On Certain Cohomological Invariants of Algebraic Number Fields

by

Eun Kyoung Lee

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

Baltimore, Maryland
May, 2005.

ABSTRACT

We see the Poincaré series from a cohomological point of view and apply the idea to a finite group G acting on any commutative ring R with unity. For a 1-cocycle c of G on the unit group $R^{\times}$, we define a $|G|$-torsion module M_c/P_c, which is independent of the choice of representatives of the cohomology class $\gamma = [c]$. We are mostly interested in determining M_c/P_c where G is the Galois group of a finite Galois extension K/k of algebraic number fields and R is the ring $\mathcal{O}_K$ of integers in K. We determine M_c/P_c and the index $i_\gamma(K/k) = [M_c : P_c]$ in terms of the ramification index and the different $\mathfrak{D}_{K/k}$. We will determine them explicitly for the case of quadratic, biquadratic, cyclotomic extensions, and the maximal real subfields of cyclotomic extensions over $\mathbf{Q}$.

Advisor: Dr. Takashi Ono

Readers: Dr. Takashi Ono, Dr. Jack Morava

ACKNOWLEDGEMENT

I would like to thank my advisor, Professor Takashi Ono, for all of his help over the past few years. None of this work would have been possible without his vision, guidance and patience during my study. I would also like to thank the faculty at Johns Hopkins University and Ewha Womans University. I owe special thanks to Professor Jack Morava and Professor Steve Zucker for their helpful advice and support, and Professor Hei-sook Lee and Professor Sun-sook Noh for their constant encouragement.

Finally, I would especially like to thank my family for their love, support, and encouragement. I am very grateful to my family-in-law for their love and prayer. Most importantly, of course, I would like to thank James for his love, encouragement and patience.

Contents

1 Introduction

Let R be a commutative ring with unit 1_R, G a finite group acting on R, and $R^\times$ the group of units of R. To each cocycle $c \in Z^1(G, R^\times)$, we set

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

and

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

Then M_c, P_c are $\mathbf{Z}$ modules in R. As we will see in Chapter 3, we have $P_c \subset M_c$, and that M_c/P_c depends only on the cohomology class $[c] \in H^1(G, R^\times)$. In other words, if $c \sim c'$, then $M_c/P_c = M_{c'}/P_{c'}$. If, in particular, $c \sim 1$, then we have $M_c/P_c = R^G/N_G(R) = \widehat{H}^0(G, R)$, where R means only its additive group R^+ structure. Moreover, for any $\gamma = [c] \in H^1(G, R^\times)$, we can think of M_c/P_c as the *twisted cohomology* $\widehat{H}^0(G, R)_\gamma$.

We are interested in studying the module $M_c/P_c = \widehat{H}^0(G, R)_\gamma$, mostly in the case where G is the Galois group of a finite Galois field extension K/k of number fields and R is the ring of integers $\mathcal{O}_K$.

This study originated from Poincaré series about automorphic functions. One remarkable result given by Poincaré about modular forms is that the space of cusp forms is generated by Poincaré series. As is in Section 2.2, we can see this in the cohomological view: Let R be the ring of holomorphic functions on the upper half plane and G be a modular group. The action of G on the ring R and on the group $R^\times$ of units allows us to consider the space M_c of modular forms belonging to a cocycle c of the G-group $R^\times$. Poincaré constructed the subspace P_c of Poincaré series and showed that $M_c = P_c$ for many cases. From the result of Poincaré, it is natural to hope that $\widehat{H}^0(G, R)_\gamma = M_c/P_c = 0$, in general. However, this is not true in the case where $G = \mathrm{Gal}(K/k)$ for number fields K/k and $R = \mathcal{O}_K$. So we find it meaningful to determine the index $i_\gamma(K/k) = [M_c : P_c]$ for each cohomology class $\gamma = [c] \in H^1(G, \mathcal{O}_K^\times)$, and to examine under what condition we have that $M_c/P_c = 0$.

For $\gamma = 1$, we have $i_1(K/k) = [\mathcal{O}_k : Tr_{K/k}\mathcal{O}_K]$. For $\gamma \neq 1$, we view c as a cocycle in $Z^1(G, K^\times)$. Then, by Hilbert theorem 90, $c(s) = \xi^{-1}\, {}^s\xi$, $s \in G$, where ξ may be chosen from $\mathcal{O}_K$.

In Chapter 4, we consider the local fields and the global fields separately. First, in Section 4.1, local fields case, we obtain, using this ξ, that $H^1(G, \mathcal{O}_K^\times)$ is a cyclic group of order $e = e(K/k)$ generated by the *canonical class* $\gamma_{K/k}$. We also obtain the formula of the index $i_\gamma(K/k)$ with respect to the ramification index and the different $\mathfrak{D} = \mathfrak{D}_{K/k}$. From this formula, we achieve one important result that $i_\gamma(K/k) = 1$ if K/k is unramified or tamely ramified. Now that we have determination of the indices for the local fields case, it is natural to think of the localization to treat the global fields case. In Section 4.3, we consider the global fields. We use ambiguous ideals, i.e., ideals in $\mathcal{O}_K$ stable under the action of G, and localization to obtain the product relation

$$i_\gamma(K/k) = \prod_{\mathfrak{p}} i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/k_{\mathfrak{p}}),$$

where for each $\mathfrak{p}$ we choose one $\mathfrak{P}$ lying over $\mathfrak{p}$. Thus the problem of indices for global fields is entirely reduced to local computations.

In Chapter 5, as applications, we present indices for quadratic extensions and biquadratic extensions explicitly. In this case, we find that 2 is the only wildly ramified prime in $\mathbf{Q}$. Denote by $\mathfrak{P}$ the prime ideal in $\mathcal{O}_K$ lying over 2. For each cohomology class $\gamma \in H^1(G, \mathcal{O}_K^\times)$, we can consider, by localization, the induced cohomology class $\gamma_{\mathfrak{P}} \in H^1(G_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$. Since $H^1(G_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$ is cyclic, $\gamma_{\mathfrak{P}} = (\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2})^{m_2}$ for some integer m_2, where $\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2}$ is the canonical class. By examining the different $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2}$, we obtain

Theorem 5.1. Let $K = \mathbf{Q}(\sqrt{m})$ where m is a square-free integer and $G = \mathrm{Gal}(K/\mathbf{Q})$ the Galois group.

(a) If $m \equiv 1 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

(b) If $m \equiv 2 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 2$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

(c) If $m \equiv 3 \pmod 4$, then

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \text{if } m_2 \text{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \text{if } m_2 \text{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

Theorem 5.3. Let $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where m and n are two distinct square-free integers and $G = \mathrm{Gal}(K/\mathbf{Q})$ the Galois group. Put $k = \frac{mn}{\gcd(m,n)^2}$.

(a) If $m \equiv n \equiv k \equiv 1 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

(b) If $m \equiv 1 \pmod 4$ and $n \equiv k \equiv 2 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 2$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

(c) If $m \equiv 1 \pmod 4$ and $n \equiv k \equiv 3 \pmod 4$, then

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \text{if } m_2 \text{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \text{if } m_2 \text{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

(d) If $m \equiv 3 \pmod 4$ and $n \equiv k \equiv 2 \pmod 4$, then

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 2 & \text{if } m_2 \equiv 1 \pmod 4 \\ 4 & \text{if } m_2 \not\equiv 1 \pmod 4. \end{cases}$$

We note that the result for the quadratic extensions agrees with the one in [5]. We also present indices for l^nth cyclotomic extensions and its maximal real subfields.

Theorem 5.4. Let l be a prime, n a natural number, and $K = \mathbf{Q}(\zeta)$, the l^nth cyclotomic field over $\mathbf{Q}$, where ζ is a primitive l^nth root of unity.

(a) If $n = 1$, then we have $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

(b) If $n \geq 2$, we have

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} l^{n-2} & \text{if } m_l \equiv a, \text{ where } 1 \leq a < l^{n-1} \\ l^{n-1} & \text{if } m_l \equiv b, \text{ where } l^{n-1} \leq b < \varphi(l^n) \text{ or } b = 0, \end{cases}$$

where m_l is given by $\gamma_{\mathfrak{P}} = (\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l})^{m_l}$ for the canonical class $\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l} \in H^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$ and a prime $\mathfrak{P}$ of K lying over l.

Theorem 5.6. Let l be an odd prime, n a natural number, ζ a primitive l^nth root of unity, and $K^+ = \mathbf{Q}(\zeta + \zeta^{-1})$. Then

(a) If $n = 1$, then we have $i_\gamma(K^+/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_{K^+}^\times)$.

(b) If $n \geq 2$, we have

$$i_\gamma(K^+/\mathbf{Q}) = \begin{cases} l^{n-2} & \text{if } m_l \equiv a, \text{ where } 1 \leq a < \frac{l^{n-1}+1}{2} \\ l^{n-1} & \text{if } m_l \equiv b, \text{ where } \frac{l^{n-1}+1}{2} \leq b < \frac{\varphi(l^n)}{2} \text{ or } b = 0, \end{cases}$$

where m_l is given by $\gamma_{\mathfrak{P}} = (\gamma_{K_{\mathfrak{P}}^+/\mathbf{Q}_l})^{m_l}$ for the canonical class $\gamma_{K^+/\mathbf{Q}_l} \in H^1(G, \mathcal{O}_{K_{\mathfrak{P}}^+}^\times)$ and a prime $\mathfrak{P}$ of K^+ lying over l.

2 Preliminaries

2.1 Cohomology

We refer to [1], [9], [14], and [15] for the definitions and properties throughout this section.

Let G be a finite group and A a G-module. We let G act on A to the left: $a \mapsto {}^{s}a$, where $s \in G,\ a \in A$. We have ${}^{1_G}a = a,\ {}^{st}a = {}^{s}({}^{t}a)$, and ${}^{s}(a+b) = {}^{s}a + {}^{s}b$, for $a, b \in A,\ s, t \in G$. Let $A^G = \{a \in A : {}^{s}a = a,\ \forall s \in G\}$. For integers $q \geq 0$, we set

$$C^q(G, A) = \{\text{functions } c : G^q \longrightarrow A\},$$

the set of *q-cochains of G with coefficients in A*, where $G^q = G \times \cdots \times G$. By convention, put $C^0 = A$. If G has a topological structure, cochains are defined to be continuous functions from G^q to A. We define the *coboundary map*

$$d_q : C^q(G, A) \longrightarrow C^{q+1}(G, A)$$

by

$$\begin{aligned}(d_q c)(s_1, \cdots, s_{q+1}) =& {}^{s_1}c(s_2, \cdots, s_{q+1}) \\ &+ \sum_{j=1}^{q}(-1)^j c(s_1, \cdots, s_j s_{j+1}, \cdots, s_{q+1}) + (-1)^{q+1} c(s_1, \cdots, s_q).\end{aligned}$$

We have $d_q \circ d_{q-1} = 0$, and so $\operatorname{Im} d_{q-1} \subset \operatorname{Ker} d_q$. Denote by $Z^q(G, A) = \operatorname{Ker} d_q$ the group of *q-cocycles*, and $B^q(G, A) = \operatorname{Im} d_{q-1}$ the group of *q-coboundaries*. We define the *q-dimensional cohomology group of G with coefficients in A* by the factor group

$$H^q(G, A) = Z^q(G, A)/B^q(G, A).$$

Remark. (1) $H^0(G, A) = A^G$.

(2) $H^1(G, A)$ is the group of equivalent classes of crossed-homomorphisms of G into A. The 1-cocycles are the (continuous) functions $c : G \to A$ such that

$$c(st) = c(s) + {}^{s}c(t),$$

and the 1-coboundaries are the (continuous) functions c such that

$$c(s) = {}^{s}b - b, \quad \text{for some } b \in A.$$

Proposition 2.1. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then we have a long exact sequence of cohomology groups*

$$\begin{aligned} 0 \longrightarrow H^0(G,A) \longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \\ \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \xrightarrow{\delta_1} H^2(G,A) \longrightarrow H^2(G,B) \longrightarrow \cdots . \end{aligned}$$

Let K/k be a finite Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. G acts on K as a group of automorphisms of the field K. Moreover, this group acts on the group $K^\times$ of nonzero elements of K, on the group $\mathcal{O}_K^\times$ of units of K, and so on. Let us restrict our interest on the case of cyclic groups $G = \langle s \rangle$ of order n for the moment. For a G-module A, we define two endomorphisms Δ and N of A such that

$$\Delta = 1 - s, \qquad N = \sum_{i=0}^{n-1} s^i.$$

From the relation $\Delta N = N\Delta = 0$, we find that $\mathrm{Im}\, N \subset \mathrm{Ker}\, \Delta$, and $\mathrm{Im}\, \Delta \subset \mathrm{Ker}\, N$. We define Tate cohomology groups of A by

$$\widehat{H}^0(A) = \mathrm{Ker}\, \Delta / \mathrm{Im}\, N, \qquad H^1(A) = \mathrm{Ker}\, N / \mathrm{Im}\, \Delta.$$

Proposition 2.2. *Let G be a finite cyclic group. For an exact sequence*

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

of G-modules A, B, and C, there exist homomorphisms δ_0 and δ_1 so that the following hexagonal sequence is exact:

$$\begin{tikzcd}
& \widehat{H}^0(A) \arrow[r, "f_0"] & \widehat{H}^0(B) \arrow[dr, "g_0"] & \\
H^1(C) \arrow[ur, "\delta_1"'] & & & \widehat{H}^0(C) \arrow[dl, "\delta_0"] \\
& H^1(B) \arrow[ul, "g_1"] & H^1(A) \arrow[l, "f_1"] &
\end{tikzcd}$$

We now introduce a non-abelian cohomology. Let G be a group and A a G-group on which G acts on the left. Note that we now allow A to be nonabelian unlike the previous setting. We write A multiplicatively. Define 0-dimensional cohomology group again as a subgroup of A

$$H^0(G, A) := A^G = \{a \in A : {}^s a = a, \ \forall s \in G\},$$

and define the set of 1-*cocycles*

$$Z^1(G, A) = \{c : G \to A \ : \ c_{st} = c_s {}^s c_t\}, \text{ where } c_s = c(s).$$

We call two cocycles c and c' are equivalent or cohomologous, denoted by $c \sim c'$, if there exists $u \in A$ such that

$$c'_s = u^{-1} c_s {}^s u,$$

for all $s \in G$. Indeed, this defines an equivalence relation for the set of cocycles. We define the *cohomology set of* G *with values in* A by the quotient set

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

We shall denote by $[c]$ the cohomology class containing a cocycle c. The trivial class or the origin $[1]$ consists of cocycles c such that $c_s = a^{-1}\, {}^s a$ for some $a \in A$. Note that $H^1(G, A)$ does not have a natural group structure if A is nonabelian. If A is abelian, this definition of cohomology set $H^1(G, A)$ coincides with the definition of the first cohomology group.

Proposition 2.3. *Given a short exact sequence of G-groups $1 \to A \to B \to C \to 1$, we have an exact sequence*

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

Theorem 2.4. (Hilbert's Theorem 90) *Let K/k be a Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. Then*

(1) $H^1(G, K^\times) = 1.$

(2) $H^1(G, GL_n(K)) = 1$ *for all* $n \in \mathbf{N}$.

Let G be a group and A be a G-group. Using a cocycle $c \in Z^1(G, A)$, we introduce a new G-module $(G, A)_c$ on which G acts by

$$^{s'}a = c_s \, ^{s}a, \quad s \in G.$$

We call that $(G, A)_c$ is obtained by twisting A using the cocycle c. If $c \sim c'$, we have a G-module isomorphism $(G, A)_c \approx (G, A)_{c'}$.

Proposition 2.5. *Let c be a cocycle in $Z^1(G, A)$ and put $A' = (G, A)_c$. To each cocycle $c' \in Z^1(G, A')$ let us associate $c'c$; this gives a cocycle in $Z^1(G, A)$, whence a bijection*

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

By taking quotients, t_c defines a bijection

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

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

2.2 Poincré Series

We refer to [3] for the definitions and properties throughout this section.

Let $\mathfrak{H} = \{z \in \mathbf{C} | \operatorname{Im} z > 0\}$, the upper half plane. The only conformal automorphisms of $\mathfrak{H}$ are the linear fractional transformations:

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

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix of real coefficients having determinant one, i.e., 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 $\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}) / \pm \mathrm{I}$. 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 2.6. An *unrestricted modular form of weight* $2k$ *for* G is a meromorphic function $f(z)$ on $\mathfrak{H}$ such that $f(\frac{az+b}{cz+d}) = (cz+d)^{2k}f(z)$ for all transformation $T : z \mapsto \frac{az+b}{cz+d}$ belonging to G, where k is an integer.

Denote $J_T(a) = \frac{dT}{dz} = (cz+d)^{-2}$ so that we can write the above equation as $f(T(z)) = J_T(z)^{-k}f(z)$. The local coordinate at ∞ is $\zeta = e^{2\pi iz/q}$ 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 $f(z)$

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

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 2.7. A *modular form* is an unrestricted modular form which is holomorphic at all points of $\mathfrak{H}$ and at all cusps of the group.

Definition 2.8. A *cusp form of weight* $2k$ *for* G is a modular form of weight $2k$ for G which vanishes at all cusps.

Definition 2.9. 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 a 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.

Theorem 2.10. *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. Furthermore,

(*a*) *$\phi_0(z)$ is zero at all finite cusps, and nonzero at ∞.*

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

Theorem 2.11. *Every cusp form is a linear combination of the Poincaré series $\phi_\nu(z)$, $\nu \geq 1$.*

Now let us turn to the coholomogical 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 $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in G$. The action is defined by

$$(s, f(z)) \mapsto {}^s f(z) := f\left(\frac{az+b}{cz+d}\right).$$

By defining $\mathcal{C} : G \to R^\times$ by $\mathcal{C}_s(z) = (cz+d)^{-2k}$ for $z \in \mathfrak{H}$, we find that $\mathcal{C}$ satisfies the definition of 1-cocycle of G with values in $R^\times$, that is, $\mathcal{C}_{st}(z) = \mathcal{C}_s(z)\, {}^s\mathcal{C}_t(z)$.

We denote by $M_\mathcal{C}$ the space of cusp forms of weight $2k$, that is,

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

Here, the formula $(cz+d)^{-2k} f(\frac{az+b}{cz+d}) = f(z)$ can be interpreted in terms of cocycle:

$$\mathcal{C}_s\, {}^s f(z) = f(z).$$

Denote by $P_\mathcal{C}$ the space generated by Poincaré series

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

where $g(z) = e^{2\pi i \nu z/q}$, $\nu \geq 1$. Then, by Theorem 2.11, we obtain $M_\mathcal{C} = P_\mathcal{C}$, that is, $M_\mathcal{C}/P_\mathcal{C} = 0$.

3 Definition of M_c/P_c and Its Structure

3.1 Definition of M_c/P_c

As noted in [10], we apply the idea of Poincaré in automorphic functions to an arbitrary ring R acted by a finite group G, where G acts to the left: $a \mapsto {}^s a$, for $s \in G$, $a \in R$. Since G naturally acts on the group $R^\times$ of units, we can define the first cohomology set $H^1(G, R^\times)$ by $Z^1(G, R^\times)/\sim$, where $Z^1(G, R^\times) = \{c : G \longrightarrow R^\times \mid c_{st} = c_s\, {}^s c_t,\ s, t \in G\}$ is the set of cocycles, and $c \sim c'$ if there exists $u \in R^\times$ such that $c'_s = u^{-1} c_s\, {}^s u$, for all $s \in G$.

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

$$M_c = \{a \in R \mid c_s\, {}^s a = a,\ s \in G\},$$
$$P_c = \left\{ p_c(a) \mid p_c(a) = \sum_{t \in G} c_t\, {}^t a,\ a \in R \right\}.$$

We first note that M_c and P_c are $\mathbf{Z}$-modules in the ring R. From the definition of cocycles, we find that

$$|G| M_c \subset P_c \subset M_c.$$

Indeed, the first inclusion is from $p_c(a) = |G|a$, for $a \in M_c$, and the second inclusion is from the equality:

$$c_s\, {}^s p_c(a) = c_s\, {}^s\!\left(\sum_{t \in G} c_t\, {}^t a \right) = \sum_{t \in G} c_s\, {}^s c_t\, {}^{st} a = \sum_{t \in G} c_{st}\, {}^{st} a = \sum_{t \in G} c_t\, {}^t a = p_c(a).$$

Hence, in particular, if $|G| 1_R$ is invertible in R, then we have $M_c/P_c = 0$ for any cocycle $c \in Z^1(G, R^\times)$.

We shall prove that the quotient module M_c/P_c depends only on the cohomology class $[c] \in H^1(G, R^\times)$. Let $c \sim c'$, i.e., $c'_s = u^{-1} c_s\, {}^s u$ for some $u \in R^\times$. Then we have

$$u M_{c'} = M_c \ \text{ and } \ u P_{c'} = P_c,$$

because

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

and also because

$$p_c(a) = \sum_{t \in G} c_t\,{}^t a = \sum_{t \in G} u c'_t ({}^t u)^{-1}\,{}^t a = u \sum c'_t\,{}^t(u^{-1}a) = u p_{c'}(u^{-1}a).$$

Consequently, we get

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

In particular, if $c \sim 1$, we have

$$M_c/P_c = M_1/P_1 = R^G/N_G R = \widehat{H}^0(G,R). \tag{3.1}$$

Moreover, in general, for any cohomology class $\gamma = [c] \in H^1(G, R^\times)$, we can modify this cohomological interpretation for M_c/P_c as seen in the following section.

3.2 Coholomogical Structure of M_c/P_c

For a cocycle $c \in Z^1(G, R^\times)$, we introduce a new G-module $(G,R)_c$ on which G acts by

$${}^{s'}a = c_s\,{}^s a, \ s \in G.$$

Putting $R' = (G,R)_c$, we find that

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

and

$$P_c = \left\{ p_c(a) = \sum_{t \in G} c_t\,{}^t a = \sum_{t \in G} {}^{t'}a \mid a \in R \right\} = N_G R'.$$

Therefore we obtain

$$M_c/P_c = R'^G/N_G R' = \widehat{H}^0(G,R)_c,$$

as a twisted Tate cohomology. Because M_c/P_c depends only on the cohomology class $\gamma = [c] \in H^1(G, R^\times)$, we have

$$M_c/P_c = \widehat{H}^0(G, R)_\gamma. \tag{3.2}$$

3.3 Galois Extensions K/k

By Theorem 2.11 which is the result of Poincaré, it is natural to hope that $\widehat{H}^0(G, R)_\gamma = M_c/P_c = 0$ for any other case. However, this is not true in general. We are mostly interested in the case where G is the Galois group of a Galois field extension K/k of number fields and R is the ring of integers $\mathcal{O}_K$.

3.3.1 M_c/P_c and $i_\gamma(K/k)$

Let k be either a global or local field of characteristic 0, that is, k is either a finite extension of the rational field $\mathbf{Q}$ or the p-adic field $\mathbf{Q}_p$. We denote by $\mathcal{O}_k$ the ring of integers of k. Let K/k be a finite Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. Then G acts on the ring $\mathcal{O}_K$ of integers of K and thus on the group $\mathcal{O}_K^\times$ of units. For a cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$, we set M_c and P_c as in Definition 3.1 with $R = \mathcal{O}_K$. Put $\gamma = [c] \in H^1(G, \mathcal{O}_K^\times)$. We are interested in determining the invariant defined by

$$i_\gamma(K/k) := [M_c : P_c] \tag{3.3}$$

and consider the question under what conditions it becomes trivial.

When we view c as a cocycle in $Z^1(G, K^\times)$, by Hilbert Theorem 90 (Theorem 2.4), we have

$$c_s = \xi^{-1}\, {}^s\xi, \quad \text{for some } \xi \in \mathcal{O}_K \setminus \{0\}.$$

We first find that

$$M_c = \xi^{-1}\mathcal{O}_k \cap \mathcal{O}_K = \xi^{-1}(\mathcal{O}_k \cap \xi\mathcal{O}_K). \tag{3.4}$$

Indeed,

$$\begin{aligned} a \in M_c &\Longleftrightarrow c_s\, {}^s a = a,\ s \in G \\ &\Longleftrightarrow \xi^{-1}\, {}^s\xi\, {}^s a = a \\ &\Longleftrightarrow \xi a = {}^s(\xi a) \\ &\Longleftrightarrow \xi a \in \mathcal{O}_k. \end{aligned}$$

Next, from $p_c(a) = \sum_{t\in G} c_t\, {}^t a = \xi^{-1} \sum_{t \in G} {}^t(\xi a)$ for $a \in \mathcal{O}_K$, we have

$$P_c = \xi^{-1} Tr_{K/k}(\xi \mathcal{O}_K). \tag{3.5}$$

Hence, we obtain, from (3.4) and (3.5), that

$$M_c/P_c = \frac{\mathcal{O}_k \cap \xi \mathcal{O}_K}{Tr_{K/k}(\xi \mathcal{O}_K)}. \tag{3.6}$$

If, in particular, $c \sim 1$, then

$$M_c/P_c = \frac{\mathcal{O}_k}{Tr_{K/k}(\mathcal{O}_K)}. \tag{3.7}$$

Remark 3.2. If we consider M_c and P_c as in Definition 3.1 with $R = K$, then, by Hilbert Theorem 90 (Theorem 2.4), every cocycle c of G in $K^\times$ is cohomologous to 1. Therefore, in view of (3.1), we have $M_c/P_c = K^G/Tr_{K/k}(K) = k/Tr_{K/k}(K) = 0$, because $Tr_{K/k} : K \to k$ is surjective.

3.3.2 Use of Ramification Theory

We shall get a partial result of $M_c/P_c = \widehat{H}^0(G, \mathcal{O}_K)$ for a trivial cocycle c using the ramification theory. Let K/k be a finite Galois extension of number fields with the Galois group $G = \mathrm{Gal}(K/k)$. We call a prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ tamely ramified if $p \nmid e_\mathfrak{p}$, and wildly ramified if $p | e_\mathfrak{p}$, where p denotes the characteristic of $\mathcal{O}_k/\mathfrak{p}$, 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, and wildly ramified if it is not tamely ramified.

We denote by $\mathcal{O}_K^*$ the fractional ideal $\{x \in K \mid Tr_{K/k}(x\mathcal{O}_K) \subset \mathcal{O}_k\}$, and define the *different* by the fractional ideal $(\mathcal{O}_K^*)^{-1}$, denoted by $\mathfrak{D}_{K/k}$. Note that $\mathfrak{D}_{K/k}$ is an integral ideal in $\mathcal{O}_K$.

From now on, we consider a Galois extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ of local fields. Put $G = \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$. We denote by $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$, respectively. We note that $\mathfrak{P}$ and $\mathfrak{p}$ are the only prime ideals in $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{p}}$, respectively. For $i \geq -1$, we put $V_{-1} = G$, and define the ith ramification group of G as

$$V_i = \{s \in G \mid {}^s a \equiv a \mod \mathfrak{P}^{i+1} \text{ for all } a \in \mathcal{O}_{\mathfrak{P}}\}.$$

Then the set $\{V_i\}$ forms a normal series of G such that $V_i = 1$ for $i \gg 1$. In [16], we find a useful formula for $t = v_{\mathfrak{P}}(\mathfrak{D}_{K/k})$ in terms of higher ramification groups:

$$t = (e-1) + \sum_{i=1}^{\infty}(|V_i| - 1). \tag{3.8}$$

In particular, if $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is a totally ramified Galois extension of $\mathfrak{p}$-adic fields, then it is well-known that such an extension can be written as $K_{\mathfrak{P}} = k_{\mathfrak{p}}(\Pi)$ with a prime element Π whose minimal polynomial $f(x) \in \mathcal{O}_k[x]$ is of Eisenstein type. Then we have a useful formula for $t = v_{\mathfrak{P}}(\mathfrak{D}_{K/k})$, which is $t = v_K(f'(\Pi))$. We will use this formula later in Chapter 5.

In [13], it is shown that

Theorem 3.3. *Let $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ be a Galois extension with the Galois group $G = \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$. Then the following conditions are all equivalent:*

(a) *$K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified, i.e., $p \nmid e_{\mathfrak{p}}$.*

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

(c) $t = e - 1$.

(d) $|V_i| = 1$ *for all* $i \geq 1$.

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

Furthermore, if there exists an integral normal basis of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$, then each of these conditions follows.

Hence, in view of (3.1), we obtain

Proposition 3.4. *Let $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ be a tamely ramified extension. Then for every trivial cocycle $c \sim 1$ in $Z^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^{\times})$, we have*

$$M_c/P_c = \widehat{H}^0(G, \mathcal{O}_{K_{\mathfrak{P}}}^{\times}) = 0.$$

In other words, $i_1(K_{\mathfrak{P}}/k_{\mathfrak{p}}) = 1$.

To obtain vanishing conditions of $i_\gamma(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ for a non-trivial cohomology class $\gamma \in H^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^{\times})$, we need a more detailed interpretation of M_c/P_c which we will see in Chapter 4. Then we will make use of the formula (3.8) of the different $\mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$.

Now let K/k be a finite Galois extension of number fields. For every prime $\mathfrak{p}$ in k, we denote by $\mathfrak{P}$ a prime in K lying over $\mathfrak{p}$. In [13], it is also shown that

Theorem 3.5. *Let K/k be a finite Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. Then the following conditions are all equivalent:*

(a) *K/k is tamely ramified, i.e. $p | e_{\mathfrak{p}}$ for every prime $\mathfrak{p}$.*

(b) *$\mathfrak{P}^{e_{\mathfrak{p}}-1} \parallel \mathfrak{D}_{K/k}$ for every prime $\mathfrak{p}$ of k and $\mathfrak{P}$ of K lying over $\mathfrak{p}$.*

(c) *$t_{\mathfrak{p}} = e_{\mathfrak{p}} - 1$ for every prime $\mathfrak{p}$ of k.*

(d) *$|V_{i,\mathfrak{p}}| = 1$ for all $i \geq 1$ and prime $\mathfrak{p}$ of k.*

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

Furthermore, if there exists an integral normal basis of K over k, then each of these conditions follows.

Hence, in view of (3.1), we obtain

Proposition 3.6. *Let K/k be a tamely ramified extension. Then for every cocycle $c \sim 1$ in $Z^1(G, \mathcal{O}_K^{\times})$, we have*

$$M_c/P_c = \widehat{H}^0(G, \mathcal{O}_K^{\times}) = 0.$$

In other words, $i_1(K/k) = 1$.

4 Determination of $i_\gamma(K/k)$

4.1 Local Fields

Let k be a $\mathfrak{p}$-adic number field, $\mathcal{O}_k$ the ring of integers and $\mathcal{O}_k^\times$ the group of units of $\mathcal{O}_k$. Let K/k be a finite Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. For a cohomology class $\gamma = [c] \in H^1(G, \mathcal{O}_K^\times)$, we shall focus on determining M_c/P_c and the index $i_\gamma(K/k)$ throughout this section.

4.1.1 Canonical Class $\gamma_{K/k}$ in Cohomology Group $H^1(G, \mathcal{O}_K^\times)$

In local field extensions, we have a nice group structure of $H^1(G, \mathcal{O}_K^\times)$. Denote by $\mathfrak{P}$ and $\mathfrak{p}$ the unique prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_k$, respectively. Let Π be a fixed prime element in K. Then there exists $c_s \in \mathcal{O}_K^\times$ such that

$$ {}^s\Pi = \Pi c_s, \tag{4.1}$$

for any $s \in G$. From $\Pi c_{st} = {}^{st}\Pi = {}^s({}^t\Pi) = {}^s(\Pi c_t) = {}^s\Pi\, {}^s c_t = \Pi c_s\, {}^s c_t$, we find that the mapping $s \mapsto c_s$ is a 1-cocycle of G in $\mathcal{O}_K^\times$.

If we consider another prime element Π' which brings another cocycle c' of G in $\mathcal{O}_K^\times$ such that ${}^s\Pi' = \Pi' c'_s$, then we find that c' is cohomologous to c. Indeed, by writing $\Pi' = \Pi u$ for some $u \in \mathcal{O}_K^\times$, we have ${}^s\Pi' = {}^s\Pi\, {}^s u$. Because we also have ${}^s\Pi' = \Pi' c'_s = \Pi u c'_s$, we get $c'_s = u^{-1}\Pi^{-1}\, {}^s\Pi\, {}^s u = u^{-1} c_s\, {}^s u$. Therefore a prime element Π can bring the *canonical class* $\gamma_{K/k} = [c]$ in the cohomology group $H^1(G, \mathcal{O}_K^\times)$. In [11], it is shown that

Proposition 4.1. *$H^1(G, \mathcal{O}_K^\times)$ is a cyclic group of order $e = e(K/k)$ generated by the canonical class $\gamma_{K/k}$.*

Proof. Let $\gamma = [c]$ be any class in $H^1(G, \mathcal{O}_K^\times)$. Viewing c as a cocycle of G in $K^\times$, by Hilbert Theorem 90 (Theorem 2.4), there is an element $a \in K^\times$ such that $c_s = a^{-1}\, {}^s a$. We write $a = \Pi^m u$ for some $u \in \mathcal{O}_K^\times$ and $m \in \mathbf{Z}$. Then in view of (4.1), we have ${}^s a = {}^s\Pi^m\, {}^s u = \Pi^m c_s^m\, {}^s u$ so that

$$c_s = a^{-1}\, {}^s a = u^{-1} c_s^m\, {}^s u, \quad \text{i.e., } c \sim c^m.$$

It follows that $\gamma = {\gamma_{K/k}}^m$ which means that $H^1(G, \mathcal{O}_K^\times)$ is a cyclic group generated by the canonical class $\gamma_{K/k}$. To count the order of this cyclic group, we consider the short exact sequence of G-groups

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \xrightarrow{v_K} \mathbf{Z} \longrightarrow 1,$$

where G acts trivially on $\mathbf{Z}$ and v_K is a valuation of K. Then we have

$$1 \longrightarrow \mathcal{O}_k^\times \longrightarrow k^\times \xrightarrow{v_K|_k} \mathbf{Z} \longrightarrow H^1(G, \mathcal{O}_K^\times) \longrightarrow H^1(G, K^\times) = 1.$$

From the relation $v_K(x) = ev_k(x)$ for $x \in k$, where $e = e(K/k)$ is the ramification index for K/k, we have $|H^1(G, \mathcal{O}_K^\times)| = e$. □

4.1.2 $i_\gamma(K/k)$

Let $\gamma = [c]$ be any cohomology class in $H^1(G, \mathcal{O}_K^\times)$. Then, from Proposition 4.1, there exists an integer m such that $\gamma = {\gamma_{K/k}}^m$, where $0 \leq m < e$. It follows, from (3.6) and (3.7), that

$$i_\gamma(K/k) = \begin{cases} (\mathfrak{p} : Tr_{K/k}\mathfrak{P}^m) & \text{for } \gamma \neq 1 \\ (\mathcal{O}_k : Tr_{K/k}\mathcal{O}_K) & \text{for } \gamma = 1. \end{cases}$$

Indeed, if $\gamma \neq 1$, i.e. $m > 0$, then, from (3.6) with $\xi = \Pi^m$, we obtain $i_\gamma(K/k) = (\mathcal{O}_k \cap \mathfrak{P}^m)/Tr_{K/k}(\mathfrak{P}^m)$. We note that $\mathcal{O}_k \cap \mathfrak{P}^m = \mathfrak{p}$ by the condition $0 < m < e$, and that $Tr_{K/k}\mathfrak{P}^m$ is an ideal in $\mathcal{O}_k$. Put $r_\gamma = v_\mathfrak{p}(Tr_{K/k}\mathfrak{P}^m)$, that is,

$$Tr_{K/k}\mathfrak{P}^m = \mathfrak{p}^{r_\gamma},$$

including the case $\gamma = 1$. Then we have

$$i_\gamma(K/k) = \begin{cases} N\mathfrak{p}^{r_\gamma - 1} & \text{for } \gamma \neq 1 \\ N\mathfrak{p}^{r_1} & \text{for } \gamma = 1, \end{cases} \tag{4.2}$$

where $N\mathfrak{p} = (\mathcal{O}_k : \mathfrak{p})$.

From now on, we shall obtain the formula of the number $r = r_\gamma$ with respect to other invariants of K/k such as the ramification index and the different $\mathfrak{D}_{K/k}$. We note that $\mathfrak{p} = \mathfrak{P}^e$. Then, from $Tr_{K/k}\mathfrak{P}^m = \mathfrak{p}^r$, we have

$$\mathcal{O}_k = \mathfrak{p}^{-r}Tr_{K/k}\mathfrak{P}^m = Tr_{K/k}(\mathfrak{p}^{-r}\mathfrak{P}^m) = Tr_{K/k}\mathfrak{P}^{-er+m}. \tag{4.3}$$

Let $\mathfrak{D}_{K/k}$ be the different for K/k, which is an ideal of $\mathcal{O}_K$. We write $\mathfrak{D} = \mathfrak{P}^t$, where $t = v_{\mathfrak{P}}(\mathfrak{D}_{K/k})$. From (4.3), we have $\mathfrak{P}^{-er+m} \subset \mathfrak{D}^{-1}$ which implies that $-er + m \geq -t$, i.e., $r \leq \frac{t+m}{e}$. On the other hand, from $Tr_{K/k}\mathfrak{P}^m \not\subset \mathfrak{p}^{r+1}$, we have $\mathfrak{P}^{-e(r+1)+m} \not\subset \mathfrak{D}^{-1}$, and so $\frac{t+m}{e} < r + 1$. Consequently we get

$$r = \lfloor \frac{t+m}{e} \rfloor,$$

and so, by (4.2), we obtain the formula

$$i_\gamma(K/k) = \begin{cases} N\mathfrak{p}^{\lfloor \frac{t+m}{e} \rfloor - 1} & \text{for } \gamma \neq 1 \\ N\mathfrak{p}^{\lfloor \frac{t}{e} \rfloor} & \text{for } \gamma = 1. \end{cases} \tag{4.4}$$

4.1.3 Vanishing of $i_\gamma(K/k)$

From the above formula (4.4), we may answer the question under what condition we have $i_\gamma(K/k) = 0$. As we have already seen in Section 3.3.2, we have a useful formula for $t = v_{\mathfrak{P}}(\mathfrak{D}_{K/k})$:

$$t = \sum_{i=0}^{\infty}(|V_i| - 1) = (e-1) + \sum_{i=1}^{\infty}(|V_i| - 1),$$

where $e = e(K/k)$ is the ramification index for K/k. From this, we find that $t \geq e - 1$, and by Theorem 3.3, we have $t = e - 1 \iff V = V_1 = 1 \iff p \nmid e \iff$ K/k is tamely ramified, where p denotes the characteristic of $\mathcal{O}_k/\mathfrak{p}$. It follows that if K/k is tamely ramified, then $i_\gamma(K/k) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$. We also find that if K/k is unramified, then $i_\gamma(K/k) = 1$. Note that $\gamma = 1$ always in this case.

Let us now consider a wildly ramified case. If $\gamma = 1$, then $i_1(K/k)$ cannot be 1, because $\lfloor \frac{t}{e} \rfloor = 0$ implies that $t < e$ which is impossible, from $0 < e - 1 < t$. If $\gamma \neq 1$, then we find that $i_\gamma(K/k) = 1$ if and only if $e \leq t + m < 2e$. Consequently, we have

Theorem 4.2. (a) *If K/k is unramified, then $i_1(K/k) = 1$.*

(b) *If K/k is tamely ramified, then $i_\gamma(K/k) = 1$ for every γ.*

(c) *If K/k is wildly ramified, then $i_\gamma(K/k) = 1$ if and only if $\gamma \neq 1$ and $e \leq t+m < 2e$.*

4.2 M_c/P_c for a Particular Cocycle c

Motivated by Hilbert Theorem 90 and the canonical class in local field extensions, we have the following

Theorem 4.3. *Let k be either a local or global fields and K/k be a finite Galois extension with the Galois group $G = \mathrm{Gal}(K/k)$. Let $\mathfrak{p}$ be a prime of k and $\mathfrak{P}$ a prime of K lying above $\mathfrak{p}$, where*

(a) *K/k is totally ramified at $\mathfrak{p}$, i.e., $\mathfrak{p} = \mathfrak{P}^e$ for $e = [K : k]$*

(b) *$\mathfrak{P}$ is principal, i.e., $\mathfrak{P} = (\Pi)$ for some $\Pi \in \mathcal{O}_K$*

(c) *$\mathfrak{D}_{K/k} = \mathfrak{P}^t$.*

Then $c_s = \frac{{}^s\Pi}{\Pi}$ defines the cocycle in $Z^1(G, \mathcal{O}_K^\times)$, and

$$M_c/P_c \approx \mathcal{O}_k/\mathfrak{p}^{\lfloor \frac{t+1}{e} \rfloor - 1}.$$

Proof. By (a), we have ${}^s\mathfrak{P}^e = {}^s\mathfrak{p} = \mathfrak{p} = \mathfrak{P}^e$, and so ${}^s\mathfrak{P} = \mathfrak{P}$ for any $s \in G$. Since $\mathfrak{P}$ is principal, we have $({}^s\Pi) = {}^s(\Pi) = {}^s\mathfrak{P} = \mathfrak{P} = (\Pi)$. Hence we find that $c_s = \frac{{}^s\Pi}{\Pi} \in \mathcal{O}_K^\times$, and $c_{st} = c_s\, {}^sc_t$ which implies that $c \in Z^1(G, \mathcal{O}_K^\times)$. From the formula (3.6), we find

$$M_c/P_c = \frac{\mathcal{O}_k \cap \Pi\mathcal{O}_K}{Tr_{K/k}(\Pi\mathcal{O}_K)} = \frac{\mathcal{O}_k \cap \mathfrak{P}}{Tr_{K/k}(\mathfrak{P})} = \frac{\mathfrak{p}}{Tr_{K/k}(\mathfrak{P})}.$$

By the following equivalences:

$$\begin{aligned} \mathfrak{p}^h \,|\, Tr_{K/k}(\mathfrak{P}) &\iff \mathfrak{p}^h\mathfrak{D}_{K/k}^{-1}|\mathfrak{P} \iff \mathfrak{p}^h \,|\, \mathfrak{P}\mathfrak{D}_{K/k} = \mathfrak{P}^{t+1} \\ &\iff eh \leq t+1 \iff h \leq \left\lfloor \frac{t+1}{e} \right\rfloor, \end{aligned}$$

we find the prime factorization $Tr_{K/k}(\mathfrak{P}) = \mathfrak{p}^{\left\lfloor \frac{t+1}{e_\mathfrak{p}} \right\rfloor}$ which implies that

$$M_c/P_c \approx \mathcal{O}_k/\mathfrak{p}^{\lfloor \frac{t+1}{e} \rfloor - 1}.$$

□

4.3 Global Fields

From now on, we consider a Galois extension of number fields K/k with the Galois group $G = \mathrm{Gal}(K/k)$. Revisiting the formula (3.6), we have

$$M_c/P_c = \frac{\mathcal{O}_k \cap \xi\mathcal{O}_K}{Tr_{K/k}\xi\mathcal{O}_K} = \frac{(\xi\mathcal{O}_K)^G}{Tr_{K/k}\xi\mathcal{O}_K}, \tag{4.5}$$

where $\xi \in \mathcal{O}_K \setminus \{0\}$ such that $c_s = \xi^{-1}\,{}^s\xi$.

4.3.1 Ambiguous Ideals

An ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is called *ambiguous* if ${}^s\mathfrak{a} = \mathfrak{a}$ for every $s \in G$. An ambiguous ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has a prime decomposition

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}, \text{ where } \mathfrak{p}^{\#} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \text{ and } m_{\mathfrak{p}} \in \mathbf{N}. \tag{4.6}$$

Indeed, beginning with a prime decomposition $\mathfrak{a} = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{m_{\mathfrak{P}}}$, we have ${}^s\mathfrak{a} = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}} {}^s\mathfrak{P}^{m_{\mathfrak{P}}}$. For $\mathfrak{a}$ to be an ambiguous ideal, we must have $m_{\mathfrak{P}} = m_{\mathfrak{p}}$ for $\mathfrak{P}|\mathfrak{p}$.

Note that the different $\mathfrak{D}_{K/k}$ is an ambiguous ideal. So, from now on, we denote by

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}}. \tag{4.7}$$

Proposition 4.4. *Let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$ be an ambiguous ideal. Then we have*

(a) $\mathfrak{a}^G = \mathfrak{a} \cap \mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \rceil}$

(b) $Tr_{K/k}\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \rfloor}$*, where $t_{\mathfrak{p}}$ is given by the different $\mathfrak{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}}$.*

Proof. (a) We first write $m_{\mathfrak{p}} = qe_{\mathfrak{p}} + r$, where $q = \lfloor \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \rfloor$ and $0 \le r < e_{\mathfrak{p}}$. Then, since $\mathfrak{p}^{\# qe_{\mathfrak{p}}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{qe_{\mathfrak{p}}} = \mathfrak{p}^q$, we have $\mathfrak{p}^{\# m_{\mathfrak{p}}} = \mathfrak{p}^{\# qe_{\mathfrak{p}}}\mathfrak{p}^{\# r} = \mathfrak{p}^q\mathfrak{p}^{\# r}$. So

$$\mathfrak{a}^G = \mathfrak{a} \cap \mathcal{O}_k = \mathfrak{p}^q(\mathfrak{p}^{\# r} \cap \mathcal{O}_k) = \begin{cases} \mathfrak{p}^q & \text{when } r = 0 \\ \mathfrak{p}^{q+1} & \text{when } r > 0. \end{cases}$$

(b) For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$, and a natural number h, we have the following equivalences:

$$\mathfrak{p}^h \,|\, Tr_{K/k}(\mathfrak{a}) \iff \mathfrak{p}^h \mathfrak{D}_{K/k}^{-1} | \mathfrak{a} \iff \mathfrak{p}^h \,|\, \mathfrak{a}\mathfrak{D}_{K/k} \iff (\mathfrak{p}^{\#})^{e_{\mathfrak{p}} h} \,|\, \mathfrak{a}\mathfrak{D}_{K/k}$$
$$\iff (\mathfrak{p}^{\#})^{e_{\mathfrak{p}} h} \,|\, (\mathfrak{p}^{\#})^{m_{\mathfrak{p}} + t_{\mathfrak{p}}} \iff e_{\mathfrak{p}} h \leq m_{\mathfrak{p}} + t_{\mathfrak{p}} \iff h \leq \left\lfloor \frac{m_{\mathfrak{p}} + t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor .$$

□

From the choice of $\xi \in K^\times$ such that $\xi^{-1}\,{}^s\xi \in \mathcal{O}_K^\times$, we note that $\xi\mathcal{O}_K$ in (4.5) is an ambiguous ideal. Put $\xi\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$. Then, by Proposition 4.4, we obtain the formula

$$i_\gamma(K/k) = [M_c : P_c] = \prod_{\mathfrak{p}} N\mathfrak{p}^{\lfloor \frac{m\mathfrak{p} + t\mathfrak{p}}{e\mathfrak{p}} \rfloor - \lceil \frac{m\mathfrak{p}}{e\mathfrak{p}} \rceil}, \tag{4.8}$$

where $N\mathfrak{p} = [\mathcal{O}_k : \mathfrak{p}]$.

4.3.2 Localization

Let $\mathfrak{p}$ be a prime ideal of k and $\mathfrak{P}$ a prime ideal of K lying over $\mathfrak{p}$. We denote by $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$ the completions of K and k respectively. Then $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is also a Galois extension and its Galois group $G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ can be identified as the decomposition group $G_{\mathfrak{P}}$ at $\mathfrak{P}$ in G. One knows that $\mathcal{O}_K$ is embedded in $\mathcal{O}_{K_{\mathfrak{P}}}$, and so $\mathcal{O}_K^\times$ is embedded in $\mathcal{O}_{K_{\mathfrak{P}}}^\times$. For any cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$, we can consider the following diagram:

$$\begin{tikzcd}
G \arrow[r, "c"] & \mathcal{O}_K^\times \arrow[d, "i_{K_{\mathfrak{P}}}"] \\
G_{\mathfrak{P}} \arrow[u, "i_{G_{\mathfrak{P}}}"'] & \mathcal{O}_{K_{\mathfrak{P}}}^\times
\end{tikzcd}$$

Then c induces a cocycle $c_{\mathfrak{P}} \in Z^1(G_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$ such that $c_{\mathfrak{P}} = i_{K_{\mathfrak{P}}} \circ c \circ i_{G_{\mathfrak{P}}}$. If $\xi \in \mathcal{O}_K \setminus \{0\}$ satisfies $c_s = \xi^{-1}\,{}^s\xi$, then it also satisfies

$$c_{\mathfrak{P},s} = \xi^{-1}\,{}^s\xi. \tag{4.9}$$

Put

$$\mathfrak{a} = \xi\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}, \tag{4.10}$$

and

$$\mathfrak{a}_{\mathfrak{P}} = \xi\mathcal{O}_{K_{\mathfrak{P}}}. \tag{4.11}$$

Then we have $m_{\mathfrak{p}} = \nu_{\mathfrak{P}}(\mathfrak{a}) = \nu_{\mathfrak{P}}(\mathfrak{a}_{\mathfrak{P}})$. Notation being as in (4.7), we have

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#t_{\mathfrak{p}}} = \prod_{\mathfrak{P}} \mathfrak{P}^{t_{\mathfrak{P}}} = \prod_{\mathfrak{P}} \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

Then, locally it follows from (4.8) that

$$[M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}] = N\mathfrak{p}^{\lfloor \frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \rfloor - \lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \rceil}. \tag{4.12}$$

Consequently, we obtain

Theorem 4.5. *Let K/k be a finite Galois extension of number fields with the Galois group $G = \mathrm{Gal}(K/k)$. Then for $\gamma = [c] \in H^1(G, \mathcal{O}_K^\times)$, we have*

$$i_\gamma(K/k) = \prod_{\mathfrak{p}} i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \tag{4.13}$$

where, for each $\mathfrak{p}$, we choose one prime $\mathfrak{P}$ in $\mathcal{O}_K$ lying over $\mathfrak{p}$, and $\gamma_{\mathfrak{P}} = [c_{\mathfrak{P}}] \in H^1(G_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$, for a cocycle $c_{\mathfrak{P}}$ induced from c by localizing at $\mathfrak{P}$.

One knows that there are only finitely many ramified primes $\mathfrak{p}$, and by Theorem 4.2, we have $[M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}] = 1$ for unramified prime $\mathfrak{p}$. Hence our product formula (4.8) and (4.13) are indeed finite products.

5 Application

According to the product formula (4.13) in Theorem 4.5, the determination of $i_\gamma(K/k)$ for global fields is entirely reduced to the local computation of $i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$. Notation being as in the previous Section 4.3.2, let us now concentrate on local field extensions $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. We fix a prime $\Pi \in K_{\mathfrak{P}}$, and consider the canonical class $\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} = [c_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}]$ given by

$$^s\Pi = \Pi\, c_{K_{\mathfrak{P}}/k_{\mathfrak{p}},s}$$

for $s \in G_{\mathfrak{P}}$. Then by Proposition 4.1, there exists a unique integer $m \pmod{e_{\mathfrak{p}}}$ such that $\gamma_{\mathfrak{P}} = {\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}}^m$, where $e_{\mathfrak{p}}$ is the ramification index. Accordingly, we have $c_{\mathfrak{P}} \sim (c_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^m$. Then, in view of (4.9) using Hilbert Theorem 90 (Theorem 2.4), there exists $u \in \mathcal{O}_{K_{\mathfrak{P}}}^\times$ such that

$$\xi^{-1}\, {}^s\xi = c_{\mathfrak{P},s} = u^{-1}(c_{K_{\mathfrak{P}}/k_{\mathfrak{p}},s})^m\, {}^su = u^{-1}\Pi^{-m}\, {}^s\Pi^m\, {}^su,$$

that is, $u\Pi^m = \xi\pi^r v$ where π is a prime element in $k_{\mathfrak{p}}$ and $v \in \mathcal{O}_{k_{\mathfrak{p}}}^\times$. In view of (4.10) and (4.11), we have $m = m_{\mathfrak{p}} + re_{\mathfrak{p}}$. We notice that $m \equiv m_{\mathfrak{p}} \pmod{e_{\mathfrak{p}}}$ so that we have

$$\gamma_{\mathfrak{P}} = {\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}}^{m_{\mathfrak{p}}}. \tag{5.1}$$

We also note that two formulae, (4.4) and (4.12) for $i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ agrees.

5.1 Quadratic Extensions

Let $K = \mathbf{Q}(\sqrt{m})$ where m is a square-free integer and $G = \mathrm{Gal}(K/\mathbf{Q})$. Denote by p a prime of $\mathbf{Q}$ and $\mathfrak{P}$ a prime of K lying over p. Let $\gamma \in H^1(G, \mathcal{O}_K^\times)$. Then by Theorem 4.5, we have $i_\gamma(K/\mathbf{Q}) = \prod_p i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/\mathbf{Q}_p)$ where $\gamma_{\mathfrak{P}} \in H^1(G_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$. Combining Theorem 4.2 and Theorem 4.5, we know that if $K/\mathbf{Q}$ is unramified or tamely ramified extension, then $i_\gamma(K/k) = 1$. Therefore, to determine $i_\gamma(K/\mathbf{Q})$, it is remained to take care of the wildly ramified case. From the condition $p|e_p = 2$, we find that 2 is the only wildly ramified prime in $\mathbf{Q}$. As is well known, the discriminant $D_{K/\mathbf{Q}} = m$ if $m \equiv 1 \pmod 4$, and $D_{K/\mathbf{Q}} = 4m$ if $m \equiv 2$ or $3 \pmod 4$. It follows from $2|D_{K/\mathbf{Q}}$ that we only need to take care of the case $m \equiv 2$ or $3 \pmod 4$. Examining each of these cases, we obtain

Theorem 5.1. *Let $K = \mathbf{Q}(\sqrt{m})$ where m is a square-free integer and $G = \mathrm{Gal}(K/\mathbf{Q})$ the Galois group.*

(a) *If $m \equiv 1 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.*

(b) *If $m \equiv 2 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 2$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.*

(c) *If $m \equiv 3 \pmod 4$, then*

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \textit{if } m_2 \textit{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \textit{if } m_2 \textit{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

Proof. Let $\mathfrak{P}$ be a prime in K dividing 2. One knows that $[K_{\mathfrak{P}} : \mathbf{Q}_2] = 1$ only when $m \equiv 1 \pmod 8$. If $m \equiv 2$ or $3 \pmod 4$, then $[K_{\mathfrak{P}} : \mathbf{Q}_2] = 2$ so that $G_{\mathfrak{P}}$ may be identified as G.

We begin with the case when $m \equiv 2 \pmod 4$. By putting $f(x)$ the minimal polynomial of $\sqrt{m}$ over $\mathbf{Q}_2$, we find that $f(x) = x^2 - m$ is of Eisenstein type. Hence the different $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = (f'(\Pi)) = (2\Pi)$, with a prime element $\Pi = \sqrt{m}$ in $K_{\mathfrak{P}}$. Since m is a square-free integer, we can write $m = 2(1 + 2k)$ for some integer k, and so $\Pi^2 = m = 2$. Note that an odd integer is a unit in $\mathbf{Q}_2$. It follows that $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{P}^3$, that is, $t_2 = 3$, and so, by (4.12), we get $i_1(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{3}{2} \rfloor} = 2$ and $i_{\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2}}(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{3+1}{2} \rfloor - 1} = 2$. Consequently, we have $i_\gamma(K/\mathbf{Q}) = 2$ for any $\gamma \in H^1(G, \mathcal{O}_K^\times)$.

Next, let $m \equiv 3 \pmod 4$. Then $f(x) = x^2 - m$ is not of Eisenstein type. Instead, $g(x) = f(x-1) = x^2 - 2x + (1-m)$ is of Eisenstein type. Hence the different $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = (g'(\Pi)) = (2(\Pi - 1)) = (2\sqrt{m})$, with a prime element $\Pi = \sqrt{m} + 1$ in $K_{\mathfrak{P}}$. Since $\sqrt{m}$ is a unit in $K_{\mathfrak{P}}$, we have $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{P}^2$, that is, $t_2 = 2$. As a result, we obtain

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \text{if } m_2 \text{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \text{if } m_2 \text{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

□

Remark. The result obtained from Theorem 5.1 agrees with the one from [5]. In fact, in case when $m \equiv 3 \pmod 4$, the central element $a_{r/2}$ of the continued fraction $[a_0; \overline{a_1, \cdots, a_r}]$ of $\sqrt{m}$ is odd if and only if $i_\gamma(K/\mathbf{Q}) = 1$. Thus the parity of m_2 is same as the parity of $a_{r/2}$.

5.2 Biquadratic Extensions

Let $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where m and n are distinct square-free integers and $G = \mathrm{Gal}(K/\mathbf{Q})$. Putting $k = \frac{mn}{\gcd(m,n)^2}$, we find that K contains $\mathbf{Q}(\sqrt{k})$. Let us consider the following cases:

(1) $m \equiv n \equiv k \equiv 1 \pmod 4$

(2) $m \equiv 1$ and $n \equiv k \equiv 2$ or $3 \pmod 4$

(3) $m \equiv 3$ and $n \equiv k \equiv 2 \pmod 4$

Then we find that these cover all the cases of biquadratic extensions K over $\mathbf{Q}$ except for rearrangements of m, n and k. Indeed, when $m \equiv n \equiv 3 \pmod 4$, one gets $K = \mathbf{Q}(m', n)$ by putting $m' = k = \frac{mn}{\gcd(m,n)^2}$ so that $m' \equiv 1 \pmod 4$ and $k' = \frac{m'n}{\gcd(m',n)^2} \equiv 3 \pmod 4$. When $m \equiv n \equiv 2$ or $6 \pmod 8$, one gets $K = \mathbf{Q}(m', n)$ by putting $m' = k = \frac{mn}{\gcd(m,n)^2}$ so that $m' \equiv 1 \pmod 4$ and $k' = \frac{m'n}{\gcd(m',n)^2} \equiv 2 \pmod 4$. Finally when $m \equiv 2$ and $n \equiv 6 \pmod 4$, one gets $K = \mathbf{Q}(m', n)$ by putting $m' = k = \frac{mn}{\gcd(m,n)^2}$ so that $m' \equiv 3 \pmod 4$ and $k' = \frac{m'n}{\gcd(m',n)^2} \equiv 2 \pmod 4$.

Before we examine each of these cases for indices $i_\gamma(K/\mathbf{Q})$, we need the following

Proposition 5.2. *Let $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where m and n are two distinct square-free integers. We put $k = \frac{mn}{\gcd(m,n)^2}$.*

(a) *If $m \equiv n \equiv k \equiv 1 \pmod 4$, then*

$$\mathcal{O}_K = \left[1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{n}}{2}\right)\right]_{\mathbf{Z}}$$

and so the discriminant $D_{K/\mathbf{Q}} = mnk$.

(b) *If* $m \equiv 1$, *and* $n \equiv k \equiv 2$ *or* 3 (mod 4), *then*

$$\mathcal{O}_K = \left[1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right]_{\mathbf{Z}}$$

and so we have $D_{K/\mathbf{Q}} = 16mnk$.

(c) *If* $m \equiv 3$, *and* $n \equiv k \equiv 2 \mod 4$, *then*

$$\mathcal{O}_K = \left[1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right]_{\mathbf{Z}}$$

and so we have $D_{K/\mathbf{Q}} = 64mnk$.

Proof. According to [6], we know that $\alpha \in K$ is an algebraic integer if and only if the relative norm $N_{K/\mathbf{Q}[m]}(\alpha)$ and trace $Tr_{K/\mathbf{Q}[m]}(\alpha)$ are algebraic integers.

(a) Let $m \equiv n \equiv k \equiv 1$ (mod 4). We first write $\alpha \in \mathcal{O}_K$ as a linear combination of field bases $1, \sqrt{m}, \sqrt{n}$, and $\sqrt{k}$ with rational coefficients, and consider its relative traces $Tr_{K/\mathbf{Q}[\sqrt{m}]}(\alpha)$, $Tr_{K/\mathbf{Q}[\sqrt{n}]}(\alpha)$, and $Tr_{K/\mathbf{Q}[\sqrt{k}]}(\alpha)$ to find that every algebraic integer is of the form $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{4}$, where a, b, c, and d are integers. Then by considering its relative norm, we find that these integers a, b, c and c are either all even or odd. Now we subtract a particular algebraic integer $d(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})$ to α, and find that $\frac{r+s\sqrt{m}+t\sqrt{n}}{4} \in \mathcal{O}_K$, where r, s, and t are integers such that $r+s+t$ is even. It follows that $\mathcal{O}_K = [1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, (\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})]_{\mathbf{Z}}$ and the discriminant $D_{K/\mathbf{Q}} = mnk$.

(b) Let $m \equiv 1$, and $n \equiv k \equiv 2$ or 3 (mod 4). Again, for $\alpha \in \mathcal{O}_K$, we begin with writing α as the linear combination of $1, \sqrt{m}, \sqrt{n}$, and $\sqrt{k}$ with rational coefficients. By considering its relative traces and norms, we find that α is of the form $\frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$ such that $a \equiv b$ (mod 2) and $c \equiv d$ (mod 2). Moreover, we obtain that $\mathcal{O}_K = \left[1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right]_{\mathbf{Z}}$ and so $D_{K/\mathbf{Q}} = 16mnk$.

(c) Let $m \equiv 3$, and $n \equiv k \equiv 2 \mod 4$. Similarly, we find that every $\alpha \in \mathcal{O}_K$ is of the form $\frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$, where $a, b, c, d \in \mathbf{Z}$ such that a and b are even, and $c \equiv d$ (mod 2). It follows that $\mathcal{O}_K = [1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}]_{\mathbf{Z}}$ and $D_{K/\mathbf{Q}} = 64mnk$.

□

We are now ready to determine the indices $i_\gamma(K/k)$ for each $\gamma \in H^1(G, \mathcal{O}_K^\times)$. We put $k_1 = \mathbf{Q}(\sqrt{m})$ and $k_2 = \mathbf{Q}(\sqrt{n})$. Denote by p a prime of $\mathbf{Q}$ and $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{P}$ primes of k_1, k_2, K, respectively, such that $\mathfrak{P}|\mathfrak{p}|p$ and $\mathfrak{P}|\mathfrak{q}|p$. We only need to take care of $i_{\gamma_\mathfrak{P}}$ for the wildly ramified case. From the condition $p|e_p$ and $e_p|4$, we find that $p = 2$ is the only wildly ramified prime in $\mathbf{Q}$, and $e_p = 2$ or 4. Applying the product formula in Theorem 4.5 to each of three cases (1), (2), and (3) for m, n, and k, we obtain the following

Theorem 5.3. *Let $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where m and n are two distinct square-free integers and $G = \mathrm{Gal}(K/\mathbf{Q})$ the Galois group.*

(a) *If $m \equiv n \equiv k \equiv 1 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.*

(b) *If $m \equiv 1 \pmod 4$ and $n \equiv k \equiv 2 \pmod 4$, then $i_\gamma(K/\mathbf{Q}) = 2$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.*

(c) *If $m \equiv 1 \pmod 4$ and $n \equiv k \equiv 3 \pmod 4$, then*

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \textit{if } m_2 \textit{ is odd, i.e., } \gamma_\mathfrak{P} \neq 1 \\ 2 & \textit{if } m_2 \textit{ is even, i.e., } \gamma_\mathfrak{P} = 1. \end{cases}$$

(d) *If $m \equiv 3 \pmod 4$ and $n \equiv k \equiv 2 \pmod 4$, then*

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 2 & \textit{if } m_2 \equiv 1 \pmod 4 \\ 4 & \textit{if } m_2 \not\equiv 1 \pmod 4. \end{cases}$$

Proof.

(a) In this case, we find that 2 is unramified, because $2 \nmid D_{K/\mathbf{Q}} = mnk$. Therefore $i_\gamma(K/\mathbf{Q}) = 1$ for all γ.

(b) , (c) Because $D_{K/\mathbf{Q}} = 16mnk$, 2 is indeed a wildly ramified prime in $\mathbf{Q}$. Especially when $m \equiv 1 \pmod 8$, we have $k_{1\mathfrak{p}} = \mathbf{Q}_2$ and $K_\mathfrak{P} = k_{2\mathfrak{q}}$ so that we can directly apply the result of the quadratic case. We shall separate each case as below.

(i) For $m \equiv 1 \pmod 8$ and $n \equiv 2 \pmod 4$, we have $e_2 = 2$ and $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = (2\sqrt{n}) = \mathfrak{P}^3$, i.e., $t_2 = 3$. So $i_\gamma(K/k) = 2$ for all γ.

(ii) For $m \equiv 1 \pmod 8$ and $n \equiv 3 \pmod 4$, we have $e_2 = 2$ and $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = (2\sqrt{n}) = \mathfrak{P}^2$, i.e., $t_2 = 2$. As a result, we get

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \text{if } m_2 \text{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \text{if } m_2 \text{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

(iii) Let $m \equiv 5 \pmod 8$ and $n \equiv 2 \pmod 4$. In this case, we have $[K_{\mathfrak{P}} : \mathbf{Q}_2] = 4$. Since $2 \nmid m$, we find that $k_{1\mathfrak{p}}/\mathbf{Q}_2$ is unramified, and so is $K_{\mathfrak{P}}/k_{2\mathfrak{q}}$. It follows that $e_2 = e_2(K_{\mathfrak{P}}/\mathbf{Q}_2) = e_2(K_{\mathfrak{P}}/k_{2\mathfrak{q}})\, e_2(k_{2\mathfrak{q}}/\mathbf{Q}_2) = 2$, and

$$\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{D}_{K_{\mathfrak{P}}/k_{2\mathfrak{q}}}\, \mathfrak{D}_{k_{2\mathfrak{q}}/\mathbf{Q}_2} = (1)\mathfrak{p}_2{}^3 = \mathfrak{P}^3, \text{ i.e., } t_2 = 3.$$

So $i_\gamma(K/\mathbf{Q}) = 2$ for all γ.

(iv) Let $m \equiv 5 \pmod 8$ and $n \equiv 3 \pmod 4$. This is also the case when $[K_{\mathfrak{P}} : \mathbf{Q}_2] = 4$, and $k_{1\mathfrak{p}}/\mathbf{Q}_2$ and $K_{\mathfrak{P}}/k_{2\mathfrak{q}}$ are unramified. So we have $e_2 = e_2(K_{\mathfrak{P}}/\mathbf{Q}_2) = e_2(K_{\mathfrak{P}}/k_{2\mathfrak{q}})\, e_2(k_{2\mathfrak{q}}/\mathbf{Q}_2) = 2$, and

$$\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{D}_{K_{\mathfrak{P}}/k_{2\mathfrak{q}}}\, \mathfrak{D}_{k_{2\mathfrak{q}}/\mathbf{Q}_2} = (1)\mathfrak{q}^2 = \mathfrak{P}^2, \text{ i.e., } t_2 = 2.$$

Thus we obtain

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 1 & \text{if } m_2 \text{ is odd, i.e., } \gamma_{\mathfrak{P}} \neq 1 \\ 2 & \text{if } m_2 \text{ is even, i.e., } \gamma_{\mathfrak{P}} = 1. \end{cases}$$

(d) Because $D_{K/\mathbf{Q}} = 64mnk$, we find that 2 is indeed a wildly ramified prime. In this case, we find $2 = \mathfrak{p}^2$, $\mathfrak{p} = \mathfrak{P}^2$, $2 = \mathfrak{q}^2$, and $\mathfrak{q} = \mathfrak{P}^2$ so that $e_2 = 4$. We notice that $\sqrt{m}$ is a unit in $K_{\mathfrak{P}}$, and find

$$\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{D}_{K_{\mathfrak{P}}/k_{2\mathfrak{q}}}\, \mathfrak{D}_{k_{2\mathfrak{q}}/\mathbf{Q}_2} = (2\sqrt{m})\mathfrak{q}^3 = \mathfrak{p}^2\mathfrak{q}^3 = \mathfrak{P}^{10}, \text{ i.e., } t_2 = 10.$$

So $i_1(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{10}{4} \rfloor} = 4$, $i_{\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2}}(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{10+1}{4} \rfloor - 1} = 2$, $i_{(\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2})^2}(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{10+2}{4} \rfloor - 1} = 4$, and $i_{(\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2})^3}(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{10+3}{4} \rfloor - 1} = 4$. Consequently,

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} 2 & \text{if } m_2 \equiv 1 \pmod 4 \\ 4 & \text{if } m_2 \not\equiv 1 \pmod 4. \end{cases}$$

□

5.3 Cyclotomic Extensions and Its Maximal Real Subfields

Let l be a prime number, n a natural number, K the l^nth cyclotomic field $\mathbf{Q}(\zeta)$, where ζ is a primitive l^nth root of unity. The Galois group $G = \mathrm{Gal}(K/\mathbf{Q}) \approx (\mathbf{Z}/\varphi(l^n)\mathbf{Z})^\times$ is cyclic. For each n, l is the only ramified prime in $\mathbf{Q}$, because the discriminant $D_{K/\mathbf{Q}} = l^{n\varphi(l^n)-l^{n-1}}$. One knows that $\mathfrak{P} = (1-\zeta)$ is a prime ideal in K lying over l such that $l = \mathfrak{P}^{\varphi(l^n)}$, i.e. $e_l = \varphi(l^n) = (l-1)l^{n-1}$.

Passing to the localization, we denote by $K_{\mathfrak{P}}$ the completion of K, and $\mathbf{Q}_l$ the field of l-adic numbers. Then, for each n, $K_{\mathfrak{P}}/\mathbf{Q}_l$ is a totally ramified Galois extension with degree $e = \varphi(l^n)$ where the Galois group $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbf{Q}_l)$ may be identified as G itself. We have the different $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbf{Q}_l} = \mathfrak{P}^{t_l}$, where $t_l = n\varphi(l^n) - l^{n-1}$. If, in particular, $n = 1$, then $K_{\mathfrak{P}}/\mathbf{Q}_l$ is tamely ramified, since $e_l = l-1$ and $t_l = l-2$. Therefore

$$i_\gamma(K/\mathbf{Q}) = 1 \text{ for all } \gamma \in H^1(G, \mathcal{O}_K^\times). \tag{5.2}$$

Now consider the case $n \geq 2$. From $l | e_l$, we find that l is the only wildly ramified prime in $\mathbf{Q}$. Denote by $\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l}$ the canonical class in $H^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$. Then by (4.12), we find

$$i_1(K_{\mathfrak{P}}/\mathbf{Q}_l) = l^{\lfloor \frac{n\varphi(l^n)-l^{n-1}}{\varphi(l^n)} \rfloor} = l^{n-1}, \tag{5.3}$$

and

$$i_{\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l}}(K_{\mathfrak{P}}/\mathbf{Q}_l) = l^{\lfloor \frac{n\varphi(l^n)-l^{n-1}+1}{\varphi(l^n)} \rfloor -1} = l^{\lfloor n - \frac{l^{n-1}-1}{(l-1)l^{n-1}} \rfloor -1} = l^{n-2}. \tag{5.4}$$

Moreover, for $\gamma_{\mathfrak{P}} = (\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l})^{m_l}$ where m_l is an integer such that $0 \leq m_l < \varphi(l^n)$, we have

$$i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/\mathbf{Q}_l) = \begin{cases} l^{n-2} & \text{for } 1 \leq m_l < l^{n-1} \\ l^{n-1} & \text{for } l^{n-1} \leq m_l < \varphi(l^n) \text{ or } m_l = 0. \end{cases}$$

Consequently, we obtain

Theorem 5.4. *Let l be a prime, n a natural number, and $K = \mathbf{Q}(\zeta)$, the l^nth cyclotomic field over $\mathbf{Q}$, where ζ is a primitive l^nth root of unity.*

(a) *If $n = 1$, then we have $i_\gamma(K/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}_K^\times)$.*

(b) *If $n \geq 2$, we have*

$$i_\gamma(K/\mathbf{Q}) = \begin{cases} l^{n-2} & \text{if } m_l \equiv a, \text{ where } 1 \leq a < l^{n-1} \\ l^{n-1} & \text{if } m_l \equiv b, \text{ where } l^{n-1} \leq b < \varphi(l^n) \text{ or } b = 0. \end{cases}$$

Remark 5.5. *The canonical class $\gamma_{\mathfrak{P}} = \gamma_{K_{\mathfrak{P}}/\mathbf{Q}_l} = [c] \in H^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$ is given by a system of cyclotomic units*

$$c_s = \frac{{}^s\Pi}{\Pi} = \frac{1 - {}^s\zeta}{1-\zeta}, \quad s \in G. \tag{5.5}$$

By putting $\xi = 1 - \zeta$ in the formula (3.6), we find $M_c/P_c = \frac{\mathbf{Z} \cap \xi\mathcal{O}_K}{Tr_{K/\mathbf{Q}}(\xi\mathcal{O}_K)}$. We obtain M_c/P_c explicitly as

$$M_c/P_c \approx \begin{cases} 0 & \text{if } n = 1 \\ \mathbf{Z}/l^{n-2}\mathbf{Z} & \text{if } n \geq 2. \end{cases}$$

Proof. Note that $\mathcal{O}_K = \mathbf{Z}[\zeta] = [1, \zeta, \zeta^2, \cdots, \zeta^{\varphi(l^n)-1}]_{\mathbf{Z}}$. For each $i,\ 0 \leq i \leq \varphi(l^n) - 1$, let us first determine $T_{K/\mathbf{Q}}\zeta^i$. Since ζ^i is conjugate to $\zeta^{\frac{l^n}{(l^n,i)}}$, we have,

$$T_{K/\mathbf{Q}}\zeta^i = T_{K/\mathbf{Q}}\zeta^{\frac{l^n}{d}} \quad \text{with } d = (l^n, i).$$

For $d | l^n$, set $K_d = \mathbf{Q}(\zeta^{\frac{l^n}{d}})$; hence $[K : K_d] = \frac{\varphi(l^n)}{\varphi(d)}$ and so

$$T_{K/\mathbf{Q}}\zeta^{\frac{l^n}{d}} = T_{K_d/\mathbf{Q}}\left(T_{K/K_d}\zeta^{\frac{l^n}{d}}\right) = [K : K_d]\ T_{K_d/\mathbf{Q}}\zeta^{\frac{l^n}{d}}.$$

According to [7] p.197, we have $T_{K_d/\mathbf{Q}}(\zeta^{\frac{l^n}{d}}) = \mu(d)$, the Möbius function. Therefore, we have

$$T_{K/\mathbf{Q}}(\zeta^i) = T_{K/\mathbf{Q}}(\zeta^{\frac{l^n}{d}}) = \frac{\varphi(l^n)}{\varphi(d)}\mu(d) = \begin{cases} \varphi(l^n), & i = 0 \\ -l^{n-1}, & l^{n-1} | i, \quad i \neq 0 \\ 0 & l^{n-1} \nmid i, \quad i \neq 0. \end{cases} \tag{5.6}$$

Going back to M_c/P_c for a cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$, we begin with the case $n = 1$. For every $\alpha \in \mathcal{O}_K, \quad \alpha = \sum_{i=0}^{l-2} n_i\zeta^i$ for some integers n_i. Since, by (5.6), $T_{K/\mathbf{Q}}(\zeta^i) = -1$

for $1 \leq i \leq l-2$, $= l-1$ for $i = 0$, we find that

$$\begin{aligned} T_{K/\mathbf{Q}}((1-\zeta)\alpha) &= \sum_{i=0}^{l-2} n_i T_{K/\mathbf{Q}}(\zeta^i) - \sum_{i=0}^{l-2} n_i T_{K/\mathbf{Q}}(\zeta^{i+1}) \\ &= n_0 T_{K/\mathbf{Q}}(1) - \sum_{i=1}^{l-2} n_i + \sum_{i=0}^{l-2} n_i = l n_0. \end{aligned}$$

It follows that $T_{K/\mathbf{Q}}((1-\zeta)\mathcal{O}_K) = l\mathbf{Z}$.

Now to find $\mathbf{Z} \cap (1-\zeta)\mathbf{Z}[\zeta]$, we first examine a general element $\alpha \in (1-\zeta)\mathbf{Z}[\zeta]$.

$$\begin{aligned} \alpha &= (1-\zeta) \sum_{i=0}^{l-2} n_i \zeta^i \quad \text{for some } n_i \in \mathbf{Z} \\ &= n_0 + \sum_{i=1}^{l-2} (n_i - n_{i-1}) \zeta^i - n_{l-2} \zeta^{l-1} \\ &= (n_0 + n_{l-2}) + \sum_{i=1}^{l-2} (n_i - n_{i-1} + n_{l-2}) \zeta^i. \end{aligned}$$

For α to be in $\mathbf{Z}$, we must have $n_i - n_{i-1} = -n_{l-2}$ for $1 \leq i \leq l-2$. This implies that $n_{l-2} - n_0 = -(l-2)n_{l-2}$, i.e. $n_0 = (l-1)n_{l-2}$ and so $n_0 + n_{l-2} = l n_{l-2}$. It follows that $\mathbf{Z} \cap (1-\zeta)\mathbf{Z}[\zeta] = l\mathbf{Z}$. Therefore

$$M_c/P_c \approx l\mathbf{Z}/l\mathbf{Z} = 0.$$

Next, let $n \geq 2$. For every $\alpha \in \mathcal{O}_K$, $\alpha = \sum_{i=0}^{\varphi(l^n)-1} n_i \zeta^i$ for some integers n_i. We have, by (5.6),

$$\begin{aligned} T_{K/\mathbf{Q}}((1-\zeta)\alpha) &= \sum_{i=0}^{\varphi(l^n)-1} n_i T_{K/\mathbf{Q}}(\zeta^i) - \sum_{i=1}^{\varphi(l^n)} n_{i-1} T_{K/\mathbf{Q}}(\zeta^i) \\ &= l^{n-1} \left[(l-1)n_0 + n_{\varphi(l^n)-1} - \sum_{\substack{1 \leq i \leq \varphi(l^n)-1 \\ l^{n-1} | i}} (n_i - n_{i-1}) \right], \end{aligned}$$

which implies that $T_{K/\mathbf{Q}}((1-\zeta)\mathcal{O}_K) = l^{n-1}\mathbf{Z}$. Now to find $\mathbf{Z} \cap (1-\zeta)\mathbf{Z}[\zeta]$, we first examine a general element $\alpha \in (1-\zeta)\mathbf{Z}[\zeta]$.

$$\begin{aligned}
\alpha &= (1-\zeta)\sum_{i=0}^{\varphi(l^n)-1} n_i\zeta^i \quad \text{for some } n_i \in \mathbf{Z} \\
&= n_0 + \sum_{i=1}^{\varphi(l^n)-1} (n_i - n_{i-1})\zeta^i - n_{\varphi(l^n)-1}\zeta^{\varphi(l^n)} \\
&= (n_0 + n_{\varphi(l^n)-1}) + \sum_{\substack{1\le i\le\varphi(m)-1 \\ l^{n-1}|i}} (n_i - n_{i-1} + n_{\varphi(l^n)-1})\zeta^i + \sum_{\substack{1\le i\le\varphi(l^n)-1 \\ l^{n-1}\nmid\, i}} (n_i - n_{i-1})\zeta^i.
\end{aligned}$$

For α to be in $\mathbf{Z}$, we must have

$$\begin{cases} n_i - n_{i-1} + n_{\varphi(l^n)-1} = 0 & \text{for } i = l^{n-1}, 2l^{n-1}, \cdots, (l-2)l^{n-1} \\ n_i = n_{i-1} & \text{for } i \text{ such that } 1 \le i \le \varphi(l^n)-1 \text{ and } l^{n-1} \nmid i. \end{cases}$$

From this recursive formula, we find

$$\begin{cases} n_{(l-2)l^{n-1}} = n_{(l-2)l^{n-1}-1} - n_{\varphi(l^n)-1} = n_0 - (l-2)n_{\varphi(l^n)-1} \\ n_{(l-2)l^{n-1}} = n_{(l-2)l^{n-1}-1} = \cdots = n_{\varphi(l^n)-1}, \end{cases}$$

and so

$$\begin{aligned}
n_0 + n_{\varphi(l^n)-1} &= \big(n_{(l-2)l^{n-1}} + (l-2)n_{\varphi(l^n)-1}\big) + n_{\varphi(l^n)-1} \\
&= n_{\varphi(l^n)-1} + (l-2)n_{\varphi(l^n)-1} + n_{\varphi(l^n)-1} \\
&= l n_{\varphi(l^n)-1}.
\end{aligned}$$

It follows that $\mathbf{Z} \cap (1-\zeta)\mathbf{Z}[\zeta] = l\mathbf{Z}$. Therefore

$$M_c/P_c \approx l\mathbf{Z}/l^{n-1}\mathbf{Z} \approx \mathbf{Z}/l^{n-2}\mathbf{Z}.$$

□

Remark. Theorem 4.3 can be applied to this l^nth cyclotomic fields case.

Remark. Let $K/\mathbf{Q}$, the mth cyclotomic field, where m is a natural number divisible by two distinct primes. Put $m = {l_1}^{a_1} \cdots {l_t}^{a_t}$, where l_i is a prime and a_i is a natural integer. Let c be the cocycle c of $\mathrm{Gal}(K/\mathbf{Q})$ consisting of cyclotomic units. Then $c \sim 1$, as $1-\zeta$ is already in $\mathcal{O}_{K_m}$. From

$$T_{K_m/\mathbf{Q}}(\mathcal{O}_{K_m}) = \left(\underset{\substack{d|m \\ d\text{: square-free}}}{\text{g.c.d.}} \left(\frac{\varphi(m)}{\varphi(d)} \right) \right) \mathbf{Z},$$

we find $Tr_{K/k}(\mathcal{O}_{K_m}) = m'\mathbf{Z}$, where $m' = {l_1}^{a_1-1}\cdots {l_t}^{a_t-1}$. Hence $M_c/P_c = \mathbf{Z}/m'\mathbf{Z}$.

Now we consider $K^+ = \mathbf{Q}(\zeta+\zeta^{-1})$, the maximal real subfield of l^nth cyclotomic field $K = \mathbf{Q}(\zeta)$, where ζ is a primitive l^nth root of unity and l is an odd prime.

When $n = 1$, $K^+/\mathbf{Q}$ is tamely ramified so that $i_\gamma(K^+/\mathbf{Q}) = 1$. When $n \geq 2$, we have $e = e(K^+/Q) = \frac{\varphi(l^n)}{2}$ so that l is the only wildly ramified prime. We put $\eta = \zeta+\zeta^{-1}$. From $l = (2-\eta)^{\varphi(l^n)/2}$, we find that $2-\eta = (1-\zeta)(1-\zeta^{-1})$ is a prime element in $\mathcal{O}_{K^+}$ lying over l. Denote by $\mathfrak{P} = (2-\eta)$ a prime in K^+ and $K^+_{\mathfrak{P}}$ the completion of K^+. Then $K^+_{\mathfrak{P}}/\mathbf{Q}_l$ is a totally ramified Galois extension with degree $e = \frac{\varphi(l^n)}{2}$ and the Galois group may be identified as $G = \mathrm{Gal}(K^+/\mathbf{Q})$. The canonical class $\gamma_{K^+_{\mathfrak{P}}/\mathbf{Q}_l} = [c_{K^+_{\mathfrak{P}}/\mathbf{Q}_l}] \in H^1(G, \mathcal{O}^\times_{K^+_{\mathfrak{P}}})$ is given by a system

$$c_{K^+_{\mathfrak{P}}/\mathbf{Q}_l,s} = \frac{2-{}^s\eta}{2-\eta}, \quad s \in G.$$

For each n, the different $\mathfrak{D}(K^+_{\mathfrak{P}}/\mathbf{Q}_l) = \mathfrak{P}^t$, where $t = \frac{(n(l-1)-1)l^{n-1}-1}{2}$. Hence

$$i_{\gamma_{K^+_{\mathfrak{P}}/\mathbf{Q}_l}}(K^+_{\mathfrak{P}}/\mathbf{Q}_l) = l^{n-2}.$$

Moreover, for $\gamma_{\mathfrak{P}} = (\gamma_{K^+_{\mathfrak{P}}/\mathbf{Q}_l})^{m_l}$ where m_l is an integer such that $0 \leq m_l < \frac{\varphi(l^n)}{2}$, we have

$$i_{\gamma_{\mathfrak{P}}}(K^+_{\mathfrak{P}}/\mathbf{Q}_l) = \begin{cases} l^{n-2} & \text{for } 1 \leq m_l < \frac{l^{n-1}+1}{2} \\ l^{n-1} & \text{for } \frac{l^{n-1}+1}{2} \leq m_l < \frac{\varphi(l^n)}{2} \text{ or } m_l = 0. \end{cases}$$

Consequently, we obtain

Theorem 5.6. *Let l be an odd prime, n a natural number, ζ a primitive l^nth root of unity, and $K^+ = \mathbf{Q}(\zeta+\zeta^{-1})$. Then*

(a) *If $n = 1$, then we have $i_\gamma(K^+/\mathbf{Q}) = 1$ for all $\gamma \in H^1(G, \mathcal{O}^\times_{K^+})$.*

(b) *If $n \geq 2$, we have*

$$i_\gamma(K^+/\mathbf{Q}) = \begin{cases} l^{n-2} & \textit{if } m_l \equiv a, \textit{ where } 1 \leq a < \frac{l^{n-1}+1}{2} \\ l^{n-1} & \textit{if } m_l \equiv b, \textit{ where } \frac{l^{n-1}+1}{2} \leq b < \frac{\varphi(l^n)}{2} \textit{ or } b = 0. \end{cases}$$

References

[1] J.W.S. Cassels and A. Frölich, Algebraic Number Theory. Academic Press, London and New York (1967)

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

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

[4] S.M. Lee, On Certain Cohomological Invariants of Quadratic Number Fields. Dissertation, Johns Hopkins University (2004)

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

[7] I. Niven, An Introduction to the Theory of Numbers. John Wiley & Sons (1991)

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

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

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

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

[12] T. Ono, On Poincaré sums for number fields. to appear in coming issue of Proc. Japan Acad.

[13] T. Ono, Lecture Notes, Topics in Algebraic Number Theory. (Fall 2003)

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

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

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

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

[18] H. Yokoi, On an Isomorphism of Galois Cohomology Groups $H^m(G, \mathcal{O}_K)$ of Integers in an Algebraic Number Field. Proc. Japan Acad., vol 38, 499-501 (1962)

[19] H. Yokoi, A Note on the Galois Cohomology Group of the Ring of Integers in an Algebraic Number Field. Proc. Japan Acad., vol 40, 245-246 (1964)

VITA

Eun Kyoung Lee was born in October 1973 in Tokyo, Japan, and raised in Seoul, Korea. She received her Bachelor of Science degree in Mathematics, magna cum laude, from Ewha Womans University in Seoul, Korea in 1996, and Master of Science degree in Mathematics from Ewha Womans University in 1998. That fall, she enrolled in the graduate program at Johns Hopkins University. She defended this thesis on March 24, 2005.