	1.0002
750000	7450	7542	7543.6	1.0126	1.0002
760000	7544	7615	7636.0	1.0122	1.0028
770000	7634	7702	7728.3	1.0124	1.0034
780000	7725	7792	7820.4	1.0124	1.0037
790000	7817	7884	7912.5	1.0122	1.0036
800000	7907	7984	8004.5	1.0123	1.0026
810000	8005	8072	8096.5	1.0114	1.0030
820000	8088	8167	8188.3	1.0124	1.0026
830000	8196	8270	8280.0	1.0103	1.0012
840000	8296	8346	8371.7	1.0091	1.0031
850000	8387	8443	8463.3	1.0091	1.0024
860000	8472	8549	8554.8	1.0098	1.0007
870000	8574	8636	8646.3	1.0084	1.0012
880000	8663	8721	8737.6	1.0086	1.0019
890000	8742	8812	8828.9	1.0099	1.0019
900000	8827	8900	8920.1	1.0106	1.0023
910000	8929	9004	9011.3	1.0092	1.0008
920000	9011	9085	9102.3	1.0101	1.0019
930000	9111	9181	9193.3	1.0090	1.0013
940000	9197	9269	9284.2	1.0095	1.0016
950000	9295	9348	9375.1	1.0086	1.0029
960000	9397	9438	9465.9	1.0073	1.0030
970000	9481	9530	9556.6	1.0080	1.0028
980000	9572	9622	9647.2	1.0079	1.0026
990000	9664	9715	9737.8	1.0076	1.0024
1E+06	9760	9804	9828.3	1.0070	1.0025

(II) Let the situation be as in Example 3.10, and let

$$U(x)=|\{p\equiv 1 \pmod{28} \mid p=a^2+b^2\leqq x,\ 7\mid ab\}|,$$

$$V(x)=|\{p\equiv 1 \pmod{28} \mid p=a^2+b^2\leqq x,\ 7\nmid ab\}|.$$

Then by (!), we have

$$U(x)\sim V(x)\sim \mathrm{Li}\,(x)/24 \qquad \text{as } x\to\infty.$$

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/24$	$\mathrm{Li}(x)/24U(x)$	$\mathrm{Li}(x)/24V(x)$
10000	50	53	51.9	1.0376	0.9788
20000	95	93	95.3	1.0033	1.0249
30000	126	134	136.5	1.0833	1.0186
40000	167	175	176.3	1.0559	1.0076
50000	205	213	215.2	1.0499	1.0105
60000	244	251	253.4	1.0386	1.0096

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/24$	$\mathrm{Li}(x)/24U(x)$	$\mathrm{Li}(x)/24V(x)$
70000	281	285	291.0	1.0356	1.0211
80000	322	315	328.1	1.0190	1.0417
90000	354	355	364.8	1.0306	1.0277
100000	390	397	401.2	1.0287	1.0106
110000	428	430	437.2	1.0216	1.0168
120000	461	466	473.0	1.0260	1.0150
130000	500	498	508.5	1.0170	1.0211
140000	535	540	543.8	1.0164	1.0070
150000	570	575	578.8	1.0155	1.0067
160000	606	605	613.7	1.0127	1.0144
170000	639	639	648.4	1.0147	1.0147
180000	671	674	682.9	1.0177	1.0132
190000	705	712	717.3	1.0174	1.0074
200000	736	747	751.5	1.0210	1.0060
210000	769	781	785.5	1.0215	1.0058
220000	801	816	819.5	1.0231	1.0042
230000	842	849	853.3	1.0134	1.0050
240000	877	888	887.0	1.0114	0.9988
250000	914	921	920.5	1.0072	0.9995
260000	943	955	954.0	1.0117	0.9990
270000	977	982	987.4	1.0106	1.0055
280000	1001	1016	1020.7	1.0196	1.0046
290000	1036	1052	1053.8	1.0172	1.0017
300000	1069	1085	1086.9	1.0168	1.0018
310000	1104	1114	1119.9	1.0144	1.0053
320000	1140	1148	1152.8	1.0112	1.0042
330000	1174	1180	1185.6	1.0099	1.0048
340000	1203	1210	1218.4	1.0128	1.0069
350000	1237	1248	1251.1	1.0114	1.0025
360000	1267	1280	1283.7	1.0132	1.0029
370000	1299	1306	1316.2	1.0132	1.0078
380000	1335	1344	1348.7	1.0102	1.0035
390000	1364	1380	1381.1	1.0125	1.0008
400000	1391	1416	1413.4	1.0161	0.9982
410000	1424	1448	1445.7	1.0152	0.9984
420000	1459	1475	1477.9	1.0129	1.0020
430000	1493	1507	1510.0	1.0114	1.0020
440000	1521	1539	1542.1	1.0139	1.0020
450000	1550	1570	1574.2	1.0156	1.0027
460000	1579	1611	1606.1	1.0172	0.9970
470000	1618	1641	1638.1	1.0124	0.9982
480000	1648	1674	1670.0	1.0133	0.9976
490000	1679	1705	1701.8	1.0136	0.9981
500000	1714	1731	1733.6	1.0114	1.0015
510000	1745	1766	1765.3	1.0116	0.9996
520000	1779	1805	1797.0	1.0101	0.9955

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/24$	$\mathrm{Li}(x)/24U(x)$	$\mathrm{Li}(x)/24V(x)$
530000	1816	1827	1828.6	1.0069	1.0009
540000	1844	1861	1860.2	1.0088	0.9996
550000	1872	1891	1891.7	1.0105	1.0004
560000	1905	1921	1923.2	1.0096	1.0012
570000	1935	1952	1954.7	1.0102	1.0014
580000	1972	1982	1986.1	1.0072	1.0021
590000	2015	2007	2017.5	1.0012	1.0052
600000	2048	2033	2048.8	1.0004	1.0078
610000	2079	2073	2080.1	1.0005	1.0034
620000	2114	2104	2111.4	0.9988	1.0035
630000	2141	2136	2142.6	1.0008	1.0031
640000	2169	2170	2173.8	1.0022	1.0017
650000	2218	2193	2204.9	0.9941	1.0054
660000	2251	2224	2236.1	0.9934	1.0054
670000	2279	2259	2267.1	0.9948	1.0036
680000	2304	2292	2298.2	0.9975	1.0027
690000	2332	2323	2329.2	0.9988	1.0027
700000	2357	2351	2360.2	1.0013	1.0039
710000	2383	2382	2391.1	1.0034	1.0038
720000	2407	2418	2422.0	1.0062	1.0017
730000	2442	2447	2452.9	1.0045	1.0024
740000	2473	2482	2483.7	1.0043	1.0007
750000	2510	2506	2514.5	1.0018	1.0034
760000	2533	2541	2545.3	1.0049	1.0017
770000	2569	2566	2576.1	1.0028	1.0039
780000	2596	2606	2606.8	1.0042	1.0003
790000	2617	2642	2637.5	1.0078	0.9983
800000	2647	2663	2668.2	1.0080	1.0019
810000	2675	2691	2698.8	1.0089	1.0029
820000	2710	2721	2729.4	1.0072	1.0031
830000	2736	2757	2760.0	1.0088	1.0011
840000	2769	2788	2790.6	1.0078	1.0009
850000	2801	2820	2821.1	1.0072	1.0004
860000	2833	2849	2851.6	1.0066	1.0009
870000	2861	2876	2882.1	1.0074	1.0021
880000	2885	2908	2912.5	1.0096	1.0016
890000	2918	2934	2943.0	1.0086	1.0031
900000	2947	2969	2973.4	1.0090	1.0015
910000	2988	3002	3003.8	1.0053	1.0006
920000	3013	3028	3034.1	1.0070	1.0020
930000	3049	3055	3064.4	1.0051	1.0031
940000	3075	3089	3094.7	1.0064	1.0019
950000	3103	3120	3125.0	1.0071	1.0016
960000	3133	3151	3155.3	1.0071	1.0014
970000	3170	3175	3185.5	1.0049	1.0033
980000	3203	3206	3215.7	1.0040	1.0030

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/24$	$\mathrm{Li}(x)/24U(x)$	$\mathrm{Li}(x)/24V(x)$
990000	3230	3230	3245.9	1.0049	1.0049
1E+06	3247	3262	3276.1	1.0090	1.0043

(III) Let the situation be as in Example 5.8, and let

$$U(x)=|\{p\equiv 1 \pmod{56} \mid p=a^2+2b^2\leqq x,\ 7\mid ab\}|,$$

$$V(x)=|\{p\equiv 1 \pmod{56} \mid p=a^2+2b^2\leqq x,\ 7\nmid ab\}|.$$

Then by (!),

$$U(x)\sim V(x)\sim \mathrm{Li}(x)/48 \qquad \text{as } x\to\infty.$$

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/48$	$\mathrm{Li}(x)/48U(x)$	$\mathrm{Li}(x)/48V(x)$
10000	23	27	25.9	1.1278	0.9607
20000	47	46	47.7	1.0140	1.0360
30000	63	68	68.2	1.0833	1.0036
40000	79	86	88.2	1.1160	1.0252
50000	97	102	107.6	1.1094	1.0550
60000	117	121	126.7	1.0829	1.0471
70000	137	139	145.5	1.0621	1.0468
80000	154	156	164.1	1.0654	1.0517
90000	172	174	182.4	1.0606	1.0484
100000	192	193	200.6	1.0448	1.0394
110000	204	212	218.6	1.0717	1.0312
120000	220	227	236.5	1.0750	1.0418
130000	238	243	254.3	1.0683	1.0463
140000	257	266	271.9	1.0579	1.0221
150000	274	285	289.4	1.0563	1.0155
160000	291	299	306.8	1.0545	1.0263
170000	310	310	324.2	1.0458	1.0458
180000	331	323	341.4	1.0316	1.0571
190000	344	343	358.6	1.0425	1.0456
200000	362	362	375.7	1.0379	1.0379
210000	379	381	392.8	1.0363	1.0309
220000	400	397	409.7	1.0243	1.0321
230000	417	418	426.6	1.0231	1.0207
240000	437	435	443.5	1.0148	1.0195
250000	454	453	460.3	1.0138	1.0161
260000	469	471	477.0	1.0171	1.0128
270000	483	490	493.7	1.0221	1.0075
280000	499	502	510.3	1.0227	1.0166
290000	517	518	526.9	1.0192	1.0172
300000	528	539	543.5	1.0293	1.0083
310000	542	555	559.9	1.0331	1.0089
320000	558	573	576.4	1.0330	1.0059

x	$U(x)$	$V(x)$	$\mathrm{Li}(x)/48$	$\mathrm{Li}(x)/48U(x)$	$\mathrm{Li}(x)/48V(x)$
330000	576	592	592. 8	1. 0292	1. 0014
340000	590	605	609. 2	1. 0325	1. 0069
350000	610	621	625. 5	1. 0255	1. 0073
360000	631	631	641. 8	1. 0172	1. 0172
370000	642	646	658. 1	1. 0251	1. 0187
380000	660	663	674. 3	1. 0217	1. 0171
390000	674	680	690. 5	1. 0245	1. 0155
400000	688	699	706. 7	1. 0272	1. 0110
410000	709	712	722. 8	1. 0195	1. 0152
420000	723	726	738. 9	1. 0221	1. 0178
430000	738	741	755. 0	1. 0231	1. 0189
440000	753	755	771. 1	1. 0240	1. 0213
450000	764	778	787. 1	1. 0302	1. 0117
460000	781	793	803. 1	1. 0283	1. 0127
470000	798	811	819. 0	1. 0264	1. 0099
480000	814	825	835. 0	1. 0258	1. 0121
490000	832	837	850. 9	1. 0227	1. 0166
500000	846	854	866. 8	1. 0246	1. 0150
510000	861	870	882. 6	1. 0251	1. 0145
520000	879	892	898. 5	1. 0222	1. 0073
530000	896	906	914. 3	1. 0204	1. 0092
540000	918	915	930. 1	1. 0132	1. 0165
550000	932	929	945. 9	1. 0149	1. 0182
560000	947	944	961. 6	1. 0154	1. 0187
570000	959	965	977. 3	1. 0191	1. 0128
580000	976	978	993. 1	1. 0175	1. 0154
590000	993	996	1008. 7	1. 0159	1. 0128
600000	1010	1005	1024. 4	1. 0143	1. 0193
610000	1027	1019	1040. 1	1. 0127	1. 0207
620000	1048	1035	1055. 7	1. 0073	1. 0200
630000	1063	1052	1071. 3	1. 0078	1. 0184
640000	1077	1065	1086. 9	1. 0092	1. 0206
650000	1094	1082	1102. 5	1. 0077	1. 0189
660000	1105	1102	1118. 0	1. 0118	1. 0145
670000	1124	1115	1133. 6	1. 0085	1. 0167
680000	1139	1128	1149. 1	1. 0089	1. 0187
690000	1154	1147	1164. 6	1. 0092	1. 0153
700000	1169	1156	1180. 1	1. 0095	1. 0208
710000	1184	1173	1195. 6	1. 0098	1. 0192
720000	1197	1192	1211. 0	1. 0117	1. 0159
730000	1219	1198	1226. 4	1. 0061	1. 0237
740000	1238	1216	1241. 9	1. 0031	1. 0213
750000	1255	1231	1257. 3	1. 0018	1. 0213
760000	1269	1247	1272. 7	1. 0029	1. 0206
770000	1288	1259	1288. 0	1. 0000	1. 0231
780000	1302	1279	1303. 4	1. 0011	1. 0191

x	$U(x)$	$V(x)$	Li$(x)/48$	Li$(x)/48U(x)$	Li$(x)/48V(x)$
790000	1315	1297	1318.8	1.0029	1.0168
800000	1327	1306	1334.1	1.0053	1.0215
810000	1340	1322	1349.4	1.0070	1.0207
820000	1357	1338	1364.7	1.0057	1.0200
830000	1371	1353	1380.0	1.0066	1.0200
840000	1393	1364	1395.3	1.0016	1.0229
850000	1410	1380	1410.6	1.0004	1.0221
860000	1428	1393	1425.8	0.9985	1.0236
870000	1443	1406	1441.0	0.9986	1.0249
880000	1454	1421	1456.3	1.0016	1.0248
890000	1467	1434	1471.5	1.0031	1.0261
900000	1481	1452	1486.7	1.0038	1.0239
910000	1502	1470	1501.9	0.9999	1.0217
920000	1514	1488	1517.1	1.0020	1.0195
930000	1532	1505	1532.2	1.0001	1.0181
940000	1545	1520	1547.4	1.0015	1.0180
950000	1561	1535	1562.5	1.0010	1.0179
960000	1575	1549	1577.6	1.0017	1.0185
970000	1590	1567	1592.8	1.0017	1.0164
980000	1606	1587	1607.9	1.0012	1.0132
990000	1623	1595	1623.0	1.0000	1.0175
1E+06	1636	1608	1638.1	1.0013	1.0187

References

[0] Y. Akagawa, A tripling on the algebraic number field, Osaka J. Math., **23** (1986), 151–179.

[1] E. Artin, Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg, **3** (1924), 89–108.

[2] M. Bauer, Zur Theorie der algebraischen Zahlkörper, Math. Ann., **77** (1916), 353–356.

[3] K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. Reine Angew. Math., **235** (1969), 175–184.

[4] L. E. Dickson, Cyclotomy, higher congruences, and Waring's problem, Amer. J. Math., **57** (1935), 391–424.

[5] ——, Cyclotomy and trinomial congruences, Trans. Amer. Math. Soc., **37** (1935), 363–380.

[6] A. Fröhlich, On fields of class two, Proc. London Math. Soc., (3) **4** (1954), 235–256.

[7] ——, The restricted biquadratic residue symbol, Proc. London Math. Soc., (3) **9** (1959), 189–207.

[8] ——, The rational characterization of certain sets of relatively Abelian extensions, Philosophical Transactions Royal Soc. London, (A) **251** (1959), 385–425.

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

[10] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, **10** (1958), 46–54.

[11] ——, Über die zentrale Klassenzahl eines Relativ-Galoisschen Zahlkörpers, J. Number Theory, **3** (1971), 318–322.

[12] ——, Note on class number factors and prime decompositions, Nagoya Math. J., **66** (1977), 167–182.
[13] ——, 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.
[14] ——, A prime decomposition symbol and integral quadratic forms, Japan. J. Math., **7** (1981), 213–216.
[15] ——, A norm residue map for central extensions of an algebraic number field, Nagoya Math. J., **93** (1984), 61–69.
[16] ——, Gauss's ternary form reduction and its application to a prime decomposition symbol, Nagoya Math. J., **98** (1985), 77–86.
[17] —— and P. Kaplan, On quadratic and quartic characters of quadratic units, Sci. Rep. Kanazawa Univ., **26** (1981), 27–30.
[18] C. F. Gauss, Theoria residuorum biquadraticorum, Werke, vol. 2.
[19] S. Gurak, On the representation theory for full decomposable forms, J. Number Theory, **13** (1981), 421–442.
[20] ——, On the rational equivalence of full decomposable forms, J. Number Theory, **14** (1982), 251–259.
[21] H. Hasse, Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols, J. Reine Angew. Math., **162** (1930), 134–144.
[22] ——, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II. Reziprozitätsgesetze, Jber. Deutsch. Math.-Verein. Ergänzungsband **6** (1930), 204 S.
[23] ——, Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelsher Zahlkörper, J. Fac. Sci. Tokyo Imp. Univ., **2** (1934), 477–498.
[24] F.-P. Heider, Strahlknoten und Geschlechterkörper mod $\mathfrak{m}$, J. Reine Angew. Math., **320** (1980), 52–67.
[25] S. Iyanaga, Zur Theorie der Geschlechtermoduln, J. Reine Angew. Math., **171** (1934), 12–18.
[26] C. G. J. Jacobi, Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie, J. Reine Angew. Math., **30** (1846), 166–182; Gesammelte Werke, vol. 6 (1891), 254–274.
[27] E. Jacobsthal, Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier Quadrate, J. Reine Angew. Math., **132** (1907), 238–245.
[28] P. Kaplan and K. S. Williams, An Artin character and representations of primes by binary quadratic forms, Manuscripta Math., **33** (1981), 339–356.
[29] F. Halter-Koch, P. Kaplan and K. S. Williams, An Artin character and representations of primes by binary quadratic forms II, Manuscripta Math., **37** (1982), 357–381.
[30] L. Kronecker, Zur Theorie der Abelschen Gleichungen, J. Reine Angew. Math., **93** (1882), 338–364.
[31] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitäsgesetzen, J. Reine Angew. Math., **44** (1852), 93–146.
[32] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nichtabelschen galoisschen Körpern, J. Math. Soc. Japan, **3** (1951), 148–156.
[33] E. Lehmer, Criteria for cubic and quartic residuacity, Mathematika, **5** (1958), 20–29.
[34] H. H. Mitchell, On the generalized Jacobi-Kummer cyclotomic function, Trans. Amer. Math. Soc., **17** (1916), 165–177.
[35] J. C. Parnami, M. K. Agrawal and A. R. Rajwade, A congruence relation between the coefficients of the Jacobi sum, Indian J. pure appl. Math., **12** (1981), 804–806.
[36] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I, J. Reine Angew. Math., **180**

(1939), 1–43.
[37] A. Scholz, Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen. II, J. Reine Angew. Math., **182** (1940), 217–234.
[38] L. von Schrutka, Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n+1$ in ein einfaches und ein dreifaches Quadrat, J. Reine Angew. Math., **140** (1911), 252–265.
[39] K. Schwering, Zur Theorie der arithmetischen Functionen, welche von Jacobi $\psi(\alpha)$ genannt werden, J. Reine Angew. Math., **93** (1882), 334–337.
[40] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.
[41] ——, A remark concerning the 2-adic number field, Nagoya Math. J., **71** (1978), 87–90.
[42] ——, On Galois groups of class two extensions over the rational number field, Nagoya Math. J., **75** (1979), 121–131.
[43] ——, On the central ideal class group of cyclotomic fields, Nagoya Math. J., **75** (1979), 133–143.
[44] ——, On the prime ideal decomposition in certain class two extensions (Japanese), Sûrikaisekikenkyûsho Kôkyûroku, **440** (1981), 131–144 (published by the Research Institute for Mathematical Sciences. Kyoto University).
[45] M. Stern, Eine Bemerkung zur Zahlentheorie, J. Reine Angew. Math., **32** (1846), 89–90.
[46] Z. Suetuna, Analytical Theory of Numbers (Japanese), Iwanami Shoten, 1950.
[47] H. Suzuki, A tripling symbol for central extensions of algebraic number fields, this book, 9–23.
[48] H. S. Vandiver, On Kummer's memoir of 1857 concerning Fermat's last theorem, Bull. Amer. Math. Soc., **28** (1922), 400–407.
[49] H. Weber, Theorie der Abel'schen Zahlkörper, Acta Math., **8** (1886), 193–263.
[50] A. L. Whiteman, Theorems analogous to Jacobsthal's theorem, Duke Math. J., **16** (1949), 619–626.
[51] ——, Cyclotomy and Jacobsthal sums, Amer. J. Math., **74** (1952), 89–99.
[52] ——, Theorems on Brewer and Jacobsthal sums. I, Proc. Sympos. Pure Math., vol. VIII, 44–55. Amer. Math. Soc., Providence, R. I., 1965.
[53] P. Bachmann, Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie, Leipzig, 1872.

Mathematics Department
Toyama Medical and Pharmaceutical University
Sugitani, Toyama 930–01
Japan