On Certain Cohomological Invariants of Quadratic Number Fields

by

Seok-Min Lee

A dissertation submitted to the Johns Hopkins University in conformity with the requirements for the degree of Doctor of Philosophy.

Baltimore, Maryland

May, 2004.

ABSTRACT

An idea of Poincaré about automorphic functions can be applied to an arbitrary (G, R) with a group G acting on a ring R. For a 1-cocycle c on the unit group $R^\times$, we can define a module M_c/P_c, which is an invariant depending only on the cohomology class $[c]$. We are mainly interested in the case where $G = \mathrm{Gal}(K/k)$ is the Galois group of number field extension and $R = \mathcal{O}_K$ is the ring of integers. We determine M_c/P_c completely for the case $K = \mathbf{Q}(\sqrt{m})$ the quadratic number field over $\mathbf{Q}$. For a nontrivial cocycle, the index depends on the parity of the coefficient v of the fundamental unit $\varepsilon = u + v\omega$ of $\mathcal{O}_K^\times$, and it is related to the central element of the continued fraction expansion of $\sqrt{m}$. We may generalize this computation using Hilbert 90.

Advisor: Takashi Ono.

ACKNOWLEDGEMENT

I would like to express my deep gratitude to my advisor, Professor Takashi Ono, for his advice, encouragement and patience throughout my research. This project would not have been possible without his guidance.

I also would like to express my thanks to Professor Hyun Kwang Kim, Professor Christian Popescu, Professor Qiao Zhang, Professor Yuichiro Taguchi and Professor Richard Mollin for their helpful comments.

I would like to extend my gratitude to my fellow peers Michael Krebs, Byungchul Cha, Nick Gajkowski, and Eun Kyung Lee for their great assistance on this project and several others.

I am very grateful to my parents, my parents in law, and my grandfather for their constant support and prayer. Finally, special thanks go to my wife Ok-Hee Jeon for her love and encouragement, and to my wonderful son Gene Jeon Lee.

Contents

1 Introduction

One important result about modular forms is that the space of cusp forms is generated by Poincaré series. This statement can be viewed in terms of cohomology. In this form, the statement is that $M_c/P_c = 0$, as in Section 2.2.2, where c is a cocycle of the modular group G in the unit group of the ring R of holomorphic functions on the upper half plane. (See Section 2.2.) We may apply this idea for a finite group G acting on a ring R, as noted by Ono [15] and Shafarevich [24, p. 395]. The cohomology set $H^1(G, R^\times)$ is defined to be the quotient set $Z^1(G, R^\times)/\sim$, where $Z^1(G, R^\times) = \{c : G \to R^\times \mid c_{st} = c_s\, {}^s c_t,\ c, t \in G\}$ is the set of cocycles, and the equivalence relation $\sim$ is defined by $c \sim c'$ if and only if there exists $u \in R^\times$ such that $c'_s = u^{-1} c_s\, {}^s u$ for all $s \in G$.

The set $H^1(G, R^\times)$ forms a group if R is commutative. For a cocycle c, we associate two modules M_c and P_c, as follows:

$$M_c = \{a \in R \mid c_s\, {}^s a = a,\ s \in G\}$$

and

$$P_c = \left\{ p_c(x) = \sum_{t \in G} c_t\, {}^t x \,\middle|\, x \in R \right\}.$$

M_c and P_c are $\mathbf{Z}$-modules in R. It is easy to see that $P_c \subset M_c$ and that M_c/P_c depends only on the class of c. In other words, $M_c/P_c = M_{c'}/P_{c'}$ for $c \sim c'$. In particular, if $c \sim 1$, we have $M_c/P_c = R^G/N_G R = \widehat{H}^0(G, R)$. Motivated by this, we think of M_c/P_c as the *twisted cohomology* $\widehat{H}^0(G, R)_\gamma$, where $\gamma = [c] \in H^1(G, R^\times)$. In view of Poincaré's results, it is natural to study the module $M_c/P_c = \widehat{H}^0(G, R)_\gamma$.

We are most interested in the case where $G = \mathrm{Gal}(K/k)$ for a Galois extension of number fields K/k, and $R = \mathcal{O}_K$ is the ring of integers of K. In particular, we have concrete descriptions for quadratic number fields.

Let $K = \mathbf{Q}(\sqrt{m})$ be a quadratic field; let $\mathcal{O}_K = [1, \omega]$ be the ring of integers of K where $\omega = \sqrt{m}$ if $m \equiv 2, 3 \pmod 4$ and $\omega = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$; and let $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle s \rangle$ with $s^2 = 1$. We can identify a cocycle c with a unit in $\mathcal{O}_K^\times$ of norm $N(c) = 1$. If $m > 0$, $\mathcal{O}_K^\times = \{\pm\varepsilon^j \mid j \in \mathbf{Z}\}$ where ε is the fundamental unit. The set of nonequivalent cocycle representatives for $H^1(G, \mathcal{O}_K^\times)$ consists of $\{1, i\}$ if $m = -1$, $\{\pm 1\}$ if $m < 0$ or $m > 0$ with $N(\varepsilon) = -1$, $\{\pm 1, \pm\varepsilon\}$ if $m > 0$ with $N(\varepsilon) = 1$.

For $c = \pm 1$, $M_c/P_c = 0$ if $m \equiv 1 \pmod 4$ and $M_c/P_c = \mathbf{Z}/2\mathbf{Z}$ otherwise. For $m = -1$ and $c = i$, we have that $M_c/P_c = 0$. For nontrivial cocycles $c = \pm\varepsilon$, the structure of the module M_c/P_c depends on m mod 4 and the parity of coefficient of the fundamental unit.

For $c = \pm\varepsilon = \pm(u + v\omega)$, define Δ_m by the relation $\mathbf{Z}/\Delta_m\mathbf{Z} = M_c/P_c$. (We have that $\Delta_m = 1$ or 2.) We denote by (a, b) the greatest common divisor of a and b. Let $d = (v, u-1)$ and $D = v/(v, u+1)$. In [15], it is shown that $\Delta_m = [M_\varepsilon : P_\varepsilon] = d/(D, d)$. (We provide full detailed verification of this fact in Section 4.2.) As one of our main results, we give a concrete description of $\Delta_m = |M_c/P_c|$ in terms of m and v.

Theorem (4.11 and 4.12). *If $m \equiv 1 \pmod 4$, then $|M_c/P_c| = 1$. If $m \equiv 2 \pmod 4$, then $|M_c/P_c| = 2$. If $m \equiv 3 \pmod 4$, then $|M_c/P_c| = 1$ if v is odd and $|M_c/P_c| = 2$ if v is even.*

To prove this theorem, we use the following results, each of which is a main lemma:

1. If v is odd, then $\Delta_m = 1$.
2. If v is even and ν is the maximal power of 2 in v, then $\Delta_m = 1$ if and only if $u \not\equiv \pm 1 \pmod{2^\nu}$.
3. If $\varepsilon = u + v\sqrt{m}$ with u, v integers and v even, then $\Delta_m = 2$.

For the case $m \equiv 3 \pmod 4$, the result is less explicit since the behavior of the fundamental unit is not well understood. The most practical way to compute the fundamental unit is through the continued fraction expansion of $\sqrt{m}$. Our second main result, which appears in Section 4.4.2, says that the parity of the central entry of the continued fraction expansion of $\sqrt{m}$ determines Δ_m.

Theorem (4.21). *Let $m \equiv 3 \pmod 4$, and let $[a_0; \overline{a_1, \ldots, a_r}]$ be the continued fraction expansion of $\sqrt{m}$. Then $a_{r/2} \equiv v \pmod 2$. Moreover, $a_{r/2}$ is odd if and only if $\Delta_m = 1$.*

Note that $N(\varepsilon) = 1$ guarantees that r is even, and that $a_{r/2}$ is the central element of the symmetry $a_i = a_{r-i}$ for $i = 1, \ldots, r-1$.

Also, we have another result related to a Diophantine equation in Section 4.6.

Theorem (4.31). *Let $m \equiv 3 \pmod 4$ be square free, let $K = \mathbf{Q}(\sqrt{m})$, and let $\varepsilon = u + v\sqrt{m}$ be the fundamental unit of $\mathcal{O}_K$. Then the following are equivalent.*

(a) $\Delta_m = 1$

(b) *v is odd.*

(c) *The ideal $[d, \sqrt{m}]$ is not principal for $1 < d < m$, $d \mid m$.*

(d) *$|dx^2 - \frac{m}{d}y^2| = 1$ has no integer solutions for $1 < |d| < m$, $d \mid m$.*

When $m \equiv 3 \pmod 4$, the above theorem directly implies the following results:

1. If m is prime, then $\Delta_m = 1$.

2. Suppose for any proper decomposition of $m = m_1 m_2$, we have that m_1 and m_2 are not quadratic residues for each other. Then $\Delta_m = 1$.

In Chapter 5, we introduce full determination of M_c/P_c for a Galois extension of local fields which is proved in [16]. The vanishing of M_c/P_c is related to the ramification of the extension.

In Chapter 6, we suggest some methods due to Ono [17] for a generalization. A new method allows us to determine M_c/P_c for a general Galois extension of number fields K/k using Hilbert 90. Moreover, we can generalize M_c/P_c itself by using certain elements or ideals of $\mathcal{O}_K$.

Furthermore, we may replace the ring R with the matrix ring over $\mathcal{O}_K$. By using Hilbert's 90 for matrices, we also have a new method to determine M_c/P_c as above. For the matrix case, we need more information about the cohomology set $H^1(G, \mathrm{GL}_n(\mathcal{O}_K))$. However, we do have an exact sequence of G-groups

$$1 \to SL_n(\mathcal{O}_K) \to GL_n(\mathcal{O}_K) \to \mathcal{O}_K^\times \to 1$$

which induces long exact sequence of pointed sets

$$\begin{aligned} 1 \to SL_n(\mathcal{O}_k) \to GL_n(\mathcal{O}_k) \to \mathcal{O}_k^\times \\ \to H^1(G, SL_n(\mathcal{O}_K)) \to H^1(G, GL_n(\mathcal{O}_K)) \to H^1(G, \mathcal{O}_K^\times). \end{aligned}$$

In Chapter 7, we prove some fragmental results on $H^1(G, SL_2(\mathcal{O}_K))$ for quadratic extensions K over $\mathbf{Q}$.

2 Preliminaries

2.1 Cohomology

The concepts of cohomology groups and nonabelian cohomology are introduced in [21], [20], and [11], which we refer to for definitions and basic properties of cohomology throughout this section.

2.1.1 Definition of Cohomology Group

Let G be a group and let A be a left G-module, denoting the action by $(s, a) \mapsto {}^s a$ for $s \in G$ and $a \in A$. We have ${}^{1_G}a = a$, ${}^s(a+b) = {}^s a + {}^s b$, and ${}^{st}a = {}^s({}^t a)$. Let A^G be the submodule consisting of the element fixed by G.

Denote by $C^n(G, A)$ the set of *n-cochains*, that is, the set of all maps of G^n to A. (If G has a topological structure, cochains are defined as continuous functions of G^n to A.) It is convenient to define $C^0(G, A) = \{1_G\}$, the identity element of G. Define the coboundary map

$$d_{n+1} : C^n(G, A) \longrightarrow C^{n+1}(G, A)$$

by

$$\begin{aligned}(d_{n+1}f)(s_1, \ldots, s_{n+1}) = {}& {}^{s_1}f(s_2, \ldots, s_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(s_1, \ldots, s_i s_{i+1}, \ldots, s_{n+1}) \\ & + (-1)^{n+1} f(s_1, \ldots, s_n).\end{aligned}$$

We have $d_{n+1} \circ d_n = 0$ and $\operatorname{im} d_n \subset \ker d_{n+1}$. We define the *n-th cohomology group* by $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ where $Z^n(G, A) = \ker d_{n+1}$ is called the group of *cocycles*, and $B^n(G, A) = \operatorname{im} d_n$ is called the group of *coboundaries*.

Remark 2.1. (a) $H^0(G, A) = A^G$, as usual.

(b) $H^1(G, A)$ is the group of equivalent classes of crossed-homomorphisms of G into A:

$$Z^1(G, A) = \{f : G \to A \mid f(st) = f(s) + {}^s f(t)\}.$$

$$B^1(G, A) = \{g : G \to A \mid g(s) = {}^s b - b \text{ for some } b \in A\}.$$

(c) $H^2(G, A)$:

The 2-cocycles are the (continuous) functions $f : G \times G \to A$ such that

$$f(st, u) + f(s, t) = f(s, tu) + {}^s f(s, t).$$

The 2-coboundaries are the functions

$$f(s, t) = g(s) - g(st) + {}^s g(t)$$

with an arbitrary 1-cochain $g : G \to A$.

2.1.2 Long Exact Sequence

Given an exact sequence of G-groups

$$0 \to A \to B \to C \to 0$$

we have a long exact sequence of cohomology groups:

$$\begin{aligned} 0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta_1} H^1(G, A) \\ \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta_2} H^2(G, A) \to H^2(G, B) \to H^2(G, C) \to \cdots \end{aligned}$$

2.1.3 Nonabelian Cohomology

Let G be a group and A a group on which G acts on the left. We now allow the case that A is nonabelian. We can define $H^0(G, A)$ and $H^1(G, A)$ only. $H^0(G, A)$ is defined again as the group A^G of elements of A fixed by G. A *cocycle* is defined as a map $s \mapsto c_s$ of G into A such that $c_{st} = c_s \, {}^s c_t$. Denote by $Z^1(G, A)$ the set of all cocycles. We call c and c' are *cohomologous*, denoted by $c \sim c'$, if there exists $u \in A$ such that $c'_s = u^{-1} c_s \, {}^s u$ for all $s \in G$. This defines an equivalence relation on the set of cocycles. We define the *cohomology set of G with value in A* as the quotient set

$$H^1(G, A) = Z^1(G, A)/\sim .$$

If A is abelian, this definition coincides with the definition of the first cohomology group for the abelian case. Notice that $Z^1(G, A)$ and $H^1(G, A)$ do not attain a natural group structure if A is nonabelian. Yet there is a distinguished element, which is the class of the unit cocycle $c_s = 1$, and we regard $H^1(G, A)$ as a *pointed set*.

If $f : A \to B$ is a G-group homomorphism, then we define

$$f_0 : H^0(G, A) \to H^0(G, B)$$
$$f_1 : H^1(G, A) \to H^1(G, B)$$

as follows: f_0 is the restriction of f to A^G, then the image of f_0 is the set of fixed elements. f_1 is defined by $f_1(c)_s = f(c_s)$, and this is compatible with the equivalence relation. f_0 is a group homomorphism and f_1 is a morphism of pointed sets, which means that f sends the unit cocycle of A onto the unit cocycle of B. We can define *kernel* of a morphism of pointed sets as the pre-image of the distinguished element. This enables us to consider an exact sequence of pointed sets. We also have a long exact sequence for the cohomology sets, but in general the sequence does not extend to H^2.

Proposition 2.2. *Let $1 \to A \to B \to C \to 1$ be an exact sequence on nonabelian G-groups. Then the sequence of pointed sets below is exact:*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

The proof can be found in [21], p125.

Remark. If A is in the center of B, then A is abelian, so $H^2(G, A)$ is defined and the long exact sequence is extended up to $H^2(G, A)$.

2.1.4 Twisting

Let A be a G-group. We define a new action of G on A twisted by a 1-cocycle element c as follows: Let $c \in Z^1(G, A)$, denote by ${}_cA$ the set A on which G acts by the formula

$$^{s'}a = c_s \, {}^s a c_s^{-1}. \tag{1}$$

One says that ${}_cA$ is obtained by twisting A using the cocycle c.

Proposition 2.3. *Let $c \in Z^1(G, A)$, and let $A' = {}_cA$. To each cocycle d_s in A' we associate $d_s c_s$, which is a cocycle of G in A. Thus we have bijections*

$$t_c : Z^1(G, A') \longrightarrow Z^1(G, A)$$

and

$$\tau_c : H^1(G, A') \longrightarrow H^1(G, A)$$

induced by t_c, mapping the neutral element of $H^1(G, A')$ into the class of c.

For proof, see [20].

2.2 Poincaré Series

2.2.1 Modular Forms

The Poincaré's idea about Poincaré series can be found in [2] and [24]. We follow the definitions and theorems from Gunning's book ([2]). Denote by $\mathfrak{H} = \{z \in \mathbf{C} \mid \operatorname{im} z > 0\}$ the upper half plane. The only conformal automorphisms of $\mathfrak{H}$ are the linear fractional transformations:

$$T : z \longmapsto \frac{az+b}{cz+d},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix of real coefficients having determinant one, in other word, an element of $\mathrm{SL}_2(\mathbf{R})$. We define the *inhomogeneous modular group* Γ to be the group of linear fractional transformations associated to integral matrices. We have that Γ is isomorphic to $\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z})/\pm I$. Let G be a subgroup of finite index in Γ. A transformation T is called *parabolic* if it has only one fixed point on the real line or at ∞. A fixed point of a parabolic transformation in G is called a *parabolic vertex*, or a *cusp* of G.

Definition 2.4. An *unrestricted modular form of weight* $2k$ *for* G is a meromorphic function $f(z)$ on $\mathfrak{H}$ such that $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$ for all transformations $T : z \mapsto \frac{az+b}{cz+d}$ belonging to G, where k is an integer.

Denote $J_T(z) = \frac{dT}{dz} = (cz+d)^{-2}$ so that we can write the above equation as $f(T(z)) = J_T(z)^{-k} f(z)$. The local coordinate at $i\infty$ is $\zeta = e^{2\pi i z/q}$ where q is the least positive integer such that the translation $z \mapsto z+q$ is in the group G. Let $\hat{f}(\zeta) = f(z)$. An unrestricted modular form $f(z)$ is said to be *holomorphic at* ∞ if $\hat{f}(\zeta)$ is holomorphic in $|\zeta| < 1$. In particular, $\hat{f}(\zeta)$ has a Taylor expansion in ζ

$$\hat{f}(\zeta) = \sum_{m=0}^{\infty} a_m \zeta^m,$$

and this induces a Fourier expansion for $f(z)$

$$f(z) = \sum_{m=0}^{\infty} a_m e^{2\pi i m z/q}.$$

Let p be a parabolic fixed point of G, not ∞. Let $S \in \Gamma$ map p to ∞, and $g(z) = J_{S^{-1}}(z)^k f(S^{-1}z)$. We call $f(z)$ is *holomorphic at* p if $g(z)$ is holomorphic at ∞.

Definition 2.5. A *modular form* is an unrestricted modular form which is holomorphic at all points of $\mathfrak{H}$ and at all parabolic vertices of the group.

Definition 2.6. The *Poincaré series* of weight $2k$ and of character ν for G is the series

$$\phi_\nu(z) = \sum_{T \in \mathcal{R}} e^{2\pi i \nu T(z)/q} J_T(z)^k$$

where ν is nonnegative integer, $\mathcal{R}$ is the set of coset representatives of G mod G_0, and G_0 is the infinite cyclic subgroup of translation in G, generated by the least translation $T : z \mapsto z + q$ in G.

Definition 2.7. A *cusp form* of weight $2k$ for G is a modular form of weight $2k$ for G which vanishes at all parabolic vertices (cusps).

It is known that the set of cusp forms of weight k for G forms a finite dimensional Hilbert space with the Petersson Inner Product:

$$\langle f, g \rangle := \int_D f(z)\overline{g(z)} y^{2(k-1)} dx \wedge dy.$$

where D is a fundamental domain for G.

Theorem 2.8. *The Poincaré series*

$$\phi_\nu(z) = \sum_{T \in \mathcal{R}} e^{2\pi i \nu T(z)/q} (cz + d)^{-2k}$$

converges absolutely uniformly on compact subsets of $\mathfrak{H}$, for $\nu > 0$ and $k \geq 1$, and for $\nu = 0$ and $k > 1$. $\phi_\nu(z)$ converges absolutely uniformly on every fundamental domain D for G and represents a modular form of weight $2k$ for G. Further,

(a) *$\phi_0(z)$ is zero at all finite parabolic vertices, nonzero at $i\infty$.*

(b) *$\phi_\nu(z)$ is a cusp form for $\nu \geq 1$.*

Theorem 2.9. *Every cusp form is a linear combination of the Poincaré series $\phi_\nu(z)$, $\nu \geq 1$.*

2.2.2 Cohomological View

We will see the previous section in the cohomological point of view. Let R be the ring of holomorphic functions on $\mathfrak{H}$. Then G acts on R and $R^\times$, the unit group of R, as follows:

Let $s = \begin{pmatrix} a & b \\ c & c \end{pmatrix}^{-1} \in G$. The action is defined by $(s, f(z)) \mapsto {}^s f(z) := f\left(\frac{az+b}{cz+d}\right)$. Now define $\mathcal{C} : G \to R^\times$ by $\mathcal{C}_s(z) = (cz+d)^{-2k}$ for $z \in \mathfrak{H}$. Then $\mathcal{C}$ satisfies the definition of 1-cocycle of G with values in $R^\times$. Indeed, if $t = \begin{pmatrix} e & f \\ g & h \end{pmatrix}^{-1} \in G$,

$$\begin{aligned}
\mathcal{C}_s(z)\, {}^s\mathcal{C}_t(z) &= (cz+d)^{-2k}\, {}^s(gz+h)^{-2k} \\
&= (cz+d)^{-2k} \left(g\frac{az+b}{cz+d} + h\right)^{-2k} \\
&= (g(az+b) + h(cz+d))^{-2k} \\
&= ((ag+ch)z + (bg+dh))^{-2k} \\
&= \mathcal{C}_{st}(z)
\end{aligned}$$

since $(st)^{-1} = t^{-1}s^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} --- & --- \\ ag+ch & bg+dh \end{pmatrix}$.

Denote by $M_{\mathcal{C}}$ the space of cusp forms of weight $2k$:

$$M_{\mathcal{C}} = \left\{ f \in R \,\middle|\, (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) = f(z),\ f \text{ vanishes at all cusps} \right\}.$$

The condition $(cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) = f(z)$ can be written as $\mathcal{C}_s\, {}^s f(z) = f(z)$. Denote by $P_{\mathcal{C}}$ the space generated by Poincaré's series:

$$\begin{aligned}
\phi_\nu &= \sum_{T \in \mathcal{R}} e^{2\pi i \nu T(z)/q} (cz+d)^{-2k} \\
&= \sum_{s \in \mathcal{R}} \mathcal{C}_s(z)\, {}^s g(z)
\end{aligned}$$

where $g(z) = e^{2\pi i \nu z/q}$, $\nu \geq 1$. Theorem 2.9 says that $M_{\mathcal{C}} = P_{\mathcal{C}}$ i.e. $M_{\mathcal{C}}/P_{\mathcal{C}} = 0$.

3 Definition of M_c/P_c

3.1 Cohomology

Poincaré's idea in automorphic functions can be applied to an arbitrary (G, R) with a group G acting on a ring R as noted by T. Ono ([15]). Let R be a ring and G a finite group acting on R from the left, $(s, a) \mapsto {}^s a$ for $s \in G$, $a \in R$. Naturally G acts on the group $R^\times$ of units. The first cohomology set $H^1(G, R^\times)$ is defined by $Z^1(G, R^\times)/\sim$ where $Z^1(G, R^\times) = \{c : G \to R^\times \mid \ c_{st} = c_s\, {}^s c_t,\ s, t \in G\}$ the set of cocycles, and $c \sim c'$ if there exists $u \in R^\times$ such that $c'_s = u^{-1} c_s\, {}^s u$, $s \in G$.

3.2 Definition of M_c/P_c

Definition 3.1. For a cocycle $c \in Z^1(G, R^\times)$, we set

$$M_c = \{a \in R \mid \ c_s\, {}^s a = a,\ s \in G\},$$

$$P_c = \left\{ p_c(x) \,\middle|\, p_c(x) = \sum_{t \in G} c_t\, {}^t x,\ x \in R \right\}.$$

M_c and P_c are $\mathbf{Z}$-modules in the ring R. We have $P_c \subset M_c$, since $c_s\, {}^s p_c(x) = c_s\, {}^s \left(\sum_{t \in G} c_t\, {}^t x\right) = \sum_{t \in G} c_s\, {}^s c_t\, {}^{st} x = \sum_{t \in G} c_{st}\, {}^{st} x = \sum_{t \in G} c_t\, {}^t x = p_c(x)$.

Also, we have

$$|G| M_c \subset P_c \subset M_c \tag{2}$$

Indeed, for $a \in M_c$, $p_c(a) = \sum_{t \in G} c_t\, {}^t a = \sum_{t \in G} a = |G| a$. Hence, if $|G| 1_R$ is invertible in R, then we have $M_c/P_c = 0$ for any cocycle c.

We prove that M_c/P_c depends only on the cocycle class of c as follows: Let $c \sim c'$, that is, $c'_s = u^{-1} c_s\, {}^s u$ for some $u \in R^\times$. Then

$$\begin{aligned} a \in M_{c'} &\Leftrightarrow c'_s\, {}^s a = a \text{ for some } s \in G \\ &\Leftrightarrow u^{-1} c_s\, {}^s u\, {}^s a = a \Leftrightarrow c_s\, {}^s (ua) = ua \Leftrightarrow ua \in M_c. \end{aligned}$$

Because $u c'_t ({}^s u)^{-1} = c_t$, We have that $\sum c_t\, {}^t a = \sum u c'_t ({}^s u)^{-1}\, {}^t a = u \sum c'_t\, {}^s (u^{-1} a)$. Hence $u M_{c'} = M_c$ and $u P_{c'} = P_c$, so that

$$M_c/P_c = M_{c'}/P_{c'}. \tag{3}$$

3.3 Twisted Cohomology

In the case of $c \sim 1$, we have $M_c/P_c = R^G/N_G R = \widehat{H}^0(G, R)$. Motivated by this, for any $\gamma = [c] \in H^1(G, R^\times)$, M_c/P_c can be considered as the *twisted cohomology set* $\widehat{H}^0(G, R)_\gamma$ in the following way. For a cocycle $c \in Z^1(G, R^\times)$, we define a new twisted action on R by $(s, a) \mapsto {}^{s'}a := c_s\, {}^s a$, and we write ${}_cR$ as the set R with this new action. Note that ${}_cR$ is a G-module. Then we have

$$M_c = \{a \in R \mid {}^{s'}a = a\} = {}_cR^G$$

and

$$P_c = \left\{ \sum_{t \in G} {}^{t'}x \;\middle|\; x \in R \right\} = N_{Gc} R.$$

Hence

$$M_c/P_c = {}_cR^G/N_{Gc}R = \widehat{H}^0(G, {}_cR),$$

the twisted cohomology. By the equation (3), if $\gamma = [c] \in H^1(G, R^\times)$ is the cohomology class of c, we have

$$M_c/P_c = \widehat{H}^0(G, R)_\gamma.$$

3.4 Number Field Case

From the result of Poincaré (Theorem 2.9), it would be natural to hope that $M_c = P_c$ (that is, $\widehat{H}^0(G, R)_\gamma = M_c/P_c = 0$). However, this is not true in the general situation.

We are most interested in the case where G is a Galois group of a Galois extension of number fields K/k and R is the ring of integers $\mathcal{O}_K$. As a first step, we examine quadratic number fields.

4 Determination of M_c/P_c for Quadratic Fields

4.1 Basic Computations

4.1.1 Initial Setup

Let m be a square free positive integer, $K = \mathbf{Q}(\sqrt{m})$ the corresponding real quadratic field, $\mathcal{O}_K$ the ring of integers of K, $\mathcal{O}_K^\times$ the group of units of K and $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle s \rangle$ of order 2. G acts on K, $\mathcal{O}_K$, and $\mathcal{O}_K^\times$ as ${}^s(a + b\sqrt{m}) = a - b\sqrt{m}$. We want to determine M_c/P_c in this case. First, we write $\mathcal{O}_K = [1, \omega]$ where

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4 \\ \sqrt{m} & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

Note that

$${}^s\omega = \begin{cases} 1 - \omega & \text{if } m \equiv 1 \pmod 4 \\ -\omega & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

We have

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } m = -1, \ \ i = \sqrt{-1} \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } m = -3 \text{ where } \omega = \frac{1+\sqrt{-3}}{2} \\ \{\pm 1\} & \text{if } m < 0, m \neq -1, m \neq -3 \\ \{\pm\varepsilon^j \mid j \in \mathbf{Z}\} & \text{if } m > 0 \end{cases}$$

where $\varepsilon = u + v\omega$, $u, v \in \mathbf{Z}$ is the fundamental unit, that is, the least positive unit in $\mathcal{O}_K^\times$.

The cocycles $c \in Z^1(G, \mathcal{O}_K^\times)$ are unit elements in $\mathcal{O}_K$ with norm 1. Indeed, a cocycle $c : G \to \mathcal{O}_K^\times$ is fully determined by the image of s, the generator of G. Since $1 = c_1 = c_{s \cdot s} = c_s \, {}^s c_s = N(c_s)$, the element c_s is of norm 1. So,

$$Z^1(G, \mathcal{O}_K^\times) = \begin{cases} \mathcal{O}_K^\times & \text{if } m < 0, \text{ or } m > 0 \text{ and } N(\varepsilon) = 1 \\ \{\pm\varepsilon^{2j} \mid j \in \mathbf{Z}\} & \text{if } m > 0 \text{ and } N(\varepsilon) = -1. \end{cases}$$

The coboundary group is

$$\begin{aligned} B^1(G,\mathcal{O}_K^\times) = [1] &= \{v/{}^s v \mid v \in \mathcal{O}_K^\times\} \\ &= \{v^2/N(v) \mid N(v) = \pm 1\} \\ &= \begin{cases} \{v^2 \mid v \in \mathcal{O}_K^\times\} & \text{if } m < 0, \text{ or } m > 0 \text{ and } N(\varepsilon) = 1 \\ \{\pm v^2 \mid v \in \mathcal{O}_K^\times, \text{ sign} = N(v)\} & \text{if } m > 0 \text{ and } N(\varepsilon) = -1. \end{cases} \\ &= \begin{cases} \{v^2 \mid v \in \mathcal{O}_K^\times\} & \text{if } m < 0 \\ \{\varepsilon^{2j} \mid j \in \mathbf{Z}\} & \text{if } m > 0 \text{ and } N(\varepsilon) = 1 \\ \{(-1)^j \varepsilon^{2j} \mid j \in \mathbf{Z}\} & \text{if } m > 0 \text{ and } N(\varepsilon) = -1. \end{cases} \end{aligned}$$

Hence the cohomology group is

$$H^1(G,\mathcal{O}_K^\times) = \begin{cases} \mathbf{Z}/2\mathbf{Z} & \text{if } m < 0, \text{ or } m > 0 \text{ and } N(\varepsilon) = 1 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} & \text{if } m > 0 \text{ and } N(\varepsilon) = -1 \end{cases}$$

with cocycle representatives

$$\begin{aligned} \{1, i\} &\quad \text{if } m = -1 \\ \{\pm 1\} &\quad \text{if } m < -1 \text{ or } m > 0 \text{ with } N(\varepsilon) = -1 \\ \{\pm 1, \pm\varepsilon\} &\quad \text{if } m > 0 \text{ with } N(\varepsilon) = 1. \end{aligned}$$

Now we consider M_c and P_c for c the representative elements. We have

$$M_c = \{\alpha \in \mathcal{O}_K \mid c\,{}^s\alpha = \alpha\},$$

$$P_c = \{p_c(z) = z + c\,{}^s z \mid z \in \mathcal{O}_K\}.$$

The module M_c/P_c is of order 1 or 2; we have $2M_c \subset P_c \subset M_c$ by (2), so $|M_c/P_c| \leq |M_c/2M_c| = 2$ since M_c is a subgroup of $\mathcal{O}_K$.

We have $M_c/P_c \approx M_{-c}/P_{-c}$, i.e. the index is unchanged if c is replaced by $-c$. Indeed, if $\alpha \in M_c$ then $\alpha\sqrt{m} \in M_{-c}$ and if $p_c(x) \in P_c$ then $p_c(x)\sqrt{m} = p_{-c}(x\sqrt{m}) \in P_{-c}$.

4.1.2 Trivial Case

Proposition 4.1. *If $c = \pm 1$,*

$$M_c/P_c = \widehat{H}^0(G,\mathcal{O}_K^\times) = \begin{cases} 0 & \textit{if } m \equiv 1 \pmod 4 \\ \mathbf{Z}/2\mathbf{Z} & \textit{otherwise.} \end{cases}$$

If $m = -1$ and $c = i$, $M_c/P_c = 0$.

Proof. If $c = 1$, $M_c = \{\alpha \in \mathcal{O}_K \mid {}^s\alpha = \alpha\} = \mathbf{Z}$ and $P_c = \{\beta + {}^s\beta \mid \beta \in \mathcal{O}_K\} = T(\mathcal{O}_K)$. For $a + b\omega \in \mathcal{O}_K$,

$$T(a+b\omega) = \begin{cases} 2a+b & \text{if } m \equiv 1 \pmod 4 \\ 2a & \text{if } m \equiv 2,3 \pmod 4 \end{cases}$$

so

$$T(\mathcal{O}_K) = \begin{cases} \mathbf{Z} & \text{if } m \equiv 1 \pmod 4 \\ 2\mathbf{Z} & \text{if } m \equiv 2,3 \pmod 4. \end{cases}$$

Now let $m = -1$ and $c = i$. Then $a + bi \in M_c$ if and only if $i(\overline{a+bi}) = a + bi$ if and only if $ai + b = a + bi$ if and only if $a = b$. So $M_c = (1+i)\mathbf{Z}$. For $p_c(a+bi) \in P_c$, we have $(a+bi) + i(a-bi) = (a+b) + (a+b)i$ so $P_c = (1+i)\mathbf{Z} = M_c$. □

4.2 Computation for Fundamental Unit Case (1)

Computation of $|M_c/P_c|$ for $c = \pm\varepsilon$ is not so trivial. We write the fundamental unit ε as $\varepsilon = u + v\omega$, $u, v \in \mathbf{Z}$. Note that $(u, v) = 1$. We may set $c = \varepsilon$. Let $\alpha = a + b\omega \in M_c$. Then $(u+v\omega)(a+b\,{}^s\omega) = (a+b\omega)$ or $au + bu(T-\omega) + av\omega + bvN = a + b\omega$ if we write $T = T(\omega) = \omega + {}^s\omega$ and $N = N(\omega) = \omega\,{}^s\omega$. We get the system of equations

$$a = au + b(uT + vN)$$
$$b = -bu + av$$

and we can rewrite it in the matrix form

$$\begin{pmatrix} u-1 & uT+vN \\ -v & 1+u \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The coefficient matrix has determinant 0. Indeed, since $1 = N(\varepsilon) = u^2 + uvT + v^2N$, we have

$$1 - u^2 = (1-u)(1+u) = v(uT + vN). \tag{4}$$

Hence the determinant of the above matrix is $u^2 - 1 + v(uT + vN) = 0$ and two equations are equivalent. So $\alpha \in M_c$ if and only if $av = b(1+u)$. Denote $e = \gcd(v, 1+u)$, $D = v/e$,

and $C = (1+u)/e$. We have

$$\begin{aligned} M_c &= \{a + b\omega \mid av = b(1+u)\} \\ &= \{a + b\omega \mid aD = bC\} \\ &= (C + D\omega)\mathbf{Z}. \end{aligned}$$

Now, let $p_c(z) = p_c(x + y\omega) \in P_c$.

$$\begin{aligned} z + \varepsilon\, {}^s z &= (x + y\omega) + (u + v\omega)(x + y\, {}^s\omega) \\ &= x(1+u) + y(uT + vN) + (y(1-u) + xv)\omega \\ &= A + B\omega \end{aligned}$$

where

$$\begin{aligned} A &= x(1+u) + y(uT + vN) \\ B &= xv + y(1-u) \end{aligned}$$

for arbitrary integers x, y. Then by (4), $Av = B(u+1)$. Now $A+B\omega \in P_c \Leftrightarrow Av = B(u+1)$, $(1+u, uT+vN) \mid A$, and $d := (v, 1-u) \mid B$. But $(1+u, uT+vN) \mid A$ follows from $Av = B(u+1)$ and $(v, 1-u) \mid B$ by (4) again. Hence

$$\begin{aligned} P_c &= \{A + B\omega \mid Av = B(u+1), d \mid B\} \\ &= \{A + B\omega \mid AD = BC, d \mid B\} \\ &= (C + [D, d]\omega)\mathbf{Z} \end{aligned}$$

where $[D, d]$ is the least common multiple of D and d. Hence, we get $M_c/P_c \approx D\mathbf{Z}/[D,d]\mathbf{Z} = \mathbf{Z}/\frac{d}{(D,d)}\mathbf{Z}$.

Proposition 4.2 ([15]). *For $c = \pm\varepsilon$, $M_c/P_c = \mathbf{Z}/\Delta_m\mathbf{Z}$ where $\Delta_m = \frac{d}{(D,d)}$, $d = (v, u-1)$, $e = (v, u+1)$, and $D = v/e$.*

4.3 Computation for Fundamental Unit Case (2)

Now we determine $\Delta_m = [M_\varepsilon/P_\varepsilon]$ in terms of $\varepsilon = u + v\omega$ in the simple way.

Proposition 4.3. $\Delta_m = 1 \Leftrightarrow de \mid v$.

Proof. $\frac{d}{(D,d)} = 1 \Leftrightarrow d = (D,d) \Leftrightarrow d \mid D \Leftrightarrow d \mid \frac{v}{e} \Leftrightarrow de \mid v$ □

Proposition 4.4. *If v is odd, then $\Delta_m = 1$.*

Proof. Note that $(v, u-1)$ and $(v, u+1)$ are odd divisors of v but $(u+1, u-1) \mid 2$. Then $(v, u-1)$ and $(v, u+1)$ are mutually prime both dividing v. Hence we get

$$(v, u-1)(v, u+1) \mid v.$$

□

When v is even (then u is odd), let $v' = v/2$ and $u' = (u-1)/2$. Then

$$d = (v, u-1) = (2v', 2u') = 2(v', u') = 2d'$$

with $d' = (u', v')$ and

$$e = (v, u+1) = (2v', 2u'+2) = 2(v', u'+1) = 2e'$$

with $e' = (v', u'+1)$. Note that d' and e' are are mutually prime both dividing v'. Hence we have

$$d'e' = (v', u')(v', u'+1) \,\Big|\, v', \tag{5}$$

that is,

$$d' \,\Big|\, \frac{v'}{e'} = \frac{2v'}{2e'} = \frac{v}{e} = D. \tag{6}$$

We have two cases;

(i) $2d'e' \mid v'$: we have $de = 4d'e' \mid 2v' = v$ so $\Delta_m = 1$ by Proposition 4.3.

(ii) $2d'e' \nmid v'$: we have $de \nmid v$ and $d \nmid \frac{v}{e} = D$. Since $d' \mid D$, $(D, d) = (D, 2d') = d'$ and hence $\Delta_m = \frac{d}{(D,d)} = \frac{d}{d'} = 2$.

Therefore we have $\Delta_m = 1$ or 2 for any m and;

Proposition 4.5. *If v is even, using the notations above,*

$$2d'e' \mid v' \Leftrightarrow \Delta_m = 1,$$

or equivalently,

$$2d'e' \nmid v' \Leftrightarrow \Delta_m = 2.$$

Proposition 4.6. *If v is even (and u is odd), let $\nu \geq 1$ be such that*

$$2^\nu \parallel v$$

i.e. the largest positive integer such that $2^\nu \mid v$. Then

$$u \equiv \pm 1 \pmod{2^\nu} \Leftrightarrow \Delta_m = 2.$$

Proof. (Case 1) $\nu = 1$: $v \equiv 2 \pmod 4$ so v' is odd, and $2d'e' \nmid v'$. Hence $\Delta_m = 2$ by Proposition 4.5. On the other hand, u is odd so $u \equiv \pm 1 \pmod 2$.

(Case 2) $\nu \geq 2$: $2^\nu \parallel v$ then $2^{\nu-1} \parallel v' = \frac{v}{2}$. Since $u' = \frac{u-1}{2}$, note that $u \equiv \pm 1 \pmod{2^\nu} \Leftrightarrow$ one of $u+1$, $u-1 \equiv 0 \pmod{2^\nu} \Leftrightarrow$ one of u', $u'+1 \equiv 0 \pmod{2^{\nu-1}}$.

($\Leftarrow$) If $u \not\equiv \pm 1 \pmod{2^\nu}$, neither u' nor $u'+1$ is congruent to 0 mod $2^{\nu-1}$. Since (v', u') and $(v', u'+1)$ are mutually prime, we have $2^{\nu-1} \nmid (v', u')(v', u'+1)$. But since $(v', u')(v', u'+1) \mid v'$ and $2^{\nu-1} \mid v'$, we have $2(v', u')(v', u'+1) \mid v'$ and thus $\Delta_m = 1$.

($\Rightarrow$) If $u \equiv \pm 1 \pmod{2^\nu}$, one of u', $u'+1 \equiv 0 \pmod{2^{\nu-1}}$. So $2^{\nu-1} \mid (v', u')(v', u'+1)$ and $2^\nu \mid 2(v', u')(v', u'+1)$. But $2^\nu \nmid v'$ so $2(v', u')(v', u'+1) \nmid v'$ and hence $\Delta_m = 2$.

□

Proposition 4.7. *If v is even but $8 \nmid v$ then $\Delta_m = 2$.*

Proof. For $\nu = 1$ or 2 (respectively), odd u should be congruent to $\pm 1 \pmod 2$ or $\pmod 4$ (respectively). □

Lemma 4.8. *For $\nu \geq 3$,*

$$a^2 \equiv 1 \pmod{2^\nu} \Leftrightarrow a \equiv \pm 1 \pmod{2^\nu} \text{ or } a \equiv \pm(2^{\nu-1} - 1) \pmod{2^\nu}.$$

Proof. First, $(\pm 1)^2 = 1$ and $(\pm(2^{\nu-1}-1))^2 = 2^{2\nu-2} - 2^\nu + 1 \equiv 1 \pmod{2^\nu}$ since $2\nu - 2 \geq \nu$ for $\nu \geq 3$. It is known that the unit group mod 2^ν is isomorphic to the direct product of two cyclic groups of order 2 and $2^{\nu-2}$:

$$(\mathbf{Z}/2^\nu\mathbf{Z})^\times \simeq \langle -1 \rangle \times \langle 5 \rangle$$

where $(-1)^2 \equiv 1$ and $5^{2^{\nu-2}} \equiv 1 \pmod{2^\nu}$. Let $a \in (\mathbf{Z}/2^\nu\mathbf{Z})^\times$ such that $a^2 \equiv 1 \pmod{2^\nu}$ other than ± 1. We can write $a = (-1)^i 5^j$ with $i = 0$ or 1 and $1 \leq j < 2^{\nu-2}$.

$$\begin{aligned} a^2 \equiv 1 \pmod{2^\nu} &\Leftrightarrow 5^{2j} \equiv 1 \pmod{2^\nu} \\ &\Leftrightarrow 2^{\nu-2} \mid 2j \\ &\Leftrightarrow 2^{\nu-3} \mid j. \end{aligned}$$

Since $1 \leq j < 2^{\nu-2}$, $j = 2^{\nu-3}$. So we have only four elements ± 1, $\pm 5^{2^{\nu-3}}$, with square $\equiv 1 \pmod{2^\nu}$. □

Lemma 4.9. *If a, b are integers and b is even such that $a^2 - mb^2 = 1$ and $2^\nu \parallel b$ where $\nu \geq 2$ then $a \equiv \pm 1 \pmod{2^{\nu+1}}$.*

Proof. First note that

$$2^\nu \parallel b \Rightarrow a^2 \equiv 1 \pmod{2^{2\nu}}. \tag{7}$$

Then by the previous lemma, $a \equiv \pm 1$ or $\pm(2^{2\nu-1}-1) \pmod{2^{2\nu}}$. Since $\nu \geq 2$, $2\nu - 1 \geq \nu + 1$ so $\pm(2^{2\nu-1} - 1) \equiv \mp 1 \pmod{2^{\nu+1}}$. □

Proposition 4.10. *If $\varepsilon = u + v\sqrt{m}$ with v even, then $\Delta_m = 2$.*

Proof. If $8 \nmid v$ then $\Delta_m = 2$ by Proposition 4.7. If $2^\nu \parallel v$ with $\nu \geq 3$ then $u \equiv \pm 1 \pmod{2^\nu}$ by Lemma 4.9, hence $\Delta_m = 2$ by Proposition 4.6. □

Theorem 4.11. *If $m \equiv 2 \pmod 4$ then $\Delta_m = 2$.*
For $m \equiv 3 \pmod 4$, $\Delta_m = 1 \Leftrightarrow v$ is odd.

Proof. If $m \equiv 2 \pmod 4$ then $1 = u^2 - mv^2 \equiv u^2 - 2v^2 \pmod 4$. Since the only squares modulo 4 are 0 and 1, the only possibility is $v^2 \equiv 0$ and $u^2 \equiv 1$. So v is even. The rest follows from Proposition 4.4 and Propositon 4.10. □

Theorem 4.12. *If $m \equiv 1 \pmod 4$ then $\Delta_m = 1$.*

Proof. By Proposition 4.4, we may assume that v is even. Denote $\varepsilon = u + v\omega = a + b\sqrt{m}$ where $a = u + \frac{v}{2}$ and $b = v/2$. Then $1 = a^2 - mb^2 \equiv a^2 - b^2 \pmod 4$. Since $0, 1$ are all squares mod 4, the only possible case is for $b^2 \equiv 0$ and $a^2 \equiv 1 \pmod 4$ and so a is odd and b is even. Now, consider the equation $a^2 - mb^2 \equiv 1 \pmod 8$. The only square mod 8 are 0,1, and 4. Since a is odd, $a^2 \equiv 1 \pmod 8$. We have $b^2 \equiv 0$ or $4 \pmod 8$, and $m \equiv 1$ or

$m \equiv 5 \pmod 8$. Only possible case is $b^2 \equiv 0 \pmod 8$. We get $b \equiv 0 \pmod 4$ and so $8 \mid v$. Let $\nu \geq 3$ be the integer such that $2^\nu \parallel v$. Then $2^{\nu-1} \parallel b$, and we get $a \equiv \pm 1 \pmod{2^\nu}$ by Lemma 4.9. Since $2^\nu \nmid b$, $u = a - b \equiv \pm 1 - 2^{\nu-1} \not\equiv \pm 1 \pmod{2^\nu}$. Then by Proposition 4.6, we get $\Delta_m = 1$. □

4.4 Continued Fractions

Now it remains to determine Δ_m for $m \equiv 3 \pmod 4$. It depends on the parity of the coefficient v of the fundamental unit $\varepsilon = u + v\sqrt{m}$, but it is hard to find a rule to derive the v in terms of m directly. The most practical way to obtain the fundamental unit is using the continued fraction expansion of $\sqrt{m}$. We will classify the index Δ_m in this way.

4.4.1 Basic Properties

The basic properties for the continued fractions can be found in [22] and [18]. Let $\alpha = \alpha_0 \in \mathbf{R}$. We denote by $\lfloor x \rfloor$ the greatest integer not exceeding x (usually written as $[x]$ also). We have (finite or infinite) sequences α_i's and a_i's as follows:

$$\begin{aligned} a_i &= \lfloor \alpha_i \rfloor \\ \alpha_{i+1} &= \frac{1}{a_i - \alpha_i}, \quad \text{if } \alpha_i \notin \mathbf{Z} \end{aligned}$$

with $a_i \in \mathbf{Z}$, positive when $i > 1$, and $0 \leq \frac{1}{\alpha_i} < 1$, $\alpha_i = a_i + \frac{1}{\alpha_{i+1}}$. Then we have

$$\begin{aligned} \alpha &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \, \cfrac{1}{\alpha_n}}}} \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} \end{aligned}$$

We denote this as $\alpha = [a_0, a_1, \cdots, a_{n-1}, \alpha_n] = [a_0, a_1, a_2, \cdots]$. If all entries are integers, we call it as *(standard) continued fraction expansion* of α.

Conversely, for any integral sequence $\{a_n\}_{n \geq 0}$, $a_n > 0$ for $n \geq 1$, we can construct partial continued fractions $[a_0, a_1, \cdots, a_n]$ and the infinite continued fractions $[a_0, a_1, \cdots]$ is regarded as the limit of the partial continued fractions. It is known that every such sequence of partial continued fractions is convergent.

First we can notice that

Remark 4.13. The continued fraction expansion of α is finite if and only if $\alpha \in \mathbf{Q}$.

For $\beta \in \mathbf{R}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a matrix with integer entries, denote

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \beta = \frac{a\beta + b}{c\beta + d}$$

if $c\beta + d \neq 0$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta \right) = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \beta$$

with standard matrix product. Then

$$[a_0, a_1, \cdots, a_n, x] = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} x.$$

We denote

$$P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \tag{8}$$

by setting

$$P_0 = \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$P_{n+1} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{n+1}p_n + p_{n-1} & p_n \\ a_{n+1}q_n + q_{n-1} & q_n \end{pmatrix},$$

in other words,

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2}, \tag{9}$$

$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2}. \tag{10}$$

Then

$$\frac{p_n}{q_n} = [a_0, a_1, \cdots, a_n] \tag{11}$$

since

$$[a_0, a_1, \cdots, a_n] = P_{n-1} a_n = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

Remark 4.14. For any n,

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1} \tag{12}$$

Proof. By (8), since $\det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = -1$, $\det P_n = (-1)^{n+1}$. □

Fact 4.15. (a) The continued fraction expansion of α is periodic (for some $N, r \in \mathbf{Z}$, $a_n = a_{n+r}$ for all $n > N$, denoted by $\alpha = [a_0, \cdots, a_N; \overline{a_{N+1}, \cdots, a_{N+r}}]$)

$\iff$ α is *quadratic*, i.e. a solution of an irreducible quadratic polynomial.

(b) The continued fraction expansion of α is purely periodic ($\alpha = [\overline{a_0, \cdots, a_{r-1}}]$)

$\iff$ α is *reduced* quadratic, i.e. $\alpha > 0$, $-1 < {}^s\alpha < 0$, where ${}^s\alpha$ is the quadratic conjugate of α as usual.

The proof of (a) and (b) will be found in [18] or [22].

Proposition 4.16. *If* $\alpha = [\overline{a_0, \cdots, a_{r-1}}]$ *has a purely periodic continued fraction expansion, then* $-\frac{1}{{}^s\alpha} = [\overline{a_{r-1}, \cdots, a_0}]$.

Proof. First, we have $-\frac{1}{{}^s\alpha} > 1$ and $-1 < -\frac{1}{\alpha} < 0$ from $\alpha > 1$ and $-1 < {}^s\alpha < 0$. So $-\frac{1}{{}^s\alpha}$ is also a reduced quadratic number. Since

$$\alpha = [a_0, a_1, \cdots, a_{r-1}, \alpha] = P_{r-1}\alpha = \frac{p_{r-1}\alpha + p_{r-2}}{q_{r-1}\alpha + q_{r-2}},$$

we have

$$q_{r-1}\alpha^2 + (q_{r-2} - p_{r-1})\alpha - p_{r-2} = 0$$

$$q_{r-1}\,{}^s\alpha^2 + (q_{r-2} - p_{r-1})\,{}^s\alpha - p_{r-2} = 0$$

$$q_{r-1} + (q_{r-2} - p_{r-1})\frac{1}{{}^s\alpha} - p_{r-2}\frac{1}{{}^s\alpha^2} = 0$$

$$p_{r-2}\left(-\frac{1}{{}^s\alpha}\right)^2 + (q_{r-2} - p_{r-1})\left(-\frac{1}{{}^s\alpha}\right) - q_{r-1} = 0$$

so

$$\left(p_{r-2}\left(-\frac{1}{{}^s\alpha}\right) + q_{r-2}\right)\left(-\frac{1}{{}^s\alpha}\right) = p_{r-1}\left(-\frac{1}{{}^s\alpha}\right) + q_{r-1}.$$

Hence

$$
\begin{aligned}
-\frac{1}{{}^s\alpha} &= \frac{p_{r-1}\left(-\frac{1}{{}^s\alpha}\right)+q_{r-1}}{p_{r-2}\left(-\frac{1}{{}^s\alpha}\right)+q_{r-2}} = \begin{pmatrix} p_{r-1} & q_{r-1} \\ p_{r-1} & q_{r-2} \end{pmatrix}\left(-\frac{1}{{}^s\alpha}\right) \\
&= P_{r-1}^T\left(-\frac{1}{{}^s\alpha}\right) \\
&= \left[\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_{r-1} & 1 \\ 1 & 0 \end{pmatrix}\right]^T\left(-\frac{1}{{}^s\alpha}\right) \\
&= \begin{pmatrix} a_{r-1} & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\left(-\frac{1}{{}^s\alpha}\right).
\end{aligned}
$$

Therefore

$$-\frac{1}{{}^s\alpha} = [\overline{a_{r-1},\cdots,a_0}].$$

□

Now we consider the continued fraction expansion of $\sqrt{m}$. Let $a_0 = \lfloor\sqrt{m}\rfloor$ then $\alpha = \sqrt{m}+a_0$ is reduced since $\alpha > 0$ and $-1 < {}^s\alpha = a_0 - \sqrt{m} < 0$. So continued fraction expansion of α is purely periodic. Since $\lfloor\alpha\rfloor = 2a_0$, we have $\alpha = [\overline{2a_0, a_1, \cdots, a_{r-1}}]$ with the least period r. Then $\sqrt{m} = \alpha - a_0 = [a_0; \overline{a_1, \cdots, a_{r-1}, 2a_0}]$. By Proposition 4.16, we have $-\frac{1}{{}^s\alpha} = -\frac{1}{a_0-\sqrt{m}} = [\overline{a_{r-1}, \cdots, 2a_0}]$, or,

$$\frac{1}{\sqrt{m}-a_0} = a_{r-1} + \cfrac{1}{a_{r-2}+\cfrac{1}{\ddots}}$$

then

$$\sqrt{m}-a_0 = \cfrac{1}{a_{r-1}+\cfrac{1}{a_{r-2}+\cfrac{1}{\ddots}}}$$

$$\sqrt{m} = a_0 + \cfrac{1}{a_{r-1}+\cfrac{1}{a_{r-2}+\cfrac{1}{\ddots}}} = [a_0; \overline{a_{r-1}, \cdots, a_1, 2a_0}].$$

Comparing with $\sqrt{m} = [a_0; \overline{a_1, \cdots, a_{r-1}, 2a_0}]$, we have $a_i = a_{r-i}$ for $i = 1, \ldots, r-1$.

Remark 4.17. The continued fraction expansion of $\sqrt{m}$ is of form

$$[a_0; \underbrace{\overline{a_1, a_2, \cdots, a_2, a_1, 2a_0}}_{r}]$$

with reflective symmetry.

Lemma 4.18. *For* $\sqrt{m} = [a_0; \overline{a_1, \cdots, a_{r-1}, 2a_0}]$ *and* $j \in \mathbf{N}$,

$$\begin{pmatrix} mq_{jr-1} & p_{jr-1} \\ p_{jr-1} & q_{jr-1} \end{pmatrix} = \begin{pmatrix} p_{jr-1} & p_{jr-2} \\ q_{jr-1} & q_{jr-2} \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. We have

$$\begin{aligned} \sqrt{m} &= [a_0, a_1, \cdots, a_{jr-1}, a_0 + \sqrt{m}] \\ &= P_{jr-1}(a_0 + \sqrt{m}) \\ &= \frac{p_{jr-1}(a_0 + \sqrt{m}) + p_{jr-2}}{q_{jr-1}(a_0 + \sqrt{m}) + q_{jr-2}}. \end{aligned}$$

So $\sqrt{m}(a_0 q_{jr-1} + q_{jr-2} - p_{jr-1}) = a_0 p_{jr-1} + p_{jr-2} - m q_{jr-1}$, i.e.

$$\begin{aligned} m q_{jr-1} &= a_0 p_{jr-1} + p_{jr-2}, \\ p_{jr-1} &= a_0 q_{jr-1} + q_{jr-2}. \end{aligned}$$

□

Looking at the determinant of the matrix in the previous lemma, we get

$$p_{jr-1}^2 - m q_{jr-1}^2 = (-1)^{jr-1}(-1) = (-1)^{jr}.$$

Remark 4.19. It is known that the integral solution for the *Pell's equation* $x^2 - my^2 = \pm 1$ are only these $(\pm p_{jr-1}, \pm q_{jr-1})$. Therefore, for $m \equiv 2, 3 \pmod 4$, the fundamental unit $\varepsilon = u + v\sqrt{m}$ is given by $u = p_{r-1}$, $v = q_{r-1}$. Furthermore, $N(\varepsilon) = (-1)^r$ so $N(\varepsilon)$ has norm -1 if and only if r is odd. Since we are considering the fundamental units with norm $+1$ only, so we may assume that r is even. If m has a prime divisor $p \equiv 3 \pmod 4$, then the norm of fundamental unit is $u^2 - mv^2 \equiv u^2 \pmod p$, and it never attains the value -1 since -1 is not a quadratic residue mod p. Hence if $m \equiv 3 \pmod 4$ is not square, then r should be even, and we have the central element of the symmetry in the period of continued fraction expansion of $\sqrt{m}$:

$$\sqrt{m} = [a_0; \underbrace{\overline{a_1, a_2, \cdots, a_{r/2}, \cdots, a_2, a_1, 2a_0}}_{r}].$$

4.4.2 Determination for $m \equiv 3 \pmod 4$ case

Lemma 4.20.

$$v = q_{s-1}(q_s + q_{s-2}) = q_{s-1}(a_s q_{s-1} + 2q_{s-2})$$
$$mv = p_{s-1}(p_s + p_{s-2}) = p_{s-1}(a_s p_{s-1} + 2p_{s-2})$$

where $s = r/2$.

Proof.

$$\begin{aligned} P_{r-1} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s \left(\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} P_{s-1} \right)^T \\ &= P_s P_{s-1}^T \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}. \end{aligned}$$

Then by Lemma 4.18,

$$\begin{aligned} \begin{pmatrix} mq_{r-1} & p_{r-1} \\ p_{r-1} & q_{r-1} \end{pmatrix} &= P_{r-1} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s P_{s-1}^T \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s P_{s-1}^T \\ &= \begin{pmatrix} p_s & p_{s-1} \\ q_s & q_{s-1} \end{pmatrix} \begin{pmatrix} p_{s-1} & q_{s-1} \\ p_{s-2} & q_{s-2} \end{pmatrix} \\ &= \begin{pmatrix} p_{s-1}(p_s + p_{s-2}) & p_s q_{s-1} + p_{s-1} q_{s-2} \\ p_{s-1} q_s + p_{s-2} q_{s-1} & q_{s-1}(q_s + q_{s-2}) \end{pmatrix}. \end{aligned}$$

Note that $v = q_{r-1}$. □

Theorem 4.21. *For* $m \equiv 3 \pmod 4$ *and* $\sqrt{m} = [a_0; \overline{a_1, a_2, \cdots, a_r}]$ *, then* $v \equiv a_s \pmod 2$ *where* $s = r/2$. *So* $\Delta_m = 1$ *if and only if* a_s *is odd.*

Proof. By Lemma 4.20, $v \equiv a_s p_{s-1} \pmod 2$ and $v \equiv a_s q_{s-1} \pmod 2$. Since p_{s-1} and q_{s-1} are mutually prime by the equation (12), they cannot be both even. One of the congruences says $v \equiv a_s \pmod 2$. □

Remark. This theorem also holds for $m \equiv 2 \pmod 4$. Indeed, we know that v is even. By Lemma 4.20, $0 \equiv v \equiv a_s q_{s-1} \pmod 2$ and $0 \equiv mv \equiv a_s p_{s-1} \pmod 2$. Since $(p_{s-1}, q_{s-1}) = 1$, we see that a_s is even.

Example 4.22. (a) $183 = 3 \cdot 61 \equiv 3 \pmod 4$ and $\sqrt{183} = [13; \overline{1, 1, 8, 1, 1, 26}]$. The period $r = 6$ and the central element is $a_3 = 8$. By the previous theorem, we get $\Delta_{183} = 2$. Using p_5, q_5, we get $\varepsilon = 487 + 36\sqrt{183}$.

(b) $247 = 13 \cdot 19 \equiv 3 \pmod 4$ and $\sqrt{247} = [15; \overline{1, 2, 1, 1, 9, 1, 9, 1, 1, 2, 1, 30}]$ with period 12. The central element is $a_6 = 1$ so $\Delta_{247} = 1$. By the way, $\varepsilon = 85292 + 5427\sqrt{247}$.

(c) Here are classified lists of $m \equiv 3 \pmod 4$, squarefree, < 1000, which is obtained by calculating continued fraction expansions.

$\Delta_m = 1$:

3, 7, 11, 15, 19, 23, 31, 35, 43, 47, 51, 59, 67, 71, 79, 83, 87, 91, 103, 107, 115, 119, 123, 127, 131, 139, 143, 151, 159, 163, 167, 179, 187, 191, 195, 199, 211, 215, 219, 223, 227, 231, 235, 239, 247, 251, 255, 263, 267, 271, 283, 287, 291, 303, 307, 311, 319, 323, 331, 335, 339, 347, 359, 367, 379, 383, 391, 399, 403, 411, 415, 419, 427, 431, 435, 439, 443, 447, 451, 455, 463, 467, 479, 483, 487, 491, 499, 503, 511, 515, 519, 523, 527, 535, 547, 551, 555, 563, 571, 587, 591, 595, 599, 607, 611, 615, 619, 623, 627, 631, 635, 643, 647, 659, 671, 679, 683, 691, 699, 703, 707, 715, 719, 723, 727, 731, 739, 743, 751, 767, 771, 779, 787, 795, 799, 803, 807, 811, 815, 823, 827, 835, 839, 843, 851, 859, 863, 871, 879, 883, 887, 899, 907, 911, 919, 923, 935, 947, 951, 959, 967, 971, 983, 991

$\Delta_m = 2$:

39, 55, 95, 111, 155, 183, 203, 259, 295, 299, 327, 355, 371, 395, 407, 471, 543, 559, 579, 583, 651, 655, 663, 667, 687, 695, 755, 759, 763, 791, 831, 895, 903, 915, 939, 943, 955, 979, 987, 995

4.4.3 ERD-type

For some type of numbers, Mollin determined in [10] the full entry of continued fraction expansions of their square roots. So we can see Δ_m immediately for those numbers.

Definition 4.23. A positive integer m is said to be of Extended-Richaud-Degert-type (ERD-type) if it is written in the form $m = b^2 + s$ where $s \mid 4b$.

Theorem 4.24 (R.Mollin). *If m is of ERD-type,*

(a) $b = a_0 = [\sqrt{m}]$,

$$s \mid 2b \Longrightarrow a_{r/2} = \frac{2b}{s}$$

$$s \nmid 2b \Longrightarrow \begin{cases} a_{r/2} = \frac{8b}{s} & \text{if } b \text{ is odd} \\ a_{r/2} = \frac{b}{2} - 1 & \text{if } b \text{ is even} \end{cases}$$

(b) $b = a_0 + 1$,

$$s \mid 2b \Longrightarrow \begin{cases} a_{r/2} = -\frac{2b}{s} - 2 & \text{if } s \neq -b, -2b \\ a_{r/2} = 2 & \text{if } s = -b \end{cases}$$

$$s \nmid 2b \Longrightarrow \begin{cases} a_{r/2} = \frac{b}{2} - 1 & \text{if } b \text{ is even} \\ a_{r/2} = -\frac{8b}{s} - 2 & \text{if } b \text{ is odd} \end{cases}$$

$$s = -4b/3 \Longrightarrow \begin{cases} a_{r/2} = \frac{b}{2} - 1 & \text{if } b \text{ is even} \\ a_{r/2} = 4 & \text{if } b \text{ is odd} \end{cases}$$

4.5 Some special case of $m \equiv 3 \pmod 4$

The case $m \equiv 3 \pmod 4$ is fully determined in terms of continued fractions. We have another description of Δ_m depending on the decomposition for certain numbers as follows.

For the fundamental unit $\varepsilon = u + v\sqrt{m}$, note that

$$u \text{ is even } \Leftrightarrow v \text{ is odd } (\Leftrightarrow \Delta_m = 1) \tag{13}$$

by seeing the equation $u^2 - mv^2 = 1$ modulo 4.

Proposition 4.25. *If $m = p$ an odd prime $\equiv 3 \pmod 4$, then $\Delta_m = 1$.*

Proof. Trivial. $u^2 - pv^2 = 1$ so $u^2 \equiv 1 \pmod p$ then $u \equiv \pm 1 \pmod p$. u is even. □

Proposition 4.26. *Suppose that for any proper decomposition of $m = m_1 m_2$ ($m_1, m_2 \neq 1$), the Jacobi symbol $\left(\frac{m_1}{m_2}\right) = -1$. Then $\Delta_m = 1$.*

Remark. We have $\left(\frac{m_1}{m_2}\right) = \left(\frac{m_2}{m_1}\right)$ since one of them $\equiv 1 \pmod 4$.

Proof. Assume that $\Delta_m = 2$, that is, v is even and u is odd. Let $v' = v/2$. From $u^2 - 4mv'^2 = 1$, we get $(u-1)(u+1) = 4mv'^2$. Let $u' = (u-1)/2 \in \mathbf{Z}$ then $u'(u'+1) = mv'^2$. Since u' and $u'+1$ are mutually prime, we set $u' = m_1 v_1^2$, $u'+1 = m_2 v_2^2$ where $m_1 m_2 = m$ (mutually prime) and $v_1 v_2 = v'$ (mutually prime). We get

$$m_1 v_1^2 + 1 = m_2 v_2^2. \tag{14}$$

We claim $m_1, m_2 \neq 1$. Indeed, suppose $m_1 = 1$. We have $v_1^2 + 1 = m v_2^2$ so $v_1^2 + v_2^2 \equiv -1 \pmod 4$, which is impossible. And suppose $m_2 = 1$. We have $m v_1^2 + 1 = v_2^2$ so $v_2^2 - m v_1^2 = 1$. This is a contradiction since (u, v) is the smallest positive solution of $x^2 - my^2 = 1$ and $v_1 < v$. Hence $m_1, m_2 \neq 1$. Now consider the equation (14) modulo m_1. We have $1 \equiv m_2 v_2^2 \pmod{m_1}$. Since m_1, m_2 are mutually prime, we can deduce that the inverse of m_2 mod m_1 is a quadratic residue mod m_1, and equivalently, m_2 is a quadratic residue mod m_1. The Jacobi symbol $\left(\frac{m_1}{m_2}\right) = \left(\frac{m_2}{m_1}\right) = -1$ means m_2 is a quadratic nonresidue mod m_1, and this completes the proof. □

Example 4.27. $231 = 3 \cdot 7 \cdot 11 \equiv 3 \pmod 4$ and for all decomposition,

$$\left(\frac{7 \cdot 11}{3}\right) = \left(\frac{3 \cdot 11}{7}\right) = \left(\frac{3 \cdot 7}{11}\right) = -1$$

so $\Delta_{231} = 1$.

Corollary 4.28. *If $m = pq \equiv 3 \pmod 4$ where p, q are odd primes such that $\left(\frac{p}{q}\right) = -1$, then $\Delta_m = 1$.*

Proposition 4.29. *For $m = pq \equiv 3 \pmod 4$ where p, q are odd primes and $\left(\frac{p}{q}\right) = 1$, if $p, q \not\equiv 1 \pmod 8$, then $\Delta_m = 2$.*

Proof. Let $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Assume that $\left(\frac{p}{q}\right) = 1$ and $p \not\equiv 1 \pmod 8$ (i.e. $p \equiv 5 \pmod 8$) but $\Delta_m = 1$ (u is even and v is odd). From $u^2 - pqv^2 = 1$, we get $(u-1)(u+1) = pqv^2$. Since u is even, $(u-1, u+1) = 1$. We have four possible cases for the decomposition $v = v_1 v_2$;

(1) $u - 1 = v_1^2$, $u + 1 = pqv_2^2$.

(2) $u - 1 = pv_1^2$, $u + 1 = qv_2^2$.

(3) $u-1=qv_1^2$, $u+1=pv_2^2$.

(4) $u-1=pqv_1^2$, $u+1=v_2^2$.

For each case, we have (1) $pqv_2^2=v_1^2+2$, (2) $qv_2^2=pv_1^2+2$, (3) $pv_2^2=qv_1^2+2$, and (4) $v_2^2=pqv_1^2+2$. Consider these modulo p, we have (1) -2, (2) $2q^{-1}$, (3) $-2q^{-1}$ and (4) 2 are quadratic residues mod p, where q^{-1} represents inverse of q mod p. All cases are impossible. Indeed, since $\left(\frac{q}{p}\right)=1$, $\left(\frac{q^{-1}}{p}\right)=1$. And since $p\equiv 5 \pmod 8$, $\left(\frac{-1}{p}\right)=1$ and $\left(\frac{2}{p}\right)=-1$. This shows $\left(\frac{-2}{p}\right)=\left(\frac{2q^{-1}}{p}\right)=\left(\frac{-2q^{-1}}{p}\right)=\left(\frac{2}{p}\right)=-1$. □

4.6 Parity Problem

Here we give more general and equivalent condition for $\Delta_m=1$ when $m\equiv 3 \pmod 4$. Δ_m depends on the parity of the coefficient of the fundamental unit $\varepsilon=u+v\sqrt{m}$. For convenience, we will use a new notation $Ir(a+b\sqrt{m})=b$ the coefficient of the irrational part of quadratic number $a+b\sqrt{m}\in\mathbf{Q}(\sqrt{m})$. $Ir(\alpha)\in\mathbf{Z}$ or $\frac{1}{2}\mathbf{Z}$ if $\alpha\in\mathcal{O}_K$, and it is an integer if $m\equiv 2,3 \pmod 4$. We can see some similarity between the determination of parity of $Ir(\varepsilon)$ where $m\equiv 3 \pmod 4$, and the determination of sign of $N(\varepsilon)$ where $m\not\equiv 3 \pmod 4$ has no prime factor $\equiv 3 \pmod 4$. (We exclude the case $m\equiv 2 \pmod 4$ for determining parity of $Ir(\varepsilon)$ since it is even only, and we exclude the case that there exists $p\mid m$ with $p\equiv 3 \pmod 4$ for determining sign of $N(\varepsilon)$ since $N(\varepsilon)$ should be $+1$ because -1 is not a quadratic residue modulo p.) If $N(\varepsilon)=1$, then all units are of norm 1, while if $N(\varepsilon)=-1$, then the units that are odd powers of ε times (± 1) have norm -1 and the units that are even powers of ε times (± 1) have norm $+1$. Likewise, if $Ir(\varepsilon)$ is even, then all units have even Ir, but if $Ir(\varepsilon)$ is odd, then units that are odd powers of ε times (± 1) have odd Ir and units that are even powers of ε times (± 1) have even Ir. This property enables us to obtain conditions that determine the parity of $Ir(\varepsilon)$; these conditions are analogous to those that determine the sign of $N(\varepsilon)$.

4.6.1 A Result Inspired by Trotter's Theorem

First we have a connection with a certain Diophantine Equation. H.F. Trotter proved the following theorem in [25].

Theorem 4.30 (Trotter). *Let m be square free with no prime factor $\equiv 3 \pmod 4$ and let $K=\mathbf{Q}(\sqrt{m})$ and ε be the fundamental unit of $\mathcal{O}_K$. Then the followings are equivalent:*

(a) $N(\varepsilon) = -1$.

(b) *The ideal* $[d, \sqrt{m}]$ *is not principal for* $1 < d < m$, $d \mid m$.

(c) $|dx^2 - \frac{m}{d}y^2| = 4$ *has no integer solutions for* $1 < |d| < m$, $d \mid m$.

With some modification, we can prove an analogy of this theorem: We write the pair (a, b) for the quadratic integer $a + b\sqrt{m}$ and (a, b) does not denote the greatest common divisor in this section. First, we will introduce a new equivalent relation of $\mathcal{O}_K = [1, \sqrt{m}]$. For $a_1 + b_1\sqrt{m}$ and $a_2 + b_2\sqrt{m} \in \mathcal{O}_K$, define

$$a_1 + b_1\sqrt{m} \sim_2 a_2 + b_2\sqrt{m}$$

if $a_1 \equiv a_2 \pmod 2$ and $b_1 \equiv b_2 \pmod 2$. We obtain four equivalent classes $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ in $\mathcal{O}_K$. We write $\bar{x}$ as residue class of x mod 2 and we may omit the bar for 0 and 1. For $a + b\sqrt{m}$, we can write $(a, b) = (\bar{a}, \bar{b})$ as the class of $a + b\sqrt{m}$ and call $a + b\sqrt{m}$ is of type (a, b). Denote by V the set of such classes. We have induced ring operators

$$(a, b) + (c, d) = (a + b, c + d),$$

$$(a, b)(c, d) = (ac + bd, ad + bc)$$

since m is odd. Then we can identify (a, b) with an element $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ of the ring $M_{2\times 2}(\mathbf{Z}/2\mathbf{Z})$ of the 2×2 matrices over $\mathbf{Z}/2\mathbf{Z}$ with the standard matrix operations. Therefore the set of classes V forms a ring. Denote the elements

$$0 = (0, 0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad I = (1, 0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\delta = (0, 1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \gamma = (1, 1) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

The multiplicative rule is;

(a) commutative.

(b) $xI = x$ and $x0 = 0$ for all $x \in V$.

(c) $\delta^2 = I$, $\gamma^2 = 0$, and $\delta\gamma = \gamma$.

Now we look at unit elements of $\mathcal{O}_K$. We have $U_K = \mathcal{O}_K^\times = \{\pm 1\} \times \langle \varepsilon \rangle$. If v is even, $\varepsilon \in (1,0) = I$ and $\varepsilon^n \in I$ so all units are of type $(1,0)$. If v is odd, $\varepsilon \in (0,1) = \delta$ so odd power of ε is in $\delta = (0,1)$ and even power of ε is in $I = (1,0)$. In this case, $(1,0)$-type units are in $\pm(U_K)^2$.

Theorem 4.31. *Let $m \equiv 3 \pmod 4$ squarefree and $\varepsilon = u + v\sqrt{m}$ with $N(\varepsilon) = 1$. Followings are equivalent:*

(a) *v is odd.* ($\Leftrightarrow \Delta_m = 1$.)

(b) *The ideal $[d, \sqrt{m}]$ of $\mathcal{O}_K$ is not principal for $1 < d < m$, $d \mid m$.*

(c) *$|dx^2 - \frac{m}{d}y^2| = 1$ has no integer solutions for $1 < |d| < m$, $d \mid m$.*

Proof. (b) $\Leftrightarrow$ (c): For each prime integer $p \mid m$, the prime ideal $\mathfrak{p} = [p, \sqrt{m}]$ ramifies; $p = \mathfrak{p}^2$, ${}^s\mathfrak{p} = \mathfrak{p}$, and $N(\mathfrak{p}) = p$. Actually, $\mathfrak{p}$ is the unique ideal with norm p. For $d \mid m$, there exists the unique ideal $[d, \sqrt{m}]$ of norm $|d|$, which is principal if and only if there exists $\alpha \in \mathcal{O}_K$ with $N(\alpha) = \pm d$. Now, there exists $\alpha = a + b\sqrt{m}$ with $N(\alpha) = a^2 - mb^2 = \pm d$ if and only if

$$|a^2 - mb^2| = |d| \tag{15}$$

has an integer solution. For any solution (x, y) of equation of (c), $a = dx$ and $b = y$ gives solution of (15). For any solution (a, b) of (15), since $d \mid m$ and m is squarefree, $d \mid a$, and if we put $x = a/d$, $y = b$ then (x, y) is a solution of equation in (c).

(a) $\Rightarrow$ (b): Suppose $d \mid m$ and $[d, \sqrt{m}] = (\alpha)$ is principal. Since ${}^s[d, \sqrt{m}] = [d, \sqrt{m}]$, ${}^s\alpha = \eta\alpha$ for some unit η. Write $\alpha = a + b\sqrt{m}$ and $\eta = r + s\sqrt{m}$ then $a \not\equiv b \pmod 2$ and η is of type $(0,1)$. Indeed, since $\sqrt{m} \in [d, \sqrt{m}] = (\alpha)$, there exists $\beta = c + d\sqrt{m}$ such that $\alpha\beta = \sqrt{m}$. As the class of the relation $\sim_2$, $(a,b)(c,d) = (0,1) = \delta$. Then $(a,b) \neq 0, \gamma$ by the multiplicity rule of V. So $a \not\equiv b \pmod 2$. On the other hand, from $\alpha\eta = {}^s\alpha$, $(a,b)(r,s) = (a,b)$. Since $(a,b) = I$ or δ, $(r,s) = I$, i.e. η is of type $(1,0)$. Suppose v is odd. Then $\eta \in \pm(U_K)^2$ so $\eta = \pm\mu^2$ for some unit μ. Then $\pm d = {}^s\alpha\alpha = \pm\mu^2\alpha^2$ so $|d|$ is a perfect square in $\mathcal{O}_K$. Hence $|d| = 1$ or m.

(b) $\Rightarrow$ (a): Suppose the fundamental unit ε is of type $(1,0)$. Since $N(\varepsilon) = +1$, by Hilbert 90, $\varepsilon = \alpha/{}^s\alpha$ for some $\alpha \in \mathcal{O}_K$. We may assume α and ${}^s\alpha$ have no common factor. We have ${}^s\alpha\varepsilon = \alpha$ so the ideal ${}^s(\alpha) = (\alpha)$. Then $(\alpha) = (l)\prod[p_i, \sqrt{m}]$ where $l \in \mathbf{Z}$ whose prime divisors are primes inert in $\mathcal{O}_K$, and $p_i \mid m$. Then $l \mid \alpha$ and $l \mid {}^s\alpha$ so by the

assumption of no common factor, we have $(\alpha) = \prod[p_i, \sqrt{m}]$ for some $p_i \mid m$. It can be written as $(\alpha) = [d, \sqrt{m}]$ for some $d \mid m$. If $d = 1$ or m, then $(\alpha) = \mathcal{O}_K$ or $(\sqrt{m})$, so $\alpha = \eta$ or $\eta\sqrt{m}$ for some unit η. Then $\varepsilon = \pm\eta^2$. Indeed, $\varepsilon = \alpha/\,{}^s\alpha = \eta/\,{}^s\eta = \eta^2$ since ${}^s\eta\eta = 1$, or $\varepsilon = \alpha/\,{}^s\alpha = \frac{\eta\sqrt{m}}{-{}^s\eta\sqrt{m}} = -\eta^2$. This contradicts the fact that ε is the fundamental unit. Hence d is a proper divisor of m. □

Remark. Propositions 4.25 and 4.26 are direct corollaries to this theorem.

An equivalent result was proved by R. Mollin independently in [8] starting from a different point of view. We emphasize here the similarity between the criterion for $N(\varepsilon)$ to be equal to -1 and the one for $Ir(\varepsilon)$ to be congruent to 1 mod 2, while Mollin gives the concrete solutions of the Diophantine equation in terms of the continued fraction expansion of $\sqrt{m}$.

Theorem 4.32 (Mollin). *Suppose that $D > 1$ is not a perfect square and r, the least period of continued fraction expansion of $\sqrt{D}$, is even. Then the following are equivalent.*

(a) *The central quotient $a_{r/2}$ in the simple continued fraction expansion of $\sqrt{D}$ is even*

(b) *There exists a factorization $D = ab$ with $1 < a < b$ such that the equation $ax^2 - by^2 = \pm 1$ has an integer solution.*

(c) *There does not exist a factorization $D = ab$ with $1 \leq a < b$ such that the equation $ax^2 - by^2 = \pm 2$ has an integer solution with xy odd.*

Remark. The fundamental solution for the equation in (b) is that $a = e_{r/2}$, $b = m/a$, $x = p_{r/2-1}/a$, and $y = q_{r/2-1}$, where e_m is the integer such that α_m is written as $(c_m + \sqrt{m})/e_m$.

Mollin also gives a criterion to be $N(\varepsilon) = -1$ in [8].

Theorem 4.33 (Mollin). *Let $D > 2$, not a perfect square. Then r, the least period of continued fraction expansion of $\sqrt{m}$, is even ($\Leftrightarrow N(\varepsilon) = +1$) if and only if one of the following holds.*

(a) *There exists a factorization $D = ab$ with $1 < a < b$ such that equation*

$$ax^2 - by^2 = \pm 1 \quad \textit{with } (x, y) = 1$$

has an integral solution.

(b) *There exists a factorization $D = ab$ with $1 \leq a < b$ such that equation*

$$ax^2 - by^2 = \pm 2$$

has an integral solution where xy is odd.

Remark 4.34. It is known that (a) and (b) in the previous theorem can not hold simultaneously. Hence, for $m \equiv 3 \pmod 4$, v is odd if and only if there exists a factorization $D = ab$ with $1 \leq a < b$ such that $ax^2 - by^2 = \pm 2$ has an integral solution with xy odd.

4.6.2 An Open Problem about Class Numbers of Real Quadratic Fields

Another criterion for condition $N(\varepsilon) = -1$ is related to the class number of $K = \mathbf{Q}(\sqrt{m})$. In [9], the condition equivalent to $N(\varepsilon) = -1$ for $K = \mathbf{Q}(\sqrt{m})$, $m > 0$ has been founded:

Theorem 4.35 (Gauss). *Let h be the ideal class number of K. Then $2^{t-2} \mid h$, where t is the number of ramified prime ideals of $\mathcal{O}_K$. Moreover, $2^{t-1} \mid h$ iff $N(\varepsilon) = -1$.*

But the proof in [9] does not seemed to use properties similar to the one of odd Ir case. One possibility is using Nguyen-Quang-do Thong's theorem, which was used to prove the Theorem 4.35 in [23].

Theorem 4.36 (Nguyen-Quang-do Thong). *We have an exact sequence of groups*

$$U_K^{(1)} \longrightarrow \mathcal{R} \longrightarrow \mathcal{H}_{reg} \longrightarrow 1$$

where $U_K^{(1)}$ is the set of unit elements of norm 1 in the ring of integer, $\mathcal{R}$ is the group whose elements are ramified prime ideals where the operation is symmetric difference of sets, and $\mathcal{H}_{reg}$ is subgroup of regular classes in the ideal class group, where the regular class is a class containing a G-invariant ideal.

The condition for $N(\varepsilon) = -1$ with $m \not\equiv 3 \pmod 4$ and the one for odd $Ir(\varepsilon)$ with $m \equiv 3 \pmod 4$ are similar, and in the same vein, we hope to find some analogy of Theorem 4.36, and of Theorem 4.35, using an exact sequence starting from $U_K^{(even)}$ (the set of unit elements with even Ir).

5 Structure of M_c/P_c and Ramification Theory

5.1 Ramification Theory

The vanishing of 0-cohomology is related to the existence of integral normal basis (INB) and the ramification theory. Let K/k be a finite Galois extension of number fields with the Galois group G. A ramified prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ is called *tamely ramified* if $p \nmid e_{\mathfrak{p}}$ where $p = \mathbf{Z} \cap \mathfrak{p}$ and $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ in K/k. We call the extension K/k *tamely ramified* if every prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ is tamely ramified. If a prime ideal or an extension is not tamely ramified, then it is called *wildly ramified*.

As we see below, a Galois extension K/k is tamely ramified if and only if $\widehat{H}^0(G, \mathcal{O}_K) = 0$. Both of these follow from the existence of an INB.

Denote by $\mathcal{O}_K^*$ the fractional ideal $\{x \in K \mid T_{K/k}(x\mathcal{O}_K) \subset \mathcal{O}_k\}$. The *different* is defined as the fractional ideal $(\mathcal{O}_K^*)^{-1}$, which is an ideal in $\mathcal{O}_K$ and denoted by $\mathcal{D}_{K/k}$.

Let $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ be a Galois extension of local fields. Let $G = \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ and denote by $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$, respectively. There is the unique prime ideal in the ring of integers: $\mathfrak{P}$ in $\mathcal{O}_{\mathfrak{P}}$, and $\mathfrak{p}$ in $\mathcal{O}_{\mathfrak{p}}$. The *ramification index* e is the integer satisfying $\mathfrak{p} = \mathfrak{P}^e$ in $\mathcal{O}_{\mathfrak{P}}$. Let $G_{-1} = G$ and set a sequence of subgroups of G

$$G_i := \{s \in G \mid {}^s\xi \equiv \xi \pmod{\mathfrak{P}^i} \text{ for all nonzero } \xi \in \mathcal{O}_{\mathfrak{P}}\}.$$

Then we have

$$G = G_{-1} \supset G_0 \supset \cdots \supset G_i \supset \cdots .$$

Let $t = \nu_{\mathfrak{P}}(\mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})$ the index of $\mathfrak{P}$ in $\mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$, that is, $\mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} = \mathfrak{P}^t$. In [17], Ono showed that

Theorem 5.1 (T. Ono, Local Case). *Let $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ be a Galois extension. The followings are equivalent, each of which follows from the existence of INB:*

(a) *$K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified.*

(b) *$p \nmid e$.*

(c) *$\mathfrak{P}^{e-1} \parallel \mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$.*

(d) *$t = e - 1$.*

(e) *$|G_i| = 1$ for $i \geq 1$.*

(f) $\widehat{H}^0(G, \mathcal{O}_{\mathfrak{P}}) = 0$.

(g) $T_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{P}}) = \mathcal{O}_{\mathfrak{p}}$.

Now let K/k be a Galois extension. For every prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ and for $\mathfrak{P}$ lying above $\mathfrak{p}$, we have the extension of completions $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, and we may define $t_{\mathfrak{p}}$ and $G_{i,\mathfrak{p}}$ for this extension as above.

Theorem 5.2 (T. Ono, Global Case). *Let K/k be a Galois extension. The followings are equivalent, each of which follows from the existence of INB:*

(a) *K/k is tamely ramified.*

(b) *$p \nmid e_{\mathfrak{p}}$ for all prime p.*

(c) *$\mathfrak{P}^{e_{\mathfrak{p}}-1} \parallel \mathcal{D}_{K/k}$ for all prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ and $\mathfrak{P} \mid \mathfrak{p}$.*

(d) *$t_{\mathfrak{p}} = e_{\mathfrak{p}} - 1$ for all prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$.*

(e) *$|G_{i,\mathfrak{p}}| = 1$ for $i \geq 1$.*

(f) *$\widehat{H}^0(G, \mathcal{O}_K) = 0$.*

(g) *$T_{K/k}(\mathcal{O}_K) = \mathcal{O}_k$.*

5.2 Local Case

In [16], T. Ono gave complete determination of M_c/P_c for the Galois extension of local fields $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. We use the notations in the previous section. We fix a prime element Π in K. Denote by $U_{\mathfrak{P}}$ and $U_{\mathfrak{p}}$ the unit group of the ring of integers $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{p}}$, respectively.

First, we know that

Proposition 5.3 (T. Ono). *The cohomology group $H^1(G, U_{\mathfrak{P}})$ is cyclic of order e generated by $\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$, where $\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ is the class of the cocycle $s \mapsto z_s$ such that ${}^s\Pi = \Pi z_s$.*

For a cohomology class $\gamma = \gamma^m_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ and a cocycle c in the class γ, We can construct $\widehat{H}^0(G, \mathcal{O}_{\mathfrak{P}})_\gamma = M_c/P_c$ as usual. The structure of M_c/P_c is given by the following theorem.

Theorem 5.4 (T. Ono). (a) *If $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is unramified, then $H^1(G, U_{\mathfrak{P}}) = 1$ and M_c/P_c is trivial.*

(b) *If $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified, then $|M_c/P_c| = 1$ for all $\gamma \in H^1(G, U_{\mathfrak{P}})$.*

(c) *If $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is wildly ramified, then $|M_c/P_c| = 1$ if and only if $\gamma \neq 1$ and $e \leq t+m < 2e$.*

The proof can be found in [16].

5.3 Vanishing of M_c/P_c

By (b) of Theorem 5.4, if a Galois extension of local fields $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified, then $M_c/P_c = \widehat{H}^0(G, \mathcal{O}_{\mathfrak{P}})_\gamma = 0$ for all $\gamma \in H^1(G, \mathcal{O}_{\mathfrak{P}}^\times)$.

In the global case, this statement is not proved yet. The quadratic extension over $\mathbf{Q}$ satisfies this property. For the quadratic field $K = \mathbf{Q}(\sqrt{m})$, $m \equiv 1 \pmod 4$ if and only if $\mathcal{O}_K$ has an INB over $\mathbf{Q}$ and $K/\mathbf{Q}$ is tamely ramified. We have $\widehat{H}^0(G, \mathcal{O}_K)_\gamma = M_c/P_c = 0$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$ for $m \equiv 1 \pmod 4$. Furthermore, it is very interesting if we can give some level of wild ramification: For $m \equiv 2 \pmod 4$, $\widehat{H}^0(G, \mathcal{O}_K)_\gamma \neq 0$ for all γ. For $m \equiv 3 \pmod 4$, there exists γ such that $\widehat{H}^0(G, \mathcal{O}_K)_\gamma = 0$ only if $m = -1$ or, $m > 0$ and v is odd where $\varepsilon = u + v\omega$ is the fundamental unit of $\mathcal{O}_K$. We may hope that this suggests a classification of wildly ramified extensions in terms of M_c/P_c for general K/k.

6 Use of Hilbert's Theorem 90

It is very important to determine M_c/P_c for general Galois number field extension K/k, or even generalize the object M_c/P_c itself.

6.1 For General Number Fields

There are many open problems for determining the twisted cohomology M_c/P_c for a given Galois number field extension K/k, taking $R = \mathcal{O}_K$. The module M_c/P_c is defined from the first cohomology of unit group. To determine the module thoroughly, it is important to have the concrete structure of the first cohomology group. Unfortunately, $H^1(G, \mathcal{O}_K^\times)$ has not been determined yet for many number fields. If we use Hilbert 90, we may reduce the calculation for determining M_c/P_c for general K/k.

Theorem 6.1 (Hilbert's Theorem 90). *Let K/k be a Galois extension of fields and G its Galois group. Then*

(a) $H^1(G, K^\times) = 1$,
i.e. any 1-cocycle $c \in Z^1(G, K^\times)$, there is $a \in K^\times$ such that $c_s = \frac{{}^s a}{a}$ (or, $c_s = \frac{a}{{}^s a}$) for all $s \in G$.

(b) $H^1(G, \mathrm{GL}_n(K)) = 1$ *for all* $n \in \mathbf{N}$,
i.e. for any $c \in Z^1(G, \mathrm{GL}_n(K))$, there is $U \in \mathrm{GL}_n(K)$ such that $c_s = U^{-1}\,{}^s U$ for all $s \in G$.

Remark 6.2. Since

$$c_s = \frac{a}{{}^s a} \Leftrightarrow c_s\, {}^s a = a,$$

we have $M_c = \{a \mid a \text{ satisfies Hilbert 90 for } c\}$, if we consider the ring $R = K$ as initial setting. The proof of Hilbert 90 shows the existence of nonzero element of form $p_c(x) = \sum_{s \in G} c_s\, {}^s x$ for some $x \in K^\times$. Since the 1-cohomology on $K^\times$ is trivial, $M_c/P_c = k/\operatorname{Tr}(K)$, which is also trivial.

Let $c \in Z^1(G, \mathcal{O}_K^\times)$ then $c_s \in \mathcal{O}_K^\times \subset K^\times$ so we may regard $c \in Z^1(G, K^\times)$. By Hilbert 90, there exists $\xi \in K^\times$ such that $c_s = \frac{{}^s \xi}{\xi}$ for all $s \in G$. We may assume $\xi \in \mathcal{O}_K^\times$. Indeed, there exists $b \in \mathcal{O}_k$ such that $b\xi \in \mathcal{O}_k$, so $\frac{{}^s(b\xi)}{b\xi} = \frac{b\,{}^s\xi}{b\xi} = \frac{{}^s\xi}{\xi}$. Now, $a \in M_c \Leftrightarrow c_s\, {}^s a = a\ \forall s \Leftrightarrow \frac{{}^s\xi}{\xi}\, {}^s a = a\ \forall s \Leftrightarrow {}^s(\xi a) = \xi a\ \forall s \Leftrightarrow \xi a \in \mathcal{O}_k \cap \xi \mathcal{O}_K$. Hence $\xi M_c = \mathcal{O}_k \cap \xi \mathcal{O}_K$.

For $x \in \mathcal{O}_K$, $p_c(x) = \sum_{t\in G} c_t\, {}^t x = \sum_{t\in G} \frac{{}^t\xi}{\xi}\, {}^t x = \frac{1}{\xi}\sum_{t\in G} {}^t(\xi x) = \frac{1}{\xi} T_{K/k}(\xi x)$, the trace. So $\xi P_c = T_{K/k}(\xi\mathcal{O}_K)$. Hence

$$M_c/P_c = (\mathcal{O}_k \cap \xi\mathcal{O}_K)/T_{K/k}(\xi\mathcal{O}_K). \tag{16}$$

Remark 6.3. This formula might give easier method to compute M_c/P_c. Assume that $\mathcal{O}_k$ is UFD (also PID), and we have an integral basis $\{\omega_1, \ldots, \omega_n\}$ of $\mathcal{O}_K$ over $\mathcal{O}_k$. $\mathcal{O}_k \cap \xi\mathcal{O}_K$ and $T_{K/k}(\xi\mathcal{O}_K)$ are principal ideals in $\mathcal{O}_k$. If $\xi = \sum_{i=1}^n b_i\omega_i$, $b_i \in \mathcal{O}_k$, then we have

$$N_{K/k}(\xi)/d^{n-1} \in \mathcal{O}_k \cap \xi\mathcal{O}_K$$

where $d = gcd(b_1, \ldots, b_n) \in \mathcal{O}_k$ since $\xi/d \in \mathcal{O}_K$, $\xi\prod_{s\neq 1} {}^s\xi/d = N_{K/k}(\xi)/d^{n-1}$. Also, we have

$$\begin{aligned} T_{K/k}(\xi\mathcal{O}_K) &= \left\{ T_{K/k}\left(\xi\sum_{i=1}^n a_i\omega_i\right) \middle| a_i \in \mathcal{O}_k \right\} = \left\{ \sum_{i=1}^n a_i T_{K/k}(\xi\omega_i) \middle| a_i \in \mathcal{O}_k \right\} \\ &= \gcd(\xi\omega_1, \ldots, \xi\omega_n)\mathcal{O}_k. \end{aligned}$$

We can generalize M_c/P_c as $(\mathcal{O}_k \cap \xi\mathcal{O}_K)/T_{K/k}(\xi\mathcal{O}_K)$ for general $\xi(\neq 0) \in \mathcal{O}_k$. Now generalized M_c/P_c, $(\mathcal{O}_k \cap \xi\mathcal{O}_K)/T_{K/k}(\xi\mathcal{O}_K)$ may not be restricted by a cocycle $c \in Z^1(G, \mathcal{O}_K)$ if ${}^s\xi/\xi \notin \mathcal{O}_K^\times$. But we notice that arbitrary ξ may not guarantee $T_{K/k}(\xi\mathcal{O}_K) \subset \mathcal{O}_k \cap \xi\mathcal{O}_K$:

Example 6.4. For $K/k = \mathbf{Q}(\sqrt{m})/\mathbf{Q}$, $m \equiv 2, 3 \pmod 4$, let $\xi = 1 + \sqrt{m}$. Then

$$\xi\mathcal{O}_K = \{(1+\sqrt{m})(x + y\sqrt{m}) \mid x, y \in \mathbf{Z}\} = \{(x + ym) + (x + y)\sqrt{m} \mid x, y \in \mathbf{Z}\}.$$

Then we have

$$T_{K/\mathbf{Q}}(\xi\mathcal{O}_K) = \{2(x + ym) \mid x, y \in \mathbf{Z}\} = 2(1, m)\mathbf{Z} = 2\mathbf{Z}$$

and

$$\mathbf{Z} \cap \xi\mathcal{O}_K = \{x + ym \mid x + y = 0\} = (1 - m)\mathbf{Z}.$$

If $m \neq 2, 3, -1$, then $T_{K/\mathbf{Q}}(\xi\mathcal{O}_K) \nsubseteq \mathbf{Z} \cap \xi\mathcal{O}_K$.

Remark 6.5. We may generalize M_c/P_c further: We see $\xi\mathcal{O}_K$ as a principal ideal in $\mathcal{O}_K$, then we may generalize M_c/P_c to $(\mathcal{O}_k \cap \mathfrak{a})/T_{K/k}(\mathfrak{a})$ for an ideal $\mathfrak{a}$ in $\mathcal{O}_K$. Also, it is not true that $T_{K/k}(\mathfrak{a}) \subset \mathcal{O}_k \cap \mathfrak{a}$ for all ideals $\mathfrak{a}$. Note that $\mathcal{O}_k \cap \mathfrak{a}$ and $T_{K/k}(\mathfrak{a})$ are ideals in $\mathcal{O}_k$.

6.2 Quadratic Field Case

Let $K = \mathbf{Q}(\sqrt{m})$, m squarefree. Denote by $T = T_{K/\mathbf{Q}}$ the trace and $N = N_{K/\mathbf{Q}}$ the norm. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$ such that $T(\mathfrak{a}) \subset \mathbf{Z} \cap \mathfrak{a}$. We have equivalently $T(\mathfrak{a}) \subset \mathfrak{a}$ or ${}^s\mathfrak{a} \subset \mathfrak{a}$, since for all $\alpha \in \mathfrak{a}$, $\alpha + {}^s\alpha \in \mathfrak{a}$ i.e. ${}^s\alpha \in \mathfrak{a}$. It follows that $\mathfrak{a} = a\prod \mathfrak{p}_i$ for some $a \in \mathbf{Z}$ where $\mathfrak{p}_i$ are all those prime ideal dividing the discriminant $d_{K/\mathbf{Q}}$ (i.e. ${}^s\mathfrak{p} = \mathfrak{p}$) and dividing $\mathfrak{a}$. Then we have $\mathbf{Z} \cap \mathfrak{a} = c\mathbf{Z}$ where $c = a\prod p_i$, $p_i \mid d_{K/\mathbf{Q}}$ and $p_i \mid \mathbf{Z} \cap \mathfrak{a}$. Now denote $T(\mathfrak{a}) = e\mathbf{Z}$. By assumption, $e\mathbf{Z} \subset c\mathbf{Z}$, or $c \mid e$. Since $2c = 2a\prod_i p_i = T(a\prod_i p_i) \in T(\mathfrak{a}) = e\mathbf{Z}$, we have $2c\mathbf{Z} \subset e\mathbf{Z}$, or $c \mid e \mid 2c$. Hence we have $[\mathbf{Z} \cap \mathfrak{a} : T(\mathfrak{a})] = 1$ or 2 for this general case also. Determining this index for ideals $\mathfrak{a}$ in a general and concrete way is still an open problem.

Now, we consider $(\mathbf{Z} \cap \xi\mathcal{O}_K)/T(\xi\mathcal{O}_K)$ for nonzero $\xi \in \mathcal{O}_K$.

$$\begin{aligned} T(\xi\mathcal{O}_K) \subset \mathbf{Z} \cap \xi\mathcal{O}_K &\Leftrightarrow T(\xi\mathcal{O}_K) \subset \xi\mathcal{O}_K \Leftrightarrow \xi \mid T(\xi\mathcal{O}_K) \text{ in } \mathcal{O}_K \\ &\Leftrightarrow \xi \mid \xi\beta + {}^s(\xi\beta) \text{ for all } \beta \in \mathcal{O}_K \\ &\Leftrightarrow \xi \mid {}^s\xi\,{}^s\beta \text{ for all } \beta \in \mathcal{O}_K \Leftrightarrow \xi \mid {}^s\xi \\ &\Leftrightarrow \frac{{}^s\xi}{\xi} \in \mathcal{O}_K \end{aligned}$$

This ${}^s\xi/\xi$ defines a cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$ by $c_s = {}^s\xi/\xi$. Hence, $(\mathbf{Z} \cap \xi\mathcal{O}_K)/T(\xi\mathcal{O}_K)$ does not generalize M_c/P_c for a cocycle c. Yet this gives a new computing method to determine M_c/P_c. The condition $c_s = {}^s\xi/\xi$ is equivalent to $\xi c_s = {}^s\xi$, or $c_s\,{}^s({}^s\xi) = {}^s\xi$, in other words, ${}^s\xi \in M_c$. For given cocycle c, we may choose nonzero $\xi \in \mathcal{O}_K$ as ${}^s\xi \in P_c$, say, take $\xi = {}^sp_c(\alpha) = {}^s\alpha + {}^sc\alpha$ for some $\alpha(\neq 0) \in \mathcal{O}_K$.

By Remark 6.3,

$$T(\xi\mathcal{O}_K) = (T(\xi), T(\xi\omega))\mathbf{Z}. \tag{17}$$

Furthermore, we have

$$\mathbf{Z} \cap \xi\mathcal{O}_K = N(\xi)/d\mathbf{Z} \tag{18}$$

where $d = (a, b)$ with $\xi = a + b\omega$. Indeed, for $\alpha = x + y\omega \in \mathcal{O}_K$,

$$\xi\alpha = (ax - byN(\omega)) + (bx + (a + bT(\omega))y)\omega$$

so we have

$$\mathbf{Z} \cap \xi\mathcal{O}_K = \{ax - byN(\omega) \mid x, y \in \mathbf{Z},\ bx + (a + bT(\omega))y = 0\}.$$

First note that

$$\mathbf{Z} \cap \xi\mathcal{O}_K \subset (a, bN(\omega))\mathbf{Z} = \{ax - byN(\omega) \mid x, y \in \mathbf{Z}\} \tag{19}$$

We have $bx + (a + bT(\omega))y = 0$ if and only if $x = \frac{a+bT(\omega)}{d}j$, $y = -\frac{b}{d}j$ for $j \in \mathbf{Z}$ where $d = (a + bT(\omega), b) = (a, b)$. Hence we have

$$ax - byN(\omega) = \frac{j}{d}\left(a\left(a + bT(\omega)\right) + b^2N(\omega)\right) = \frac{N(\xi)}{d}j.$$

Also for $\xi = a + b\omega$, we have $T(\xi) = 2a + bT(\omega)$ and $T(\xi\omega) = T(a\omega + b\omega^2) = T(a\omega + b(\omega T(\omega) - N(\omega)) = -2bN(\omega) + (a + bT(\omega))T(\omega)$.

Assume $m \equiv 2, 3 \pmod 4$. Then $T(\xi) = 2a$ and $T(\xi\omega) = -2bN(\omega) = 2bm$ so $(T(\xi), T(\xi\omega)) = 2(a, bm)$. By (19), $2(a, bm)\mathbf{Z} \subset \mathbf{Z} \cap \xi\mathcal{O}_K \subset (a, bm)\mathbf{Z}$. Note that $|M_c/P_c| = 2$ if and only if $(a, bm) \in \mathbf{Z} \cap \xi\mathcal{O}_K = N(\xi)/d\mathbf{Z}$.

For $c = \varepsilon$, we take $\xi = {}^sp_c(\sqrt{m}) = -\sqrt{m} + {}^s\varepsilon\sqrt{m} = -vm + (u-1)\sqrt{m}$, that is, $a = -vm$ and $b = u - 1$. We have $N(\xi) = v^2m^2 - (u-1)^2m = 2m(u-1)$, and $d = (u - 1, vm)$ We have

$$\begin{aligned}
|M_c/P_c| = 2 &\Leftrightarrow (a, bm) \in \mathbf{Z} \cap \xi\mathcal{O}_K = N(\xi)/d\mathbf{Z} \\
&\Leftrightarrow N(\xi) \mid d(a, bm) \\
&\Leftrightarrow 2m(u-1) \mid (u-1, vm)(-vm, (u-1)m) = m(u-1, vm)(v, u-1) \\
&\Leftrightarrow 2(u-1) \mid ((u-1)(v, u-1), vm(v, u-1)) \\
&\Leftrightarrow 2(u-1) \mid (u-1)(v, u-1) \text{ and } 2(u-1) \mid vm(v, u-1) \\
&\Leftrightarrow 2 \mid (v, u-1) \Leftrightarrow v \text{ is even}
\end{aligned}$$

since $2 \mid v \Leftrightarrow 2 \mid u - 1$, and if v and $u - 1$ are even, $2(u-1) \mid vm(v, u-1)$. Indeed, since $u^2 - 1 = mv^2$, we have

$$\frac{u+1}{2} \cdot \frac{u-1}{2} = m\left(\frac{v}{2}\right)^2.$$

Note that $\frac{u+1}{2}$ and $\frac{u-1}{2}$ are mutually prime, so we have $\frac{u-1}{2} = m_1v_1^2$ and $\frac{u+1}{2} = m_2v_2^2$ where $m = m_1m_2$ with $(m_1, m_2) = 1$, and $v/2 = v_1v_2$ with $(v_1, v_2) = 1$. We have that v_1 is a common divisor of $v/2$ and $(u-1)/2$, so we have $(u-1)/2 \mid m_1v_1(v/2, (u-1)/2)$ hence $2(u-1) \mid mv(v, u-1)$. This gives another proof of Theorem 4.11.

Remark. For $m \equiv 1 \pmod 4$, this method does not give an easy proof of Theorem 4.12.

6.3 Integral matrix over quadratic fields

We can generalize the problem in the other direction. For the same Galois extension K/k, we may take as R the ring $M_{n\times n}(\mathcal{O}_K)$, the ring of $n \times n$ matrices with entries in $\mathcal{O}_K$, as suggested in Ono's lecture [17]. The group of units is now $R^\times = \mathrm{GL}_n(\mathcal{O}_K)$. Let the Galois group $G = \mathrm{Gal}(K/k)$ act on R from the left. For $\gamma = [c] \in H^1(G, \mathrm{GL}_2(\mathcal{O}_K))$, we can associate the module M_c/P_c as before. Some of previous arguments from Chapter 4 are applied for this case: first determine the cohomology set $H^1(G, \mathrm{GL}_n(\mathcal{O}_K))$, then for given cohomology class $\gamma = [c]$, determine the module M_c/P_c. Even for the quadratic field $K = \mathbf{Q}(\sqrt{m})$ over $\mathbf{Q}$ and $n = 2$, the cohomology set $H^1(G, \mathrm{GL}_2(\mathcal{O}_K))$ is not determined completely.

For a Galois extension K/k, with Galois group G, we have the exact sequence of G-groups:

$$1 \longrightarrow \mathrm{SL}_n(\mathcal{O}_K) \longrightarrow \mathrm{GL}_n(\mathcal{O}_K) \xrightarrow{\det} \mathcal{O}_K^\times \longrightarrow 1.$$

This induces the long exact sequence of pointed sets:

$$\begin{aligned} 1 \to \mathrm{SL}_n(\mathcal{O}_k) \to \mathrm{GL}_n(\mathcal{O}_k) \to \mathcal{O}_k^\times \\ \to H^1(G, \mathrm{SL}_n(\mathcal{O}_K)) \to H^1(G, \mathrm{GL}_n(\mathcal{O}_K)) \to H^1(G, \mathcal{O}_K^\times). \end{aligned}$$

For the case $K = \mathbf{Q}(\sqrt{m})$ and $n = 2$, we have some results on determining $H^1(G, \mathrm{SL}_2(\mathcal{O}_K))$ for $G = \mathrm{Gal}(K/\mathbf{Q})$ in Chapter 7. However, the exact sequence does not fully determine $H^1(G, \mathrm{GL}_2(\mathcal{O}_K))$.

As in Section 6.1, applying Hilbert's theorem 90, we can find a nonzero $\xi \in M_{n\times n}(\mathcal{O}_K)$ such that

$$M_c/P_c = (M_{n\times n}(\mathcal{O}_k) \cap \xi M_{n\times n}(\mathcal{O}_K))/T_{K/k}(\xi M_{n\times n}(\mathcal{O}_K)). \tag{20}$$

Indeed, If c is a cocycle in $\mathrm{GL}_n(\mathcal{O}_K)$, then it can be considered as a cocycle in $\mathrm{GL}_n(K)$ since $c : G \to \mathrm{GL}_n(\mathcal{O}_K) \subset \mathrm{GL}_n(K)$. By Hilbert 90, there exists $\xi \in \mathrm{GL}_n(K)$ such that $c_s = \xi^{-1}\,{}^s\xi$. We may assume that $\xi \in M_{n\times n}(\mathcal{O}_k)$ by taking $d\xi$ where $d \in \mathcal{O}_k$ which makes $dx \in \mathcal{O}_k$ for all entries x of ξ, since $(d\xi)^{-1}\,{}^s(d\xi) = \xi^{-1}\,{}^s\xi$. We have

$$\begin{aligned} A \in M_c &\Leftrightarrow c_s\,{}^sA = A \ \text{ for all } s \in G \\ &\Leftrightarrow \xi^{-1}\,{}^s\xi\,{}^sA = A \ \text{ for all } s \in G \\ &\Leftrightarrow {}^s(\xi A) = \xi A \ \text{ for all } s \in G \\ &\Leftrightarrow \xi A \in M_{n\times n}(\mathcal{O}_k) \cap \xi M_{n\times n}(\mathcal{O}_K) \end{aligned}$$

and

$$\begin{aligned}\xi p_c(B) &= \xi \sum_{s\in G} c_s \, {}^sB = \xi \sum_{s\in G} \xi^{-1} \, {}^s\xi \, {}^sB \\ &= \sum_{s\in G} {}^s(\xi B) \\ &= T_{K/k}(\xi B)\end{aligned}$$

Hence $M_c/P_c \approx (M_{n\times n}(\mathcal{O}_k) \cap \xi M_{n\times n}(\mathcal{O}_K))/T_{K/k}(\xi M_{n\times n}(\mathcal{O}_K))$. This would make calculations easier for certain ξ.

7 On Galois Cohomology of $SL_2(\mathcal{O}_K)$ for $K = \mathbf{Q}(\sqrt{m})$

7.1 Cocycles

Let $K = \mathbf{Q}(\sqrt{m})$ be a quadratic number field with Galois group $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle s \rangle$ of order 2. G acts on $\mathcal{O}_K$; ${}^s(a+b\sqrt{m}) = (a-b\sqrt{m})$ and also acts on $SL_2(\mathcal{O}_K)$ entrywise. For $\alpha = a+b\sqrt{m} \in \mathcal{O}_K$, we denote $Ra(\alpha) = a$ the rational part and $Ir(\alpha) = b$ the coefficient of irrational part. $Ra(\alpha)$ and $Ir(\alpha)$ are either integers or half of integers if $m \equiv 1 \pmod 4$. We can write $\mathcal{O}_K = [1, \omega]$ where $\omega = \frac{1}{2}(1+\sqrt{m})$ or $\sqrt{m}$ for $m \equiv 1 \pmod 4$ or $\equiv 2, 3 \pmod 4$, respectively. The set of cocycles is $Z^1(G, \mathrm{SL}_2(\mathcal{O}_K)) = \{A \in \mathrm{SL}_2(\mathcal{O}_K) \mid {}^sA = A^{-1}\}$. Note that $Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$ is not a group. We have

$$Z^1(G, \mathrm{SL}_2(\mathcal{O}_K)) = \left\{ \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \,\middle|\, \alpha \in \mathcal{O}_K,\ b, c \in \mathbf{Z} \text{ and } N(\alpha) - mbc = 1 \right\}. \quad (21)$$

Indeed, let $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$ such that ${}^sA = A^{-1}$ i.e. $\begin{pmatrix} {}^sx & {}^sy \\ {}^sz & {}^sw \end{pmatrix} = \begin{pmatrix} w & -y \\ -z & x \end{pmatrix}$. Then ${}^sx = w$, ${}^sy = -y$, and ${}^sz = -z$ which implies y and z are of form $j\sqrt{m}$ for some integer j. Now, for two elements A and A' in $Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$, $A' \sim A$ is defined as $A' = C^{-1}A\,{}^sC$ for some $C \in SL_2(\mathcal{O}_K)$. $\sim$ is an equivalence relation and we get the cohomology set $H^1(G, \mathrm{SL}_2(\mathcal{O}_K)) = Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))/\sim$. Our aim is to identify $H^1(G, \mathrm{SL}_2(\mathcal{O}_K))$ for $K = \mathbf{Q}(\sqrt{m})$.

7.2 Basic Equivalence Rules

For $A \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$, denote by $[A]$ the class of A in $H^1(G, \mathrm{SL}_2(\mathcal{O}_K))$.

Proposition 7.1. *Let $C \in \mathrm{SL}_2(\mathcal{O}_K)$ and $A \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$ then $C^{-1}A\,{}^sC \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$.*

Proof. ${}^s({}^sC^{-1}A\,{}^sC) = {}^s(C^{-1})\,{}^sA\,{}^{s^2}C = ({}^sC)^{-1}A^{-1}C = (C^{-1}A\,{}^sC)^{-1}$. □

Proposition 7.2 (Power Rule). *For $A \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$, $A \sim A^{-1}$ and $A^2 \sim I$. In general, $A^{2j+1} \sim A$ and $A^{2j} \sim I$ for $j \in \mathbf{Z}$.*

Proof. For integers i and j, $(A^i)^{-1}A^j\,{}^s(A^i) = (A^i)^{-1}A^j({}^sA)^i = A^{-i}A^jA^{-i} = A^{j-2i}$. □

Proposition 7.3 (Transpose Rule). *For $A \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$, $A \sim A^T$, the transpose of A.*

Proof. Let $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathcal{O}_K)$ and $A = \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$.

$$C^{-1}A\,{}^sC = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} {}^s\alpha & -c\sqrt{m} \\ -b\sqrt{m} & \alpha \end{pmatrix} = \left(A^T\right)^{-1}$$

so $A \sim \left(A^T\right)^{-1}$. Combining with Proposition 7.2, we get $A \sim A^T$. □

Take $C = \begin{pmatrix} 1 & 0 \\ {}^sx & 1 \end{pmatrix}$ for any $x \in \mathcal{O}_K$. Then

$$\begin{aligned} C^{-1}A\,{}^sC &= \begin{pmatrix} 1 & 0 \\ -{}^sx & 1 \end{pmatrix} \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha + xb\sqrt{m} & b\sqrt{m} \\ c\sqrt{m} - {}^sx\alpha + x\,{}^s\alpha - x\,{}^sxb\sqrt{m} & {}^s\alpha - {}^sxb\sqrt{m} \end{pmatrix} \\ &= \begin{pmatrix} \alpha + xb\sqrt{m} & b\sqrt{m} \\ (c + 2Ir(x\,{}^s\alpha) - N(x)b)\sqrt{m} & {}^s\alpha - {}^sxb\sqrt{m} \end{pmatrix} \end{aligned}$$

For the cocycles with $b \neq 0$, the (2,1)- and the (2,2)-components are determined uniquely by α and b. So we may consider the (1,1)- and the (1,2)-components only and denote

$$A = \begin{pmatrix} \alpha & b\sqrt{m} \\ \text{—} & \text{—} \end{pmatrix}.$$

We have proved:

Proposition 7.4 (Reduction Rule). *For $\begin{pmatrix} \alpha & b\sqrt{m} \\ \text{—} & \text{—} \end{pmatrix} \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_K))$ with $b \neq 0$, we have*

$$\begin{pmatrix} \alpha & b\sqrt{m} \\ \text{—} & \text{—} \end{pmatrix} \sim \begin{pmatrix} \alpha + xb\sqrt{m} & b\sqrt{m} \\ \text{—} & \text{—} \end{pmatrix}$$

for any $x \in \mathcal{O}_K$.

Remark 7.5. In [26], Vaserstein showed that if K is real quadratic, then the group $\mathrm{SL}_2(\mathcal{O}_K)$ is generated by the matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \qquad \text{for } x, y \in \mathcal{O}_K.$$

This is equivalent to that the group $\mathrm{SL}_2(\mathcal{O}_K)$ is generated by the matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } x \in \mathcal{O}_K,$$

which derive the above three rules. Hence we have that the above rules define every cohomologous relation for the real quadratic field.

Proposition 7.6. *Let* $A = \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_k))$ *and* β *be a unit.*

(a) *If* $N(\beta) = 1$,

$$\begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \sim \begin{pmatrix} \alpha\beta^2 & b\sqrt{m} \\ c\sqrt{m} & {}^s(\alpha\beta^2) \end{pmatrix}.$$

(b) *If* $N(\beta) = -1$,

$$\begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \sim -\begin{pmatrix} \alpha\beta^2 & b\sqrt{m} \\ c\sqrt{m} & {}^s(\alpha\beta^2) \end{pmatrix}.$$

Proof. If $N(\beta) = 1$, take $C = \begin{pmatrix} {}^s\beta & 0 \\ 0 & \beta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$. Then

$$C^{-1} A\, {}^sC = \begin{pmatrix} \beta & 0 \\ 0 & {}^s\beta \end{pmatrix} \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & {}^s\beta \end{pmatrix} = \begin{pmatrix} \alpha\beta^2 & b\sqrt{m} \\ c\sqrt{m} & {}^s(\alpha\beta^2) \end{pmatrix}.$$

If $N(\beta) = -1$, take $C = \begin{pmatrix} {}^s\beta & 0 \\ 0 & -\beta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$. Then

$$C^{-1} A\, {}^sC = \begin{pmatrix} -\beta & 0 \\ 0 & {}^s\beta \end{pmatrix} \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & -{}^s\beta \end{pmatrix} = \begin{pmatrix} -\alpha\beta^2 & -b\sqrt{m} \\ -c\sqrt{m} & -{}^s(\alpha\beta^2) \end{pmatrix}.$$

□

7.3 Unit components

Define $U(\sqrt{m})$ as the subset of $Z^1(G, \mathrm{SL}_2(\mathcal{O}_k))$ containing all elements with (norm 1) unit diagonals (and zero(s) for other component). In this section, we will count cohomology representatives in $U(\sqrt{m})$. Denote by u_m the number of representatives in $U(\sqrt{m})$. By Proposition 7.3, we may assume the the (2,1)-component is zero and

$$U(\sqrt{m}) = \left\{ \begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \middle| \alpha \in \mathcal{O}_K, b \in \mathbf{Z}, N(\alpha) = 1 \right\}.$$

Proposition 7.7. *Let $\alpha \in \mathcal{O}_K$ with norm 1.*

(a) *If $m \equiv 1 \pmod 4$, $\begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \sim \begin{pmatrix} \alpha & 0 \\ 0 & {}^s\alpha \end{pmatrix}$ for all $b \in \mathbf{Z}$ so there is only one class representative for given α.*

(b) *If $m \equiv 2, 3 \pmod 4$, for all $b \in \mathbf{Z}$, $\begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \sim \begin{pmatrix} \alpha & (2j+b)\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$ for any integer j. So there are two possible class representatives, $\begin{pmatrix} \alpha & 0 \\ 0 & {}^s\alpha \end{pmatrix}$ and $\begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$, which are not equivalent. Moreover, the matrix of form $\begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$ is not equivalent to matrices of form $\begin{pmatrix} \beta & 0 \\ 0 & {}^s\beta \end{pmatrix}$ for all β with norm 1.*

Proof. Let $A = \begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$. Denote $\alpha = a_1 + a_2\omega$ where $a_1, a_2 \in \mathbf{Z}$. Since $N(\alpha) = 1$, $(a_1, a_2) = 1$. For any integer j, we have $x_1, x_2 \in \mathbf{Z}$ such that $a_2x_1 - a_1x_2 = j$. Set $x = x_1 + x_2\omega$ and $C = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned} C^{-1}AC &= \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \begin{pmatrix} 1 & {}^sx \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha & \alpha\,{}^sx - {}^s\alpha x + b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \\ &= \begin{pmatrix} \alpha & (2Ir(\alpha\,{}^sx) + b)\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}. \end{aligned}$$

Now,

$$\begin{aligned}\alpha\,{}^s x &= (a_1+a_2\omega)(x_1+x_2\,{}^s\omega)\\ &= a_1x_1+a_2x_1\omega+a_1x_2\,{}^s\omega+a_2x_2N(\omega)\\ &= \begin{cases} a_1x_2+a_2x_2\frac{1-m}{4}+a_1x_2+(a_2x_1-a_1x_2)\omega & \text{if } m\equiv 1 \pmod 4\\ a_1x_1-a_2x_2m+(a_2x_1-a_1x_2)\sqrt{m} & \text{if } m\equiv 2,3 \pmod 4,\end{cases}\end{aligned}$$

so

$$2Ir(\alpha\,{}^s x)=\begin{cases}(a_2x_1-a_1x_2)=j & \text{if } m\equiv 1 \pmod 4\\ 2(a_2x_1-a_1x_2)=2j & \text{if } m\equiv 2,3 \pmod 4.\end{cases}$$

Hence we have

$$C^{-1}AC=\begin{pmatrix}\alpha & (j+b)\sqrt{m}\\ 0 & {}^s\alpha\end{pmatrix}\qquad \text{if } m\equiv 1 \pmod 4$$

and

$$C^{-1}AC=\begin{pmatrix}\alpha & (2j+b)\sqrt{m}\\ 0 & {}^s\alpha\end{pmatrix}\qquad \text{if } m\equiv 2,3 \pmod 4.$$

Now we want to show $\begin{pmatrix}\beta & 0\\ 0 & {}^s\beta\end{pmatrix}\nsim\begin{pmatrix}\alpha & \sqrt{m}\\ 0 & {}^s\alpha\end{pmatrix}$ for $m\equiv 2,3 \pmod 4$. Suppose there is a matrix $C=\begin{pmatrix}x & y\\ z & w\end{pmatrix}\in \mathrm{SL}_2(\mathcal{O}_K)$ such that $C^{-1}\begin{pmatrix}\beta & 0\\ 0 & {}^s\beta\end{pmatrix}{}^sC=\begin{pmatrix}\alpha & \sqrt{m}\\ 0 & {}^s\alpha\end{pmatrix}$. We have

$$C^{-1}\begin{pmatrix}\beta & 0\\ 0 & {}^s\beta\end{pmatrix}{}^sC=\begin{pmatrix}— & \beta\,{}^s yw-{}^s\beta y\,{}^s w\\ — & —\end{pmatrix}=\begin{pmatrix}— & 2Ir(\beta\,{}^s yw)\sqrt{m}\\ — & —\end{pmatrix}.$$

So the (2,1)-component should have an even integer as the coefficient of irrational part. □

Proposition 7.8. *Let* $A=\begin{pmatrix}\alpha & 0\\ 0 & {}^s\alpha\end{pmatrix}$ *for* $N(\alpha)=1$. *Then* $A\nsim -A$ *unless* $m=-1$.

Proof. Suppose $A\,{}^sC=-CA$ for some $C=\begin{pmatrix}x & y\\ z & w\end{pmatrix}\in \mathrm{SL}_2(\mathcal{O}_K)$. We have

$$\begin{pmatrix}\alpha\,{}^s x & \alpha\,{}^s y\\ {}^s\alpha\,{}^s z & {}^s\alpha\,{}^s w\end{pmatrix}=-\begin{pmatrix}\alpha x & {}^s\alpha y\\ \alpha z & {}^s\alpha w\end{pmatrix}.$$

From the (1,1)-component, ${}^s x=-x$, so $x=x'\sqrt{m}$ for some $x'\in\mathbf{Z}$.

From the (2,2)-component, ${}^s w=-w$, so $w=w'\sqrt{m}$ for some $w'\in\mathbf{Z}$.

From the (1,2)-component, we have ${}^s(\alpha\,{}^s y) = -\alpha\,{}^s y$, so set ${}^s\alpha y = y'\sqrt{m}$ for some integer y'. From the (2,1)-component, we have ${}^s(\alpha z) = -\alpha z$, so set $\alpha z = z'\sqrt{m}$ for some integer z'. Now, Since $\alpha\,{}^s\alpha = 1$, we get $1 = \det(C) = xw - yz = xw - {}^s\alpha y\alpha z = (x'w' - y'z')m$, which does not happen unless $m = -1$. □

Proposition 7.9. *For* $m \equiv 2, 3 \pmod 4$, $\begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} \nsim \begin{pmatrix} -\alpha & \sqrt{m} \\ 0 & -{}^s\alpha \end{pmatrix}$ *if* $m \neq -1, \pm 2$.

Proof. Suppose $\begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} {}^sC = C \begin{pmatrix} -\alpha & \sqrt{m} \\ 0 & -{}^s\alpha \end{pmatrix}$ for some $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$. We have

$$\begin{pmatrix} \alpha\,{}^s x + {}^s z\sqrt{m} & \alpha\,{}^s y + {}^s w\sqrt{m} \\ {}^s\alpha\,{}^s z & {}^s\alpha\,{}^s w \end{pmatrix} = \begin{pmatrix} -\alpha x & -{}^s\alpha y + x\sqrt{m} \\ -\alpha z & -{}^s\alpha w + z\sqrt{m} \end{pmatrix}.$$

From the (2,1)-component, we have $\alpha z = z'\sqrt{m}$ for some $z' \in \mathbf{Z}$.
From the (1,1)-component, $\alpha x + \alpha\,{}^s x = -{}^s z\sqrt{m}$. Multiply ${}^s\alpha$ and we get

$$x + {}^s x = 2Ra(x) = -{}^s(\alpha z)\sqrt{m} = z'm.$$

From the (2,2)-component, ${}^s\alpha\,{}^s w + {}^s\alpha w = z\sqrt{m}$. Multiply α and we get

$${}^s w + w = 2Ra(w) = \alpha z\sqrt{m} = z'm.$$

From the (1,2)-component, $\alpha\,{}^s y + {}^s\alpha y = 2Re({}^s\alpha y) = (x - {}^s w)\sqrt{m}$. So we have

$$2Ra({}^s\alpha y) = mIr(x - {}^s w) = m(Ir(x) - Ir(w)).$$

We have $2 = 2\det(C) = 2xw - 2yz = 2xy - 2\,{}^s\alpha y\alpha z$. By looking only at the rational part, we have that

$$2Ra(x)Ra(w) + 2Ir(x)Ir(w)m - 2Ra({}^s\alpha y)Ra(\alpha z) - 2Ir({}^s\alpha y)Ir(\alpha z)m = 2.$$

Reduce this mod m, we have

$$2Ra(x)Ra(w) - 2Ra({}^s\alpha y)Ra(\alpha z) \equiv 2 \pmod m.$$

Since $2Ra(x), 2Ra({}^s\alpha y) \equiv 0 \pmod m$, this is a contradiction unless $2 \equiv 0 \pmod m$, that is, $m \mid 2$. □

Now we can have candidates of representatives as $\begin{pmatrix} \alpha & 0 \\ 0 & {}^s\alpha \end{pmatrix}$ for $m \equiv 1 \pmod 4$, and $\begin{pmatrix} \alpha & 0 \\ 0 & {}^s\alpha \end{pmatrix}, \begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$ for $m \equiv 2, 3 \pmod 4$, where $N(\alpha) = 1$.

Note that $\begin{pmatrix} -\alpha & \sqrt{m} \\ 0 & -{}^s\alpha \end{pmatrix} \sim -\begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$.

Proposition 7.10. *Let $m < 0$, squarefree.*

(a) *If $m \equiv 1 \pmod 4$, then $u_m = 2$ with representatives $\{\pm I\}$.*

(b) *If $m \equiv 2, 3 \pmod 4$, $m \neq -1, -2$, then $u_m = 4$ with representatives* $\left\{ \pm I, \pm \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} \right\}$.

(c) $u_{-1} = 3$ *with* $\left\{ I, \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\}$.

(d) $u_{-2} = 3$ *with* $\left\{ \pm I, \begin{pmatrix} 1 & \sqrt{-2} \\ 0 & 1 \end{pmatrix} \right\}$.

Proof. For $m < -3$, since only units are ± 1, (a) and (b) follows from Propositions 7.7, 7.8, 7.9.

For $m = -2$, $\begin{pmatrix} 1 & \sqrt{-2} \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 + \sqrt{-2}\sqrt{-2} & \sqrt{-2} \\ \text{—} & \text{—} \end{pmatrix} = \begin{pmatrix} -1 & \sqrt{-2} \\ \text{—} & \text{—} \end{pmatrix}$ by the reduction rule.

For $m = -3$, we have units $\pm 1, \pm w, \pm w^2$ where $w = \frac{-1+\sqrt{-3}}{2}$. Note that $w^3 = 1$ and ${}^s w = w^2$. By Proposition 7.6,

$$\pm \begin{pmatrix} \omega & 0 \\ 0 & w^2 \end{pmatrix} \sim \pm \begin{pmatrix} ww^2 & 0 \\ 0 & w^2 w^4 \end{pmatrix} = \pm I$$

and

$$\pm \begin{pmatrix} w^2 & 0 \\ 0 & w \end{pmatrix} \sim \pm \begin{pmatrix} w^2 w^4 & 0 \\ 0 & ww^2 \end{pmatrix} = \pm I.$$

Since $-3 \equiv 1 \pmod 4$, $\{\pm I\}$ are the only nonequivalent representatives.

Now let $m = -1$, ${}^s\alpha = \bar{\alpha}$. Here we have units $\pm 1, \pm i$. For any unit α,

$$\begin{pmatrix} \alpha & bi \\ 0 & \bar{\alpha} \end{pmatrix} \sim \begin{pmatrix} \alpha i^2 & bi \\ 0 & \bar{\alpha}(-i)^2 \end{pmatrix} = \begin{pmatrix} -\alpha & bi \\ 0 & -\bar{\alpha} \end{pmatrix}$$

by Proposition 7.6. So we have four candidates:

$$I, \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} i & i \\ 0 & -i \end{pmatrix}.$$

By Proposition 7.4 using $x = 1 + i$, $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1+(1+i)i & i \\ \text{—} & \text{—} \end{pmatrix} = \begin{pmatrix} i & i \\ \text{—} & \text{—} \end{pmatrix}$. $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \nsim \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ or I by Proposition 7.7. Now we will prove $I \nsim \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Suppose there is $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$ such that

$$\begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{w} \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} xi & -yi \\ zi & -wi \end{pmatrix}.$$

We have $\bar{x} = xi \quad \bar{y} = -yi \quad \bar{z} = zi \quad \bar{w} = -wi$. Write $x = x_1 + x_2 i$, $y = y_1 + y_2 i$, $z = z_1 + z_2 i$, and $w = w_1 + w_2 i$. Then we get $x_1 = -x_2$, $y_1 = y_2$, $z_1 = -z_2$ and $w_1 = w_2$. From the determinant, $1 = Ra(xw - yz) = x_1 w_1 - x_2 w_2 - y_1 z_1 + y_2 z_2 = 2(x_1 w_1 + y_1 z_1)$, which is a contradiction. □

Proposition 7.11. *Let $m > 1$. Denote by ε the fundamental unit in the ring of integers of $\mathbf{Q}(\sqrt{m})$.*

(a) *The case $m \equiv 1 \pmod 4$.*

If $N(\varepsilon) = +1$, then $u_m = 4$ with the representatives $\left\{ \pm I, \pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix} \right\}$.

If $N(\varepsilon) = -1$, then $u_m = 2$ with the representatives $\{\pm I\}$.

(b) *The case $m \equiv 2, 3 \pmod 4$.*

If $N(\varepsilon) = +1$, then $u_m = 8$ with the representatives

$$\left\{ \pm I, \pm \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix}, \pm \begin{pmatrix} \varepsilon & \sqrt{m} \\ 0 & {}^s\varepsilon \end{pmatrix} \right\}.$$

If $N(\varepsilon) = -1$ and $m \neq 2$, then $u_m = 4$ with the representatives $\left\{ \pm I, \pm \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} \right\}$.

If $m = 2$, then $u_2 = 3$ with the representatives $\left\{ \pm I, \begin{pmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{pmatrix} \right\}$.

Proof. First, note that the set of units is $\mathcal{O}_K^\times = \{\pm\varepsilon^j \mid j \in \mathbf{Z}\}$. If $N(\varepsilon) = -1$, units with norm one are $\pm\varepsilon^{2j}$. By Proposition 7.6, we have $\pm \begin{pmatrix} \alpha^{2j} & b\sqrt{m} \\ 0 & {}^s(\alpha^{2j}) \end{pmatrix} \sim \pm \begin{pmatrix} 1 & b\sqrt{m} \\ 0 & 1 \end{pmatrix}$ and $\pm \begin{pmatrix} \alpha^{2j+1} & b\sqrt{m} \\ 0 & {}^s(\alpha^{2j+1}) \end{pmatrix} \sim \pm \begin{pmatrix} \alpha & b\sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$ where $\alpha = \varepsilon$ if $N(\varepsilon) = 1$ and $\alpha = \varepsilon^2$ if $N(\varepsilon) = -1$.

Let $m \equiv 1 \pmod 4$. If $N(\varepsilon) = 1$, we have candidates $\left\{ \pm I, \pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix} \right\}$. If $N(\varepsilon) = -1$, we have candidates $\left\{ \pm I, \pm \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & {}^s(\varepsilon^2) \end{pmatrix} \right\}$, but by Proposition 7.6, $\pm I \sim \mp \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & {}^s(\varepsilon^2) \end{pmatrix}$.

Let $m \equiv 2, 3 \pmod 4$. If $N(\varepsilon) = 1$, we have candidates
$\left\{ \pm I, \pm \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix}, \pm \begin{pmatrix} \varepsilon & \sqrt{m} \\ 0 & {}^s\varepsilon \end{pmatrix} \right\}$.

If $N(\varepsilon) = -1$, we have candidates $\left\{ \pm I, \pm \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & {}^s(\varepsilon^2) \end{pmatrix}, \pm \begin{pmatrix} \varepsilon^2 & \sqrt{m} \\ 0 & {}^s(\varepsilon^2) \end{pmatrix} \right\}$,
but by Proposition 7.6, $\pm \begin{pmatrix} 1 & b\sqrt{m} \\ 0 & 1 \end{pmatrix} \sim \mp \begin{pmatrix} \varepsilon^2 & b\sqrt{m} \\ 0 & {}^s(\varepsilon^2) \end{pmatrix}$.

If $m = 2$, $\varepsilon = 1+\sqrt{2}$ with norm -1. Here, $\begin{pmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1-\sqrt{2}\sqrt{2} & \sqrt{2} \\ \text{—} & \text{—} \end{pmatrix} = \begin{pmatrix} -1 & \sqrt{2} \\ 0 & -1 \end{pmatrix}$.

Now we need to show that if $N(\varepsilon) = 1$,

$$\pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix} \nsim I, \qquad \pm \begin{pmatrix} \varepsilon & \sqrt{m} \\ 0 & {}^s\varepsilon \end{pmatrix} \nsim \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} \text{ (for } m \equiv 2, 3 \pmod 4\text{)}.$$

Let $\alpha = \pm\varepsilon$. Suppose that

$$\begin{pmatrix} {}^sx & {}^sy \\ {}^sz & {}^sw \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & {}^s\alpha \end{pmatrix} = \begin{pmatrix} \alpha x & {}^s\alpha y \\ \alpha z & {}^s\alpha w \end{pmatrix}$$

for some $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$. We get

$$ {}^sx = \alpha x, \quad {}^sy = {}^s\alpha y, \quad {}^sz = \alpha z, \quad {}^sw = {}^s\alpha w. \tag{22}$$

Denote $\alpha = a_1+a_2\sqrt{m}$, $x = x_1+x_2\sqrt{m}$, $y = y_1+y_2\sqrt{m}$, $z = z_1+z_2\sqrt{m}$, and $w = w_1+w_2\sqrt{m}$.

Note that $a_1 \neq \pm 1$. The equations (22) yield four systems of linear equations

$$\begin{pmatrix} a_1 - 1 & ma_2 \\ a_2 & a_1 + 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} a_1 - 1 & ma_2 \\ a_2 & a_1 + 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$\begin{pmatrix} a_1 - 1 & -ma_2 \\ -a_2 & a_1 + 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} a_1 - 1 & -ma_2 \\ -a_2 & a_1 + 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{23}$$

Since the determinants of the coefficient matrices are zero, two equations in each system are equivalent. We get

$$\begin{aligned} (a_1 + 1)x_2 &= -a_2 x_1 & (a_1 + 1)z_2 &= -a_2 z_1 \\ (a_1 + 1)y_2 &= a_2 y_1 & (a_1 + 1)w_2 &= a_2 w_1, \end{aligned} \tag{24}$$

or, equivalently,

$$\begin{aligned} (a_1 - 1)x_1 &= -ma_2 x_2 & (a_1 - 1)z_1 &= -ma_2 z_2 \\ (a_1 - 1)y_1 &= ma_2 y_2 & (a_1 - 1)w_1 &= ma_2 w_2. \end{aligned} \tag{25}$$

We apply these equations to the determinant $xw - yz = 1$. From $Ra(xw - yz) = 1$, we get

$$(x_1 w_1 + m x_2 w_2) - (y_1 z_1 + m y_2 z_2) = 1. \tag{26}$$

Multiply $(a_1 + 1)^2$ to the previous equation, we get by equations (24),

$$((a_1 + 1)^2 - m a_2^2)(x_1 w_1 - y_1 z_1) = (a_1 + 1)^2,$$

or

$$2(x_1 w_1 - y_1 z_1) = a_1 + 1. \tag{27}$$

Putting this back to the equation (26), we get

$$2m(x_2 w_2 - y_2 z_2) = 1 - a_1. \tag{28}$$

If we change variables x_1, y_1, z_1, w_1 in the equation (27) into x_2, y_2, z_2, w_2 using (24) again, we get

$$-2(a_1 + 1)(x_2 w_2 - y_2 z_2) = a_2^2. \tag{29}$$

If $m \equiv 2, 3 \pmod 4$, all terms are integers. a_1 is odd by (27) and a_2 is even by (29). Since $a_1^2 - 1 = m a_2^2$, we get

$$\left(\frac{a_1 - 1}{2}\right)\left(\frac{a_1 + 1}{2}\right) = m\left(\frac{a_2}{2}\right)^2. \tag{30}$$

Since $\left(\frac{a_1-1}{2}, \frac{a_1+1}{2}\right) = 1$ and $m \mid \frac{a_1-1}{2}$ by (28), we have

$$\left|\frac{a_1+1}{2}\right| = b_1^2 \qquad \left|\frac{a_1-1}{2}\right| = mb_2^2$$

where b_1, b_2 are mutually prime positive integers such that $b_1 b_2 = \left|\frac{a_2}{2}\right|$. Then

$$b_1^2 - mb_2^2 = \pm 1,$$

which contradicts the minimality of fundamental unit or non-existance of norm -1 element. Hence, $\pm \begin{pmatrix} \varepsilon & 0 \\ 0 & {}^s\varepsilon \end{pmatrix} \nsim I$.

Now, consider $m \equiv 2, 3 \pmod 4$ and suppose $C^{-1} \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} {}^sC = \begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix}$ for some $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K)$. We have

$$C^{-1} \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} {}^sC = \begin{pmatrix} \text{—} & \text{—} \\ x\,{}^sz - {}^sxz - z\sqrt{m} & \text{—} \end{pmatrix}$$

so $(2Ir(x\,{}^sz) - z)\sqrt{m} = 0$ and

$$z = 2Ir(x\,{}^sz). \tag{31}$$

This means $z \in \mathbf{Z}$ and so $2zIr(x) = z$. If $z \neq 0$, we have $Ir(x) = 1/2$, which is impossible. So $z = 0$. Then x is a unit since $\det C = xw = 1$, and we denote $x = \pm {}^s\alpha$. Note that $N(x) = 1$ and ${}^sx = 1/x = \pm\alpha^{-j}$. Since $\begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \begin{pmatrix} \alpha & \sqrt{m} \\ 0 & {}^s\alpha \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} {}^sx & {}^sy \\ 0 & {}^sw \end{pmatrix}$, we get ${}^sx = \alpha x$ from the (1,1)-component. Then $\alpha^{-j} = \alpha^{j+1}$, a contradiction. Hence $\pm \begin{pmatrix} \varepsilon & \sqrt{m} \\ 0 & {}^s\varepsilon \end{pmatrix} \nsim \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix}$. □

Theorem 7.12. *For $|m| \leq 3$, $|H^1(G, \mathrm{SL}_2(\mathcal{O}_K))| = u_m$.*

Proof. Let $A = \begin{pmatrix} \alpha & b\sqrt{m} \\ c\sqrt{m} & {}^s\alpha \end{pmatrix} \in Z^1(G, \mathrm{SL}_2(\mathcal{O}_k))$ which is not in $U(\sqrt{m})$, i.e. $N(\alpha) \neq 1$. We may assume $b > 0, b \leq |c|$ by taking one of A^{-1}, A^T, and $(A^T)^{-1}$. By the reduction rule, $A \sim A' = \begin{pmatrix} \alpha' & b\sqrt{m} \\ c'\sqrt{m} & {}^s\alpha' \end{pmatrix}$ where $\alpha' = a_1 + a_2\sqrt{m}$ such that

$$|a_1| \leq \frac{|m|b}{2}, \qquad |a_2| \leq \frac{b}{2}. \tag{32}$$

Also we have

$$c' = \frac{N(\alpha) - 1}{mb} = \frac{a_1^2 - 1}{mb} - \frac{a_2^2}{b}. \tag{33}$$

If we get $|c'| < b$, by applying three rules repeatedly, A is equivalent to an element of $U(\sqrt{m})$.

Case 1: $m < 0$. Suppose $A' \notin U(\sqrt{m})$. We have $N(\alpha') = 0$ only when $m = -1$ with elements $\pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, which is equivalent to $\begin{pmatrix} i & i \\ 0 & -i \end{pmatrix}$ by the reduction rule. So we may assume $N(\alpha') \geq 2$. Since $N(\alpha') - mbc' = 1$ and $mb < 0$, we have $c' < 0$. Then by (32),

$$\begin{aligned} |c'| = -c' &= -\frac{a_1^2}{mb} + \frac{1}{mb} + \frac{a_2^2}{b} \\ &= \frac{a_1^2}{|m|b} - \frac{1}{|m|b} + \frac{a_2^2}{b} \\ &< \frac{a_1^2}{|m|b} + \frac{a_2^2}{b} \\ &\leq \frac{|m|b}{4} + \frac{b}{4} \\ &= \frac{b}{4}(|m| + 1) \\ &\leq b \end{aligned}$$

since $|m| \leq 3$.

Case 2: $m > 0$. First, suppose $c' > 0$. Then by (32),

$$c' = \frac{a_1^2}{mb} - \frac{1}{mb} - \frac{a_2^2}{b} \leq \frac{mb}{4} - \frac{1}{mb} - \frac{a_2^2}{b} < \frac{mb}{4} < b$$

since $m < 4$.

Now suppose $c' < 0$. Then by (32),

$$|c'| = -\frac{a_1^2}{mb} + \frac{1}{mb} + \frac{a_2^2}{b} < \frac{1}{mb} + \frac{a_2^2}{b} \leq \frac{1}{mb} + \frac{b}{4} < \frac{1}{2} + \frac{b}{4} < b$$

since $m \geq 2$ and $b \geq 1$. □

7.4 Orders of $H^1(G, \mathrm{SL}_2(\mathcal{O}_K))$

We summarize the result of this chapter.

1. $-3 \leq m \leq 3$;

$$|H^1(G, \mathrm{SL}_2(\mathcal{O}_K))| = u_m = \begin{cases} 8 & \text{if } m = 3 \\ 3 & \text{if } m = 2, -1, -2 \\ 4 & \text{if } m = -3 \end{cases}$$

2. $|m| > 3$;

$$|H^1(G, \mathrm{SL}_2(\mathcal{O}_K))| \geq \begin{cases} 2 & \text{if } m < 0, m \equiv 1 \pmod 4 \\ & \text{or } m > 0, m \equiv 1 \pmod 4 \text{ and } N(\varepsilon) = -1 \\ 4 & \text{if } m < 0, m \equiv 2, 3 \pmod 4 \\ & \text{or } m > 0, m \equiv 1 \pmod 4 \text{ and } N(\varepsilon) = +1 \\ & \text{or } m > 0, m \equiv 2, 3 \pmod 4 \text{ and } N(\varepsilon) = -1 \\ 8 & \text{if } m \equiv 2, 3 \pmod 4 \text{ and } N(\varepsilon) = +1 \end{cases}$$

References

[1] A. Fröhlich and M.J. Taylor, Algebraic Number Theory. Cambridge University Press, Cambridge (1991)

[2] R.C. Gunning, Lectures on Modular Forms. Princeton University Press, Princeton, New Jersey (1962)

[3] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York (1990)

[4] N. Jacobson, Basic Algebra II, W.H. Freeman and Company (1989)

[5] S.M. Lee and T. Ono, On a certain invariant for real quadratic fields. Proc. Japan Acad. Ser. A, vol. 79, no. 8, 119-122 (2003)

[6] Q. Lin and T. Ono, On Two Questions of Ono, Proc. Japan Acad., 78, Ser. A (2002) 181-184

[7] D.A. Marcus, Number Fields. Springer-Verlag, New York (1977)

[8] R.A. Mollin, A Continued Fraction Approach to the Diophantine Equation $ax^2 - by^2 = \pm 1$, preprint

[9] R.A. Mollin, Algebraic Number Theory, Chapman and Hall/CRC Press, Boca Raton, London, New York, Washington D.C. (1999)

[10] R.A. Mollin, Quadratics, CRC Press, Boca Raton, London, New York, Washington D.C. (1996)

[11] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields. Springer-Verlag, Berlin, Heidelberg, New York, (2000)

[12] J. Neukirch, Algebraic Number Theory. Springer-Verlag, Berlin, Heidelberg, New York, (1999)

[13] M. Newman, Integral Matrices. Academic Press, New York, London (1972)

[14] A. Ogg, Survey of modular functions of one variable, Notes by F. van Oystaeyen, Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 1-35. Lecture Notes in Math. Vol. 320, Springer, Berlin, 1973.

[15] T. Ono, A Note on Poincaré sums for finite groups. Proc. Japan Acad. Ser. A, vol. 79, no. 4, 95-97 (2003)

[16] T. Ono, On Poincaré sums for local fields. Proc. Japan Acad. Ser. A, vol. 79, no. 7, 115-118 (2003)

[17] T. Ono, Lecture Notes on Topics in Number Theory, Fall 2003 (Not published)

[18] T. Ono, An Introduction to Algebraic Number Theory. Plenum Press, New York (1990)

[19] A.J. van der Poorten, Fractions of the Period of the Continued Fraction Expension of Quadratic Integers, Bull. Austral. Math. Soc. Vol. 44 (1991) 155-169

[20] J.P. Serre, Galois Cohomology. Springer-Verlag, Berlin Heidelberg New York (1997)

[21] J.P. Serre, Local Fields. Springer-Verlag, New York (1979)

[22] Stark, H. M.: An Introduction to Number Theory. The MIT Press, Cambridge, Massachusetts, and London, England (1978).

[23] Nguyen-Quang-Do Thong, Unités de norme (-1) d'um corps quadratique réel. Séminaire Delange-Pisot-Poitou (Groupe d'étude de théorie des nombres) 17e année, 1975/76, n^0 G6, 3 p.

[24] I.R. Shafarevich, Basic Algebraic Geometry, Springer-Verlag, Berlin, New York (1974)

[25] H.F. Trotter, On the Norms of Units in Quadratic Fields. Proc. AMS, v.22,1. 198-201 (1969)

[26] L.N. Vaserstein, On the Group of SL_2 over Dedekind rings of arithmetic type, Math. USSR Sbornik Vol. 18, No. 2, 321-332 (1972)

VITA

SEOK-MIN LEE

Seok-Min Lee was born in April, 1969 in Seoul, Korea. He received his Bachelor of Science degree in Mathematics Education from Korea University in Seoul, Korea in 1992, and Master of Science degree in Mathematics from Korea University in 1994.

He served the Republic of Korea Air Force as a full-time lecturer in the Korea Air Force Academy for 3 years since 1994.

He enrolled in the graduate program at the Johns Hopkins University in 1998. His dissertation was completed under the direction of Professor Takashi Ono.