CONSTRUCTION OF CLASS FIELDS OVER IMAGINARY BIQUADRATIC FIELDS

JA KYUNG KOO AND DONG SUNG YOON

Abstract

Let $K$ be an imaginary biquadratic field, $K_1$, $K_2$ be its imaginary quadratic subfields and $K_3$ be its real quadratic subfield. For integers $N > 0$, $\mu \geq 0$ and an odd prime $p$ with $(N,p) = 1$, let $K_{(Np^\mu)}$ and $(K_i)_{(Np^\mu)}$ for $i = 1, 2, 3$ be the ray class fields of $K$ and $K_i$, respectively, modulo $Np^\mu$. We first present certain class fields $\widetilde{K}_{N,p,\mu}^{1,2}$ of $K$, in the sense of Hilbert, which are generated by ray class invariants of $(K_i)_{(Np^\mu+1)}$ for $i = 1, 2$ over $K_{(Np^\mu)}$ and find the exact extension degree $[K_{(Np^\mu+1)} : K_{N,p,\mu}]$. And we shall further construct a primitive generator of the composite field $K_{(Np^\mu)}(K_3)_{(Np^\mu+1)}$ over $K_{(Np^\mu)}$ by means of norms of the above ray class invariants, which is a real algebraic integer. Using this value we also generate a primitive generator of $(K_3)_{(p)}$ over the Hilbert class field of the real quadratic field $K_3$, and further find its normal basis.

Contents

1 Introduction 2

2 Siegel modular forms 4

3 Shimura’s reciprocity law 6

4 Siegel functions 9

2010 Mathematics Subject Classification. 11F03, 11F46, 11G15, 11R37.
Key words and phrases. class field theory, complex multiplication, Shimura’s reciprocity law, Siegel modular forms

This work was supported by the National Research Foundation of Korea grant funded by MISP (2013042157).
1 Introduction

In 1900 Hilbert asked at the Paris ICM, as his 12-th problem, that what kind of analytic functions and algebraic numbers are necessary to construct all abelian extensions of given number fields. For any number field $F$ and a modulus $\mathfrak{m}$, it is well known that there is a unique maximal abelian extension of $F$ unramified outside $\mathfrak{m}$ with certain ramification condition ([38] or [7, Theorem 8.6]), which we call the ray class field of $F$ modulo $\mathfrak{m}$. Since any abelian extension of $F$ is contained in some ray class field modulo $\mathfrak{m}$ by class field theory, in order to approach the problem we first need to construct ray class fields of given number fields as Ramachandra did in [26] over imaginary quadratic fields.

Historically, over imaginary quadratic fields, after Hasse ([10]) one can now construct it by using the theory of complex multiplication of elliptic curves together with the singular values of modular functions and elliptic functions ([19, Chapter 10] or [33]). However, for any other number fields we know relatively little until now. For example, over cyclotomic field see [15], [27] (also [22]), [29], and over biquadratic fields we refer to [1], [2], [3], [4], [36] and [41].

In this paper we will concentrate on the case of imaginary biquadratic fields $K$. There are two imaginary quadratic subfields $K_1$, $K_2$ and one real quadratic subfield $K_3$ in $K$. For integers $N > 0$, $\mu \geq 0$ and an odd prime $p$ with $(N, p) = 1$, we denote by $K_{(Np^\mu)}$ and $(K_i)_{(Np^\mu)}$ for $i = 1, 2, 3$ the ray class fields of $K$ and $K_i$ modulo $Np^\mu$, respectively. In Section 3, we apply Shimura’s reciprocity law on the composite field of imaginary quadratic fields and put emphasis on the necessity of using modular units to construct class fields over $K$ as Hilbert proposed. In Section 4 we shall introduce the Siegel functions as modular units, and explain some arithmetic properties of these functions. On the other hand, Jung-Koo-Shin ([12, Theorem 3.5]) constructed relatively simple ray class invariants over imaginary quadratic fields by means of the singular values of certain Siegel functions. Using this idea we define in Section 6 and 7 certain class field $\tilde{K}_{N, p, \mu}$ of $K$ which is generated by ray class invariants of $(K_i)_{(Np^{\mu+1})}$ for $i = 1, 2$ over $K_{(Np^\mu)}$, and find the
exact extension degree of $K_{(Np^\mu+1)}$ over $\overline{K_{1,2}^{N,p,\mu}}$ (Theorem 6.7 and 7.4). Furthermore, we provide a necessary and sufficient condition for the field $K_{1,2}^{N,p,\mu}$ to contain $(K_3)_{(Np^\mu+1)}$ and construct a primitive generator of $K_{(Np^\mu)}(K_3)_{(Np^\mu+1)}$ over $K_{(Np^\mu)}$ by means of norm of the above ray class invariants, which is a real algebraic integer (Theorem 6.12 and 7.8). And, in Section 8 using such primitive generator of $K_{(Np^\mu)}(K_3)_{(p)}$ over $K_{(Np^\mu)}$ we shall construct $(K_3)_{(p)}$ over the Hilbert class field $(K_3)_{(p)}$ as well as $(K_3)_{(p\infty)}$ over $(K_3)_{(p)}$, where $\infty$ stands for the modulus of the real quadratic field $K_3$ including all real infinite primes and $(K_3)_{(p\infty)}$ is the ray class field of $K_3$ modulo $p\mathcal{O}_{K_3} \cdot \infty$ (Theorem 8.4 and Corollary 8.6).

On the other hand, when $L/F$ is a finite Galois extension, we know by the normal basis theorem (10) that there exists an element $x \in L$ whose Galois conjugates form a basis of $L$ over $F$ as a vector space. But, as far as we understand, not much seems to be known so far how to construct it. For instance, Okada (25) constructed in 1980 a normal basis of the maximal real subfield of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$ by extending Chowla’s work (3) with cotangent function. After Okada, Taylor (39) and Schertz (28) established Galois module structures of ring of integers of certain abelian extensions over an imaginary quadratic field and also found normal bases by making use of special values of modular functions. And, Komatsu (15) further considered certain abelian extensions $L$ and $F$ of the cyclotomic field $\mathbb{Q}(e^{2\pi i/5})$ and constructed a normal basis of $L$ over $F$ in terms of special values of Siegel modular functions. Unlike their works, however, Koo-Shin recently found a new algorithm in (16) to generate a normal basis of abelian extensions of number fields. In Section 9 by making use of this idea we shall present a normal basis of $(K_3)_{(p)}$ over $(K_3)_{(1)}$ and give an explicit example (Theorem 9.4 and Example 9.5).

Notation 1.1. For $z \in \mathbb{C}$, we denote by $\overline{z}$ the complex conjugate of $z$ and by $\text{Im}(z)$ the imaginary part of $z$, and put $e(z) = e^{2\pi iz}$. If $R$ is a ring with identity and $r, s \in \mathbb{Z}_{>0}$, $M_{r \times s}(R)$ indicates the ring of all $r \times s$ matrices with entries in $R$. In particular, we set $M_r(R) = M_{r \times r}(R)$. The identity matrix of $M_r(R)$ is written by $\mathbf{1}_r$ and the transpose of a matrix $\alpha$ is written as $^t\alpha$. And, $R^\times$ means the group of all invertible elements of $R$. If $G$ is a group and $g_1, g_2, \ldots, g_r$ are elements of $G$, let $\langle g_1, g_2, \ldots, g_r \rangle$ be the subgroup of $G$ generated by $g_1, g_2, \ldots, g_r$. For a number field $F$ and a positive integer $N$, let $\mathcal{O}_F$ be the ring of integers of $F$. If $a \in \mathcal{O}_F$ we denote by $(a)$ the principal ideal of $F$ generated by $a$. For a finite extension $L$ of $F$, let $[L : F]$ be the extension degree of $L$ over $F$. When $L/F$ is abelian, we mean by $\left( \frac{L/F}{-} \right)$ the Artin map of $L/F$. Further, we let $\zeta_N = e^{2\pi i/N}$ be a primitive $N$th root of unity.
2 Siegel modular forms

In this section we shall briefly recall Siegel modular forms and explain the action of the group $G_{A+}$ on the Siegel modular functions whose Fourier coefficients lie in some cyclotomic fields.

Let $n$ be a positive integer and

$$J = J_n = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix}.$$  

For a commutative ring $R$ with unity, we let

$$(2.1) \quad GSp_{2n}(R) = \{ \alpha \in GL_{2n}(R) \mid ^t\alpha J \alpha = \nu(\alpha)J \text{ with } \nu(\alpha) \in R^\times \}.$$  

Considering $\nu$ as a homomorphism $GSp_{2n}(R) \rightarrow R^\times$ we denote its kernel by $Sp_{2n}(R)$, namely

We set $G_{\mathbb{Q}} = GSp_{2n}(\mathbb{Q})$ and $G_{\mathbb{Q}+} = \{ \alpha \in G_{\mathbb{Q}} \mid \nu(\alpha) > 0 \}$. Let

$$\mathbb{H}_n = \{ z \in M_n(\mathbb{C}) \mid ^t z = z, \ \text{Im}(z) > 0 \}$$

be the Siegel upper half-space of degree $n$. Here, for a hermitian matrix $\xi$ we write $\xi > 0$ to mean that $\xi$ is positive definite. An element $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of $G_{\mathbb{Q}+}$ acts on $\mathbb{H}_n$ by

$$\alpha(z) = (Az + B)(Cz + D)^{-1},$$

where $A, B, C, D \in M_n(\mathbb{Q}).$

For every positive integer $N$, let

$$\Gamma(N) = \{ \gamma \in Sp_{2n}(\mathbb{Z}) \mid \gamma \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z})} \}.$$  

For an integer $m$, a holomorphic function $f : \mathbb{H}_n \rightarrow \mathbb{C}$ is called a (classical) Siegel modular form of degree $n$, weight $m$ and level $N$ if

$$(2.2) \quad f(\gamma(z)) = \det(Cz + D)^m f(z)$$

for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma(N)$ and $z \in \mathbb{H}_n$, plus the requirement when $n = 1$ that $f$ is holomorphic at every cusp. A Siegel modular form $f$ of degree $n$ and level $N$ has a Fourier expansion of the form

$$f(z) = \sum_\xi A(\xi)e(tr(\xi z)/N)$$
with \( A(\xi) \in \mathbb{C} \), where \( \xi \) runs over all positive semi-definite half-integral symmetric matrices of degree \( n \) \([14, \text{§4 Theorem 1}]\). Here, a symmetric matrix \( \xi \in GL_n(\mathbb{Q}) \) is called \textit{half-integral} if \( 2\xi \) is an integral matrix whose diagonal entries are even. For a subfield \( F \) of \( \mathbb{C} \), let \( \mathcal{M}_m^{n}(\Gamma(N), F) \) be the vector space of all Siegel modular forms \( f \) of degree \( n \), weight \( m \) and level \( N \) whose Fourier coefficients \( A(\xi) \) belong to \( F \) and let 
\[
\mathcal{M}_m^{n}(F) = \bigcup_{N=1}^{\infty} \mathcal{M}_m^{n}(\Gamma(N), F).
\]
We denote by \( \mathfrak{A}_m^n(F) \) the space of all meromorphic functions of the form \( g/h \) with \( g \in \mathcal{M}_{r+m}^{n}(F), \ 0 \neq h \in \mathcal{M}_r^{n}(F) \) (with any \( r \in \mathbb{Z} \)), and by \( \mathfrak{A}_m^n(\Gamma(N), F) \) the space of all \( f \) in \( \mathcal{M}_m^n(F) \) satisfying \((2.2)\). In particular, we set
\[
\mathfrak{F}_N^n = \mathfrak{A}_0^n(\Gamma(N), \mathbb{Q}(\zeta_N)), \\
\mathfrak{F}^n = \bigcup_{N=1}^{\infty} \mathfrak{F}_N^n.
\]

Let \( G_{\mathbb{A}} \) be the adelization of the group \( G_\mathbb{Q} \), \( G_0 \) the non-archimedean part of \( G_{\mathbb{A}} \), and \( G_{\infty} \) the archimedean part of \( G_{\mathbb{A}} \). Then \( \nu \) in \((2.1)\) defines a homomorphism \( G_{\mathbb{A}} \to \mathbb{Q}_\mathbb{A}^\times \). We put \( G_{\infty+} = \{ x \in G_\infty \mid \nu(x) > 0 \} \) and \( G_{\mathbb{A}+} = G_0G_{\infty+} \). For every algebraic number field \( F \), let \( F_{ab} \) be the maximal abelian extension of \( F \), and \( F^\mathbb{A} \) the idele group of \( F \). By class field theory every element \( x \) of \( F^\mathbb{A} \) acts on the field \( F_{ab} \) as an automorphism. We then write this automorphism as \([x,F]\). On the other hand, any element of \( G_{\mathbb{A}+} \) acts on the space \( \mathfrak{A}_0^n(\mathbb{Q}_{ab}) \) as an automorphism \([32, \text{p.680}]\). If \( x \in G_{\mathbb{A}+} \) and \( f \in \mathfrak{A}_0^n(\mathbb{Q}_{ab}) \), we mean by \( f^x \) the image of \( f \) under \( x \).

For a positive integer \( N \), let
\[
R_N \ = \ \mathbb{Q}^\times \cdot \{ a \in G_{\mathbb{A}+} \mid a_p \in GL_2n(\mathbb{Z}_p), a_p \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z}_p)} \} \text{ for all rational primes } p,
\]
\[
\Delta \ = \ \left\{ \begin{pmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{pmatrix} \mid x \in \prod_{p} \mathbb{Z}_p^\times \right\}.
\]

**PROPOSITION 2.1.** For every positive integer \( N \), we have
\[
G_{\mathbb{A}+} = R_N \Delta G_{\mathbb{A}+}.
\]

**PROOF.** \([30, \text{Proposition 3.4}] \) and \([31, \text{p.535 (3.10.3)}]\). \( \square \)

**PROPOSITION 2.2.** Let \( f(z) = \sum_\xi A(\xi)e(tr(\xi z)/N) \in \mathfrak{F}_N^n \).

(i) \( f^\beta = f \) for \( \beta \in R_N \). Moreover, \( \mathfrak{F}_N^n \) is the subfield of \( \mathfrak{A}_0^n(\mathbb{Q}_{ab}) \) consisting of all the \( R_N \)-invariant elements.

(ii) Let \( y = \begin{pmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{pmatrix} \in \Delta \) and \( t \) be a positive integer such that \( t \equiv x_p \pmod{N\mathbb{Z}_p} \) for all rational primes \( p \). Then we derive
\[
f^y = \sum_\xi A(\xi)^ae(tr(\xi z)/N),
\]
where $\sigma$ is the automorphism of $\mathbb{Q}(\zeta_N)$ satisfying $\zeta_N^\sigma = \zeta_N^t$.

(iii) $f^\alpha = f \circ \alpha$ for $\alpha \in G_{Q+}$.

**Proof.** [32, p.681] and [34, Theorem 26.8].

Now, we consider the case $n = 1$. Then we have $G_Q = GL_2(\mathbb{Q})$, $G_A = GL_2(\mathbb{Q}_A)$ and $\mathfrak{F}_1 = \mathcal{A}_1(\mathbb{Q}_{ab})$ ([33, Chapter 6]). It is well-known that $\mathfrak{F}_1$ and $\mathfrak{F}_1$ are Galois extensions of $\mathfrak{F}_1$ and $\mathfrak{F}_1$.

For any element $u = (u_p)_p \in \prod_p GL_2(\mathbb{Z}_p) \times G_\infty$. Then $G_{Q+} = UG_{Q+}$ and the sequence

$$1 \to \{\pm 1\} \cdot G_\infty \to U \to \text{Gal}(\mathfrak{F}_1/\mathfrak{F}_1) \to 1$$

is exact ([33, Lemma 6.19 and Proposition 6.21]. Hence we have

$$\text{Gal}(\mathfrak{F}_1/\mathfrak{F}_1) \cong U/\{\pm 1\} \cdot G_\infty \cong \prod_p GL_2(\mathbb{Z}_p)/\{\pm 1\}.$$

For any element $u = (u_p)_p \in \prod_p GL_2(\mathbb{Z}_p)$ and $N \in \mathbb{Z}_{>0}$, there is an integral matrix $\alpha$ in $G_{Q+}$ such that $\alpha \equiv u_p \pmod{N \cdot M_2(\mathbb{Z}_p)}$ for all rational primes $p$ dividing $N$ by the Chinese remainder theorem. Thus, the action of $u$ on $\mathfrak{F}_1$ can be described by the action of $\tilde{\alpha}$, where $\tilde{\alpha}$ is the image of $\alpha$ in $GL_2(\mathbb{Z}/N\mathbb{Z})$ ([12]).

### 3 Shimura’s reciprocity law

In this section we shall apply Shimura’s reciprocity law [34, §26] to a composite field of imaginary quadratic fields.

Let $n$ be a positive integer. For each index $1 \leq i \leq n$, let $K_i = \mathbb{Q}(\sqrt{-d_i})$ be an imaginary quadratic field with square-free positive integer $d_i$ and set

$$\rho_i = \begin{cases} -\frac{1}{\sqrt{-d_i}} & \text{if } -d_i \equiv 1 \pmod{4} \\ \frac{-1}{2\sqrt{-d_i}} & \text{if } -d_i \equiv 2,3 \pmod{4}. \end{cases}$$

Note that $\rho_i$ is the number in $K_i$ for which $-\rho_i^2$ is totally positive, $\text{Im}(\rho_i) > 0$ and $\text{Tr}_{K_i/\mathbb{Q}}(\rho_i x) \in \mathbb{Z}$ for all $x \in \mathcal{O}_{K_i}$. Let $L_i = \mathcal{O}_{K_i}$ be a lattice in $\mathbb{C}$. Then, for $z_i, w_i \in \mathbb{C}$ we define an $\mathbb{R}$-bilinear form $E_i(z_i, w_i)$ on $\mathbb{C}$ by

$$E_i(z_i, w_i) = \rho_i(z_i\overline{w_i} - \overline{z_i}w_i).$$

And, $E_i$ becomes a non-degenerate Riemann form on the complex torus $\mathbb{C}/L_i$ satisfying

$$E_i(\alpha_i, \beta_i) = \text{Tr}_{K_i/\mathbb{Q}}(\rho_i \alpha_i \overline{\beta_i}) \text{ for } \alpha_i, \beta_i \in K_i,$$
which makes it an elliptic curve as a polarized abelian variety ([34, p.43–44]). Let

\[ \theta_i = \begin{cases} \frac{-1 + \sqrt{-d_i}}{2} & \text{if } -d_i \equiv 1 \pmod{4} \\ \sqrt{-d_i} & \text{if } -d_i \equiv 2, 3 \pmod{4} \end{cases} \]

and let \( \Omega_i = (\theta_i, 1) \in M_{1 \times 2}(\mathbb{C}) \). Then \( \mathcal{O}_{K_i} = \mathbb{Z}[\theta_i] \) and \( \Omega_i \) satisfies

\[
L_i = \left\{ \Omega_i \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\},
\]

\[
E_i(\Omega_i x, \Omega_i y) = ^t x J_1 y \quad \text{for } (x, y) \in \mathbb{R}^2 \times \mathbb{R}^2.
\]

On the other hand, we define a ring monomorphism \( h_i : K_i \to M_2(\mathbb{Q}) \) by

\[
\begin{pmatrix} \alpha_i \theta_i \\ \alpha_i \end{pmatrix} = h_i(\alpha_i) \begin{pmatrix} \theta_i \\ 1 \end{pmatrix} \quad \text{for } \alpha_i \in K_i,
\]

in other words, \( h_i(\alpha_i) \) is the regular representation of \( \alpha_i \) with respect to \( \{ \theta_i, 1 \} \). Then \( \theta_i \) is the CM-point of \( \mathbb{H}_1 \) induced from \( h_i \) which corresponds to the elliptic curve \( (\mathbb{C}/L_i, E_i) \) ([32, p.684-685] or [34, §24.10]).

Now, let \( Y = K_1 \oplus \cdots \oplus K_n \) be a CM-algebra so that \( [Y : \mathbb{Q}] = 2n \), \( \mathcal{O}_Y = \mathcal{O}_{K_1} \oplus \cdots \oplus \mathcal{O}_{K_n} \) and \( \rho = (\rho_1, \ldots, \rho_n) \in Y \). We denote by \( v(\alpha) \), for \( \alpha = (\alpha_1, \ldots, \alpha_n) \in Y \), the vector of \( \mathcal{O}_n \) whose components are \( \alpha_1, \ldots, \alpha_n \). Let \( L = \{ v(\alpha) \mid \alpha \in \mathcal{O}_Y \} \) be a lattice in \( \mathbb{C}^n \). For \( z = (z_1, z_2, \ldots, z_n) \) and \( w = (w_1, w_2, \ldots, w_n) \) in \( \mathbb{C}^n \), we define an \( \mathbb{R} \)-bilinear form \( E(z, w) \) on \( \mathbb{C}^n \) by

\[
E(z, w) = \sum_{i=1}^{n} E_i(z_i, w_i).
\]

Then \( E \) becomes a non-degenerate Riemann form on the complex torus \( \mathbb{C}^n / L \) satisfying

\[
E(v(\alpha), v(\beta)) = \text{Tr}_{Y/\mathbb{Q}}(\rho \alpha \overline{\beta}) = \sum_{i=1}^{n} \text{Tr}_{K_i/\mathbb{Q}}(\rho_i \alpha_i \overline{\beta_i}) \quad \text{for } \alpha = (\alpha_i), \beta = (\beta_i) \in Y,
\]

which also makes it a polarized abelian variety ([34, p.43–44, 129–130]). Let

\[
\Omega = \begin{pmatrix} \theta_1 & 1 \\ \vdots & \ddots & \ddots \\ \theta_n & \cdots & 1 \end{pmatrix} \in M_{n \times 2n}(\mathbb{C}).
\]

Then \( \Omega \) satisfies

\[
L = \left\{ \Omega \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{Z}^n \right\},
\]

\[
E(\Omega x, \Omega y) = ^t x J_n y \quad \text{for } (x, y) \in \mathbb{R}^{2n} \times \mathbb{R}^{2n}.
\]
Here, we write $\Omega = (\Omega_1, \Omega_2) = (v(e_1), v(e_2), \ldots, v(e_{2n}))$ with $\Omega_1, \Omega_2 \in M_n(\mathbb{C})$ and $e_1, e_2, \ldots, e_{2n} \in Y$. Then $\{e_1, e_2, \ldots, e_{2n}\}$ is a free $\mathbb{Q}$-basis of $Y$, so we can define a ring monomorphism $h : Y \to M_{2n}(\mathbb{Q})$ by

$$
\begin{pmatrix}
\alpha e_1 \\
\vdots \\
\alpha e_{2n}
\end{pmatrix} = h(\alpha) \begin{pmatrix} e_1 \\
\vdots \\
e_{2n} \end{pmatrix} \quad \text{for } \alpha \in Y,
$$

that is, $h(\alpha)$ is the regular representation of $\alpha$ with respect to $\{e_1, e_2, \ldots, e_{2n}\}$. One can then readily show that $z_0 = \Omega_2^{-1} \Omega_1 = \begin{pmatrix} \theta_1 & & \\
& \ddots & \\
& & \theta_n \end{pmatrix}$ is the CM-point of $\mathbb{H}_n$ induced from $h$ which corresponds to the polarized abelian variety $\mathbb{C}^n/L$, $E$ (32 p.684-685 or 34 §24.10).

Let $K$ be the composite field $K_1 \cdots K_n$, $Y_a = \prod_{i=1}^n(K_i)_a$ and $Y_{a}^\times = \prod_{i=1}^n(K_i)_a^\times$. We define a map $\varphi : K_{a}^\times \to Y_{a}^\times$ by

$$\varphi(x) = \left(N_{K_i/K}(x)\right)_{1 \leq i \leq n} \quad \text{for } x \in K_{a}^\times.$$ 

Then the map $h$ can be naturally extended to a homomorphism $Y_a \to M_{2n}(\mathbb{Q}_a)$, which we denote again by $h$. Hence, for every $b \in K_{a}^\times$ we get $\nu(h(\varphi(b))) = N_{K/b}(b)$ and $h(\varphi(b)^{-1}) \in G_{a+}$ (34 p.172).

**Proposition 3.1** (Shimura’s reciprocity law). Let $Y$, $h$, $z_0$ and $K$ be as above. Then for every $f \in \mathfrak{A}_0^n(\mathbb{Q}_a)$ which is finite at $z_0$, the value $f(z_0)$ belongs to $K_{a}$. Moreover, if $b \in K_{a}^\times$, then $f^{h(\varphi(b)^{-1})}$ is finite at $z_0$ and

$$f(z_0)^{[b,K]} = f^{h(\varphi(b)^{-1})}(z_0).$$

**Proof.** [34] Theorem 26.8.

**Remark 3.2.** For any $f \in \mathfrak{A}_0^n(\mathbb{Q}_a)$ which is finite at $z_0$, the value $f(z_0)$ indeed belongs to the class field $\widetilde{K}_{a}$ of $K$ corresponding to the kernel of $\varphi$.

Now, we define a subset $\mathbb{H}_n^{\text{diag}}$ of the Siegel upper half-space $\mathbb{H}_n$ by

$$\mathbb{H}_n^{\text{diag}} = \{\text{diag}(z_1, \ldots, z_n) \mid z_1, \ldots, z_n \in \mathbb{H}_1\},$$

where $\text{diag}(z_1, \ldots, z_n)$ is the diagonal matrix with the diagonal entries $z_1, \ldots, z_n$. Clearly, the CM-point $z_0$ belongs to $\mathbb{H}_n^{\text{diag}}$. A function $f$ in $\mathfrak{A}_N^n$ is called a *modular unit of level* $N$ if it has no zeros and poles on $\mathbb{H}_1$ [17] p.36.
Proposition 3.3. Let $N \geq 2$ be an integer and $f \in \mathfrak{F}_N^n$. Then $f$ has no zeros and poles on $\mathbb{H}_n^{\text{diag}}$ if and only if there exist modular units $f_1, f_2, \ldots, f_n$ of level $N$ such that

$$f(\text{diag}(z_1, \ldots, z_n)) = \prod_{i=1}^{n} f_n(z_i).$$

Proof. See [9]. \qed

Thus, we see from Proposition 3.3 that it is natural to investigate the class field of $K$ generated by the singular values $f(\theta_i)$ of modular units $f$.

4 Siegel functions

In this section we shall introduce the well-known modular units, Siegel functions, and review some necessary facts about the singular values of Siegel functions for later use.

For a rational vector $(r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, we define the Siegel function $g_{(r_1, r_2)}(\tau)$ on $\tau \in \mathbb{H}_1$ by the following infinite product

$$g_{(r_1, r_2)}(\tau) = -q_\tau^{\frac{1}{2}B_2(r_1)} e^{\pi i r_2 (r_1 - 1)} (1 - q_z) \prod_{n=1}^{\infty} (1 - q_z^n q_z) (1 - q_z^n q_z^{-1}),$$

where $B_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial, $q_\tau = e^{2\pi i \tau}$ and $q_z = e^{2\pi iz}$ with $z = r_1 \tau + r_2$. Then a Siegel function is a modular unit, namely, it has no zeros and poles on $\mathbb{H}_1$ ([33] or [17, p.36]).

Proposition 4.1. Let $(r_1, r_2) \in \frac{1}{N} \mathbb{Z}^2 \setminus \mathbb{Z}^2$ for an integer $N \geq 2$.

(i) $g_{(r_1, r_2)}^{12N}(\tau)$ satisfies the relation

$$g_{(r_1, r_2)}^{12N}(\tau) = g_{(-r_1, -r_2)}^{12N}(\tau) = g_{(r_1, r_2)}^{12N}(\tau'),$$

where $\langle X \rangle$ is the fractional part of $X \in \mathbb{R}$ such that $0 \leq \langle X \rangle < 1$.

(ii) $g_{(r_1, r_2)}^{12N}(\tau)$ belongs to $\mathfrak{F}^1_N$. Moreover, $\alpha \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ acts on it by

$$g_{(r_1, r_2)}^{12N}(\tau)^\alpha = g_{(r_1, r_2)}^{12N}(\tau).$$

Proof. [12, Proposition 1.1]. \qed

Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with square-free positive integer $d$ and let

$$\theta = \begin{cases} \frac{-1+\sqrt{-d}}{2} & \text{if } -d \equiv 1 \pmod{4} \\ \sqrt{-d} & \text{if } -d \equiv 2, 3 \pmod{4} \end{cases}$$

9
so that $O_F = \mathbb{Z}[\theta]$. Then its minimal polynomial over $\mathbb{Q}$ is
\[X^2 + B\theta X + C\theta = \begin{cases} X^2 + X + \frac{1+d}{4} & \text{if } -d \equiv 1 \pmod{4} \\ X^2 + d & \text{if } -d \equiv 2, 3 \pmod{4}. \end{cases}\]

We define a map $h : F_\mathbb{A} \to M_2(\mathbb{Q}_\mathbb{A})$ for $Y = F$ with respect to \{\theta, 1\} as in Section 3.

**Proposition 4.2.** Let $N \geq 2$ be an integer and $(r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$. Then the singular value $g^{12N}_{(r_1, r_2)}(\theta)$ belongs to $F_{(N)}$. Moreover, if $\omega \in O_F$ prime to $N$ then
\[g^{12N}_{(r_1, r_2)}(\theta) \left( \frac{F_{(N)}/F}{(\omega)} \right) = g^{12N}_{(r_1, r_2)} \left( t - B\theta s \quad -C\theta s \atop s \quad t \right)(\theta),\]
where $\omega = s\theta + t$ for $s, t \in \mathbb{Z}$.

**Proof.** The field $F(\mathfrak{F}_{1,N}(\theta))$ generated over $F$ by all singular values $f(\theta)$ with $f \in \mathfrak{F}_{1,N}$, which are finite at $\theta$, is the ray class field $F_{(N)}$ over $F$ ([19, Chapter 10, Corollary to Theorem 2]). Hence by Proposition 4.3 we obtain $g^{12N}_{(r_1, r_2)}(\theta) \in F_{(N)}$ for $(r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$. Now, set
\[\tilde{\omega} = \prod_{v \text{ finite}} (\omega^{-1})_v \times \prod_{v \text{ finite}} 1_v \times \prod_{v \text{ infinite}} 1_v \in F_\mathbb{A}^\times.\]
Here $x_v$ is the $v$-component of $x \in F_\mathbb{A}$.
And, observe that for all rational primes $p$ dividing $N$,
\[h(\tilde{\omega}^{-1})_p \equiv h(\omega) \equiv \left( t - B\theta s \quad -C\theta s \atop s \quad t \right) \pmod{N \cdot M_2(\mathbb{Z}_p)}\]
([12, p.417]). Therefore, by [19, Chapter 8 §4], Proposition 3.1 and 4.1 we attain
\[g^{12N}_{(r_1, r_2)} \left( \frac{F_{(N)}/F}{(\omega)} \right) = g^{12N}_{(r_1, r_2)}(\theta) \left[ \tilde{\omega}, F \right] = g^{12N}_{(r_1, r_2)}(\theta) = g^{12N}_{(r_1, r_2)} \left( t - B\theta s \quad -C\theta s \atop s \quad t \right)(\theta),\]

**Lemma 4.3.** Let $N \geq 2$ be an integer and $(r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$. Then we have
\[g^{12N}_{(r_1, r_2)}(\theta) = \begin{cases} g^{12N}_{(r_1, r_1 - r_2)}(\theta) & \text{if } -d \equiv 1 \pmod{4} \\ g^{12N}_{(r_1, -r_2)}(\theta) & \text{if } -d \equiv 2, 3 \pmod{4}. \end{cases}\]

**Proof.** If $-d \equiv 1 \pmod{4}$, then $\tilde{\theta} = -\theta + 1$, $\overline{\theta} = q_{r_1\theta + r_1 - r_2}$ and $\overline{\theta}^n = q_{\theta}^n$ for $n \in \mathbb{Z}_{\geq 0}$. And, note that
\[e^{\pi i B_2(r_1)} \cdot e^{-\pi i r_2(r_1 - 1)} = \zeta_{12} \cdot e^{\pi i (r_1 - r_2)(r_1 - 1)}.\]
Thus we achieve
\[
g^{12N}_{(r_1, r_2)}(\theta) = \left( - e^{\pi i (\theta + 1)} B_2(r_1) e^{-\pi i r_2(r_1 - 1)} (1 - q_{r_1\theta + r_1 - r_2}) \prod_{n=1}^{\infty} (1 - q_{\theta}^n q_{r_1\theta + r_1 - r_2})^2 \right)^{12N}
\]
\[
= \left( - \zeta_{12} \cdot q_{\theta} B_2(r_1) e^{\pi i (r_1 - r_2)(r_1 - 1)} (1 - q_{r_1\theta + r_1 - r_2}) \prod_{n=1}^{\infty} (1 - q_{\theta}^n q_{r_1\theta + r_1 - r_2})^2 \right)^{12N}
\]
\[
= g^{12N}_{(r_1, r_1 - r_2)}(\theta).
\]

If \(-d \equiv 2, 3 \pmod{4}\), then \(\overline{\theta} = -\theta\), \(\overline{q_x} = q_{r_1\theta - r_2}\) and \(\overline{q_{\theta}^n} = q_{\theta}^n\) for \(n \in \mathbb{Z}_{>0}\). Therefore, we derive
\[
g^{12N}_{(r_1, r_2)}(\theta) = \left( - e^{-\pi i (-\theta)} B_2(r_1) e^{\pi i (-r_2)(r_1 - 1)} (1 - q_{r_1\theta - r_2}) \prod_{n=1}^{\infty} (1 - q_{\theta}^n q_{r_1\theta - r_2})^2 \right)^{12N}
\]
\[
= g^{12N}_{(r_1, -r_2)}(\theta).
\]

\[\square\]

**Proposition 4.4.** Let \(N \geq 2\) be an integer. Assume that \(F \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\). Then for any positive integer \(n\), we get
\[
F(N) = F\left(g^{12N_n}_{(0, N)}(\theta)\right).
\]
Moreover, the singular value \(g^{12N_n}_{(0, N)}(\theta)\) is a real algebraic integer.

**Proof.** [12, Theorem 3.5 and Remark 3.6] \[\square\]

For an ideal \(\mathfrak{f}\) of \(\mathcal{O}_F\), let \(\pi_\mathfrak{f} : \mathcal{O}_F \to \mathcal{O}_F/\mathfrak{f}\) be the natural surjection.

**Proposition 4.5.** Let \(N \geq 2\) be an integer and \(L\) be a finite abelian extension of \(F\) such that \(F \subset L \subset F(N)\). If \(\mathcal{O}_F = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}\), we set
\[
\hat{e}_i = \# \ker \left( \text{the natural projection } \pi_{\mathcal{O}_F}(\mathcal{O}_F^\times) / \pi_{\mathcal{O}_F}(\mathcal{O}_F^\times) \to \pi_{\mathcal{O}_F/\mathfrak{p}_i}(\mathcal{O}_{F/\mathfrak{p}_i}^\times) / \pi_{\mathcal{O}_F/\mathfrak{p}_i}(\mathcal{O}_{F/\mathfrak{p}_i}^\times) \right),
\]
\[
e_i = \# \ker \left( \text{the natural projection } \pi_{\mathcal{O}_F}(\mathcal{O}_F^\times) / \pi_{\mathcal{O}_F}(\mathcal{O}_F^\times) \to \pi_{\mathcal{O}_{F/\mathfrak{p}_i}}(\mathcal{O}_{F/\mathfrak{p}_i}^\times) / \pi_{\mathcal{O}_{F/\mathfrak{p}_i}}(\mathcal{O}_{F/\mathfrak{p}_i}^\times) \right),
\]
for each \(i = 1, \ldots, m\). Assume that for each index \(1 \leq i \leq m\) there is an odd prime \(\mathfrak{p}_i\) such that \(\nu_{\mathfrak{p}_i} \nmid \hat{e}_i\) and \(\ord_{\mathfrak{p}_i}(\hat{e}_i) > \ord_{\mathfrak{p}_i}(\nu_{F(N)/L})\). Then for any positive integer \(n\), the singular value
\[
N_{F(N)/L} \left( g^{12N_n}_{(0, N)}(\theta) \right)
\]
generates \(L\) over \(F\).

**Proof.** [8, Theorem 2.7 and Remark 2.8]. \[\square\]
5 Pell conics over a finite field

Let $\Delta$ be an integer, $p$ be an odd prime and $q = p^n$ with a positive integer $n$. Consider an affine curve

$$C : x^2 - \Delta y^2 = 1$$

defined over a finite field $\mathbb{F}_q$. Assume that $C$ is smooth, that is, $p \nmid \Delta$. We call the curve $C$ the Pell conic over $\mathbb{F}_q$. Lemmermeyer \cite{21} defined a group law on the Pell conic $C$ and presented some properties of $C(\mathbb{F}_q)$. The group law on $C$ is given by

$$(r, s) \oplus (t, u) = (rt + \Delta su, ru + st)$$

for points $(r, s), (t, u)$ on $C$. Then the identity element of $C$ is $(1, 0)$ and the inverse of $(r, s)$ is $(r, -s)$. We can then define an injective group homomorphism $f : C(\mathbb{F}_q) \rightarrow \mathbb{F}_q(\sqrt{\Delta})^\times$ by $f((r, s)) = r + s\sqrt{\Delta}$. Indeed, if $f((r, s)) = 1$ for some $(r, s) \in C(\mathbb{F}_q)$, then $r + s\sqrt{\Delta} = 1$. Since $r^2 - \Delta s^2 = 1$, we have $r - s\sqrt{\Delta} = 1$. Hence $(r, s) = (1, 0)$, and so $f$ is injective.

Since $\mathbb{F}_q(\sqrt{\Delta})^\times$ is cyclic, so is $C(\mathbb{F}_q)$.

**Lemma 5.1.** Let $p$ and $C$ be as above. Then we derive

$$C(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z}$$

where $m = q - \left(\frac{\Delta}{p}\right)^n$. Here $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

**Proof.** If $\left(\frac{\Delta}{p}\right) = 1$, then $\Delta = D^2$ for some $D \in \mathbb{F}_p$. And, it is easy to check that the map

$$\begin{align*}
C(\mathbb{F}_q) &\longrightarrow \{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q \mid uv = \Delta\} \\
(x, y) &\mapsto \left(\frac{x-1}{y}, \frac{x+1}{y}\right) \quad \text{if } (x, y) \neq (\pm 1, 0) \\
(\pm 1, 0) &\mapsto \pm (D, D)
\end{align*}$$

is a bijection. Hence $|C(\mathbb{F}_q)| = \left|\{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q \mid uv = \Delta\}\right| = q - 1$, so we obtain $C(\mathbb{F}_q) \cong \mathbb{Z}/(q - 1)\mathbb{Z}$.

If $\left(\frac{\Delta}{p}\right) = -1$, then $\mathbb{F}_p(\sqrt{\Delta}) = \mathbb{F}_p^2$. Thus $\mathbb{F}_p(\sqrt{\Delta}) \subset \mathbb{F}_q$ if and only if $n$ is even. If $n$ is even, then $\sqrt{\Delta} \in \mathbb{F}_q$; hence $\Delta = D^2$ for some $D \in \mathbb{F}_q$. And, likewise in the above one can show that $C(\mathbb{F}_q) \cong \mathbb{Z}/(q - 1)\mathbb{Z}$. If $n$ is odd, then $\sqrt{\Delta} \notin \mathbb{F}_q$, which yields $\mathbb{F}_q(\sqrt{\Delta}) = \mathbb{F}_q^2$.

Now, consider the norm map $N : \mathbb{F}_q(\sqrt{\Delta})^\times \rightarrow \mathbb{F}_q^\times$ such that

$$N(x + y\sqrt{\Delta}) = x^2 - \Delta y^2 \quad \text{for } x, y \in \mathbb{F}_q.$$

Then $C(\mathbb{F}_q)$ corresponds to the kernel of the norm map $N$. Here we observe that

$$\text{Gal}(\mathbb{F}_q(\sqrt{\Delta})/\mathbb{F}_q) = \{1, \sigma_q\}$$
where \( \sigma_q \) is the Frobenius automorphism of \( \mathbb{F}_q(\sqrt{\Delta}) \) over \( \mathbb{F}_q \). Thus we achieve
\[
N(\alpha) = \alpha \cdot \alpha^{\sigma_q} = \alpha^{q+1} \quad \text{for} \quad \alpha \in \mathbb{F}_q(\sqrt{\Delta})^\times.
\]
Since the equation \( x^{q+1} - 1 = 0 \) has at most \( q + 1 \) roots, \( |\ker(N)| \leq q + 1 \). Thus
\[
|\text{Im}(N)| = \frac{|\mathbb{F}_q(\sqrt{\Delta})^\times|}{|\ker(N)|} \geq q - 1 = |\mathbb{F}_q^\times|,
\]
from which we have \( \text{Im}(N) = \mathbb{F}_q^\times \) and \( |\mathcal{C}(\mathbb{F}_q)| = |\ker(N)| = q + 1 \). Therefore, we establish \( \mathcal{C}(\mathbb{F}_q) \cong \mathbb{Z}/(q + 1)\mathbb{Z} \) in this case, which completes the proof.

**Corollary 5.2.** Let \( F = \mathbb{Q}(\sqrt{\Delta}) \) be a quadratic field with square-free integer \( \Delta \) and \( p \) be an odd prime such that \( p \nmid \Delta \). Then we attain
\[
\{ \omega + p\mathcal{O}_F \in (\mathcal{O}_F/p\mathcal{O}_F)^\times \mid N_{F/\mathbb{Q}}(\omega) \equiv 1 \pmod{p} \} \cong \mathbb{Z}/m\mathbb{Z},
\]
where \( m = p - \left( \frac{\Delta}{p} \right) \). Moreover, the norm map
\[
\widehat{N}_{F/\mathbb{Q}} : (\mathcal{O}_F/p\mathcal{O}_F)^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times
\]
\[
\omega + p\mathcal{O}_F \quad \longrightarrow \quad N_{F/\mathbb{Q}}(\omega) + p\mathbb{Z}
\]
is surjective.

**Proof.** Since \( (2,p) = 1 \), we obtain
\[
\mathcal{O}_F/p\mathcal{O}_F = \{ x + y\sqrt{\Delta} + p\mathcal{O}_F \mid x, y \in \mathbb{F}_p \}.
\]
And, the map
\[
\{ \omega + p\mathcal{O}_F \in (\mathcal{O}_F/p\mathcal{O}_F)^\times \mid N_{F/\mathbb{Q}}(\omega) \equiv 1 \pmod{p} \} \longrightarrow \mathcal{C}(\mathbb{F}_p)
\]
\[
x + y\sqrt{\Delta} + p\mathcal{O}_F \quad \longrightarrow \quad (x, y)
\]
is an isomorphism, where \( \mathcal{C} : x^2 - \Delta y^2 = 1 \) is the Pell conic over \( \mathbb{F}_p \). The first assertion can be deduced from Lemma 5.1. Note that \( |\ker(\widehat{N}_{F/\mathbb{Q}})| = |\mathcal{C}(\mathbb{F}_p)| = m \), and by [23, Theorem V.1.7] we claim that
\[
|(\mathcal{O}_F/p\mathcal{O}_F)^\times| = (p - 1)m = \begin{cases} 
(p - 1)^2 & \text{if } \left( \frac{\Delta}{p} \right) = 1 \\
(p - 1)(p + 1) & \text{if } \left( \frac{\Delta}{p} \right) = -1.
\end{cases}
\]
Therefore, we get \( |\text{Im}(\widehat{N}_{F/\mathbb{Q}})| = p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times| \), and so \( \widehat{N}_{F/\mathbb{Q}} \) is surjective. \( \square \)
6 Class fields over imaginary biquadratic fields (I)

We shall consider an imaginary biquadratic field \( K = \mathbb{Q}(\sqrt{-d_1}, \sqrt{-d_2}) \) where \( d_1, d_2 \) are square-free positive integer such that \(-d_1 \equiv 1 \pmod{4}, -d_2 \equiv 2, 3 \pmod{4} \) and \((d_1, d_2) = 1\). Then we have two imaginary quadratic subfields \( K_1 = \mathbb{Q}(\sqrt{-d_1}), K_2 = \mathbb{Q}(\sqrt{-d_2}) \) and one real quadratic subfield \( K_3 = \mathbb{Q}(\sqrt{d_1d_2}) \) in \( K \).

**Lemma 6.1.** Let \( K \) be as above. Then the ring of integers \( \mathcal{O}_K \) of \( K \) is \( \mathbb{Z}\left\lbrack \frac{-1+\sqrt{-d_1}}{2}, \sqrt{-d_2} \right\rbrack \). Consequently,

\[
\mathcal{O}_K = \left\{ \frac{1}{2} \left[ a + b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1d_2} \right] \mid a, b, c, d \in \mathbb{Z}, \ a \equiv b \ (\text{mod}2), \ c \equiv d \ (\text{mod}2) \right\}.
\]

**Proof.** By \( [11, \text{Theorem 9,5}] \) we have \( \mathcal{O}_K = \mathcal{O}_{K_1}\mathcal{O}_{K_2} = \mathbb{Z}\left\lbrack \frac{-1+\sqrt{-d_1}}{2}, \sqrt{-d_2} \right\rbrack \). Hence we deduce

\[
\mathcal{O}_K = \left\{ A + B \left( \frac{-1+\sqrt{-d_1}}{2} \right) + C\sqrt{-d_2} + D \left( \frac{-\sqrt{-d_2} + \sqrt{d_1d_2}}{2} \right) \mid A, B, C, D \in \mathbb{Z} \right\}
\]

\[
= \left\{ \frac{1}{2} \left[ (2A - B) + B\sqrt{-d_1} + (2C - D)\sqrt{-d_2} - D\sqrt{d_1d_2} \right] \mid A, B, C, D \in \mathbb{Z} \right\}
\]

\[
= \left\{ \frac{1}{2} \left[ a + b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1d_2} \right] \mid a, b, c, d \in \mathbb{Z}, \ a \equiv b \ (\text{mod}2), \ c \equiv d \ (\text{mod}2) \right\}.
\]

\( \square \)

Let \( N \) be a positive integer and \( p \) be an odd prime such that \((N, p) = 1\). For a non-negative integer \( \mu \), we set

\[
S_{N,p,\mu} = \{ a \in K^\times \mid a \equiv 1 \pmod{Np^\mu \mathcal{O}_K}, \ a \text{ is prime to } p\mathcal{O}_K \},
\]

\[
S_{N,p,\mu}^{(i)} = \{ a \in K_i^\times \mid a \equiv 1 \pmod{Np^\mu \mathcal{O}_{K_i}}, \ a \text{ is prime to } p\mathcal{O}_{K_i} \} \text{ for } i = 1, 2, 3.
\]

Further, we let

\[
H_{N,p,\mu} = S_{N,p,\mu+1}(S_{N,p,\mu} \cap \mathcal{O}_K^\times),
\]

\[
H_{N,p,\mu}^{(i)} = S_{N,p,\mu+1}(S_{N,p,\mu}^{(i)} \cap \mathcal{O}_{K_i}^\times) \text{ for } i = 1, 2, 3.
\]

Then we achieve the isomorphisms

\begin{align}
\text{Gal}(K_{(Np^{\mu+1})}/K_{(Np^{\mu})}) & \cong S_{N,p,\mu} \mathcal{O}_K^\times / S_{N,p,\mu+1} \mathcal{O}_K^\times \cong S_{N,p,\mu} / H_{N,p,\mu} \\
\text{Gal}((K_i)_{(Np^{\mu+1})}/(K_i)_{(Np^{\mu})}) & \cong S_{N,p,\mu} \mathcal{O}_{K_i}^\times / S_{N,p,\mu+1} \mathcal{O}_{K_i}^\times \cong S_{N,p,\mu}^{(i)} / H_{N,p,\mu}^{(i)}
\end{align}

by class field theory (\( [11, \text{Chapter V \S 6}] \)). Since \( N_{K/K_i}(H_{N,p,\mu}) \subset H_{N,p,\mu}^{(i)} \) for \( i = 1, 2, 3 \), we can define three homomorphisms

\[
\varphi_{N,p,\mu}^3: S_{N,p,\mu}/H_{N,p,\mu} \rightarrow \prod_{i=1}^{3} S_{N,p,\mu}^{(i)}/H_{N,p,\mu}^{(i)},
\]

\[
\varphi_{N,p,\mu}^{ij}: S_{N,p,\mu}/H_{N,p,\mu} \rightarrow S_{N,p,\mu}^{(i)}/H_{N,p,\mu}^{(i)} \times S_{N,p,\mu}^{(j)}/H_{N,p,\mu}^{(j)} \text{ for } 1 \leq i < j \leq 3,
\]

\[
\varphi_{N,p,\mu}^i: S_{N,p,\mu}/H_{N,p,\mu} \rightarrow S_{N,p,\mu}^{(i)}/H_{N,p,\mu}^{(i)} \text{ for } i = 1, 2, 3.
\]
by
\[
\varphi_{N,\mu}(aH_{N,\mu}) = \left( N_{K/K_i}(a)H_{N,\mu}^{(i)} \right)_{1 \leq i \leq 3},
\]
\[
\varphi_{N,\mu}^{ij}(aH_{N,\mu}) = \left( N_{K/K_i}(a)H_{N,\mu}^{(i)}, N_{K/K_j}(a)H_{N,\mu}^{(j)} \right),
\]
\[
\varphi_{N,\mu}^i(aH_{N,\mu}) = N_{K/K_i}(a)H_{N,\mu}^{(i)}.
\]

Let \( \overline{K}_{N,\mu} \), \( \overline{K}_{N,\mu}^{ij} \) and \( \overline{K}_{N,\mu}^i \) be the class fields of \( K \) corresponding to \( \ker(\widetilde{\varphi}_{N,\mu}) \), \( \ker(\widetilde{\varphi}_{N,\mu}^{ij}) \) and \( \ker(\widetilde{\varphi}_{N,\mu}^i) \), respectively. Note that \( \overline{K}_{N,\mu}^{1,2} = K_{(N^\mu)}(K_{(N^\mu+1)} \cap \overline{K}_{ab}) \), where \( \overline{K}_{ab} \) is the class field of \( K \) described in Remark 3.2.

**Lemma 6.2.** With the notations as above, for a non-negative integer \( \mu \) we obtain
\[
\overline{K}_{N,\mu} = K_{(N^\mu)}(K_1)_{(N^\mu+1)}(K_2)_{(N^\mu+1)}(K_3)_{(N^\mu+1)},
\]
\[
\overline{K}_{N,\mu}^{ij} = K_{(N^\mu)}(K_1)_{(N^\mu+1)}(K_j)_{(N^\mu+1)} \quad \text{for} \ 1 \leq i < j \leq 3,
\]
\[
\overline{K}_{N,\mu}^i = K_{(N^\mu)}(K_i)_{(N^\mu+1)} \quad \text{for} \ i = 1, 2, 3.
\]

**Proof.** For each index \( 1 \leq i \leq 3 \), let \( \gamma_i \) be a primitive generator of \( (K_i)_{(N^\mu+1)} \) over \( (K_i)_{(N^\mu)} \). Since \( (K_i)_{(N^\mu+1)} \subset K_{(N^\mu)} \) for \( i = 1, 2, 3 \), we attain
\[
K_{(N^\mu)}(K_1)_{(N^\mu+1)}(K_2)_{(N^\mu+1)}(K_3)_{(N^\mu+1)} = K_{(N^\mu)}(\gamma_1, \gamma_2, \gamma_3).
\]

If \( aH_{N,\mu} \in \ker(\widetilde{\varphi}_{N,\mu}) \), then \( N_{K/K_i}(a) \in H_{N,\mu}^{(i)} \) for \( i = 1, 2, 3 \). Since \( \gamma_i \in (K_i)_{(N^\mu+1)} \), we have
\[
\gamma_i \left( \frac{K_{(N^\mu+1)/K_1}}{\mu} \right) = \gamma_i \left( \frac{K_{(N^\mu+1)/K_i}}{N_{K/K_1}(\mu)} \right) = \gamma_i \quad \text{for} \ i = 1, 2, 3
\]
([11], Chapter III §3). Hence \( \overline{K}_{N,\mu} \supset K_{(N^\mu)}(\gamma_1, \gamma_2, \gamma_3) \).

Conversely, let \( bH_{N,\mu} \in S_{N,\mu}/H_{N,\mu} \) such that
\[
\gamma_i \left( \frac{K_{(N^\mu+1)/K}}{\mu} \right) = \gamma_i \quad \text{for} \ i = 1, 2, 3.
\]

Since \( \gamma_i \) is the primitive generator of \( (K_i)_{(N^\mu+1)}/(K_i)_{(N^\mu)} \), we obtain \( N_{K/K_i}(b) \in H_{N,\mu}^{(i)} \) for \( i = 1, 2, 3 \) by (6.1). Thus \( bH_{N,\mu} \in \ker(\widetilde{\varphi}_{N,\mu}) \), and so \( \overline{K}_{N,\mu} \subset K_{(N^\mu)}(\gamma_1, \gamma_2, \gamma_3) \). In like manner, one can show that \( \overline{K}_{N,\mu}^{ij} = K_{(N^\mu)}(\gamma_i, \gamma_j) \) and \( \overline{K}_{N,\mu}^i = K_{(N^\mu)}(\gamma_i) \). \( \square \)

For a non-negative integer \( \mu \) and \( i = 1, 2 \), we let
\[
(6.2) \quad \gamma_{\mu,i} = g_{(12N^\mu)}(\theta_i),
\]
where \( \theta_1 = \frac{-1 + \sqrt{-d_1}}{2} \) and \( \theta_2 = \sqrt{-d_2} \).
Corollary 6.3. Assume that $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. For any positive integers $n_1, n_2$, the value $\gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2}$ generates $K_{N,p,\mu}^{1,2}$ over $K_{(Np^\mu)}$.

Proof. It follows from Proposition 6.3 and Lemma 6.2 that $K_{N,p,\mu}^{1,2} = K_{(Np^\mu)}(\gamma_{\mu+1,1}^{n_1}, \gamma_{\mu+1,2}^{n_2})$. Note that $|\sigma\gamma_{\mu+1,1}^{n_1}| > |\gamma_{\mu+1,2}^{n_2}|$ for $i = 1, 2$ and $\sigma \in \text{Gal}((K_i)_{(Np^\mu+1)/K_i}) \setminus \{\text{Id}\}$ (Theorem 3.5 and Remark 3.6)). Hence

$$(\gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2})^\sigma \neq \gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2} \quad \text{for } \sigma \in \text{Gal}\left(\frac{K_{N,p,\mu}^{1,2}}{K_{(Np^\mu)}}\right) \setminus \{\text{Id}\}.$$ 

Therefore, $\gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2}$ generates the field $K_{N,p,\mu}^{1,2}$ over $K_{(Np^\mu)}$. \hfill $\Box$

In this section we shall consider only the case $\mu = 0$. As for the other cases, see Section 7.

Lemma 6.4. With the notation as above, we get

$$|S_{N,p,0}/S_{N,p,1}| = p^4 \cdot \prod_{p \mid \mathcal{O}_K, p \text{ prime}} \left(1 - \frac{1}{Np}\right)$$

$$|S_{N,p,0}^{(i)}/S_{N,p,1}^{(i)}| = p^{2i} \cdot \prod_{p \mid \mathcal{O}_K, p \text{ prime}} \left(1 - \frac{1}{Np}\right) \quad \text{for } i = 1, 2, 3,$$

where $N$ is the absolute norm of an ideal.

Proof. Note that for any coset $aS_{N,p,1}$ in $S_{N,p,0}/S_{N,p,1}$, there is an element $a' \in S_{N,p,0} \cap \mathcal{O}_K$ such that $aS_{N,p,1} = a'S_{N,p,1}$. Here we claim that the map

$$\psi : S_{N,p,0}/S_{N,p,1} \longrightarrow (\mathcal{O}_K/p\mathcal{O}_K)^\times$$

$$\omega S_{N,p,1} \quad \mapsto \quad \omega + p\mathcal{O}_K \quad \text{for } \omega \in S_{N,p,0} \cap \mathcal{O}_K$$

is an isomorphism. Indeed, if $\omega, \omega' \in S_{N,p,0} \cap \mathcal{O}_K$ such that $\omega S_{N,p,1} = \omega' S_{N,p,1}$, then $\omega' = \omega \alpha$ for some $\alpha \in S_{N,p,1}$. We can then write $\alpha = \alpha' \omega$ with $a, b \in \mathcal{O}_K$ such that $a, b$ are prime to $Np\mathcal{O}_K$ and $a \equiv b \pmod{Np\mathcal{O}_K}$. So $\omega'b = \omega a \equiv \omega b \pmod{p\mathcal{O}_K}$, from which we have $\omega' \equiv \omega \pmod{p\mathcal{O}_K}$. Thus $\psi$ is a well-defined homomorphism. If $\omega S_{N,p,1} \in \ker(\psi)$ then $\omega \equiv 1 \pmod{p\mathcal{O}_K}$. Since $(N, p) = 1$, we obtain $\omega \equiv 1 \pmod{Np\mathcal{O}_K}$, and so $\psi$ is injective. For given $\omega + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$, we can find $a \in \mathcal{O}_K$ such that $\omega + pa \equiv 1 \pmod{N\mathcal{O}_K}$. Therefore $\psi$ is surjective, and hence the claim is proved. In a similar way, one can show that $S_{N,p,0}^{(i)}/S_{N,p,1}^{(i)} \cong (\mathcal{O}_K/p\mathcal{O}_K)^\times$ for $i = 1, 2, 3$. By [23, Theorem V.1.7]
we derive
\[
| (O_K/pO_K)^x | = \mathcal{N}(pO_K) \cdot \prod_{p \mid pO_K \text{ prime}} \left( 1 - \frac{1}{\mathcal{N}p} \right)
\]
(6.4)
\[
| (O_{K_i}/pO_{K_i})^x | = \mathcal{N}(pO_{K_i}) \cdot \prod_{p \mid pO_{K_i} \text{ prime}} \left( 1 - \frac{1}{\mathcal{N}p} \right)
\]
for \( i = 1, 2, 3 \).

This completes the proof.

Now, we assume that \( N \neq 2, K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \) and \( \left( \frac{d_1d_2}{p} \right) = -1 \). Let \( \varepsilon_0 \) be the fundamental unit of the real quadratic field \( K_3 \). Since \( d_1 \equiv 3 \) (mod 4), the norm of \( \varepsilon_0 \) is 1. We let \( m_0 \) be the smallest positive integer such that \( \varepsilon_0^{m_0} \equiv \pm 1 \) (mod \( N O_K \)), and set
\[
\varepsilon' = \begin{cases} \\
\varepsilon_0^{m_0} & \text{if } N \neq 1 \text{ and } \varepsilon_0^{m_0} \equiv +1 \text{ (mod } N O_K) \\
-\varepsilon_0^{m_0} & \text{if } N \neq 1 \text{ and } \varepsilon_0^{m_0} \equiv -1 \text{ (mod } N O_K) \\
\varepsilon_0 & \text{if } N = 1.
\end{cases}
\]
Further, we let \( n_0 \) be the smallest positive integer for which \( (\varepsilon'_0)^{n_0} \equiv 1 \) (mod \( NpO_K \)). Observe that \( \varepsilon_0 + pO_{K_3} \in \{ \omega + pO_{K_3} \in O_{K_3}/pO_{K_3} \mid N_{K_3/K}(\omega) \equiv 1 \text{ (mod } p) \} \). Hence by Corollary 5.2, if \( \varepsilon'_0 = -\varepsilon_0^{m_0} \), then \( n_0 \) divides \( \frac{p+1}{(m_0, p+1)} \). Otherwise, \( n_0 \) divides \( \frac{p+1}{(m_0, p+1)} \).

**Lemma 6.5.** Let \( N \) be a positive integer and \( p \) be an odd prime such that \( (N, p) = 1 \) and \( \left( \frac{d_1d_2}{p} \right) = -1 \). Assume that \( N \neq 2 \) and \( K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \). Then we deduce
\[
| H_{N,p,0}/S_{N,p,1} | = \begin{cases} \\
n_0 & \text{if } N \neq 1 \\
2n_0 \cdot Q(K) & \text{if } N = 1 \text{ and } n_0 \text{ is odd} \\
n_0 \cdot Q(K) & \text{if } N = 1 \text{ and } n_0 \text{ is even},
\end{cases}
\]
\[
| H_{N,p,0}^{(3)}/S_{N,p,1}^{(3)} | = \begin{cases} \\
n_0 & \text{if } N \neq 1 \text{ or } n_0 \text{ is even} \\
2n_0 & \text{if } N = 1 \text{ and } n_0 \text{ is odd},
\end{cases}
\]
where \( Q(K) = [O_K^x : O_{K_1}^x O_{K_2}^x O_{K_3}^x] \).

**Proof.** By the assumption, \( O_{K_1}^x = O_{K_2}^x = \{ \pm 1 \} \) so that \( O_{K_1}^x O_{K_2}^x O_{K_3}^x = O_{K_3}^x \). Observe that
\[
| H_{N,p,0}/S_{N,p,1} | = | H_{N,p,0}/S_{N,p,1}(S_{N,p,0} \cap O_{K_3}^x) | \cdot | S_{N,p,1}(S_{N,p,0} \cap O_{K_3}^x)/S_{N,p,1} |.
\]
First, we consider the group \( H_{N,p,0}/S_{N,p,1}(S_{N,p,0} \cap O_{K_3}^x) \). Suppose \( N \neq 1 \). Then we claim that \( S_{N,p,0} \cap O_K^x \subset \mathbb{R} \), namely, \( H_{N,p,0} = S_{N,p,1}(S_{N,p,0} \cap O_{K_3}^x) \). Indeed, let \( \varepsilon \in S_{N,p,0} \cap O_K^x \). By Lemma 6.1, we can write
\[
\varepsilon = \frac{1}{2} \left[ a + b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1d_2} \right]
\]
with \( a, b, c, d \in \mathbb{Z} \) such that \( a \equiv b \pmod{2} \), \( c \equiv d \pmod{2} \). Since \( \varepsilon \equiv 1 \pmod{N\mathcal{O}_K} \), we have \( a \equiv 2 \pmod{N} \) and so \( a \neq 0 \). Here we note that

\[
\varepsilon^2 = \frac{1}{4}\left[(a^2 - b^2d_1 - c^2d_2 + d^2d_1d_2 + 2(\sqrt{d_1} + \sqrt{d_2} + (ad - bc)\sqrt{d_1d_2})\right]
\in \mathcal{O}_{K_1}^\times \mathcal{O}_{K_2}^\times \mathcal{O}_{K_3}^\times \subset \mathbb{R}
\]

because \( Q(K) = 1 \) or 2. And, we obtain

\[
(6.5) \quad \begin{align*}
ab + cdd_2 &= 0 \\
ac + bdd_1 &= 0,
\end{align*}
\]

hence \( d(b^2d_1 - c^2d_2) = 0 \). If \( d = 0 \), then \( \varepsilon = 0 \) which enables us to get \( b = c = 0 \). Thus \( \varepsilon = \frac{1}{2}a \in \mathbb{R} \) in this case. Now, suppose that \( d \neq 0 \) and \( b^2d_1 - c^2d_2 = 0 \). Then it follows from (6.5) that \( -\frac{a^2}{dd_2} = \varepsilon = -bddd_1 \), and we have \( b(a^2 - d^2d_1d_2) = 0 \). If \( b = 0 \) then \( c = 0 \), and hence \( \varepsilon = \frac{1}{2}(a + d\sqrt{d_1d_2}) \in \mathbb{R} \). If \( a^2 - d^2d_1d_2 = 0 \), then we obtain

\[
\begin{align*}
N_{K_1/K}(\varepsilon) &= \frac{1}{4}\left[a^2 - b^2d_1 + c^2d_2 - d^2d_1d_2 + 2(ab - cdd_2)\sqrt{d_1}\right] \\
&= \frac{1}{2}(ab - cdd_2)\sqrt{d_1} \\
&\neq \pm 1.
\end{align*}
\]

This contradicts the assumption \( \mathcal{O}_{K_1} = \{\pm 1\} \), and the claim is justified.

If \( N = 1 \), then \( S_{1,p,0} \cap \mathcal{O}_K^\times = \mathcal{O}_K^\times \) and \( S_{1,p,0} \cap \mathcal{O}_{K_3}^\times = \mathcal{O}_{K_3}^\times \). Hence one can show \( S_{1,p,1} \cap \mathcal{O}_K^\times \subset \mathbb{R} \) in a similar fashion as in the above claim. And, we establish

\[
H_{1,p,0}/S_{1,p,0}(S_{1,p,0} \cap \mathcal{O}_{K_3}^\times) = S_{1,p,1}\mathcal{O}_K^\times/S_{1,p,1}\mathcal{O}_{K_3}^\times \\
\cong \mathcal{O}_K^\times/\mathcal{O}_{K_3}^\times(S_{1,p,1} \cap \mathcal{O}_K^\times) \\
\cong \mathcal{O}_K^\times/\mathcal{O}_{K_3}^\times.
\]

Therefore we attain

\[
(6.6) \quad |H_{N,p,0}/S_{N,p,1}(S_{N,p,0} \cap \mathcal{O}_{K_3}^\times)| = \begin{cases} 
1 & \text{if } N \neq 1 \\
Q(K) & \text{if } N = 1.
\end{cases}
\]

Next, we consider the group \( S_{N,p,1}(S_{N,p,0} \cap \mathcal{O}_{K_3}^\times)/S_{N,p,1} \). If \( N \neq 1 \), then \( S_{N,p,0} \cap \mathcal{O}_{K_3}^\times = \{(\varepsilon_0')^n \mid n \in \mathbb{Z}\} \), and hence we have

\[
|S_{N,p,1}(S_{N,p,0} \cap \mathcal{O}_{K_3}^\times)/S_{N,p,1}| = |(\varepsilon_0'S_{N,p,1})| = n_0.
\]

Now, suppose \( N = 1 \). If \( n_0 \) is odd, then \((\varepsilon_0')^n \neq -1 \pmod{p\mathcal{O}_K}\) for all \( n \in \mathbb{Z}_{>0} \). Indeed, if \((\varepsilon_0')^n \equiv -1 \pmod{p\mathcal{O}_K}\) for some \( n \in \mathbb{Z}_{>0} \), then \((\varepsilon_0')^{2n} \equiv 1 \pmod{p\mathcal{O}_K}\). By definition of \( n_0 \) we see that \( n_0 \) divides \( 2n \). Since \( n_0 \) is odd, \( n_0 \) divides \( n \). But \((\varepsilon_0')^n \neq 1 \pmod{p\mathcal{O}_K}\),
so it gives a contradiction. If \( n_0 \) is even, then \( (\varepsilon'_0)^{n_0} \) is the root of the equation \( X^2 \equiv 1 \pmod{p\mathcal{O}_{K_3}} \). Write \( (\varepsilon'_0)^{n_0} = \alpha + \beta \sqrt{d_1d_2} \) with \( \alpha, \beta \in \mathbb{Z} \). Then we get

\[
\alpha^2 + d_1d_2\beta^2 \equiv 1 \pmod{p} \\
2\alpha\beta \equiv 0 \pmod{p}.
\]

If \( p \) divides \( \alpha \), then \( d_1d_2\beta^2 \equiv 1 \pmod{p} \). This contradicts the assumption \( \left( \frac{d_1d_2}{p} \right) = -1 \).

Thus \( p \) divides \( \beta \), and we achieve \( (\varepsilon'_0)^{n_0} \equiv -1 \pmod{p\mathcal{O}_K} \) by the minimality of \( n_0 \). Since \( \mathcal{O}^\times_{K_3} = \{ \pm (\varepsilon'_0)^n \mid n \in \mathbb{Z} \} \), we derive that

\[
S_{1,p,1}(S_{1,p,0} \cap \mathcal{O}^\times_{K_3})/S_{1,p,1} = S_{1,p,1}\mathcal{O}_{K_3}^{\times}/S_{1,p,1} \cong \begin{cases} 
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n_0\mathbb{Z} & \text{if } n_0 \text{ is odd} \\
\mathbb{Z}/n_0\mathbb{Z} & \text{if } n_0 \text{ is even.}
\end{cases}
\]

And, we deduce

\[
(6.7) \quad |S_{N,p,1}(S_{N,p,0} \cap \mathcal{O}^\times_{K_3})/S_{N,p,1}| = \begin{cases} 
n_0 & \text{if } N \neq 1 \text{ or } n_0 \text{ is even} \\
2n_0 & \text{if } N = 1 \text{ and } n_0 \text{ is odd.}
\end{cases}
\]

Therefore, the lemma follows from \((6.6)\) and \((6.7)\).

**Corollary 6.6.** With the notations and assumptions as in Lemma 6.3, we get

\[
\left[ K_{(Np)} : K_{(N)} \right] = \begin{cases} 
\frac{(p+1)^2(p-1)^2}{n_0^2} & \text{if } N \neq 1 \\
\frac{(p+1)^2(p-1)^2}{2n_0^2} & \text{if } N = 1 \text{ and } n_0 \text{ is odd} \\
\frac{(p+1)^2(p-1)^2}{n_0^2Q(K)} & \text{if } N = 1 \text{ and } n_0 \text{ is even,}
\end{cases}
\]

\[
\left[ (K_{3})_{(Np)} : (K_{3})_{(N)} \right] = \begin{cases} 
\frac{(p+1)(p-1)}{n_0^2} & \text{if } N \neq 1 \text{ or } n_0 \text{ is even} \\
\frac{(p+1)(p-1)}{2n_0} & \text{if } N = 1 \text{ and } n_0 \text{ is odd.}
\end{cases}
\]

**Proof.** Since \( \left( \frac{d_1d_2}{p} \right) = -1 \), \( p\mathcal{O}_{K_3} \) is a prime ideal of \( K_3 \) and \( p\mathcal{O}_K = p_1p_2 \) for some prime ideals \( p_1 \neq p_2 \) of \( K \). And, by Lemma 6.4 we have

\[
(6.8) \quad |S_{N,p,0}/S_{N,p,1}| = p^4 \cdot \left( 1 - \frac{1}{p^2} \right) = (p+1)^2(p-1)^2 \\
|S^{(3)}_{N,p,0}/S^{(3)}_{N,p,1}| = p^2 \cdot \left( 1 - \frac{1}{p^2} \right) = (p+1)(p-1).
\]

Then the corollary is an immediate consequence of \((6.1)\), \((6.8)\) and Lemma 6.3.

For \( i = 1, 2 \), let

\[
W^{i}_{N,p,0} = \begin{cases} 
\{ \omega \in S_{N,p,0} \mid N_{K/K_i}(\omega) \equiv 1 \pmod{Np\mathcal{O}_{K_i}} \} & \text{if } N \neq 1 \\
\{ \omega \in S_{1,p,0} \mid N_{K/K_i}(\omega) \equiv \pm 1 \pmod{p\mathcal{O}_{K_i}} \} & \text{if } N = 1,
\end{cases}
\]
and let

$$W_{N,p,0}^3 = \begin{cases} 
\{ \omega \in S_{N,p,0} \mid N_{K/K_3}(\omega) \equiv (\varepsilon_0')^n \pmod{npO_{K_3}} \text{ for some } n \in \mathbb{Z} \} & \text{if } N \neq 1 \\
\{ \omega \in S_{1,p,0} \mid N_{K/K_3}(\omega) \equiv \pm(\varepsilon_0')^n \pmod{pO_{K_3}} \text{ for some } n \in \mathbb{Z} \} & \text{if } N = 1,
\end{cases}$$

so that $\ker(\varphi_{N,p,0}) = W_{N,p,0}^i/H_{N,p,0}$ for $i = 1, 2, 3$. Further, let

$$W_{N,p,0}^{ij} = W_{N,p,0}^i \cap W_{N,p,0}^j \quad \text{for } 1 \leq i < j \leq 3,$$

$$W_{N,p,0} = \bigcap_{i=1}^{3} W_{N,p,0}^i,$$

and so $\ker(\varphi_{N,p,0}) = W_{N,p,0}^{ij}/H_{N,p,0}$ and $\ker(\varphi_{N,p,0}) = W_{N,p,0}/H_{N,p,0}$. Here, we mean by $W_{N,p,0}$, $W_{N,p,0}^{ij}$ and $W_{N,p,0}$ the images of $W_{N,p,0}/S_{N,p,0}$, $W_{N,p,0}/S_{N,p,1}$ and $W_{N,p,0}/S_{N,p,1}$, respectively, in $(O_K/pO_K)^{\times}$ via the isomorphism $\{O_K/pO_K\}$.

**Theorem 6.7.** Let $K$ and $K_i$ ($1 \leq i \leq 3$) be as above. Let $N$ be a positive integer and $p$ be an odd prime such that $(N, p) = 1$, $p \equiv 1 \pmod{4}$ and $\left(\frac{d_1d_2}{p}\right) = -1$. Assume that $N \neq 2$ and $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. Then we deduce

$$\left[K(N_p) : K_{N,p,0}\right] = \begin{cases} 
\frac{p+1}{n_0} & \text{if } N \neq 1 \\
\frac{n_0}{2(p+1)} & \text{if } N = 1 \text{ and } n_0 \text{ is odd} \\
\frac{n_0}{4(p+1)} & \text{if } N = 1 \text{ and } n_0 \text{ is even},
\end{cases}$$

$$\left[K(N_p) : K_{N,p,0}\right] = \begin{cases} 
2 & \text{if } N \neq 1 \text{ and } n_0 \text{ is odd} \\
1 & \text{if } N \neq 1 \text{ and } n_0 \text{ is even} \\
\frac{4}{Q(K)} & \text{if } N = 1.
\end{cases}$$

Hence, $K_{N,p,0} = K_{N,p,0}^{1/2}$ if and only if $n_0 = \frac{p+1}{2}$ or $p+1$.

**Proof.** Let

$$W_{N,p,0}^i' = \{ \omega + pO_K \in (O_K/pO_K)^{\times} \mid N_{K/K_i}(\omega) \equiv 1 \pmod{pO_{K_i}} \} \quad \text{for } i = 1, 2, 3,$$

$$W_{N,p,0}^{ij}' = W_{N,p,0}^i' \cap W_{N,p,0}^j' \quad \text{for } 1 \leq i < j \leq 3,$$

$$W_{N,p,0}' = W_{N,p,0}^1' \cap W_{N,p,0}^2' \cap W_{N,p,0}^3',$$

and let $i_0, i'_0 \in \{1, 2\}$ such that $\left(\frac{-d_{i_0}}{p}\right) = 1$ and $\left(\frac{-d_{i'_0}}{p}\right) = -1$. By the assumption there exist $A, D_{i_0} \in \mathbb{Z}/p\mathbb{Z}$ for which $A^2 \equiv -1 \pmod{p}$ and $D_{i_0}^2 \equiv -d_{i_0} \pmod{p}$. For $\omega + pO_K \in O_K/pO_K$ we can write $\omega = a + b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1d_2}$ with $a, b, c, d \in \mathbb{Z}$ due to the fact $(2, p) = 1$. 

20
First, we consider the group \( \hat{W}_{N,p,0}^{1,2} \). If \( \omega + p\mathcal{O}_K \in \hat{W}_{N,p,0}^{1,2} \), then we have

\[
\begin{align*}
\text{(6.9)} & \\
a^2 - b^2d_1 + c^2d_2 - d^2d_1d_2 & \equiv 1 \pmod{p} \\
ab - cdd_2 & \equiv 0 \pmod{p},
\end{align*}
\]

and

\[
\begin{align*}
\text{(6.10)} & \\
a^2 + b^2d_1 - c^2d_2 - d^2d_1d_2 & \equiv 1 \pmod{p} \\
ac - bdd_1 & \equiv 0 \pmod{p}.
\end{align*}
\]

Since \( c^2dd_2 \equiv abc \equiv b^2dd_1 \pmod{p} \), we obtain \( d(b^2d_1 - c^2d_2) \equiv 0 \pmod{p} \). If \( b^2d_1 - c^2d_2 \equiv 0 \pmod{p} \), then \( p \) must divide \( b, c \) because \( \left( \frac{d}{p} \right) = -1 \). Thus we get \( a^2 - d^2d_1d_2 \equiv 1 \pmod{p} \). If \( b^2d_1 - c^2d_2 \not\equiv 0 \pmod{p} \) and \( d \equiv 0 \pmod{p} \), then \( ab \equiv ac \equiv 0 \pmod{p} \) and so \( a \equiv 0 \pmod{p} \). But it follows from (6.9), (6.10) that \( b^2d_1 - c^2d_2 \equiv -1 \equiv 1 \pmod{p} \), which is a contradiction. Therefore we derive

\[
\hat{W}_{N,p,0}^{1,2} \sim \begin{cases}
\{ a + d\sqrt{d_1d_2} + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid a^2 - d^2d_1d_2 \equiv 1 \pmod{p} \} & \\
\sim \{ \omega + p\mathcal{O}_{K_3} \in (\mathcal{O}_{K_3}/p\mathcal{O}_{K_3})^\times \mid N_{K_3/Q}(\omega) \equiv 1 \pmod{p} \} & \\
\sim \mathbb{Z}/(p+1)\mathbb{Z} & \text{(by Corollary 5.2)}. 
\end{cases}
\]

If \( N \neq 1 \), then \( \hat{W}_{N,p,0}^{1,2} = \hat{W}_{N,p,0}^{1,2} \) and by Lemma 6.5 we attain

\[
\left[ K_{(Np)} : \hat{K}_{N,p,0}^{1,2} \right] = \left| \hat{W}_{N,p,0}^{1,2} / H_{N,p,0} \right| = \frac{|\hat{W}_{N,p,0}^{1,2}|}{|H_{N,p,0}|} = \frac{p + 1}{n_0}.
\]

If \( N = 1 \), then since \( N_{K/K_{i_0}}(D_{i_0}^{-1}\sqrt{-d_{i_0}}) \equiv 1 \pmod{p\mathcal{O}_{K_{i_0}}}, \ N_{K/K_{i_0}}(D_{i_0}^{-1}\sqrt{-d_{i_0}}) \equiv -1 \pmod{p\mathcal{O}_{K_{i_0}}}, \) and \( N_{K/K_1}(A) \equiv -1 \pmod{p\mathcal{O}_K} \) for \( i = 1, 2 \); hence we achieve

\[
\text{(6.11)} \hat{W}_{1,p,0}^{1,2} = \bigcup_{0 \leq i, j < 2} A^i(D_{i_0}^{-1}\sqrt{-d_{i_0}})j \cdot \hat{W}_{1,p,0}^{1,2}.
\]

Thus \( \left| \hat{W}_{1,p,0}^{1,2} \right| = 4(p + 1) \), and so by Lemma 6.5 we derive

\[
\left[ K_{(p)} : \hat{K}_{1,p,0}^{1,2} \right] = \left| \hat{W}_{1,p,0}^{1,2} / H_{1,p,0} \right| = \frac{|\hat{W}_{1,p,0}^{1,2}|}{|H_{1,p,0}|} = \left\{ \begin{array}{ll}
\frac{2(p+1)}{n_0 Q(K)} & \text{if } n_0 \text{ is odd} \\
\frac{4(p+1)}{n_0 Q(K)} & \text{if } n_0 \text{ is even}.
\end{array} \right.
\]

Next, we consider the group \( \hat{W}_{N,p,0}^{1,2} \). If \( \omega + p\mathcal{O}_K \in \hat{W}_{N,p,0}^{1,2} \), then \( \omega \) satisfies (6.9), (6.10) and

\[
\text{(6.12)} \begin{align*}
a^2 + b^2d_1 + c^2d_2 + d^2d_1d_2 & \equiv 1 \pmod{p} \\
ad + bc & \equiv 0 \pmod{p}.
\end{align*}
\]
Since $\omega + p\mathcal{O}_K \in \widetilde{W}_{N,p,0}$, we get $a^2 - d^2d_1d_2 \equiv 1 \pmod{p}$ and $b, c \equiv 0 \pmod{p}$. And, by Lemma 6.5, we have $a \equiv \pm 1 \pmod{p}$ and $d \equiv 0 \pmod{p}$, so we conclude

$$\widetilde{W}_{N,p,0} = \{ \pm 1 + p\mathcal{O}_K \} \cong \mathbb{Z}/2\mathbb{Z}.$$ 

Let $\omega_0$ be an element of $\mathcal{O}_{K_3}$ such that $\omega_0 + p\mathcal{O}_K$ is a generator of $\widetilde{W}_{N,p,0}$. Observe that $N_{K/K_3}(\omega_0) \equiv 1 \pmod{p\mathcal{O}_K_i}$ for $i = 1, 2$, and

$$\widetilde{W}_{N,p,0} = \{ \pm 1 + p\mathcal{O}_K \} \times \langle \omega_0^2 + p\mathcal{O}_K \rangle.$$ 

Suppose $N \neq 1$. If $n_0$ is odd, then $(\varepsilon_0')^n \not\equiv -1 \pmod{p\mathcal{O}_K}$ for all $n \in \mathbb{Z}_{>0}$ as in the proof of Lemma 6.5. Hence $\varepsilon_0' + p\mathcal{O}_K \in \langle \omega_0^2 + p\mathcal{O}_K \rangle \cong \mathbb{Z}/(p^2+1)\mathbb{Z}$, and so $\langle \varepsilon_0' + p\mathcal{O}_K \rangle = \langle (\varepsilon_0')^2 + p\mathcal{O}_K \rangle$ because $\frac{p^2+1}{2}$ is odd. Since $N_{K/K_3}(\varepsilon_0') \equiv (\varepsilon_0')^2 \pmod{p\mathcal{O}_K}$, we deduce

$$\widetilde{W}_{N,p,0} = \bigsqcup_{0 \leq i < n_0} (\varepsilon_0')^i \cdot \widetilde{W}_{N,p,0},$$ 

and hence $|\widetilde{W}_{N,p,0}| = 2n_0$ in this case. If $n_0$ is even, then $(\varepsilon_0')^{\frac{p^2+1}{2}} \equiv -1 \pmod{p\mathcal{O}_K}$ again as in the proof of Lemma 6.5. Hence $\varepsilon_0' + p\mathcal{O}_K \not\in \langle \omega_0^2 + p\mathcal{O}_K \rangle$, and so

$$N_{K/K_3}(\varepsilon_0') \equiv \omega_0^2 \not\equiv \varepsilon_0' \pmod{p\mathcal{O}_K}$$ 

for all $\ell \in \mathbb{Z}_{>0}$. Thus we have the decomposition

$$\widetilde{W}_{N,p,0} = \bigsqcup_{0 \leq i < \frac{p^2+1}{2}} (\varepsilon_0')^i \cdot \widetilde{W}_{N,p,0},$$ 

and $|\widetilde{W}_{N,p,0}| = n_0$ in this case. Therefore, by Lemma 6.5 we conclude that

$$\left[ K_{(N_p)} : K_{N,p} \right] = |\widetilde{W}_{N,p,0}/H_{N,p,0}| = \frac{|\widetilde{W}_{N,p,0}|}{|H_{N,p,0}/S_{N,p,1}|} = \begin{cases} 2 & \text{if } N \neq 1 \text{ and } n_0 \text{ is odd} \\ 1 & \text{if } N \neq 1 \text{ and } n_0 \text{ is even.} \end{cases}$$

Now, suppose $N = 1$. If $n_0$ is odd, then $\varepsilon_0' + p\mathcal{O}_K \in \langle \omega_0^2 + p\mathcal{O}_K \rangle$, and so $\langle \varepsilon_0' + p\mathcal{O}_K \rangle = \langle (\varepsilon_0')^2 + p\mathcal{O}_K \rangle$. Since $-1 + p\mathcal{O}_K \not\in \langle \omega_0^2 + p\mathcal{O}_K \rangle$, there does not exist $\omega \in \mathcal{O}_K$ such that $N_{K/K_3}(\omega) \equiv 1 \pmod{p\mathcal{O}_K_i}$ for $i = 1, 2$ and $N_{K/K_3}(\omega) \equiv -1 \pmod{p\mathcal{O}_K_3}$. Therefore we attain

$$\widetilde{W}_{1,p,0} = \bigsqcup_{0 \leq i < n_0} (\varepsilon_0')^i A^i(D_{i_0}^{-1}\sqrt{-d_{i_0}})^k \cdot \widetilde{W}_{1,p,0},$$ 

from which we get $|\widetilde{W}_{1,p,0}| = 8n_0$. If $n_0$ is even, then $\varepsilon_0' + p\mathcal{O}_K \not\in \langle \omega_0^2 + p\mathcal{O}_K \rangle$ and

$$\{ \pm (\varepsilon_0')^n + p\mathcal{O}_K \mid n \in \mathbb{Z} \} = \{ (\varepsilon_0')^n + p\mathcal{O}_K \mid n \in \mathbb{Z} \}.$$
In a similar fashion as above, one can show that
\[ \widetilde{W}_{1,p,0} = \bigcup_{0 \leq i < \frac{n_0}{2}} \bigcup_{0 \leq j,k < 2} (\varepsilon_i' + p\mathcal{O}_K)^j \cdot \widetilde{W}_{1,p,0}', \]
and so \( |\widetilde{W}_{1,p,0}| = 4n_0. \) And, by Lemma \[6.5\] we claim that
\[ [K(p) : \tilde{K}_{1,p,0}] = |\widetilde{W}_{1,p,0}/H_{1,p,0}| = \frac{|\widetilde{W}_{1,p,0}|}{|H_{1,p,0}/S_{1,p,1}|} = \frac{4}{Q(K)}. \]
This proves the theorem. \( \square \)

From now on we adopt the notations and assumptions in Theorem \[6.7\]. Further, we assume that \( n_0 = \frac{p+1}{2} \) or \( p + 1 \). Observe that
\[ (6.13) \quad \langle \varepsilon_0' + p\mathcal{O}_K \rangle = \begin{cases} \langle \omega_0^2 + p\mathcal{O}_K \rangle & \text{if } n_0 = \frac{p+1}{2} \\ \widetilde{W}_{N,p,0}' & \text{if } n_0 = p + 1, \end{cases} \]
and \( \langle \varepsilon_0'^2 + p\mathcal{O}_K \rangle = \langle \omega_0'^2 + p\mathcal{O}_K \rangle \) because \( \frac{p+1}{2} \) is odd. Moreover, if \( N = 1 \) then
\[ (6.14) \quad \{ \pm(\varepsilon_0')^n + p\mathcal{O}_K \mid n \in \mathbb{Z} \} = \widetilde{W}_{N,p,0}'^{1,2}. \]
Using \[6.9\], \[6.10\] and \[6.12\] one can show that
\[ (6.15) \quad \widetilde{W}_{N,p,0}'^{1,3} = \left\{ a + c\sqrt{-d_2} + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid a^2 - c^2(-d_2) \equiv 1 \pmod{p} \right\} \]
\[ \widetilde{W}_{N,p,0}'^{2,3} = \left\{ a + b\sqrt{-d_1} + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid a^2 - b^2(-d_1) \equiv 1 \pmod{p} \right\}. \]
And, \( \widetilde{W}_{N,p,0}'^{1,3} \cong \mathbb{Z}/(p + 1)\mathbb{Z} \) and \( \widetilde{W}_{N,p,0}'^{2,3} \cong \mathbb{Z}/(p - 1)\mathbb{Z} \) by Corollary \[5.2\]. Suppose \( N \neq 1 \).

Since \( N_K/K_3(D_{i_0}^{-1}\sqrt{-d_{i_0}}) \equiv -1 \pmod{p\mathcal{O}_K} \), we derive from \[6.13\] that
\[ (6.16) \quad \widetilde{W}_{N,p,0}'^{1,3} = \bigcup_{0 \leq i < \frac{n_0}{2}} \bigcup_{0 \leq j < 2} (\varepsilon_i') \cdot \widetilde{W}_{N,p,0}'^{1,3}, \quad \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2} \]
\[ \bigcup_{0 \leq i < \frac{n_0}{2}} (\varepsilon_i')^j (D_{i_0}^{-1}\sqrt{-d_{i_0}})^j \cdot \widetilde{W}_{N,p,0}'^{1,3}, \quad \text{if } N \neq 1 \text{ and } n_0 = p + 1. \]

Similarly, when \( N = 1 \), by \[6.14\] we have
\[ (6.17) \quad \widetilde{W}_{1,p,0}'^{1,3} = \bigcup_{0 \leq i < \frac{n_0}{2}} \bigcup_{0 \leq j,k < 2} (\varepsilon_i')^j A^k(D_{i_0}^{-1}\sqrt{-d_{i_0}})^k \cdot \widetilde{W}_{1,p,0}'^{1,3}. \]
Therefore, we achieve by Lemma 6.5

\[
(6.18) \quad \left[ K_{(N)} : \overline{K}_{N,p,0}^{i=3} \right] = \frac{|\overline{W}_{N,p,0}^{i=3}|}{|H_{N,p,0}/S_{N,1}|} = \left\{ \begin{array}{ll}
p + 1 & \text{if } N \neq 1 \\
\frac{2(p+1)}{Q(K)} & \text{if } N = 1. \end{array} \right.
\]

Let \( B \in \mathcal{O}_K \) such that

\[
B \equiv \frac{p + 1}{2} \cdot A \left[ (1 + d_i^{-1}) \sqrt{-d_i} + D_i^{-1}(1 - d_i^{-1}) \sqrt{d_i} \right] \pmod{p\mathcal{O}_K}.
\]

Here, \( d_i^{-1} \) is the inverse of \( d_i \) in \( \mathbb{Z}/p\mathbb{Z} \). Then we get \( N_{K/K_i}(B) \equiv 1 \pmod{p\mathcal{O}_{K_i}} \) and \( N_{K/K_3}(B) \equiv -1 \pmod{p\mathcal{O}_{K_3}} \). In a similar way as in the above, one can show that

\[
(6.19) \quad \overline{W}_{N,p}^{i=3} = \left\{ \begin{array}{ll}
\bigcup_{0 \leq i < \frac{p+1}{2}} (\varepsilon_0^i) \cdot \overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2} \\
\bigcup_{0 \leq i < \frac{p+1}{2}, 0 \leq j < 2} (\varepsilon_0^i)^j B \cdot \overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = p+1 \\
\bigcup_{0 \leq i < \frac{p+1}{2}, 0 \leq j, k < 2} (\varepsilon_0^i)^j A^j B^k \cdot \overline{W}_{1,p,0}^{i=3} & \text{if } N = 1,
\end{array} \right.
\]

and hence we claim that

\[
(6.20) \quad \left[ K_{(N)} : \overline{K}_{N,p,0}^{i=3} \right] = \frac{|\overline{W}_{N,p,0}^{i=3}|}{|H_{N,p,0}/S_{N,1}|} = \left\{ \begin{array}{ll}
p - 1 & \text{if } N \neq 1 \\
\frac{2(p-1)}{Q(K)} & \text{if } N = 1. \end{array} \right.
\]

Let \( \overline{W}_{N,p,0}^0 = \{ \omega + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid N_{K/K_3}(\omega) \equiv 1 \pmod{p} \} \) and let \( \overline{K}_{N,p,0} \) be the class fields of \( K \) corresponding to the inverse image of \( \overline{W}_{N,p,0}^0 \) via the isomorphism \( (B.3) \). Note that \( \overline{W}_{N,p,0}^i \subset \overline{W}_{N,p,0}^0 \) for \( i = 1, 2, 3 \). It then follows from Corollary 5.2 that

\[
\overline{W}_{N,p,0}^0 = \left\{ \omega + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid N_{K/K_3}(\omega) \equiv \omega_0^n \pmod{p\mathcal{O}_{K_3}} \text{ for some } n \in \mathbb{Z}_{>0} \right\}
\]

\[
= \left\{ \begin{array}{ll}
\overline{W}_{N,p,0}^0 & \text{if } N \neq 1 \text{ and } n_0 = p+1, \text{ or } N = 1 \\
\bigcup_{0 \leq i < 2} (D_{n_0}^{-1} \sqrt{-d_{n_0}^i}) \cdot \overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2}.
\end{array} \right.
\]

Similarly, we get

\[
\overline{W}_{N,p,0}^{i=0} = \left\{ \begin{array}{ll}
\overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = p+1, \text{ or } N = 1 \\
\bigcup_{0 \leq i < 2} (D_{n_0}^{-1} \sqrt{-d_{n_0}^i}) \cdot \overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2},
\end{array} \right.
\]

\[
\overline{W}_{N,p,0}^{i=0} = \left\{ \begin{array}{ll}
\overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = p+1, \text{ or } N = 1 \\
\bigcup_{0 \leq i < 2} B^i \cdot \overline{W}_{N,p,0}^{i=3} & \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2}.
\end{array} \right.
\]
Therefore, we conclude that (6.21)
\[
\left[ K_{N,p,0}^{i_0,3} : K_{N,p,0}^{i_0} \right] = \left[ K_{N,p,0}^{i_0,3} : K_{N,p,0}^{i_0} \right] = \left[ K_{N,p,0}^{i_0,3} : K_{N,p,0}^{i_0} \right] = \begin{cases} 1 & \text{if } N \neq 1 \text{ and } n_0 = p + 1, \text{ or } N = 1 \\ 2 & \text{if } N \neq 1 \text{ and } n_0 = \frac{p+1}{2}. \end{cases}
\]

**Lemma 6.8.** Let \( p \) be an odd prime such that \( \left( \frac{d_1 d_2}{p} \right) = -1 \). Then the norm map
\[
\tilde{N}_{K/Q} : (O_K/pO_K)^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\
\omega + pO_K \longmapsto N_{K/Q}(\omega) + p\mathbb{Z}
\]
is surjective.

**Proof.** We use the same notations as in the proof of Theorem 6.7. For each index \( 1 \leq i \leq 3 \), we define the norm map \( \tilde{N}_{K/K_i} : (O_K/pO_K)^\times \rightarrow (O_{K_i}/pO_{K_i})^\times \) by
\[
\tilde{N}_{K/K_i}(\omega + pO_K) = N_{K/K_i}(\omega) + pO_{K_i}.
\]
For \( \omega + pO_K \in \ker(\tilde{N}_{K/K_i}) \) we have \( N_{K/Q}(\omega) \equiv 1 \pmod{p} \), and so \( N_{K/K_3}(\omega) \equiv \omega_0^n \pmod{pO_{K_3}} \) for some integer \( 0 \leq n < p + 1 \). Thus we derive
\[
\ker(\tilde{N}_{K/K_i}) = W_{N,p,0}^{i_0,3} = \bigsqcup_{0 \leq i < \frac{p+1}{2}} \omega_0^i (D_{i_0}^{-1} \sqrt{-d_{i_0}})^j \cdot W_{N,p,0}^{i_0,3},
\]
from which we get \( |\ker(\tilde{N}_{K/K_i})| = (p + 1)^2 \). And, we see from (6.4) that
\[
|\left( O_K/pO_K \right)^\times | = (p + 1)^2(p - 1)^2 \\
|\left( O_{K,i_0}/pO_{K,i_0} \right)^\times | = (p - 1)^2.
\]
Therefore,
\[
|\text{Im}(\tilde{N}_{K/K_i})| = \frac{|\left( O_K/pO_K \right)^\times |}{|\ker(\tilde{N}_{K/K_i})|} = \frac{|\left( O_{K,i_0}/pO_{K,i_0} \right)^\times |}{|\ker(\tilde{N}_{K/K_i})|},
\]
and hence \( \tilde{N}_{K/K_{i_0}} \) is surjective. Since \( \tilde{N}_{K/Q} = \tilde{N}_{K_{i_0}/Q} \circ \tilde{N}_{K/K_{i_0}} \), the lemma follows from Corollary 5.2.

**Remark 6.9.** In like manner one can show that all \( \tilde{N}_{K/K_i} \) are surjective.

We obtain by Lemma 6.8
\[
|W_{N,p,0}^{i_0}| = \frac{|\text{Im}(\tilde{N}_{K/Q})|}{|\ker(\tilde{N}_{K/Q})|} = \frac{|\left( O_K/pO_K \right)^\times |}{|\left( \mathbb{Z}/p\mathbb{Z} \right)^\times |} = (p + 1)^2(p - 1).
\]
And,
\[
(6.22) \quad \left[ K_{N,p,0}^{i_0} : K(N) \right] = \frac{[K_{N,p} : K(N)]}{[K_{N,p} : K_{N,p,0}]} = \frac{|\left( O_K/pO_K \right)^\times |}{|W_{N,p,0}^{i_0}|} = p - 1.
\]
By (6.18), (6.20), (6.21), (6.22), Corollary 6.6 and Theorem 6.7 we derive the following three diagrams:

(i) when \( N \neq 1 \) and \( n_0 = \frac{p+1}{2} \)

\[
K_{(Np)} = \overline{K}^{1,2}_{N,p,0}
\]

\[
K_{N,p,0} \quad K^{3}_{N,p,0} \quad K^{0}_{N,p,0} \quad K^{0}_{N,p,0}
\]

(ii) when \( N \neq 1 \) and \( n_0 = p + 1 \)

\[
K_{(N)} = \overline{K}^{i_0}_{N,p,0}
\]

\[
K_{N,p,0} \quad K^{3}_{N,p,0} \quad K^{0}_{N,p,0}
\]
(iii) when \( N = 1 \) and \( n_0 = \frac{p+1}{2} \) or \( p+1 \).

Hence \( \widetilde{K}_{3,N,p,0} \) is contained in \( \widetilde{K}_{i,N,p,0} \) for \( i = 1, 2 \) if and only if \( N \neq 1 \) and \( n_0 = p+1 \), or \( N = 1 \) and \( n_0 = \frac{p+1}{2} \) or \( p+1 \).

For \( i = 1, 2 \), let \( L_i \) be a finite abelian extension of \( K_i \), which is the fixed field of the subgroup
\[
\left\{ \left( \frac{(K_i)_{(Np)}/K_i}{\omega} \right) \mid \omega \in \mathcal{O}_{K_i}, \ \omega \equiv 1 \pmod {N\mathcal{O}_{K_i}}, N_{K_i/Q}(\omega) \equiv 1 \pmod p \right\}
\]
of \( \text{Gal}((K_i)_{(Np)})/(K_i)_{(N)}) \).

**Lemma 6.10.** Let \( N \neq 2 \) be a positive integer and \( p \) be an odd prime such that \( (N,p) = 1, p \equiv 1 \pmod 4 \) and \( \left( \frac{d_1d_2}{p} \right) = -1 \). Assume that \( K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \) and \( N \neq 1 \) and \( n_0 = p+1 \), or \( N = 1 \) and \( n_0 = \frac{p+1}{2} \) or \( p+1 \). Then we have
\[
\widetilde{K}_{3,N,p,0} = K_{(N)L_i} \text{ for } i = 1, 2.
\]

**Proof.** By Corollary 5.2 we get
\[
\{ \omega + p\mathcal{O}_{K_i} \in (\mathcal{O}_{K_i}/p\mathcal{O}_{K_i})^\times \mid N_{K_i/Q}(\omega) \equiv 1 \pmod p \} \cong \begin{cases} 
\mathbb{Z}/(p-1)\mathbb{Z} & \text{if } i = i_0 \\
\mathbb{Z}/(p+1)\mathbb{Z} & \text{if } i = i_0'.
\end{cases}
\]

Since for \( i = 1, 2 \)
\[
(6.23) \quad |H_{N,p,0}^{(i)}/S_{N,p,1}^{(i)}| = \begin{cases} 
1 & \text{if } N \neq 1 \\
2 & \text{if } N = 1,
\end{cases}
\]
we have
\[
[(K_{i_0})(Np) : L_{i_0}] = \begin{cases} 
p - 1 & \text{if } N \neq 1 \\
\frac{p-1}{2} & \text{if } N = 1,
\end{cases}
\]
(6.24)
\[
[(K'_{i_0})(Np) : L'_{i_0}] = \begin{cases} 
p + 1 & \text{if } N \neq 1 \\
\frac{p+1}{2} & \text{if } N = 1.
\end{cases}
\]

Now, consider the composite field $K(N)L_i$. By (6.21) we get
\[
\text{Gal}(K(Np)/\tilde{K}_{N,p,0}^3) = \left\{ \frac{(K_{i_0})/K}{(\omega)} \mid \omega \in O_K, \omega \equiv 1 \pmod{NO_K} \right\}.
\]
Thus for all $\alpha \in L_i$ and $\left( \frac{(K_{i_0})/K}{(\omega)} \right) \in \text{Gal}(K(Np)/\tilde{K}_{N,p,0}^3)$ we achieve
\[
\alpha \left( \frac{(K_{i_0})/K}{(\omega)} \right) = \alpha \left( \frac{(K_{i_0})/K}{(\omega)} \right) = \alpha,
\]
and $K(N)L_i \subseteq \tilde{K}_{N,p,0}^3$. By Lemma 6.2 and (6.24) we obtain
\[
[\tilde{K}_{N,p,0}^3 : K(N)L_i] \leq [(K_i)(Np) : L_i] = [\tilde{K}_{N,p,0}^3 : \tilde{K}_{N,p,0}^3],
\]
which yields $\tilde{K}_{N,p,0}^3 = K(N)L_i$ for $i = 1, 2$.

**Lemma 6.11.** With the notations and assumptions as in Lemma 6.10, for any positive integer $n$ and $i = 1, 2$ the singular value $N_{\tilde{K}_{N,p,0}^3/K_{N,p,0}^3}(\gamma_{1,i}^n)$ is a real algebraic integer. Moreover,
\[
N_{\tilde{K}_{N,p,0}^3/K_{N,p,0}^3}(\gamma_{1,i}^n)^{\sigma} \in \mathbb{R} \text{ for } \sigma \in \text{Gal}(\tilde{K}_{N,p,0}^3/K(N)).
\]
**Proof.** Since $\gamma_{1,i}^n$ is an algebraic integer by Proposition 4.4, so is $N_{\tilde{K}_{N,p,0}^3/K_{N,p,0}^3}(\gamma_{1,i}^n)$. Note that $\text{Gal}((K_i)(Np)/L_i)$ is the restriction of $\text{Gal}(\tilde{K}_{N,p,0}^3/K_{N,p,0}^3)$ to the field $(K_i)(Np)$ by Lemma 6.10 and so we have
\[
N_{\tilde{K}_{N,p,0}^3/K_{N,p,0}^3}(\gamma_{1,i}^n) = N_{(K_i)(Np)/L_i}(\gamma_{1,i}^n).
\]
(6.25)
On the other hand, it follows from (6.23), (6.24) and Lemma 6.4 that
\[
\left[ L_i : (K_i)(N) \right] = p - 1 = \left[ \tilde{K}_{N,p,0}^3 : K(N) \right].
\]
Since $\tilde{K}_{N,p,0}^3 = K(N)L_i$, it suffices to show by (6.25) that
\[
N_{(K_i)(Np)/L_i}(\gamma_{1,i}^n)^{\sigma} \in \mathbb{R} \text{ for } \sigma \in \text{Gal}(L_i/(K_i)(N)).
\]
Here we observe that
\[
\text{Gal}(L_i/(K_i)_{(N)}) = \left\{ \frac{L_i/K_i}{(\omega)} \mid \omega \in \mathcal{O}_{K_i}, \omega \equiv 1 \pmod{N\mathcal{O}_{K_i}} \right\},
\]
where \(\frac{(K_i)_{(Np)}/K_i}{(\omega)}\) runs over the group
\[
\text{Gal}((K_i)_{(Np)}/L_i) = \left\{ \frac{(K_i)_{(Np)}/K_i}{(\omega)} \mid \omega \in \mathcal{O}_{K_i}, \omega \equiv 1 \pmod{N\mathcal{O}_{K_i}} \right\}.
\]

Let \(\omega'\) be an element of \(\mathcal{O}_{K_i}\) for which \(\omega \equiv 1 \pmod{N\mathcal{O}_{K_i}}\) and \(N_{K_i/Q}(\omega) \equiv C \pmod{p}\) for some \(C \in (\mathbb{Z}/p\mathbb{Z})^\times\). Then we derive
\[
N_{(K_i)_{(Np)}/L_i}(\gamma^n_{1,i})^{(L_i/K_i)/(\omega')} = \prod_{\omega} g_{(0,\frac{1}{Np})}(\theta_i)^{\frac{(K_i)_{(Np)}/K_i}{(\omega)}},
\]
where \(\frac{(K_i)_{(Np)}/K_i}{(\omega)}\) runs over the set
\[
\left\{ \frac{(K_i)_{(Np)}/K_i}{(\omega)} \mid \omega \in \mathcal{O}_{K_i}, \omega \equiv 1 \pmod{N\mathcal{O}_{K_i}} \right\}.
\]

Write \(\omega' = a\theta_i + b\) with \(a, b \in \mathbb{Z}\). Then \(a \equiv 0 \pmod{N}\), \(b \equiv 1 \pmod{N}\) and by Proposition 4.2 we obtain
\[
g_{(0,\frac{1}{Np})}(\theta_i)^{\frac{(K_i)_{(Np)}/K_i}{(\omega)}} = g_{(0,\frac{1}{Np})}(\theta_i).
\]

If \(i = 1\), then by Proposition 4.1 and Lemma 4.3 we attain
\[
g_{(\frac{a}{Np},\frac{b}{Np})}(\theta_1)^{\frac{(K_1)_{(Np)}/K_1}{(\omega)}} = g_{(\frac{a}{Np},\frac{b}{Np})}(\theta_1) = g_{(\frac{a}{Np},\frac{-a+b}{Np})}(\theta_1) = g_{(0,\frac{1}{Np})}(\theta_1)^{\frac{(K_1)_{(Np)}/K_1}{(-a\theta_1-a+b)}}.
\]

Since \(-a\theta_1-a \equiv 1 \pmod{N\mathcal{O}_{K_1}}\) and \(N_{K_1/Q}(-a\theta_1-a+b) = N_{K_1/Q}(\omega) \equiv C \pmod{p}\), we deduce that
\[
N_{(K_1)_{(Np)}/L_1}(\gamma^n_{1,1})^{(L_1/K_1)/(\omega')} \in \mathbb{R}.
\]
If \(i = 2\), then again by Proposition 4.1 and Lemma 4.3 we achieve
\[
g_{(\frac{a}{Np},\frac{b}{Np})}(\theta_2)^{\frac{(K_2)_{(Np)}/K_2}{(\omega)}} = g_{(\frac{a}{Np},\frac{b}{Np})}(\theta_2) = g_{(\frac{a}{Np},\frac{-a+b}{Np})}(\theta_2) = g_{(0,\frac{1}{Np})}(\theta_2)^{\frac{(K_2)_{(Np)}/K_2}{(-a\theta_2+b)}}.
\]

Since \(-a\theta_2+b \equiv 1 \pmod{N\mathcal{O}_{K_2}}\) and \(N_{K_2/Q}(-a\theta_2+b) = N_{K_2/Q}(\omega) \equiv C \pmod{p}\), we conclude that
\[
N_{(K_2)_{(Np)}/L_2}(\gamma^n_{1,2})^{(L_2/K_2)/(\omega')} \in \mathbb{R}.
\]
This proves the lemma.
THEOREM 6.12. Let $N \neq 2$ be a positive integer and $p$ be an odd prime such that $(N, p) = 1$, $p \equiv 1 \pmod{4}$ and $\left(\frac{d_0'}{p}\right) = -1$. Let $i_0' \in \{1, 2\}$ such that $\left(\frac{-d_0'}{p}\right) = -1$. We assume the followings:

(i) $K_1, K_2 \neq \mathbb{Q}((\sqrt{1}), \mathbb{Q}((\sqrt{-3}))$,

(ii) $N \neq 1$ and $n_0 = p + 1$, or $N = 1$ and $n_0 = \frac{p+1}{2}$ or $p + 1$,

(iii) $N$ has no prime factor which splits completely in $K_{i_0'}$, namely, $Np$ has the prime factorization

$$Np = \prod_{i=1}^{r_1+r_2} p_i^{e_i},$$

where each $p_i$ is a rational prime such that

$$\left(\frac{-d_0'}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \leq i \leq r_1 \\ 0 & \text{if } r_1 + 1 \leq i \leq r_1 + r_2. \end{cases}$$

(iv) When $N \neq 1$, for each index $1 \leq i \leq r_1 + r_2$ there is an odd prime $\nu_i$ such that $\nu_i \nmid e_i$ and $\operatorname{ord}_{\nu_i}(\hat{c}_i) > \operatorname{ord}_{\nu_i}(\frac{p_1+1}{2})$, where

$$\hat{c}_i = \begin{cases} p_i^{2e_i-2}(p_i^{2e_i-1} - 1) & \text{if } 1 \leq i \leq r_1 \\ p_i^{2e_i-1}(p_i - 1) & \text{if } r_1 + 1 \leq i \leq r_1 + r_2, \end{cases}$$

$$e_i = \prod_{1 \leq j \leq r_1+r_2, j \neq i} \hat{c}_j.$$

When $N = 1$, there exists an odd prime $\nu$ dividing $p - 1$.

Then for any positive integer $n$, we have

$$\mathcal{K}_{N,p,0}^3 = K(N) \left( N \mathcal{K}_{N,p,0}^2 / K_{N,p,0}^2 (\gamma_{1,i_0'}) \right).$$

PROOF. We claim that $L_{i_0}$ satisfies the assumptions in Proposition 4.5 for $K_{i_0'}$. Indeed, if $N \neq 1$ then for each index $1 \leq i \leq r_1 + r_2$,

$$\hat{c}_i = \# \ker (\pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times / \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times \rightarrow \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times / \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times),$$

$$e_i = \# \ker (\pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times / \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times \rightarrow \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times / \pi_{NpO_{K_{i_0}}}(O_{K_{i_0}}) \times),$$

and by the assumption (iv) and (6.24) we get

$$\operatorname{ord}_{\nu_i}(\hat{c}_i) > \operatorname{ord}_{\nu_i}(\frac{p+1}{2}) = \operatorname{ord}_{\nu_i}( [(K_{i_0})(Np) : L_{i_0}] ).$$
because \( \nu_i \) is odd. If \( N = 1 \), then \( p\mathcal{O}_{K'_0} \) is a prime ideal of \( K'_0 \), and so by Lemma 6.10,

\[
\begin{align*}
\# \ker \left( \pi p\mathcal{O}_{K'_0} \rightarrow \mathcal{O}_{K'_0} \right) & \Rightarrow \pi \mathcal{O}_{K'_0} \rightarrow \mathcal{O}_{K'_0} \) \Rightarrow \frac{(p+1)(p-1)}{2}, \\
\# \ker \left( \pi p\mathcal{O}_{K'_0} \rightarrow \mathcal{O}_{K'_0} \right) & \Rightarrow \pi \mathcal{O}_{K'_0} \rightarrow \mathcal{O}_{K'_0} \) \Rightarrow \frac{(p+1)(p-1)}{2}, \\
\end{align*}
\]

and hence the claim is proved. And, we see from Proposition 4.4 and 4.5 that

\[
\text{Remark 6.13 (i) With the assumptions as in Lemma 6.10 we get}
\]

\[
\begin{align*}
\left[ K_{1,2}^1, K_{N,0}^1 : K_{N,0}^1 \right] \Rightarrow \left[ K_{1,2}^1, K_{N,0}^1 : K_{N,0}^1 \right], \\
\left[ K_{1,2}^1, K_{N,0}^1 : K_{N,0}^1 \right] \Rightarrow \left[ K_{1,2}^1, K_{N,0}^1 : K_{N,0}^1 \right].
\end{align*}
\]

Hence we obtain

\[
\text{Gal} \left( K_{N,0}^1 / K_{N,0}^1 \right) = \left\{ \sigma \mid K_{N,0}^1 / K_{N,0}^1 \mid \sigma \in \text{Gal} \left( K_{1,2}^1 / K_{N,0}^1 \right) \right\},
\]

\[
\text{Gal} \left( K_{1,2}^1 / K_{N,0}^1 \right) = \left\{ \sigma \mid K_{N,0}^1 / K_{N,0}^1 \mid \sigma \in \text{Gal} \left( K_{1,2}^1 / K_{N,0}^1 \right) \right\}.
\]

Thus we derive by (6.11), (6.16), (6.17) and (6.19) that

\[
\begin{align*}
\text{Gal} \left( K_{N,0}^1 / K_{N,0}^1 \right) & \Rightarrow \left\{ \left( \frac{K_{0,0}^1 / K}{\omega_{1,0}^1} \right) \times \left( \frac{K_{0,0}^1 / K}{\omega_{2,0}^1} \right) \right\} \Rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(\frac{p+1}{2})\mathbb{Z} \quad \text{if } N \neq 1, \\
\text{Gal} \left( K_{1,2}^1 / K_{N,0}^1 \right) & \Rightarrow \left\{ \left( \frac{K_{0,0}^1 / K}{\omega_{1,0}^1} \right) \times \left( \frac{K_{0,0}^1 / K}{\omega_{2,0}^1} \right) \right\} \Rightarrow \mathbb{Z}/(\frac{p+1}{2})\mathbb{Z} \quad \text{if } N = 1,
\end{align*}
\]

where \( \mathcal{D}_{i_0}, \omega_{i_0} \in \mathcal{O}_{K_{i_0}}, \omega_{i_0} \in \mathcal{O}_{K_{i_0}} \) and \( \mathcal{B} \in \mathcal{O}_K \) such that

\[
\begin{align*}
\mathcal{D}_{i_0} & \equiv \omega_{i_0} \equiv \omega_{i_0}^1 \equiv \mathcal{B} \equiv 1 \pmod{N\mathcal{O}_K}, \\
\mathcal{D}_{i_0} & \equiv D_{i_0}^{-1} \sqrt{-d_{i_0}} \pmod{p\mathcal{O}_K}, \\
\mathcal{B} & \equiv B \pmod{p\mathcal{O}_K},
\end{align*}
\]

31
and \(\omega_i + p\mathcal{O}_K\) (resp. \(\omega'_i + p\mathcal{O}_K\)) is a generator of \(\widetilde{W}_{N,p,0,x}^{0,3}\) (resp. \(\widetilde{W}_{N,p,0,x}^{0,3}\)). Therefore we can explicitly estimate the value \(N_{K_{N,p,0}/K_{N,p,0}}(\gamma_{1,i})\) for \(i = 1, 2\) by making use of Proposition 4.2.

(ii) The singular value \(N_{K_{N,p,0}/K_{N,p,0}}(\gamma_{1,i}^n)\) for \(i = 1, 2\) could be a generator of \(K_{N,p,0}\) over \(K\) without the assumptions (iii), (iv) in Theorem 6.12. Observe that

\[
\text{Gal}(K_{N,p,0}/K_{(N)}) = \left\{ \left( \frac{K_{3}}{O} \right) \right\} \mid \omega \in O_K, \: \omega \equiv 1 \pmod{N\mathcal{O}_K} \}
\]

(6.26)

\[
= \left\{ \left( \frac{K_{3}}{O} \right) \right\} \cong \mathbb{Z}/(p - 1)\mathbb{Z},
\]

where \(C\) is a primitive root modulo \(p\) and \(\omega_C\) is an element of \(O_K\) satisfying \(\omega_C \equiv 1 \pmod{N\mathcal{O}_K}\) and \(N_{K/\mathbb{Q}}(\omega_C) \equiv C \pmod{p}\). Using (6.26) one can check whether the value is a generator of \(K_{3,N,p,0}\) over \(K_{(N)}\) or not.

Example 6.14. (i) Let \(K = \mathbb{Q} \left( \sqrt{-15}, \sqrt{-26} \right)\). Then \(K_3 = \mathbb{Q} \left( \sqrt{390} \right)\) and \(\varepsilon_0 = 79 + 4\sqrt{390}\). We set \(N = 5\) and \(p = 37\) so that \(m_0 = 5, \: \varepsilon_0' = -\varepsilon_0^{m_0}\) and \(n_0 = p + 1\). Observe that \((\frac{390}{37}) = (\frac{-15}{37}) = -1\), namely, \(i_0' = 1\). Hence by Corollary 6.3 and Theorem 6.12 for any positive integers \(n_1, n_2\),

(6.27)

\[K_{(185)} = K_{5,37,0}^{1,2} = K_{(5)} \left( g_{(0, 1)}^{2220m_1}(\theta_1)g_{(0, 1)}^{2220m_2}(\theta_2) \right)\]

where \(\theta_1 = \frac{-1 + \sqrt{-15}}{2}\) and \(\theta_2 = \sqrt{-26}\).

Let \(p_1 = 5\) and \(p_2 = 37\). From the assumption (iv) in Theorem 6.12, we have

\[
\hat{\epsilon}_1 = 2^2 \cdot 5, \quad \hat{\epsilon}_2 = 2^3 \cdot 3^2 \cdot 19, \quad \epsilon_1 = 2^3 \cdot 3^2 \cdot 19, \quad \epsilon_2 = 2^2 \cdot 5.
\]

Then \(\nu_1 = 5\) and \(\nu_2 = 3\) are odd primes satisfying \(\nu_i \nmid \epsilon_i\) and \(\text{ord}_{\nu_i}(\hat{\epsilon}_i) > \text{ord}_{\nu_i}(19)\) for each \(i = 1, 2\). Therefore, for any positive integer \(\nu\) we get by Theorem 6.12

\[\widetilde{K}_{5,37,0}^3 = K_{(5)} \left( N_{K_{5,37,0}/K_{5,37,0}}(g_{(0, 1)}^{2220m_1}(\theta_1)) \right),\]

Using (6.15) we can derive

\[\widetilde{W}_{5,37,0}^{2,3} = \left\langle 3 + 16\sqrt{-15} + 37\mathcal{O}_K \right\rangle.\]

Let

\[
\omega_1 = -34 + 90\sqrt{15}, \quad \mathcal{O}_2 = -74 + 45\sqrt{-26}.
\]
so that $\omega_1 \equiv \mathcal{O}_2 \equiv 1 \pmod{5\mathcal{O}_K}$, $\omega_1 \equiv 3 + 16\sqrt{-15} \pmod{37\mathcal{O}_K}$ and $\mathcal{O}_2 \equiv 8\sqrt{-26} \pmod{37\mathcal{O}_K}$. Then by Remark 6.13 (i) we attain

$$
\text{Gal} \left( \widetilde{K}_{5,37,0}^l / \widetilde{K}_{5,37,0}^3 \right) = \left\langle \left( \frac{K_{5,37,0}^l / K}{(\mathcal{O}_2)} \right) \right\rangle \times \left\langle \left( \frac{K_{5,37,0}^l / K}{(\omega_1)} \right) \right\rangle \cong \mathbb{Z} / 2\mathbb{Z} \times \mathbb{Z} / 19\mathbb{Z}.
$$

Now that

$$
\begin{align*}
N_{K/K_1}(\omega_1) & \equiv 170\sqrt{-15} + 91 \equiv 155\theta_1 + 76 \pmod{185\mathcal{O}_K}, \\
N_{K/K_1}(\mathcal{O}_2) & \equiv 36 \pmod{185\mathcal{O}_K},
\end{align*}
$$

we deduce by Proposition 4.2 that for $(r_1, r_2) \in \frac{1}{185} \mathbb{Z}^2 \setminus \mathbb{Z}^2$

$$
\begin{align*}
ge_{(r_1, r_2)}^{2220}(\frac{K_{5,37,0}^l / K}{(\omega_1)})(\theta_1) &= g_{(r_1, r_2)}^{2220}(\theta_1) \left( \frac{(K_{1,l})_{(185)} / K_1}{(155\theta_1 + 76)} \right) \\
ge_{(r_1, r_2)}^{2220}(\frac{K_{5,37,0}^l / K}{(\mathcal{O}_2)}) = g_{(r_1, r_2)}^{2220}(\theta_1) \left( \frac{(K_{1,l})_{(185)} / K_1}{(36/0)} \right).
\end{align*}
$$

Therefore, we conclude

$$
\begin{align*}
N_{K_{5,37,0}^l / K_{5,37,0}^3}(g_{(0, 0)}^{2220}((\theta_1)) &= g_{(0, 0)}^{2220}(\theta_1) g_{(37, 0)}^{2220}(\theta_1) g_{(37, 185)}^{2220}(\theta_1) g_{(185, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 131)}^{2220}(\theta_1) g_{(131, 37)}^{2220}(\theta_1) g_{(131, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) g_{(37, 131)}^{2220}(\theta_1) g_{(131, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 131)}^{2220}(\theta_1) g_{(131, 37)}^{2220}(\theta_1) g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1) \\
&\times g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 185)}^{2220}(\theta_1) g_{(185, 37)}^{2220}(\theta_1) g_{(37, 116)}^{2220}(\theta_1) g_{(116, 37)}^{2220}(\theta_1)
\end{align*}
$$

\[ \approx 2.1204525 \times 10^{-6180}. \]

(ii) Let $K = \mathbb{Q}(\sqrt{-7}, \sqrt{-2})$. Then $K_3 = \mathbb{Q}(\sqrt{14})$ and $\varepsilon_0 = 15 + 4\sqrt{14}$. We set $N = 1$ and $p = 37$ so that $\left( \frac{1}{p} \right) = -1$, $\varepsilon'_0 = 2$ and $n_0 = p + 1$. One can then readily get

$$
W_{K_{1,37,0}^l}^{1,3} = \langle 3 + 12\sqrt{-2} + 37\mathcal{O}_K \rangle,
$$

and hence by Remark 6.13 (i) we have

$$
\text{Gal} \left( \widetilde{K}_{1,37,0}^2 / \widetilde{K}_{1,37,0}^3 \right) = \left\langle \left( \frac{K_{1,37,0}^2 / K_{1,37,0}^3}{(3 + 12\sqrt{-2})} \right) \right\rangle \cong \mathbb{Z} / 19\mathbb{Z}.
$$
If we let $\theta_2 = \sqrt{-2}$, then $N_{K_2/K_3}(3 + 12\sqrt{-2}) \equiv -2\theta_2 + 17 \pmod{37\mathcal{O}_{K_2}}$. Thus, for $(r_1, r_2) \in \frac{1}{37}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ we deduce by Proposition 4.2

$$g_{(r_1, r_2)}^{444}(\theta_2) = g_{(r_1, r_2)}^{444}(\theta_2) = g_{(r_1, r_2)}^{444}(\theta_2),$$

and so we establish

$$N_{K_1,37,0/K_1,37,0}^{1/2} \left( g_{(0, \frac{1}{37})}^{444}(\theta_2) \right) = g_{(0, \frac{1}{37})}^{444}(\theta_2) g_{(\frac{4}{37}, \frac{17}{37})}^{444}(\theta_2) g_{(\frac{6}{37}, \frac{22}{37})}^{444}(\theta_2) g_{(\frac{21}{37}, \frac{28}{37})}^{444}(\theta_2) g_{(\frac{23}{37}, \frac{3}{37})}^{444}(\theta_2)$$

$$\times g_{(\frac{444}{37}, \frac{0}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{25}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{17}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{13}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{31}{37})}^{444}(\theta_2)$$

$$\times g_{(\frac{444}{37}, \frac{23}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{28}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{22}{37})}^{444}(\theta_2) g_{(\frac{444}{37}, \frac{2}{37})}^{444}(\theta_2)$$

$$\approx 3.9908748 \times 10^{-460}.$$

Note that the class number of $K$ is 1 by (8.1) and Example 8.7 (i). Therefore, by Theorem 6.12 we achieve

$$K_{1,37,0} = \mathcal{O} \left( N_{K_1,37,0/K_1,37,0}^{1/2} \left( g_{(0, \frac{1}{37})}^{444}(\theta_2) \right) \right) \text{ for } n \in \mathbb{Z}_{>0}.$$

## 7 Class fields over imaginary biquadratic fields (II)

Following the previous section we shall consider the more general case $\mu > 0$. Let $N$ be a positive integer and $p$ be an odd prime such that $(N, p) = 1$.

**Lemma 7.1.** With the same notations as in Section 4, for a positive integer $\mu$

$$|S_{N,p,\mu}/S_{N,p,\mu+1}| = p^4,$$

$$|S_{N,p,\mu}^{(i)}/S_{N,p,\mu+1}^{(i)}| = p^2 \text{ for } i = 1, 2, 3.$$

**Proof.** Now that $S_{N,p,\mu}/S_{N,p,\mu+1}$ is isomorphic to $\mathcal{O}_{K}/p\mathcal{O}_{K}$ by a mapping

$$S_{N,p,\mu}/S_{N,p,\mu+1} \rightarrow \mathcal{O}_{K}/p\mathcal{O}_{K}$$

$$(1 + Np^\mu \omega)S_{N,p,\mu+1} \rightarrow \omega + p\mathcal{O}_{K} \text{ for } \omega \in \mathcal{O}_{K},$$

we obtain $S_{\mu}/S_{\mu+1} \cong (\mathbb{Z}/p\mathbb{Z})^4$. Similarly, one can show the isomorphism $S_{N,p,\mu}^{(i)}/S_{N,p,\mu+1}^{(i)} \cong (\mathbb{Z}/p\mathbb{Z})^2$ for $i = 1, 2, 3$. \□

Let $\varepsilon_0$ be the fundamental unit of the real quadratic field $K_3$, $\ell_0$ be the smallest positive integer such that $\varepsilon_0^{\ell_0} \equiv 1 \pmod{Np\mathcal{O}_{K}}$ and $\mu_0$ be the maximal positive integer satisfying $\varepsilon_0^{\ell_0} \equiv 1 \pmod{Np^{\mu_0}\mathcal{O}_{K}}$. Write

$$\varepsilon_0^{\ell_0} = 1 + Np^{\mu_0}(\alpha_0 + \beta_0 \sqrt{d_1d_2})$$
with $\alpha_0, \beta_0 \in \mathbb{Z}$. By the maximality of $\mu_0$ we have $\alpha_0 + \beta_0 \sqrt{d_1 d_2} \notin p\mathcal{O}_K$. Since

$$1 = N_{K_3/Q}(\varepsilon_0^\mu) \equiv 1 + 2Np^{\mu_0}\alpha_0 \pmod{Np^{\mu_0 + 1}},$$

we get $p \mid \alpha_0$ and $p \nmid \beta_0$.

**Lemma 7.2.** With the notations as in Section 6, for a positive integer $\mu$

$$|H_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)}| = \begin{cases} 1 & \text{if } \mu < \mu_0 \\ p & \text{if } \mu \geq \mu_0. \end{cases}$$

Moreover, if $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ then

$$|H_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)}| = \begin{cases} 1 & \text{if } \mu < \mu_0 \\ p & \text{if } \mu \geq \mu_0. \end{cases}$$

**Proof.** In a similar way as in the proof of Lemma 6.5, one can verify that if $\ell_0$ is odd, then $\varepsilon_0^{\ell_0} \neq -1 \pmod{NP\mathcal{O}_K}$ for all $n \in \mathbb{Z}_{>0}$. And, if $\ell_0$ is even, then we have either $\varepsilon_0^{\ell_0} \equiv -1 \pmod{NP\mathcal{O}_K}$ or $\varepsilon_0^{\ell_0} \neq -1 \pmod{NP\mathcal{O}_K}$ for all $n \in \mathbb{Z}_{>0}$. Indeed, suppose $\varepsilon_0^{\ell_0} \equiv -1 \pmod{NP\mathcal{O}_K}$. If $\varepsilon_0^{\ell_0} \equiv -1 \pmod{NP\mathcal{O}_K}$ for some $n \in \mathbb{Z}_{>0}$, then $\ell_0 \mid 2n$ and so $\ell_0 \mid n$. It contradicts the fact $(\varepsilon_0^{\ell_0})^m \neq -1 \pmod{NP\mathcal{O}_K}$ for all $m \in \mathbb{Z}_{>0}$. Next, we claim that if $\ell_0$ is even and $\varepsilon_0^{\ell_0} \equiv -1 \pmod{NP\mathcal{O}_K}$, then $\mu_0$ is the maximal positive integer such that $\varepsilon_0^{\mu_0} \equiv -1 \pmod{NP^{\mu_0}\mathcal{O}_K}$. For, write $\varepsilon_0^{\mu_0} = -1 + Np\omega$ for some $\omega \in \mathcal{O}_K$. Then

$$\varepsilon_0^{\mu_0} = 1 + Np\omega(-2 + Np\omega) \equiv 1 \pmod{NP^{\mu_0}\mathcal{O}_K}.$$ 

Since $-2 + Np\omega \not\equiv p$ for any prime ideal $p$ dividing $p\mathcal{O}_K$, $\omega$ belongs to $p^{\mu_0 - 1}\mathcal{O}_K$ and $\varepsilon_0^{\mu_0} \equiv -1 \pmod{NP^{\mu_0}\mathcal{O}_K}$. If $\varepsilon_0^{\mu_0} \equiv -1 \pmod{NP^{\mu_0}\mathcal{O}_K}$ for some $\mu > \mu_0$, then $\varepsilon_0^{\mu_0} \equiv 1 \pmod{NP^{\mu_0}\mathcal{O}_K}$, which contradicts the maximality of $\mu_0$.

Since $\mathcal{O}_K^\times = \{\pm \varepsilon_0^n \mid n \in \mathbb{Z}\}$ and $H_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)} \subseteq S_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)} \cong (\mathbb{Z}/p\mathbb{Z})^2$, we attain

$$\dim_{\mathbb{Z}/p\mathbb{Z}} \left( H_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)} \right) = 0 \text{ or } 1.$$ 

It follows from the above claim that $H_{N,p,\mu}^{(3)} / S_{N,p,\mu+1}^{(3)} = 0$ if $\mu < \mu_0$. Now, assume $\mu \geq \mu_0$. Observe that $H_{N,p,\mu_0}^{(3)} / S_{N,p,\mu_0+1}^{(3)} = \langle \varepsilon_0^{\mu_0} S_{N,p,\mu_0+1}^{(3)} \rangle \cong \mathbb{Z}/p\mathbb{Z}$ because $(2, p) = 1$. For a positive integer $m$,

$$\langle \varepsilon_0^{\mu_0} \rangle^m = 1 + mNp^{\mu_0}(\alpha_0 + \beta_0 \sqrt{d_1 d_2}) + \sum_{i=2}^{m} \binom{m}{i} \left\{ Np^{\mu_0}(\alpha_0 + \beta_0 \sqrt{d_1 d_2}) \right\}^i.$$ 

Since $\alpha_0 + \beta_0 \sqrt{d_1 d_2} \not\equiv p\mathcal{O}_K$ and $\sum_{i=2}^{p} \binom{p}{i} \left\{ Np^{\mu_0}(\alpha_0 + \beta_0 \sqrt{d_1 d_2}) \right\}^i \in Np^{\mu_0+2}\mathcal{O}_K$, $m = p$ is the smallest positive integer satisfying $\langle \varepsilon_0^{\mu_0} \rangle^m \in H_{N,p,\mu_0+1}^{(3)} \setminus S_{N,p,\mu_0+2}^{(3)}$. In a similar fashion,
one can prove by using the induction that $m = p^{\mu - \mu_0}$ is the smallest positive integer such that $(\varepsilon_0^\mu)^m \in H^{(3)}_{N,p,\mu} \setminus S^{(3)}_{N,p,\mu+1}$. Therefore, $H^{(3)}_{N,p,\mu}/S^{(3)}_{N,p,\mu+1} = (\varepsilon_0^p)^{p^{\mu - \mu_0}} S^{(3)}_{N,p,\mu+1} \cong \mathbb{Z}/p\mathbb{Z}$.

If $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then by utilizing the idea in the proof of Lemma 6.5 one can show that $S_{N,p,\mu} \cap O_K^\times \subset O_{K_3}^\times$ for all $\mu \in \mathbb{Z}_{>0}$. Here we observe that we don’t need the assumptions $N \neq 2$ and $(d_1 d_2 p) = -1$. Hence, $|H^{(3)}_{N,p,\mu}/S^{(3)}_{N,p,\mu+1}| = |H^{(3)}_{N,p,\mu}/S^{(3)}_{N,p,\mu+1}|$.

**Corollary 7.3.** With the notations and assumptions as in Lemma 7.2, for a positive integer $\mu$,

$$\left[ K_{(Np^{\mu+1})} : K_{(Np^\mu)} \right] = \begin{cases} p^4 & \text{if } \mu < \mu_0 \\ p^3 & \text{if } \mu \geq \mu_0, \end{cases}$$

$$\left[ (K_3)_{(Np^{\mu+1})} : (K_3)_{(Np^\mu)} \right] = \begin{cases} p^2 & \text{if } \mu < \mu_0 \\ p & \text{if } \mu \geq \mu_0. \end{cases}$$

**Proof.** It is immediate from (6.1), Lemma 7.1 and 7.2. 

For a positive integer $\mu$, let

$$W_{N,p,\mu}^i = \{ \omega \in S_{N,p,\mu} \mid N_{K/K_i}(\omega) \equiv 1 \pmod{Np^{\mu+1}O_{K_i}} \} \quad \text{for } i = 1, 2$$

$$W_{N,p,\mu}^3 = \begin{cases} \{ \omega \in S_{N,p,\mu} \mid N_{K/K_3}(\omega) \equiv 1 \pmod{Np^{\mu+1}O_{K_3}} \} & \text{if } \mu < \mu_0 \\ \{ \omega \in S_{N,p,\mu} \mid N_{K/K_3}(\omega) \equiv (\varepsilon_0^{p^{\mu-\mu_0} - 1}) \pmod{Np^{\mu+1}O_{K_3}} \text{ for some } n \in \mathbb{Z} \} & \text{if } \mu \geq \mu_0, \end{cases}$$

so that $\ker(\tilde{\varphi}_{N,p,\mu}) = W_{N,p,\mu}^i / H_{N,p,\mu}$ for $i = 1, 2, 3$. Furthermore, we let

$$W_{N,p,\mu}^{ij} = W_{N,p,\mu}^i \cap W_{N,p,\mu}^j \quad \text{for } 1 \leq i < j \leq 3,$$

$$W_{N,p,\mu} = \bigcap_{i=1}^3 W_{N,p,\mu}^i$$

so as to get $\ker(\tilde{\varphi}_{N,p,\mu}) = W_{N,p,\mu}^{ij} / H_{N,p,\mu}$ and $\ker(\tilde{\varphi}_{N,p,\mu}) = W_{N,p,\mu} / H_{N,p,\mu}$.

**Theorem 7.4.** Let $N$ be a positive integer and $p$ be an odd prime such that $(N, p) = 1$. Assume that $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. Then for a positive integer $\mu$, we derive

$$K_{(Np^{\mu+1})} = \tilde{K}_{N,p,\mu}.$$

Moreover,

$$\left[ K_{(Np^{\mu+1})} : \tilde{K}_{N,p,\mu}^{1,2} \right] = \begin{cases} p & \text{if } \mu < \mu_0 \\ 1 & \text{if } \mu \geq \mu_0. \end{cases}$$

36
PROOF. For any coset $\alpha S_{N,p,\mu+1}$ in $S_{N,p,\mu}/S_{N,p,\mu+1}$ we can choose $\omega \in \mathcal{O}_K \cap S_{N,p,\mu}$ such that $\alpha S_{N,p,\mu+1} = \omega S_{N,p,\mu+1}$. And, we write $\omega = 1 + Np^\mu \left( \frac{1}{2} [a + b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1 d_2}] \right)$ with $a, b, c, d \in \mathbb{Z}$ satisfying $a \equiv b \pmod{2}$, $c \equiv d \pmod{2}$.

First, we consider the group $W_{N,p,\mu}^{1,2}/S_{N,p,\mu+1}$. If $\omega \in \mathcal{O}_K \cap W_{N,p,\mu}^{1,2}$, then we have

\begin{align}
N_{K/K_1}(\omega) &\equiv 1 + Np^\mu(a + b\sqrt{-d_1}) \equiv 1 \pmod{Np^{\mu+1}O_{K_1}}, \\
N_{K/K_2}(\omega) &\equiv 1 + Np^\mu(a + c\sqrt{-d_2}) \equiv 1 \pmod{Np^{\mu+1}O_{K_2}}.
\end{align}

Since $a + b\sqrt{-d_1} = a + b + 2b\left(\frac{-1 + \sqrt{-d_1}}{2}\right) \in p\mathcal{O}_{K_1}$ and $a + c\sqrt{-d_2} \in p\mathcal{O}_{K_2}$, $p$ divides $a, b, c$. Thus we claim that

$$W_{N,p,\mu}^{1,2}/S_{N,p,\mu+1} = \left( 1 + Np^\mu \sqrt{d_1 d_2} \right) S_{N,p,\mu+1} \cong \mathbb{Z}/p\mathbb{Z},$$

and by Lemma (7.2) we get

$$\left[ K_{(Np^\mu+1)} : K_{N,p,\mu} \right] = \left| W_{N,p,\mu}^{1,2}/S_{N,p,\mu+1} \right| = \left| H_{N,p,\mu}/S_{N,p,\mu+1} \right| = \begin{cases} p & \text{if } \mu < \mu_0 \\ 1 & \text{if } \mu \geq \mu_0. \end{cases}$$

Next, we consider the group $W_{N,p,\mu}/S_{N,p,\mu+1}$. If $\omega \in \mathcal{O}_K \cap W_{N,p,\mu}$, then $\omega$ satisfies (7.1) and

$$N_{K/K_3}(\omega) \equiv 1 + Np^\mu(a + d\sqrt{d_1 d_2}) \pmod{Np^{\mu+1}O_{K_3}}$$

\begin{align}
&\equiv \begin{cases} 1 & \text{if } \mu < \mu_0 \\ \left( \varepsilon_{n,\mu\mu_0} \right)^n & \text{for some } n \in \mathbb{Z} \text{ if } \mu \geq \mu_0. \end{cases}
\end{align}

If $\mu < \mu_0$, then $a + d\sqrt{d_1 d_2} \in p\mathcal{O}_{K_3}$, so $p$ divides $d$. Hence $W_{N,p,\mu}/S_{N,p,\mu+1} = \{1\}$ and

$$\left[ K_{(Np^\mu+1)} : K_{N,p,\mu} \right] = \left| W_{N,p,\mu}/H_{N,p,\mu} \right| = 1.$$

If $\mu \geq \mu_0$, then

$$1 + Np^\mu(a + d\sqrt{d_1 d_2}) \equiv 1 + nNp^{\mu}(\alpha_0 + \beta_0 \sqrt{d_1 d_2}) \pmod{Np^{\mu+1}O_{K_3}},$$

from which we deduce $a \equiv n\alpha_0 (\text{mod } p)$, $d \equiv n\beta_0 (\text{mod } p)$. Since $p \mid \alpha_0$ and $p \nmid \beta_0$, we attain

$$W_{N,p,\mu}/S_{N,p,\mu+1} = \left( 1 + Np^\mu \sqrt{d_1 d_2} \right) S_{N,p,\mu+1} = W_{N,p,\mu}^{1,2}/S_{N,p,\mu+1}.$$ 

Therefore, if $\mu \geq \mu_0$, then we conclude

$$\left[ K_{(Np^\mu+1)} : K_{N,p,\mu} \right] = \left[ K_{(Np^\mu+1)} : K_{N,p,\mu}^{1,2} \right] = 1.$$

\[\square\]

On the other hand, let $\gamma_{\mu,i}$ be as in (6.2).
**Corollary 7.5.** With the notations and assumptions as above, if \( \mu \geq \mu_0 \), then for any positive integers \( n_1, n_2 \),

\[
K_{(Np^{\mu+1})} = K_{(Np^{\mu_0})} \left( \gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2} \right).
\]

**Proof.** By Proposition 4.4, Lemma 6.2 and Theorem 7.4 we obtain

\[
K_{(Np^{\mu+1})} = K_{(Np^{\mu})}(K_1(K_2(Np^{\mu+1})) = K_{(Np^{\mu_0})}(K_1(K_2(Np^{\mu+1})) = K_{(Np^{\mu_0})} \left( \gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2} \right).
\]

Since the only element of \( \text{Gal}(K_{(Np^{\mu+1})}/K_{(Np^{\mu_0})}) \) fixing the value \( \gamma_{\mu+1,1}^{n_1} \gamma_{\mu+1,2}^{n_2} \) is the identity, we get the conclusion ([12, Theorem 3.5 and Remark 3.6]).

We can derive by (7.1), (7.2) that

(7.3)

\[
\begin{align*}
W_{1,N,p,\mu}^{1}/S_{N,p,\mu+1} &= \left\{ (1 + Np^{\mu}(c\sqrt{-d_2} + d\sqrt{d_1d_2}))S_{N,p,\mu+1} \mid c, d \in \mathbb{Z}/p\mathbb{Z} \right\}, \\
W_{2,N,p,\mu}^{2}/S_{N,p,\mu+1} &= \left\{ (1 + Np^{\mu}(b\sqrt{-d_1} + d\sqrt{d_1d_2}))S_{N,p,\mu+1} \mid b, d \in \mathbb{Z}/p\mathbb{Z} \right\}, \\
W_{3,N,p,\mu}^{3}/S_{N,p,\mu+1} &= \begin{cases} 
\left\{ (1 + Np^{\mu}(b\sqrt{-d_1} + c\sqrt{-d_2}))S_{N,p,\mu+1} \mid b, c \in \mathbb{Z}/p\mathbb{Z} \right\} & \text{if } \mu < \mu_0 \\
\left\{ (1 + Np^{\mu}(b\sqrt{-d_1} + c\sqrt{-d_2} + d\sqrt{d_1d_2}))S_{N,p,\mu+1} \mid b, c, d \in \mathbb{Z}/p\mathbb{Z} \right\} & \text{if } \mu \geq \mu_0 
\end{cases}
\]

And, we achieve by Lemma 7.2 that

(7.4)

\[
\begin{align*}
\left[ K_{(Np^{\mu+1})} : \tilde{K}_{1,N,p,\mu} \right] &= \begin{cases} 
p^2 & \text{if } \mu < \mu_0 \\
p & \text{if } \mu \geq \mu_0 
\end{cases} \quad (i = 1, 2) \\
\left[ K_{(Np^{\mu+1})} : \tilde{K}_{3,N,p,\mu} \right] &= p^2.
\end{align*}
\]

Thus, we have the following diagrams by Corollary 7.3, Theorem 7.4 and (7.4):

(i) when \( \mu < \mu_0 \)
(ii) when $\mu \geq \mu_0$.

Observe that the field $\widetilde{K}_{3,N,p,\mu}$ is contained in $\widetilde{K}_{i,N,p,\mu}$ for $i = 1, 2$ if and only if $\mu \geq \mu_0$.

For a positive integer $\mu$ and $i = 1, 2$, let $L_{\mu,i}$ be a finite abelian extension of $K_i$ which is the fixed field of the subgroup

$$
\langle \left( (K_i)_{(Np^{\mu+1})}/K_i \right) \rangle
\simeq \mathbb{Z}/p\mathbb{Z}.
$$

**Lemma 7.6.** Let $N, \mu$ be two positive integers and $p$ be an odd prime such that $(N,p) = 1$. Assume that $K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ and $\mu \geq \mu_0$. Then we have

$$
\widetilde{K}_{3,N,p,\mu} = K_{(Np^\mu)} L_{\mu,i} \quad \text{for} \quad i = 1, 2.
$$

**Proof.** Since $|H_{N,p,\mu}^{(i)}/S_{N,p,\mu+1}^{(i)}| = 1$, we get

$$
[(K_i)_{(Np^{\mu+1})} : L_{\mu,i}] = p.
$$

Consider the composite field $K_{(Np^\mu)}L_{\mu,i}$. It then follows from (7.3) that

$$
\text{Gal}\left( (K_i)_{(Np^{\mu+1})}/K_i \right) \simeq \mathbb{Z}/p\mathbb{Z}.
$$

Since $N_{K_i/K_i}(1 + Np^\mu \sqrt{-d_i}) = (1 + Np^\mu \sqrt{-d_i})^2$, for $\alpha \in L_{\mu,i}$ the Galois action induces

$$
\alpha \left( \frac{K_{N,p,\mu}/K}{(1 + Np^\mu \sqrt{-d_i})} \right) = \alpha \left( \frac{(K_i)_{(Np^{\mu+1})}/K_i}{(1 + Np^\mu \sqrt{-d_i})} \right) = \alpha,
$$

which yields $K_{(Np^\mu)}L_{\mu,i} \subseteq \widetilde{K}_{3,N,p,\mu}$. Thus by Lemma 6.2 we have

$$
[(K_i)_{(Np^{\mu+1})} : L_{\mu,i}] = p = [(K_i)_{(Np^{\mu+1})} : \widetilde{K}_{3,N,p,\mu}] = [(K_i)_{(Np^{\mu+1})} : \widetilde{K}_{N,p,\mu} : \widetilde{K}_{3,N,p,\mu}],
$$

and so $\widetilde{K}_{3,N,p,\mu} = K_{(Np^\mu)}L_{\mu,i}$ for $i = 1, 2$. □
Lemma 7.7. With the notations and assumptions as in Lemma 7.6, for any positive integer \( n \) and \( i = 1, 2 \) the singular value \( \overline{N_{K_{N,p,\mu}/K_{3_{N,p,\mu}}}}(\gamma_{\mu+1,i}^n) \) is a real algebraic integer. Moreover,
\[
\overline{N_{K_{N,p,\mu}/K_{3_{N,p,\mu}}}}(\gamma_{\mu+1,i}^n)_{\sigma} \in \mathbb{R} \quad \text{for} \quad \sigma \in \text{Gal}(\overline{K_{N,p,\mu}}/K_{(Np^\mu)}).
\]

Proof. Since \( \gamma_{\mu+1,i}^n \) is an algebraic integer by Proposition 4.4, so is \( \overline{N_{K_{N,p,\mu}/K_{3_{N,p,\mu}}}}(\gamma_{\mu+1,i}^n) \). Note that Gal\((K_i)(Np^\mu+1)/L_{\mu,i}\) is the restriction of Gal\((\overline{K_{N,p,\mu}/K_{3_{N,p,\mu}}})\) to the field \((K_i)(Np^\mu+1)\) by Lemma 7.6 from which we attain
\[
(7.7) \quad \overline{N_{K_{N,p,\mu}/K_{3_{N,p,\mu}}}}(\gamma_{\mu+1,i}^n) = N_{(K_i)(Np^\mu+1)/L_{\mu,i}}(\gamma_{\mu+1,i}^n).
\]

And, by Corollary 7.3 (7.4) and (7.5) we have
\[
\left[ L_{\mu,i} : (K_i)(Np^\mu) \right] = p = \left[ K_{3_{N,p,\mu}} : K_{(Np^\mu)} \right].
\]

Since \( \overline{K_{3_{N,p,\mu}}} = K_{(Np^\mu)}L_{\mu,i} \), it suffices to show by (7.7) that
\[
N_{(K_i)(Np^\mu+1)/L_{\mu,i}}(\gamma_{\mu+1,i}^n)_{\sigma} \in \mathbb{R} \quad \text{for} \quad \sigma \in \text{Gal}(L_{\mu,i}/(K_i)(Np^\mu)).
\]

Now, observe that
\[
\text{Gal}(L_{\mu,i}/(K_i)(Np^\mu)) = \left\{ \left( \frac{L_{\mu,i}/K_i}{1+Np^\mu x} \right) \mid x = 0, 1, \ldots, p-1 \right\},
\]
\[
N_{(K_i)(Np^\mu+1)/L_{\mu,i}}(\gamma_{\mu+1,i}^n) = \prod_{y=0}^{p-1} g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_i)^{\frac{(K_i)(Np^\mu+1)/K_i}{(1+Np^\mu y - d_i)}}.
\]

Then, for \( x = 0, 1, \ldots, p-1 \) we establish
\[
N_{(K_i)(Np^\mu+1)/L_{\mu,i}}(\gamma_{\mu+1,i}^n) \left( \frac{L_{\mu,i}/K_i}{1+Np^\mu x} \right) = \prod_{y=0}^{p-1} g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_i)^{\frac{(K_i)(Np^\mu+1)/K_i}{(1+Np^\mu (x+y^\sqrt{-d_i}))}}.
\]

Write \( 1+Np^\mu(x+y\sqrt{-d_i}) = a\theta_i + b \) with \( a, b \in \mathbb{Z} \). Then we deduce by Proposition 4.2
\[
g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_i)^{\frac{(K_i)(Np^\mu+1)/K_i}{(1+Np^\mu (x+y\sqrt{-d_i}))}} = g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_i)^{\frac{(K_i)(Np^\mu+1)/K_i}{(1+Np^\mu (x+y^\sqrt{-d_i}))}}.
\]

If \( i = 1 \), then \( a = 2Np^\mu y \) and \( b = 1 + Np^\mu(x+y) \); hence by Proposition 4.11 and Lemma 4.3 we derive
\[
g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_1) = g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_1) = g_{(0,1+Np^\mu y)}^{12Np^\mu+1}(\theta_1)^{\frac{(K_i)(Np^\mu+1)/K_i}{(1+Np^\mu (x+y^\sqrt{-d_i}))}}.
\]
Since \(-a_1 - a + b \equiv 1 + Np^\mu (x + (p - 1)y \sqrt{-d_1}) \pmod{Np^{\mu + 1}O_{K_1}}, we get that

\[ N_{(K_1)_{(Np^{\mu + 1})/L_{p,1}}}(\gamma_{p+1,1}^{\mu}) \in \mathbb{R}. \]

If \(i = 2\), then \(a = Np^\mu y\) and \(b = 1 + Np^\mu x\), and so again by Proposition 4.1 and Lemma 4.3 we achieve

\[ g_{12}^{(Np^{\mu + 1})}N_{p,1}^{(\gamma_{p+1,1}^{\mu})}(\theta_2) = g_{12}^{(Np^{\mu + 1})}N_{p,1}^{(\gamma_{p+1,1}^{\mu})}(\theta_2) = g_{12}^{(Np^{\mu + 1})}N_{p,1}^{(\gamma_{p+1,1}^{\mu})}(\theta_2). \]

Now that \(-a_2 - b \equiv 1 + Np^\mu (x + (p - 1)y \sqrt{-d_2}) \pmod{Np^{\mu + 1}O_{K_2}}, we conclude that

\[ N_{(K_2)_{(Np^{\mu + 1})/L_{p,2}}}(\gamma_{p+1,2}^{\mu}) \in \mathbb{R}. \]

\[ \Box \]

**Theorem 7.8.** Let \(N, \mu\) be two positive integers and \(p\) be an odd prime such that \((N, p) = 1\) and \((d_i^0) \neq 1\) for some \(i_0' \in \{1, 2\}\). We assume the followings:

(i) \(K_1, K_2 \neq \mathbb{Q}(-1), \mathbb{Q}(-3)\),

(ii) \(\mu \geq \mu_0\),

(iii) \(N\) has no prime factor which splits completely in \(K_{i_0'}\), namely, \(Np^{\mu + 1}\) has the prime factorization

\[ Np^{\mu + 1} = \prod_{i=1}^{r_1 + r_2} p_i^{\epsilon_i}, \]

where each \(p_i\) is a rational prime for which

\[ \left( \frac{-d_i'}{p_i} \right) = \begin{cases} -1 & \text{if } 1 \leq i \leq r_1 \\ 0 & \text{if } r_1 + 1 \leq i \leq r_1 + r_2. \end{cases} \]

(iv) For each index \(1 \leq i \leq r_1 + r_2\) there exists an odd prime \(v_i\) such that \(v_i \nmid \epsilon_i\) and \(ord_{v_i}(\epsilon_i) > ord_{v_i}(p)\) where

\[ \tilde{\epsilon}_i = \begin{cases} p_i^{2\epsilon_i - 2}(p_i^2 - 1) & \text{if } 1 \leq i \leq r_1 \\ p_i^{2\epsilon_i - 1}(p_i - 1) & \text{if } r_1 + 1 \leq i \leq r_1 + r_2, \end{cases} \]

\[ \epsilon_i = \prod_{1 \leq j \leq r_1 + r_2, j \neq i} \tilde{\epsilon}_j. \]

Then for any positive integer \(n\), we have

\[ K_{N,p,\mu}^3 = K_{(Np^\mu)} \left( N_{K_{N,p,\mu}^3/K_{N,p,\mu}^3}(\gamma_{p+1}^n) \right). \]
PROOF. We claim that $L_{\mu,\nu_0}$ satisfies the assumptions in Proposition 4.5 for $K_{\mu_0}$. Indeed, for each index $1 \leq i \leq r_1 + r_2$,

\[ \hat{\epsilon}_i = \# \ker \left( \pi_{Np^{\mu}+1}\mathfrak{O}_{K_{\mu_0}} \left( \mathfrak{O}_{K_{\mu_0}}^\times \right) \xrightarrow{\text{proj}} \pi_{Np^{\mu}+1+p_i-\nu_0}\mathfrak{O}_{K_{\mu_0}} \left( \mathfrak{O}_{K_{\mu_0}}^\times \right) \right) \]

and by the assumption (iv) we get

\[ \text{ord}_{\nu_i}(\hat{\epsilon}_i) > \text{ord}_{\nu_i}(p) = \text{ord}_{\nu_i}(\left( (K_{\mu_0})_{(Np^{\mu}+1)} : L_{\mu,\nu_0} \right)) \].

Thus we derive by Proposition 4.5

\[ L_{\mu,\nu_0} = K_{\mu_0} \left( N(K_{\mu_0})_{(Np^{\mu}+1)} : L_{\mu,\nu_0} \left( \gamma_{\mu+1,\nu_0}^n \right) \right) \].

Therefore, the theorem follows from Lemma 7.6 and (7.7).

\[ \square \]

REMARK 7.9. When $N = 1$, the assumptions (iii), (iv) are always satisfied. Indeed, $\nu_1 = p$ is an odd prime satisfying $\text{ord}_{\nu_1}(\hat{\epsilon}_i) > \text{ord}_{\nu_1}(p)$.

EXAMPLE 7.10. Let $K = \mathbb{Q}(\sqrt{-15}, \sqrt{-26})$, $N = 5$ and $p = 37$ as in Example 6.14 (i). Then $\varepsilon_0 = 79 + 4\sqrt{390}$, $\ell_0 = 190$, $\mu_0 = 1$ and $\nu_0 = 1$. Hence by Corollary 7.5 and (6.27) we get that for any positive integers $n_1, n_2$ and $\mu$,

\[ K_{(5,37^{\mu})} = K_{(5)} \left( g_{0, \frac{60\cdot37^{\mu}n_1}{15\sqrt{15}}}^1(\theta_1)g_{0, \frac{60\cdot37^{\mu}n_2}{26\sqrt{26}}}^1(\theta_2) \right) \]

where $\theta_1 = -\frac{1+\sqrt{-15}}{2}$ and $\theta_2 = \sqrt{-26}$.

Let $p_1 = 5$ and $p_2 = 37$ so that $Np^{\mu+1} = p_1p_2^{\mu+1}$. It follows from the assumption (iv) in Theorem 7.8 that

\[ \hat{\epsilon}_1 = 2^2 \cdot 5, \quad \hat{\epsilon}_2 = 2^3 \cdot 3^2 \cdot 19 \cdot 37^{2\mu} \]

\[ \epsilon_1 = 2^3 \cdot 3^2 \cdot 19 \cdot 37^{2\mu}, \quad \epsilon_2 = 2^2 \cdot 5. \]

Then $\nu_1 = 5$ and $\nu_2 = 3$ are odd primes satisfying $\nu_i \nmid \epsilon_i$ and $\text{ord}_{\nu_i}(\hat{\epsilon}_i) > \text{ord}_{\nu_i}(37)$ for each $i = 1, 2$. Therefore, we obtain by Theorem 7.8

\[ \overline{K}_{5,37^{\mu}}^3 = K_{(5,37^{\mu})} \left( N_{K_{5,37^{\mu}}/K_{5,37^{\mu}}^3} \left( g_{0, \frac{60\cdot37^{\mu+1}n}{15\sqrt{15}}}^1(\theta_1) \right) \right) \]

for any positive integer $n$. And, by (7.6) we derive

\[ \text{Gal} \left( \overline{K}_{5,37^{\mu}}^1/\overline{K}_{5,37^{\mu}}^3 \right) = \left( \frac{\overline{K}_{5,37^{\mu}}^1/\overline{K}_{5,37^{\mu}}}{1 + 5 \cdot 37^{2\mu}\sqrt{-15}} \right). \]
Since \( N_{K/K_1}(1 + 5 \cdot 37^\mu \sqrt{-15}) \equiv 20 \cdot 37^\mu \theta_1 + 1 + 10 \cdot 37^\mu \pmod{5 \cdot 37^\mu + \mathcal{O}_{K_1}} \), it follows from Proposition 4.2 that for \((r_1, r_2) \in \frac{1}{5 \cdot 37^\mu + 1} \mathbb{Z}^2 \setminus \mathbb{Z}^2\),

\[
g_{(r_1, r_2)}(\theta_1) \left( \frac{K_3}{(1 + 5 \cdot 37^\mu \sqrt{-15})} \right) = g_{(r_1, r_2)}(\theta_1) \left( \frac{(K_1)(5 \cdot 37^\mu + 1)}{(20 \cdot 37^\mu + 1 + 10 \cdot 37^\mu)} \right) = g_{(r_1, r_2)}(\theta_1) \left( \frac{1 - 10 \cdot 37^\mu}{20 \cdot 37^\mu} \frac{31 \cdot 37^\mu}{1 + 10 \cdot 37^\mu} \right).
\]

Thus, we achieve

\[
N_{K_3/\mathbb{Q}(\sqrt{-15})}(g_{(0, \frac{1}{5 \cdot 37^\mu + 1})}(\theta_1)) = \prod_{i=0}^{p-1} g_{(0, \frac{1}{5 \cdot 37^\mu + 1})}(\theta_1) = \prod_{i=0}^{p-1} \left( \frac{1 - 10 \cdot 37^\mu}{20 \cdot 37^\mu} \frac{31 \cdot 37^\mu}{1 + 10 \cdot 37^\mu} \right)^i.
\]

### 8 Generation of ray class fields over real quadratic fields

In this section, we shall construct the ray class field \((K_3)_{(p)}\) over the Hilbert class field \((K_3)_{(1)}\) by making use of the primitive generator of the field \(\mathbb{Q}(\sqrt{-15})\). Let \(I_F(m)\) be the group of all fractional ideals of \(F\) which are relatively prime to \(m\) and \(P_{F,1}(m)\) be the subgroup of \(I_F(m)\) generated by the principal ideals \(a\mathcal{O}_F\), where \(a \in \mathcal{O}_F\) satisfies

(i) \( a \equiv 1 \pmod{m_0} \)

(ii) \( \sigma(a) > 0 \) for every real infinite prime \( \sigma \) dividing \( m_\infty \).

Further, we let \( Cl_F(m) = I_F(m)/P_{F,1}(m) \) be the ray class group modulo \( m \). For a finite extension \( L \) of \( F \), we denote by \( \Delta(L/F) \) the discriminant ideal of \( \mathcal{O}_L \) over \( \mathcal{O}_F \) [11, Chapter I §7].

**Proposition 8.1.** Let \( E, L \) be finite extensions of a number field \( F \).

(i) For a tower of number fields \( F \subset L \subset M \),

\[
\Delta(M/F) = N_{L/F}(\Delta(M/L)) \Delta(L/F)^{[M:L]}.
\]

(ii) A prime ideal \( p \) of \( F \) is ramified in \( L \) if and only if \( p \) divides \( \Delta(L/F) \).

(iii) Assume that \( E \) and \( L \) are linearly disjoint over \( F \) and \( \Delta(E/F), \Delta(L/F) \) are relatively prime. Then

\[
\Delta(EL/F) = \Delta(E/F)^{[L:F]} \Delta(L/F)^{[E:F]}.
\]
Proof. (i) [24, Chapter III, Corollary 2.10].

(ii) [24, Chapter III, Corollary 2.12].

(iii) [20, Chapter III, Proposition 17].

Proposition 8.2. With the notations as above, let $H$ be a congruence group modulo $m$ and $L$ be a class field of $F$ corresponding to $H$. For any modulus $n$ dividing $m$, we let $s_n: Cl_F(m) \to Cl_F(n)$ be the canonical surjection and set $h_{n,H} = |Cl_F(n)/s_n(H)|$, where $\mathcal{H} = H/P_{F,1}(m)$. If $m = \prod_i p_i^{e_i}$ is the prime decomposition of $m$, then

$$
\Delta(L/F) = \prod_i p_i^{e_i h_{m,H} - \sum_{j=1}^{e_i} h_{m/p_j^i,H}}.
$$

Proof. [6, Theorem 3.3]

Now, we adopt the notations in Section 6. Let $h_K$ and $h_i$ ($1 \leq i \leq 3$) be the class numbers of $K$ and $K_i$, respectively. Then we get by [18]

$$
h_K = \frac{1}{2} Q(K) h_1 h_2 h_3,
$$

where $Q(K) = [\mathcal{O}_K^\times : \mathcal{O}_{K_1}^\times \mathcal{O}_{K_2}^\times \mathcal{O}_{K_3}^\times]$. Let $p$ be an odd prime such that $p \equiv 1 \pmod{4}$ and $
\left( \frac{d}{p} \right) = -1.
$ Then $p\mathcal{O}_K$ is a prime ideal of $K_3$ and $p\mathcal{O}_K = \mathcal{P}_1 \mathcal{P}_2$ for some prime ideals $\mathcal{P}_1 \neq \mathcal{P}_2$ of $K$. Let $\theta_i$ for $i = 1, 2$ be as in (6.2) and set $i'_0 \in \{1, 2\}$ such that $\left( \frac{-d_{i_0}}{p} \right) = -1$.

Now, we assume that

$$
(i) \quad K_1, K_2 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}),
(ii) \quad N = 1 \text{ and } n_0 = \frac{p+1}{2} \text{ or } p+1,
(iii) \quad \frac{N}{{K_1, K_2, K_3}} \left( \frac{12p^2_n}{n_{I,p}}(\theta_i) \right) \text{ generates } \widehat{K}_{3,1,p,0} \text{ over } K_{(1)} \text{ for some } n \in \mathbb{Z}_{>0} \text{ and } I \in \{1, 2\}.
$$

It then follows from Theorem [6.12] that the assumption (iii) is valid for any $n \in \mathbb{Z}_{>0}$ and $I = i'_0$ if there exists an odd prime dividing $p - 1$. By (6.21), (6.22), (8.1) and Corollary
we have the following diagram

\[
\begin{array}{c}
\overset{p-1}{K_1} \quad \overset{Q(K)h_1h_2}{Q(K)} \quad (K_3)_{(p)} \quad (K_3)_{(1)} \\
\overset{h_K}{K} \quad \overset{Q(K)h_1h_2}{Q(K)} \quad p-1 \\
\overset{2}{K} \quad \overset{h_3}{K} \quad K_3.
\end{array}
\]

**Lemma 8.3.** With the notations and assumptions as above, \( p\mathcal{O}_{K_3} \) is the only prime ideal of \( K_3 \) which ramifies in the field \((K_3)_{(1)} \left( N_{K_3/\mathcal{O}_{K_3}} \left( g_{(0,1, p)}^{12\text{pn}}(\theta_I) \right) \right) \).

**Proof.** Observe that \( \Delta(K_1/\mathbb{Q}) = -d_1\mathbb{Z}, \Delta(K_2/\mathbb{Q}) = -4d_2\mathbb{Z} \) and \( \Delta(K_3/\mathbb{Q}) = 4d_1d_2\mathbb{Z} \). Since \( \Delta(K_1/\mathbb{Q}) \) and \( \Delta(K_2/\mathbb{Q}) \) are relatively prime, by Proposition 8.1 (iii) we attain

\[
\Delta(K/\mathbb{Q}) = \Delta(K_1/\mathbb{Q})^2\Delta(K_2/\mathbb{Q})^2 = 16d_1^2d_2^2\mathbb{Z}.
\]

On the other hand, we see from Proposition 8.1 (i) that

\[
\Delta(K/\mathbb{Q}) = N_{K_3/\mathbb{Q}}(\Delta(K/K_3)) \cdot 16d_1^2d_2^2\mathbb{Z}.
\]

Hence we obtain \( \Delta(K/K_3) = \mathcal{O}_{K_3}. \) Since \( \overset{K_3}{\sim}_{1,p,0} \) is a subfield of \( (K)_{(p)} \), we get by Proposition 8.2

\[
\Delta(\overset{K_3}{\sim}_{1,p,0}/K) = \prod_{i=1}^{2} p_i^{h_{p\mathcal{O}_K, G_3} - h_{p\mathcal{O}_K, G_3}},
\]

where \( G_3 \) is the congruence subgroup modulo \( p\mathcal{O}_K \) corresponding to \( \overset{K_3}{\sim}_{1,p,0} \). Note that \( \Delta(\overset{K_3}{\sim}_{1,p,0}/K) \neq \mathcal{O}_K \) because \( K_{(1)} \subsetneq \overset{K_3}{\sim}_{1,p,0} \). Thus by Proposition 8.1 (i) we derive

\[
\Delta(\overset{K_3}{\sim}_{1,p,0}/K_3) = N_{K_3/K} (\Delta(\overset{K_3}{\sim}_{1,p,0}/K)) \cdot \Delta(K/K_3)^{(p-1)h_K} = (p\mathcal{O}_{K_3})^e \text{ for some integer } e \in \mathbb{Z}_{>0}.
\]

It then follows from Proposition 8.1 (ii) that any prime ideal of \( K_3 \) which ramifies in \( \overset{K_3}{\sim}_{1,p,0} \) divides \( p\mathcal{O}_{K_3} \). Since \( (K_3)_{(1)} \left( N_{K_3/\mathcal{O}_{K_3}} \left( g_{(0,1, p)}^{12\text{pn}}(\theta_I) \right) \right) \) is a subfield of \( \overset{K_3}{\sim}_{1,p,0} \), we establish the lemma.

\[\square\]
THEOREM 8.4. Let $p$ be an odd prime such that $p \equiv 1 \pmod{4}$ and $(\frac{d_1d_2}{p}) = -1$. We admit the assumption (8.2). If $h_I = 1$ or $Q(K)h_1 h_2 = 2$, then we get

$$(K_3)_{(p)} = (K_3)_{(1)} \left( N_{\tilde{K}^3_{1,p,0}/K_3^{(1)}}(\gamma_{0}) \right).$$

Moreover, the singular value $N_{\tilde{K}^3_{1,p,0}/K_3^{(1)}}(\gamma_{0})$ is a totally real algebraic integer.

PROOF. For simplicity, we denote the value $N_{\tilde{K}^3_{1,p,0}/K_3^{(1)}}(\gamma_{0})$ by $\gamma_0$. First, assume $h_I = 1$, that is, $(K_I)_{(1)} = K_I$. And, observe that we have the decomposition

$$\text{Gal} \left( K_I(\gamma_0)/\mathbb{Q} \right) = \text{Gal} \left( K_I(\gamma_0)/K_I \right) \sqcup \rho \text{Gal} \left( K_I(\gamma_0)/K_I \right),$$

where $\rho$ stands for the complex conjugation in $\mathbb{C}$. Since $\gamma_0^\sigma \in \mathbb{R}$ for all $\sigma \in \text{Gal} \left( K_I(\gamma_0)/K_I \right)$ by Lemma 6.11, the value $\gamma_0$ is a totally real algebraic integer. Moreover, $\mathbb{Q}(\gamma_0)$ is an abelian extension of $\mathbb{Q}$. We then see from Lemma 8.3 that $(K_3)_{(1)}(\gamma_0)$ is an abelian extension of $K_3$ unramified outside the modulus $p\mathcal{O}_{K_3}$, and so we derive $(K_3)_{(1)}(\gamma_0) \subseteq (K_3)_{(p)}$. Since

$$(8.3) \quad [(K_3)_{(p)} : (K_3)_{(1)}] = p - 1 = \left[ K_I(\gamma_0) : K_I \right] \leq \left[ (K_3)_{(1)}(\gamma_0) : (K_3)_{(1)} \right]$$

by the assumption (8.2), we conclude $(K_3)_{(p)} = (K_3)_{(1)}(\gamma_0)$.

Next, we assume that $Q(K)h_1 h_2 = 2$. Then $K_{3,p,0}$ is a CM-field with a totally real subfield $(K_3)_{(p)}$. Thus the restriction of $\rho$ to $K^3_{1,p,0}$ is an automorphism of $K^3_{1,p,0}$, and $\alpha^\rho = \alpha^\sigma$ for every embedding $\sigma$ of $K^3_{1,p,0}$ into $\mathbb{C}$ and $\alpha \in K^3_{1,p,0}$ (9.4 Lemma 18.2). Hence $\gamma_0$ is a totally real algebraic integer by Lemma 6.11. Now that we have the decomposition

$$\text{Gal} \left( K^3_{1,p,0}/K_3 \right) = \text{Gal} \left( K^3_{1,p,0}/K \right) \sqcup \rho \text{Gal} \left( K^3_{1,p,0}/K \right),$$

the field $K^3_{1,p,0}$ is an abelian extension of $K_3$. Therefore, $(K_3)_{(1)}(\gamma_0)$ is an abelian extension of $K_3$ unramified outside the modulus $p\mathcal{O}_{K_3}$ again by Lemma 8.3. In a similar way as in (8.3), one can derive the theorem, too. \hfill \Box

REMARK 8.5. (i) There are 9 imaginary quadratic fields with class number 1, namely,

$$\mathbb{Q}(\sqrt{-n}), \quad n = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

(37). Hence, if $K_1$ or $K_2$ is one of these fields other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, then we can construct $(K_3)_{(p)}$ over $(K_3)_{(1)}$ for suitable odd primes $p$. 

46
(ii) We see that there are 39 imaginary biquadratic fields \( \mathbb{Q}(\sqrt{-d_1}, \sqrt{-d_2}) \) satisfying 
- \(-d_1 \equiv 1 \pmod{4} \), 
- \(-d_2 \equiv 2, 3 \pmod{4} \), 
- \((d_1, d_2) = 1\), 
- \(-d_1 \neq -3\), 
- \(-d_2 \neq -1\) and 
\(Q(K)h_1h_2 = 2\). Among them there are 6 imaginary biquadratic fields for which 
\(Q(K) = 2\) and \(h_1 = h_2 = 1\), that is,

\[
\mathbb{Q}\left(\sqrt{-n}, \sqrt{-2}\right), \quad n = 7, 11, 19, 43, 67, 163
\]

([37]). And, there are 33 imaginary biquadratic fields such that \(Q(K) = 1\) and \(h_1h_2 = 2\), namely,

\[
\begin{align*}
\mathbb{Q}\left(\sqrt{-n}, \sqrt{-2}\right), & \quad n = 15, 35, 91, 115, 403, \\
\mathbb{Q}\left(\sqrt{-7}, \sqrt{-n}\right), & \quad n = 5, 10, 13, \\
\mathbb{Q}\left(\sqrt{-11}, \sqrt{-n}\right), & \quad n = 6, 13, 58, \\
\mathbb{Q}\left(\sqrt{-19}, \sqrt{-n}\right), & \quad n = 6, 13, 37, 58, \\
\mathbb{Q}\left(\sqrt{-43}, \sqrt{-n}\right), & \quad n = 5, 6, 10, 22, 37, 58, \\
\mathbb{Q}\left(\sqrt{-67}, \sqrt{-n}\right), & \quad n = 5, 6, 10, 13, 22, \\
\mathbb{Q}\left(\sqrt{-163}, \sqrt{-n}\right), & \quad n = 5, 6, 10, 13, 22, 37, 58,
\end{align*}
\]

([3]).

We mean by \(\infty\) the modulus of \(K_3\) including all real infinite primes, and by \((K_3)_{(p, \infty)}\) the ray class field of \(K_3\) modulo \(p\mathcal{O}_{K_3} \cdot \infty\). Let

\[
S_{1,p,\infty}^{(3)} = \{ a \in K_3^* \mid a \equiv 1 \pmod{p\mathcal{O}_{K_3}}, \sigma(a) > 0 \text{ for all } \sigma \text{ dividing } \infty\},
\]
\[
H_{1,p,\infty}^{(3)} = S_{1,p,\infty}^{(3)} \cap \mathcal{O}_{K_3}^\times.
\]

Then we have

\[
\text{Gal}((K_3)_{(p, \infty)})/(K_3)_{(p)}) \cong S_{1,p,1}^{(3)} \mathcal{O}_{K_3}^\times/S_{1,p,\infty}^{(3)} \mathcal{O}_{K_3}^\times \cong S_{1,p,1}^{(3)}/H_{1,p,\infty}^{(3)}
\]

by class field theory ([34 Chapter V §6]). It is clear that \(|S_{1,p,1}^{(3)}/S_{1,p,\infty}^{(3)}| = 4\). Further, we observe that

\[
S_{1,p,1}^{(3)} \cap \mathcal{O}_{K_3}^\times = \begin{cases} 
\langle \varepsilon_0^{n_0} \rangle & \text{if } n_0 \text{ is odd} \\
\langle -\varepsilon_0^{n_0} \rangle & \text{if } n_0 \text{ is even}
\end{cases}
\]

Since \(N_{K_3/\mathbb{Q}}(\varepsilon_0) = 1\), it follows that

\[
|H_{1,p,\infty}^{(3)}/S_{1,p,\infty}^{(3)}| = \begin{cases} 
1 & \text{if } n_0 \text{ is odd} \\
2 & \text{if } n_0 \text{ is even}
\end{cases}
\]

Therefore, we attain

\[
(K_3)_{(p, \infty)}/(K_3)_{(p)} = \frac{|S_{1,p,1}^{(3)}/S_{1,p,\infty}^{(3)}|}{|H_{1,p,\infty}^{(3)}/S_{1,p,\infty}^{(3)}|} = \begin{cases} 
4 & \text{if } n_0 \text{ is odd} \\
2 & \text{if } n_0 \text{ is even}
\end{cases}
\]
COROLLARY 8.6. With the notations and assumptions as in Theorem 8.4, we derive

$$\left[ (K_3)(\infty) : K(K_3)_{(1)} \left( N_{K_1,p,0/K_1^1,p,0} \left( g_{(0,1/p)}^{12m}(\theta_I) \right) \right) \right] = \begin{cases} 2 & \text{if } n_0 = p+1 \\ 1 & \text{if } n_0 = p+1. \end{cases}$$

PROOF. The proof of Lemma 8.3 shows that $K$ is an abelian extension of $K_3$ unramified outside the modulus $\infty$. Hence $K \subseteq (K_3)(\infty)$. Since $(K_3)(p)$ is totally real, $[K(K_3)(p) : (K_3)(p)] = 2$. Then the corollary is immediate from Theorem 8.4 and (8.4).

\[\Box\]

EXAMPLE 8.7. (i) Let $K = \mathbb{Q}(\sqrt{-7}, \sqrt{-2})$, $N = 1$ and $p = 37$ as in Example 6.14

(ii). Then $K_1 = \mathbb{Q}(\sqrt{-7})$, $K_2 = \mathbb{Q}(\sqrt{-2})$, $K_3 = \mathbb{Q}(\sqrt{14})$, $h_1 = h_2 = h_3 = 1$, $Q(K) = 2$ and $n_0 = p+1$. And, it satifies the assumptions in Theorem 8.4 and hence we conclude that

$$(K_3)_{(37)} = K_3 \left( N_{K_1,37,0/K_1,37,0} \left( g_{(0,1/37)}^{444n}(\theta_I) \right) \right),$$

$$(K_3)_{(37\infty)} = K \left( N_{K_1,37,0/K_1,37,0} \left( g_{(0,1/37)}^{444n}(\theta_I) \right) \right).$$

for any positive integer $n$.

(ii) Let $K = \mathbb{Q}(\sqrt{-31}, \sqrt{-2})$. Then $K_1 = \mathbb{Q}(\sqrt{-31})$, $K_2 = \mathbb{Q}(\sqrt{-2})$, $K_3 = \mathbb{Q}(\sqrt{62})$, $h_1 = 3$, $h_2 = h_3 = 1$, $Q(K) = 2$ and $\varepsilon_0 = 63 + 8\sqrt{62}$. We set $N = 1$ and $p = 5$ so that $\left( \frac{62}{p} \right) = -1$, $i_0^* = 2$ and $n_0 = p+1$. One can then readily get

$$W_{1,5,0}^{1,3} = \langle 3 + \sqrt{-2} + 5\mathcal{O}_K \rangle,$$

and so by Remark 6.13 (i) we obtain

$$\text{Gal}(\tilde{K}_{1,5,0}/K_{1,5,0}) = \left\langle \left( \frac{\tilde{K}_{1,5,0}/K}{3 + \sqrt{-2}} \right) \right\rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

On the other hand, 2 is a primitive root modulo 5 and

$$N_{K/Q}(1 + 3\sqrt{-2} + 2\sqrt{62}) \equiv N_{K_2/Q}(\sqrt{-2}) \equiv 2 \pmod{5}.$$ 

Thus by (6.26) we achieve $\text{Gal}(\tilde{K}_{1,5,0}/K_{1,5,0}) = \left\langle \left( \frac{\tilde{K}_{1,5,0}/K}{1 + 3\sqrt{-2} + 2\sqrt{62}} \right) \right\rangle \cong \mathbb{Z}/4\mathbb{Z}.$

If we let $\theta_2 = \sqrt{-2}$, then

$$N_{K/K_2}(3 + \sqrt{-2}) \equiv \theta_2 + 2 \pmod{5\mathcal{O}_{K_2}},$$

$$N_{K/K_2}(1 + 3\sqrt{-2} + 2\sqrt{62}) \equiv \theta_2 \pmod{5\mathcal{O}_{K_2}}.$$
By Proposition 4.2 we derive that for \((r_1, r_2) \in \frac{1}{5} \mathbb{Z}^2 \setminus \mathbb{Z}^2\)
\[
g^{60}_{(r_1, r_2)}(\theta_2) \left( \frac{K_{1,5,0}^2/K}{(1+\sqrt{-3})} \right) = g^{60}_{(r_1, r_2)}(\theta_2) \left( \frac{60}{\theta_2 + 3} \right) = g^{60}_{(r_1, r_2)} \left( \begin{array}{cc} 2 & -2 \\ 1 & 2 \end{array} \right) \theta_2.
\]

Hence the conjugates of \(\gamma_0 = N_{\widehat{K}_{1,5,0}/K_{1,5,0}} \left( \frac{g^{60}_{(0,1)}(\theta_2)}{g^{60}_{(0,1)}}(\theta_2) \right)\) over \(K_{(1)}\) are
\[
\gamma_0 = g^{60}_{(0,1)}(\theta_2) g^{60}_{(1,2)}(\theta_2) g^{60}_{(2,3)}(\theta_2) \approx 1.9536503584 \times 10^{-10},
\gamma_1 = g^{60}_{(1,2)}(\theta_2) g^{60}_{(2,3)}(\theta_2) g^{60}_{(3,4)}(\theta_2) \approx 5.7741480125 \times 10^{12},
\gamma_2 = g^{60}_{(2,3)}(\theta_2) g^{60}_{(3,4)}(\theta_2) g^{60}_{(4,5)}(\theta_2) \approx 8.3960306665 \times 10^{13},
\gamma_3 = g^{60}_{(3,4)}(\theta_2) g^{60}_{(4,5)}(\theta_2) g^{60}_{(5,6)}(\theta_2) \approx 9833.1204783.
\]

Since the conjugates of \(\gamma_0\) are distinct, the singular value \(\gamma_0\) generates \(\widehat{K}_{1,5,0}\) over \(K_{(1)}\); hence by Theorem 8.4 and Corollary 8.6 we conclude that
\[
(K_3)_{(5)} = K_3 \left( N_{\widehat{K}_{1,5,0}/K_{1,5,0}} \left( g^{60}_{(0,1)}(\theta_2) \right) \right),
(K_3)_{(5\infty)} = K \left( N_{\widehat{K}_{1,5,0}/K_{1,5,0}} \left( g^{60}_{(0,1)}(\theta_2) \right) \right).
\]

Furthermore, the minimal polynomial of \(\gamma_0\) over \(\mathbb{Q}\) is
\[
\min(\gamma_0, \mathbb{Q}) = (X - \gamma_0)(X - \gamma_1)(X - \gamma_2)(X - \gamma_3)
= X^4 - (8.97344546875 \times 10^{13})X^3 + (4.8479923874121649169921875 \times 10^{26})X^2
- (4.7670893136567592620849609375 \times 10^{30})X + 9.31322574615478515625 \times 10^{20}.
\]

9 Normal basis

Let \(L\) be a finite abelian extension of a number field \(F\) with \(G = \text{Gal}(L/F)\). Then the normal basis theorem ([10]) guarantees the existence of an element \(\alpha\) in \(L\) whose Galois conjugates over \(F\) form a basis of \(L\) over \(F\) as a vector space. We call such a basis \(\{\alpha^\sigma \mid \sigma \in G\}\) a normal basis of \(L\) over \(F\). On the other hand, Jung et al ([13]) found a criterion for a normal basis induced from the Frobenius determinant relation ([19, Chapter 21]) as follows.
Proposition 9.1. The conjugates of an element $\alpha \in L$ form a normal basis of $L$ over $F$ if and only if
\[ \sum_{\sigma \in G} \chi(\sigma^{-1})\alpha^\sigma \neq 0 \quad \text{for all } \chi \in \hat{G}, \]
where $\hat{G}$ is the character group of $G$.

Proof. See [13] Proposition 2.3. \hfill \square

In this section we adopt the notations and assumptions in Theorem 8.4 and construct a normal basis of $(K_3)_{(p)}$ over the Hilbert class field $(K_3)_{(1)}$ by using the recent new idea of Koo-Shin [16]. Let $G = \text{Gal}((K_3)_{(p)}/(K_3)_{(1)})$ and $\hat{G}$ be the character group of $G$. We see from Theorem 8.4 that $G$ is the restriction of $\text{Gal}(\bar{K}_{1,p,0}/K_{(1)})$ to the field $(K_3)_{(p)}$. Observe that one can derive by (6.26)
\[ \text{Gal}(\bar{K}_{1,p,0}/K_{(1)}) = \left( \frac{\bar{K}_{1,p,0}/K_{(1)}}{\omega_C} \right) \cong \mathbb{Z}/(p-1)\mathbb{Z}, \]
where $C$ is a primitive root modulo $p$ and $\omega_C$ is an element of $\mathcal{O}_K$ satisfying $N_{K/Q}(\omega_C) \equiv C \pmod{p}$. Let $\sigma \in G$ be the restriction of $\left( \frac{K_{1,p,0}/K_{(1)}}{\omega_C} \right)$ to $(K_3)_{(p)}$ so that $\sigma = |\sigma|$. Since $G$ is cyclic, we obtain
\[ \hat{G} = \left\{ \chi_i \mid 0 \leq i \leq p-2 \right\} \]
where $\chi_i : G \to \mathbb{C}^\times$ is a character of $G$ defined by $\chi_i(\sigma) = \zeta_i^{p^k-1}$. For an integer $k$ we set
\[ \sigma_k = \sigma^k, \]
\[ \gamma_k = \left( N_{K_{1,p,0}/K_{1,p,0}}^{\omega_{C}^{\sigma_{k}}} \left( g_{(0,1,p)}^{(12,m)}(\theta_{I}) \right) \right)^{\sigma_{k}}. \]
Here, we note by Theorem 8.4 that $\gamma_k$ is a totally real algebraic integer. For two integers $0 \leq i, j \leq p-2$, we let
\[ S(i, j) = \sum_{k=0}^{p-2} \chi_i(\sigma_k^{-1})\gamma_k^j = \sum_{k=0}^{p-2} \zeta_{p^k}^{-ki}\gamma_k^j. \]

Lemma 9.2. For a given integer $0 \leq \ell \leq p-2$, we get $S(\ell, m) \neq 0$ for some integer $0 \leq m \leq p-2$.

Proof. On the contrary, suppose that $S(\ell, j) = 0$ for every integer $0 \leq j \leq p-2$. Then we derive
\[ \begin{pmatrix} S(\ell, 0) \\ S(\ell, 1) \\ \vdots \\ S(\ell, p-2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \cdots & \gamma_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{p-2} & \gamma_1^{p-2} & \cdots & \gamma_{p-2}^{p-2} \end{pmatrix} \begin{pmatrix} \chi_\ell(\sigma_0^{-1}) \\ \chi_\ell(\sigma_1^{-1}) \\ \vdots \\ \chi_\ell(\sigma_{p-2}^{-1}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \]
And, the Vandermonde determinant formula implies that

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0^1 & \gamma_1^1 & \cdots & \gamma_{p-2}^1 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{p-2} & \gamma_1^{p-2} & \cdots & \gamma_{p-2}^{p-2} \end{pmatrix} = \prod_{0 \leq i < j \leq p-2} (\gamma_j - \gamma_i) \neq 0.$$ 

Thus $\chi_{\ell}(\sigma_k^{-1}) = 0$ for all $k$, which is a contradiction. \(\square\)

Observe that $S(i, j)$ is an algebraic integer in the field $(K_3)_{(p)}(\zeta_{p-1})$. On the other hand, by Theorem 6.12 we have the following diagram:

We then write

$$\text{Gal}(K_I(\gamma_0)/K_I) = \bigsqcup_{r=1}^{h_I} \eta_r \text{Gal}(K_I(\gamma_0)/(K_I)_{(1)})$$

where $\bigsqcup$ is the disjoint union. Then the conjugates of $\gamma_k$ over $\mathbb{Q}$ are

$$\{\gamma_k^{\eta_r} | 1 \leq r \leq h_I, \ 0 \leq s \leq p-2\}.$$ 

By [12, Theorem 2.4] we know the action of $\eta_r$ on $\gamma_k$ for each $r$ and $k$. For two integers $0 \leq i, j \leq p-2$, we let

$$N(i, j) = |N(K_3)_{(p)}(\zeta_{p-1})/\mathbb{Q}(S(i, j))|.$$ 

**Lemma 9.3.** For a given sequence of $d \ (\geq 1)$ nonnegative integers

$$N_1, N_2, \ldots, N_d,$$

there exists a sequence of $d$ positive integers

$$M_1, M_2, \ldots, M_d$$

such that
(i) \(M_i \geq 1 + N_i\) for every index \(1 \leq i \leq d\),

(ii) \(\gcd(M_i, N_i) = 1\) for every index \(1 \leq i \leq d\),

(iii) \(\gcd(M_i, M_j) = 1\) for \(i \neq j\).

**Proof.** Let \(M_0 = 1\) and

\[
M_i = 1 + N_i \prod_{k=0}^{i-1} M_k \quad \text{for } 1 \leq i \leq d.
\]

Then the sequence \(\{M_i\}_{1 \leq i \leq d}\) satisfies the properties (i)∼(iii). \(\square\)

For a sequence \(\{N(i, j)\}_{0 \leq i, j \leq p-2}\), we take a sequence \(\{M(i, j)\}_{0 \leq i, j \leq p-2}\) of positive integers as in the proof of Lemma 9.3.

**Theorem 9.4.** Let \(p\) be an odd prime such that \(p \equiv 1 \pmod{4}\) and \((\frac{d_1 d_2}{p}) = -1\). We admit the assumption (8.2). If \(h_1 = 1\) or \(Q(K) h_1 h_2 = 2\), then the conjugates of the singular value

\[
\beta = \sum_{j=0}^{p-2} \left( \sum_{i=0}^{p-2} \frac{1}{M(i, j)} \right) \gamma_0^j
\]

form a normal basis of \((K_3)_p\) over \((K_3)_1\). Here, \(\gamma_0 = N_{K_3_1, p,0/K_3_{1, p,0}} \left( g_{(0, \frac{1}{p})}^{12m}(\theta_1) \right)\).

**Proof.** Suppose that

\[
\sum_{k=0}^{p-2} \chi_\ell(\sigma_k^{-1}) \beta^{\sigma_k} = 0 \quad \text{for some integer } 0 \leq \ell \leq p - 2.
\]

It follows from Lemma 9.2 that there is an integer \(0 \leq m \leq p - 2\) satisfying \(S(\ell, m) \neq 0\). Then \(N(\ell, m) \geq 1\), and so \(M(\ell, m) \geq 2\) by Lemma 9.3. And, we have

\[
0 = \sum_{k=0}^{p-2} \chi_\ell(\sigma_k^{-1}) \sum_{j=0}^{p-2} \left( \sum_{i=0}^{p-2} \frac{1}{M(i, j)} \right) \gamma_k^j = \frac{1}{M(\ell, m)} \sum_{k=0}^{p-2} \chi_\ell(\sigma_k^{-1}) \gamma_k^m + \sum_{k=0}^{p-2} \chi_\ell(\sigma_k^{-1}) \sum_{0 \leq i, j \leq p-2 \atop (i, j) \neq (\ell, m)} \frac{1}{M(i, j)} \gamma_k^j = \frac{S(\ell, m)}{M(\ell, m)} \sum_{k=0}^{p-2} \chi_\ell(\sigma_k^{-1}) \sum_{0 \leq i, j \leq p-2 \atop (i, j) \neq (\ell, m)} \frac{1}{M(i, j)} \gamma_k^j.
\]

By multiplying \(\prod_{0 \leq i, j \leq p-2 \atop (i, j) \neq (\ell, m)} M(i, j)\) we attain

\[
S(\ell, m) \prod_{0 \leq i, j \leq p-2 \atop (i, j) \neq (\ell, m)} M(i, j) = M(\ell, m) \cdot \text{(an algebraic integer)}.
\]

52
Since \( \prod_{0 \leq i,j \leq p-2 \atop (i,j) \neq (\ell,m)} M(i,j) \) and \( M(\ell,m) \) are relatively prime by Lemma 9.3, the positive integer \( M(\ell,m) \) divides \( S(\ell,m) \). Hence \( M(\ell,m) \) also divides \( N(\ell,m) = |N(K_3(p))|/Q(S(\ell,m))| \), which contradicts the fact \( (M(\ell,m), N(\ell,m)) = 1 \). Therefore, the theorem follows from Proposition 9.1.

**Example 9.5.** Let \( K = \mathbb{Q}(\sqrt{-31}, \sqrt{-2}) \), \( N = 1 \), \( p = 5 \) and \( \gamma_i \) for \( 0 \leq i \leq 3 \) as in Example 8.7 (ii). Then \( K_3 = \mathbb{Q}(\sqrt{62}) \) with class number \( h_3 = 1 \), and the totally real algebraic integer \( \gamma_0 \) generates \( (K_3)_5 \) over \( K_3 \). Observe that \( (K_3)_p \) and \( Q(\zeta_4) \) are linearly disjoint over \( \mathbb{Q} \) because \( (K_3)_p \) is totally real. Now, we are ready to construct a normal basis of \( (K_3)_5 \) over \( K_3 \) by means of \( \gamma_0 \). For an integer \( k \), let \( \gamma'_k = \gamma_k \) with \( 0 \leq k \leq 3 \) satisfying \( k \equiv k \pmod{4} \), and set

\[
N(i,j) = \left| \prod_{s=0}^{3} \left( \sum_{k=0}^{\gamma'_k} \zeta_{4}^{-k(i)} \left( \sum_{k=0}^{\gamma'_k} \zeta_{4}^{k(i)} \right)^{j} \right) \right|^2 \text{ for } 0 \leq i, j \leq 3.
\]

Here, we take a sequence \( \{ M(i,j) \}_{0 \leq i,j \leq 3} \) of positive integers as in the proof of Lemma 9.3. Then it follows from Theorem 9.3 that the singular value

\[
\sum_{j=0}^{3} \left( \sum_{i=0}^{3} \frac{1}{M(i,j)} \right) \gamma'_j \approx 3.000000000023283
\]

forms a normal basis of \( (K_3)_5 \) over the real quadratic field \( K_3 = \mathbb{Q}(\sqrt{62}) \).

**References**

[1] A. Azizi, *Construction de la tour des 2-corps de classes de Hilbert de certains corps biquadratiques*, Pacific J. Math. 208 (2003), 1–10.

[2] S. Bae and Q. Yue, *Hilbert genus fields of real biquadratic fields*, Ramanujan J. 24 (2011), 161–181.

[3] E. Benjamin, *On the 2-class field tower of some imaginary biquadratic number fields*, Ramanujan J. 11 (2006), 103–110.

[4] D. A. Buell, H. C. Williams and K. S. Williams, *On the imaginary bicyclic biquadratic fields with class-number 2*, Math. Comp. 31 (1977), 1034–1042.

[5] S. Chowla, *The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation*, J. Number Theory 2 (1970), 120–123.

[6] H. Cohen, F. Diaz y Diaz and M. Olivier, *Computing ray class groups, conductors and discriminants*, Math. Comp. 67 (1998), 773–795.
[7] D. A. Cox, *Primes of the Form \( x^2 + ny^2 \): Fermat, Class Field, and Complex Multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[8] I. S. Eum, J. K. Koo and D. H. Shin, *Ring class invariants over imaginary quadratic fields*, arXiv:1007.2309v3, 2011

[9] I. S. Eum, J. K. Koo and D. H. Shin, *Some applications of modular units*, arXiv:1207.1609v2, 2012

[10] H. Hasse, *Neue bergründung der komplexen multiplikation*, Teil I, J. für Math. 157 (1927), 115–139, Teil II, J. für Math. 165 (1931), 64-88.

[11] G. J. Janusz, *Algebraic Number Fields*, 2nd ed., Graduate Studies in Mathematics, vol. 7. American Mathematical Society, Providence, 1996.

[12] H. Y. Jung, J. K. Koo and D. H. Shin, *Ray class invariants over imaginary quadratic fields*, Tohoku Math. J., 63 (2011), 413–426.

[13] H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, Math. Zeit. 271 (2012), 109–116.

[14] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge Studies in Advanced Mathematics, 20, Cambridge University Press, Cambridge, 1990.

[15] K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. 128 (2000), 315–323.

[16] J. K. Koo and D. H. Shin, *Generators for abelian extensions of basic number fields*, arXiv:1305.6781, 2013.

[17] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.

[18] T. Kubota, *Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers*, Nagoya Math. J. 6 (1953), 119–127.

[19] S. Lang, *Elliptic Functions*, 2nd ed., Spinger-Verlag, New York, 1987.

[20] S. Lang, *Algebraic Number Theory*, 2nd ed., Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[21] F. Lemmermeyer, *Conics - a poor man's elliptic curves*, arXiv:math/0311306v1, 2003
[22] B. Mazur, *How can we construct abelian Galois extensions of basic number fields?*, Bull. Amer. Math. Soc. 48 (2011), 155–209.

[23] J. Milne, *Class field theory*, notes available at [http://www.jmilne.org/math/](http://www.jmilne.org/math/)

[24] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften 322, Springer-Verlag, Berlin, 1999.

[25] T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (4) (1980/81), 341–345.

[26] K. Ramachandra, *Some applications of Kronecker’s limit formulas*, Ann. Math. (2) 80 (1964), 104–148.

[27] K. A. Ribet, *A modular construction of unramified $p$-extensions of $\mathbb{Q}(\mu_p)$*, Invent. Math. 34 (1976), 151–162.

[28] R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (3) (1991), 285–326.

[29] G. Shimura, *On the class-fields obtained by complex multiplication of abelian varieties*, Osaka Math. J. 14 (1962), 33–44.

[30] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains*, Ann. Math. (2) 91 (1970), 144–222.

[31] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains II*, Ann. Math. (2) 92 (1970), 528–549.

[32] G. Shimura, *Theta functions with complex multiplication*, Duke Math. J. 43 (1976), 673–696.

[33] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, 1994.

[34] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.

[35] C. L. Siegel, *Lectures on advanced analytic number theory*, Tata Institute of Fundamental Research Lectures on Mathematics, 23, Tata Institute of Fundamental Research, Bombay, 1965.
[36] P. J. Sime, *Hilbert class fields of real biquadratic fields*, J. Number Theory 50 (1995), 154–166.

[37] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27.

[38] T. Takagi, *Über eine Theorie des relativ-Abelschen Zahlkörpers*, J. Coll. Sci. Univ. Tokyo 41 (1920), 1–133.

[39] M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. Math. (2) 121 (1985), 519–535.

[40] B. L. van der Waerden, *Algebra, Vol I*, Springer-Verlag, 2003.

[41] H. Yokoi, *Imaginary bicyclic biquadratic fields with the real quadratic subfield of class-number one*, Nagoya Math. J. 102 (1986), 91–100.

Ja Kyung Koo
Department of Mathematical Sciences
KAIST
Daejeon 305-701
Republic of Korea
E-mail address: jkkoo@math.kaist.ac.kr

Dong Sung Yoon
Department of Mathematical Sciences
KAIST
Daejeon 305-701
Republic of Korea
E-mail address: yds1850@kaist.ac.kr