On a class number problem of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$

$\mathbb{Q}(\sqrt{5})$の円分的$\mathbb{Z}_2$-拡大の類数問題について

February, 2020

Takuya AOKI
青木　琢哉

On a class number problem of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$

$\mathbb{Q}(\sqrt{5})$の円分的$\mathbb{Z}_2$-拡大の類数問題について

February, 2020

Waseda University
Graduate School of Fundamental Science and Engineering
Department of Pure and Applied Mathematics, Research on Number Theory

Takuya AOKI
青木　琢哉

Acknowledgements

I would like to express my sincere gratitude to Professor Keiichi Komatsu, who guided me to the number theory and has encouraged me passionately and given me productive advice since I was a third-year university student. I also thank him for acting as a referee of my thesis.

I would like to thank Professor Takashi Fukuda sincerely for his helpful instructions and comments around the computational works in Chapters 3 and 5.

I would also like to extend my sincere thanks to Professor Hiroaki Narita for reading this thesis very carefully, pointing out many incorrect expressions in this thesis and giving me fruitful suggestions as the principal referee of my thesis.

Furthermore, I would like to express my sincere thanks to Professor Kiichiro Hashimoto and Professor Manabu Ozaki for helpful comments and encouragements as referees of my thesis.

Moreover, I want to thank Professor Ryotaro Okazaki, Professor Tsuyoshi Ito and Professor Yasushi Mizusawa for giving me many instructive comments and suggestions for my forward research. I also want to thank all other members of the number theory seminars at Waseda University for giving me an instructive environment.

Finally, I shall be grateful to my parents, Hitoshi and Kayoko, my sisters, Hiromi and Minori, my grandmothers, Haruko and Takae, and my friends.

Contents

Introduction

In algebraic number theory, the class number of an algebraic number field is one of the most important and fundamental objects. It is still an open problem whether there exist infinitely many algebraic number fields with class number one. In order to approach this problem, we study *Weber's class number problem*. The aim of this thesis is to generalize *Weber's class number problem* for the cases of real quadratic fields. This study can be said to be unprecedented.

Let p be a prime number. We denote by $\mathbb{B}_{p,n}$ the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We also denote by $h_{p,n}$ the class number of $\mathbb{B}_{p,n}$. Then we consider the following problem:

Weber's class number problem. Is the class number $h_{p,n}$ equal to 1 for any prime number p and any positive integer n ?

In the case of $p = 2$, Weber [43] showed that $h_{2,n}$ is odd for any positive integer n. He also showed that $h_{2,1} = h_{2,2} = h_{2,3} = 1$. Though Weber conjectured that $h_{2,4}$ is not equal to 1, it was shown that $h_{2,4} = 1$ by Cohn [6], Bauer [3] and Masley [25]. Moreover, van der Linden [24] showed that $h_{2,5} = 1$. Linden also showed that $h_{2,6} = 1$ holds under the assumption of generalized Riemann hypothesis. In 2014, Miller [28] showed that $h_{2,6} = 1$ holds without the assumption. He also showed that $h_{2,7} = 1$ under generalized Riemann hypothesis.

In the case of $p \neq 2$, on the other hand, it is known that $h_{p,n} = 1$ for $(p, n) \in \{(3, 1), (3, 2), (3, 3), (5, 1), (7, 1)\}$ by [3] and [24]. Linden also showed that, if we assume generalized Riemann hypothesis, then we have $h_{p,n} = 1$ for $(p, n) \in \{(3, 4), (5, 2), (11, 1), (13, 1)\}$. Recently, Miller showed that $h_{p,n} = 1$ for $(p, n) \in \{(5, 2), (11, 1), (13, 1)\}$ without the assumption.

In 2012, Coates [5] asked the generalized version of *Weber's class number problem*. Let F be a totally real number field and $F(\mathrm{cyc})$ the composite of the cyclotomic $\mathbb{Z}_p$-extension for all prime number p. For each positive integer m, we denote by $F(m)$ the unique intermediate field of $F(\mathrm{cyc})/F$ which satisfies $[F(m) : F] = m$. Let $h(F(m))$ be the class number of $F(m)$. Then Coates asked the following question:

Problem. Does there exist a number $C(F) > 0$, which is not depending on m, such that $h(F(m))$ is at most $C(F)$ for all positive integer m ?

This problem is so difficult because, even in the case of $F = \mathbb{Q}$ and $m = p^n$ for a prime number p and a positive integer n, it is too difficult for large p^n to calculate $h(\mathbb{Q}(p^n)) = h_{p,n}$ directly. Therefore, we study the ℓ-divisibility of $h(F(m))$ for a prime number ℓ:

Problem. Does there exist a prime number ℓ dividing $h(F(m))$ for a totally real number field F and positive integer m ?

The ℓ-indivisibility of $h_{p,n}$ has been studied actively. In the case of $\ell = p$, Iwasawa [23] proved that p does not divide $h_{p,n}$ for any positive integer n. For each prime number $\ell \neq p$, Washington [41] showed that the ℓ-part of $h_{p,n}$ is bounded as n tends to ∞.

K. Horie [13, 14, 15, 16] and K. Horie and M. Horie [18, 19, 20, 21, 22] gave an effective breakthrough for proving ℓ-indivisibility of $h_{p,n}$. We shall cite a part of their results:

Theorem 0.1 (K. Horie, K Horie and M. Horie)**.**
(i) *Assume that* $3 \leq p \leq 23$ *and a prime number* ℓ *is a primitive root modulo* p^2*. Then* ℓ *does not divide* $h_{p,n}$ *for any positive integer* n*.*
(ii) *Assume that* $p = 2$ *and a prime number* ℓ *satisfies that* $\ell \equiv \pm 1 \pmod 8$*. Then* ℓ *does not divide* $h_{2,n}$ *for any positive integer* n*.*
(iii) *Assume that* $p \leq 101$ *and a prime number* ℓ *does not exceed* 13*. Then* ℓ *does not divide* $h_{p,n}$ *for any positive integer.*

In the case of $p = 2$, Fukuda and Komatsu [7, 8, 9] studied ℓ-indivisibility of $h_{2,n}$ deeply:

Theorem 0.2 (Fukuda and Komatsu)**.** *Let* ℓ *be an odd prime number. If* ℓ *is less than* 10^9 *or satisfies* $\ell \not\equiv \pm 1 \pmod{32}$*, then* ℓ *does not divide* $h_{2,n}$ *for any positive integer.*

Recently, Morisawa and Okazaki [33] showed that ℓ does not divide $h_{2,n}$ for any positive integer n if $\ell \not\equiv \pm 1 \pmod{64}$.

In the case of $p = 3$, Morisawa [30, 31] showed the following:

Theorem 0.3 (Morisawa). *Let ℓ be a prime integer. If ℓ is less than 10^9 or satisfies $\ell \not\equiv \pm 1 \pmod{27}$, then ℓ does not divide $h_{3,n}$ for any positive integer n.*

In this thesis, we study the class numbers of the intermediate fields of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$. The reason why we treat $\mathbb{Q}(\sqrt{5})$ is because $\mathbb{Q}(\sqrt{5})$ has the minimal discriminant in those of all real quadratic fields. This case can be said to be a most accessible one as a generalization of Weber's class number problem to real quadratic extensions.

Through this thesis, we put

$$K_n := \mathbb{Q}\left(\sqrt{5}, 2\cos\frac{2\pi}{2^{n+2}}\right) \tag{0.0.1}$$

for each non-negative integer n. Then K_n is the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $K_0 = \mathbb{Q}(\sqrt{5})$. We also denote by h_n the class number of K_n. For an odd prime number ℓ, let δ_ℓ be 0 or 1 according as $\ell \equiv 1 \pmod 4$ or not and 2^{c_ℓ} the exact power of 2 dividing $\ell^{\delta_\ell+1} - 1$. For a real number x, we denote by $\lfloor x \rfloor$ the greatest integer not exceeding x.

Now we describe our results:

Theorem 0.4. *Let ℓ be an odd prime. Put*

$$m_\ell := \begin{cases} 2c_\ell + \lfloor \log_2(5\ell - 1) \rfloor - \delta_\ell - 2 & \text{if } \ell \neq 5, \\ 4 & \text{if } \ell = 5. \end{cases}$$

Then ℓ does not divide h_n/h_{m_ℓ} for any $n \geq m_\ell$.

Theorem 0.5. *Let ℓ be an odd prime number less than $6 \cdot 10^4$. Then ℓ does not divide h_n for any positive integer n.*

Theorem 0.6. *The class number of K_5 is at most 133.*

Theorem 0.7. *The class numbers of K_4 and K_5 are 1.*

In chapter 1, we recall fundamental facts of an algebraic number field, that is, the class number, the integral basis, the discriminant, the root discriminant and the cyclotomic $\mathbb{Z}_p$-extension. In particular, the explicit integral basis and the value of discriminant of K_n play important role in chapter 5. So we study them precisely.

In chapter 2, we shall prove theorem 0.4. m_ℓ, given in theorem 0.4, is an explicit bound of Washington's theorem for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$.

In chapter 3, we shall explain how to obtain theorem 0.5 by using the result in chapter 2 and a computer.

In chapter 4, we shall study Miller's method to establish an upper bound of the class number of a totally real field with large root discriminant by using Poitou version of Weil's explicit formula and class field theory. The result of this chapter plays an important role in the next chapter.

In chapter 5, we shall prove theorems 0.6 and 0.7. In order to apply Miller's result in chapter 4, we need to construct a large set of prime numbers each of which splits completely into a product of principal prime ideals of K_5. We also explain the algorithm to find such prime numbers.

In chaper 6, we shall describe perspectives of our research by referring to previous researches for Weber's class number problem.

Chapter 1

Fundamental Facts of Algebraic Number Fields

In this chapter, we recall fundamental facts of an algebraic number field K, that is, the ideal class group, the discriminant and the root discriminant of K. Next, we also recall the definition of the cyclotomic $\mathbb{Z}_p$-extension $K_{p,\infty}$ of K and some properties of the class number of $K_{p,n}$, where $K_{p,n}$ is the n-th layer of $K_{p,\infty}/K$.

If we do not remark anything, we shall give proofs in this chapter following Washington [42].

1.1 Ideal Class Groups of Algebraic Number Fields

Let K be an algebraic number field with finite degree over $\mathbb{Q}$. We denote by $Cl(K)$ the ideal class group of K. We also denote by $h(K)$ the cardinal of $Cl(K)$, which is finite. We call $h(K)$ the class number of K. Then we have the following:

Lemma 1.1. *Let L/K be an extension of algebraic number fields which contains no nontrivial unramified abelian subextension. Then the norm map from $Cl(L)$ to $Cl(K)$ is surjective.*

Proof. We denote by $H(L)$ and $H(K)$ the Hilbert class field of L and K, respectively. By the class field theory, we have the following commutative diagram (cf. Washington [42, Appendix § 3]):

$$\begin{array}{ccc} Cl(L) & \xrightarrow{\sim} & \mathrm{Gal}(H(L)/L) \\ {\scriptstyle \mathrm{norm}}\downarrow & & \downarrow{\scriptstyle \mathrm{restriction}} \\ Cl(K) & \xrightarrow{\sim} & \mathrm{Gal}(H(K)/K), \end{array} \tag{1.1.1}$$

where both of horizontal maps are the Artin maps. By the assumption, we have $H(K) \cap L = K$. Since $H(K)L/L$ is an unramified abelian extension, we have $H(K)L \subset H(L)$ and

$$\mathrm{Gal}(H(L)/L) \twoheadrightarrow \mathrm{Gal}(H(K)L/L) \cong \mathrm{Gal}(H(K)/K),$$

which implies that the restriction from $\mathrm{Gal}(H(L)/L)$ to $\mathrm{Gal}(H(K)/K)$ is surjective. By (1.1.1), the norm map from $Cl(L)$ to $Cl(K)$ is surjective. □

For a prime number ℓ, we denote by $A(K)$ the ℓ-Sylow subgroup of $Cl(K)$. We define $D(L/K)$ the kernel of the norm map from $A(L)$ to $A(K)$:

Lemma 1.2. *Let L/K be an extension of algebraic number fields with degree prime to ℓ. Then the natural map from $A(K)$ to $A(L)$ is injective and we have*

$$A(L) \cong A(K) \oplus D(L/K). \tag{1.1.2}$$

Proof. We put $m := [L : K]$. Since m is prime to ℓ, the composite map

$$A(K) \xrightarrow{\text{natural map}} A(L) \xrightarrow{\text{norm map}} A(K) \xrightarrow{m^{-1}} A(K)$$

is the identity of $A(K)$. Therefore, the natural map form $A(K)$ to $A(L)$ is injective and the sequence

$$1 \to D(L/K) \to A(L) \to A(K) \to 1$$

is split. This completes the proof. □

1.2 Integral Basis and Discriminants of Algebraic Number Fields

Let ζ_m be a primitive m-th root of unity in $\mathbb{C}$ for a positive integer m. For an algebraic number field K with $n := [K : \mathbb{Q}] < \infty$, let

$$\{\omega_1, \omega_2, \cdots, \omega_n\}$$

be an integral basis of K. As well-known results, we give two examples of integral basis.

Example 1.3. For a quadratic field $\mathbb{Q}(\sqrt{d})$ with square free rational integer $d \neq 1$, the set

$$\mathfrak{B} = \begin{cases} \{1, \sqrt{d}\} & \text{if } d \not\equiv 1 \pmod 4, \\ \left\{1, \frac{1+\sqrt{d}}{2}\right\} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

forms an integral basis of $\mathbb{Q}(\sqrt{d})$.

Example 1.4. For a cyclotomic field $\mathbb{Q}(\zeta_m)$ with positive integer $m \not\equiv 2 \pmod 4$, the set

$$\{1, \zeta_m, \zeta_m^2, \cdots, \zeta_m^{\phi(m)-1}\},$$

forms an integral basis of $\mathbb{Q}(\zeta_m)$, where $\phi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ is the Euler function.

For the maximal real subfield $\mathbb{Q}(\zeta_m)^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ of $\mathbb{Q}(\zeta_m)$, we can also obtain an integral basis of $\mathbb{Q}(\zeta_m)^+$ explicitly:

Proposition 1.5. *The set*

$$\{1, \zeta_m + \zeta_m^{-1}, (\zeta_m + \zeta_m^{-1})^2, \cdots, (\zeta_m + \zeta_m^{-1})^{\phi(m)/2-1}\}$$

forms an integral basis of $\mathbb{Q}(\zeta_m)^+$.

Proof. Since the minimal polynomial of $\zeta_m + \zeta_m^{-1}$ has degree $\phi(m)/2$, it is enough to show that the integer ring of $\mathbb{Q}(\zeta_m)^+$ is $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. We assume that $\alpha \in \mathbb{Q}(\zeta_m)^+$ is an algebraic integer and put

$$\alpha = a_0 + a_1(\zeta_m + \zeta_m^{-1}) + \cdots a_N(\zeta_m + \zeta_m^{-1})^N$$

with $N \leq \phi(m)/2 - 1$ and $a_i \in \mathbb{Q}$. Multiplying ζ_m^N and expanding the result as a polynomial in ζ_m, we have

$$\zeta_m^N \alpha = a_N + \cdots + a_N \zeta_m^{2N}.$$

Since $\{1, \zeta_m, \zeta_m^2, \cdots, \zeta_m^{\phi(m)-1}\}$ is an integral basis and $2N \leq \phi(m) - 2$,

$$\{1, \zeta_m, \cdots, \zeta_m^{2N}\}$$

is a subset of an integral basis of $\mathbb{Q}(\zeta_m)$. Since $\zeta_m^N \alpha$ is an algebraic integer of $\mathbb{Q}(\zeta_m)$, we have $a_N \in \mathbb{Z}$. Therefore, it is true that

$$\alpha - a_N(\zeta_m + \zeta_m^{-1})^N = a_0 + a_1(\zeta_m + \zeta_m^{-1}) + \cdots a_{N-1}(\zeta_m + \zeta_m^{-1})^{N-1}$$

is an algebraic integer of $\mathbb{Q}(\zeta_m)^+$. By induction, we have $a_i \in \mathbb{Z}$ for all integer i with $0 \leq i \leq N$. This completes the proof. $\square$

let $d(K)$ be the discriminant of K, i.e.,

$$d(K) := \left(\det \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \cdots & \sigma_n(\omega_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \cdots & \sigma_n(\omega_n) \end{pmatrix} \right)^2,$$

where $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is the set of all embeddings of K into $\mathbb{C}$. Denoting by $\mathrm{Tr}_{K/\mathbb{Q}}$ the trace mapping from K to $\mathbb{Q}$, we obtain

$$\begin{aligned} d(K) &= \det \left(\begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \cdots & \sigma_n(\omega_2) \\ \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \cdots & \sigma_n(\omega_n) \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \cdots & \sigma_2(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{pmatrix} \right) \\ &= \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_n) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\omega_2\omega_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\omega_2\omega_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(\omega_n\omega_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\omega_n\omega_n) \end{pmatrix} \qquad (1.2.1) \end{aligned}$$

It is well known that $d(K)$ is a rational integer and the absolute value of $d(K)$ is greater than 1 if $K \neq \mathbb{Q}$.

Odlyzko [38] gave lower bounds for discriminants of totally real number fields:

Theorem 1.6 (Odlyzko). *There exist pairings of non-negative real numbers (A, E) satisfying*

$$d(K) > A^n \mathrm{e}^{-E} \tag{1.2.2}$$

for any totally real number field K with $n = [K : \mathbb{Q}]$.

Table 1.1: the pairing of (A, E) in Odlyzko's theorem[1]

A	E	A	E
18.916	5.3334	54.333	26.667
21.512	6.0001	55.335	29.334
24.016	6.6667	56.129	32.001
28.668	8.0001	57.286	37.334
36.347	10.667	58.070	42.667
42.018	13.334	58.624	48.001
46.138	16.001	59.028	53.334
51.371	21.334	59.896	74.667
53.047	24.001	60.704	200.01

The table 1.1 is an abstract from the table in Odlyzko [39]. Odlyzko calculated these pairings analytically (cf. [36, Theorem 1] or [37, Theorem 1]).

Finally, we introduce the following proposition to determine the discriminant and an integral basis of a composite field of two algebraic number fields (cf. Neukirch [35]):

Proposition 1.7. *Let K, resp. K', be a Galois extension over $\mathbb{Q}$ with degree n, resp. n'. We denote by $\{\omega_1, \omega_2, \cdots, \omega_n\}$, resp. $\{\omega'_1, \omega'_2, \cdots, \omega'_{n'}\}$, an integral basis of K, resp. K'. If $K \cap K' = \mathbb{Q}$ and $d(K)$ and $d(K')$ are coprime, then*

$$\mathfrak{B} := \{\omega_i \omega'_j \mid 1 \leq i \leq n, 1 \leq j \leq n'\}$$

is an integral basis of KK' and

$$d(KK') = d(K)^{n'} d(K')^n.$$

[1] abstracted from Odlyzko [39]

Proof. Since K is a Galois extension over $\mathbb{Q}$ and $K \cap K' = \mathbb{Q}$, we have $[KK' : \mathbb{Q}] = nn'$. Thus $\mathfrak{B}$ is a basis of $KK'/\mathbb{Q}$. Let α be an algebraic integer of KK' and write

$$\alpha = \sum_{j=1}^{n_2} \sum_{i=1}^{n_1} a_{i,j} \omega_i \omega'_j$$

with $a_{i,j} \in \mathbb{Q}$. We put

$$\beta_j = \sum_{i=1}^{n_1} a_{i,j} \omega_i \in K.$$

Let $\mathrm{Gal}(KK'/K') = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ and $\mathrm{Gal}(KK'/K) = \{\sigma'_1, \sigma'_2, \cdots, \sigma'_{n'}\}$. Then we have

$$\mathrm{Gal}(KK'/\mathbb{Q}) = \{\sigma_k \sigma'_l \mid k = 1, 2, \cdots, n,\ l = 1, 2, \cdots, n'\}.$$

Putting

$$X = \begin{pmatrix} \sigma'_1(\omega'_1) & \cdots & \sigma'_{n'}(\omega'_1) \\ \vdots & \ddots & \vdots \\ \sigma'_1(\omega'_{n'}) & \cdots & \sigma'_{n'}(\omega'_{n'}) \end{pmatrix}, \ \mathbf{a} = \begin{pmatrix} \sigma'_1(\alpha) \\ \vdots \\ \sigma'_{n'}(\alpha) \end{pmatrix}, \ \mathbf{b} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n'} \end{pmatrix},$$

we have $\det(X)^2 = d(K')$ and

$$\mathbf{a} = X\mathbf{b}.$$

We denote by $\tilde{X}$ the adjoint matrix of X. Then we obtain

$$\det(X)\mathbf{b} = \tilde{X}\mathbf{a}.$$

Since all the elements of $\tilde{X}\mathbf{a}$ are algebraic integers of KK', all the elements of $d(K')\mathbf{b}$, $d(K')\beta_j = \sum_{i=1}^{n_1} d(K')a_{i,j}\omega_i$, are algebraic integers of K. Thus we have $d(K')a_{i,j} \in \mathbb{Z}$. Changing the roles of ω_i's and ω'_j's, we also have $d(K)a_{i,j} \in \mathbb{Z}$. Since there exist $x, x' \in \mathbb{Z}$ satisfying

$$xd(K) + x'd(K') = 1,$$

we have

$$a_{i,j} = xd(K)a_{i,j} + x'd(K')a_{i,j} \in \mathbb{Z}.$$

Therefore, $\mathfrak{B}$ is an integral basis of KK'.

In order to compute $d(KK')$, we calculate the determinant of the $nn' \times nn'$-matrix

$$M := \left(\sigma_k\sigma_l'(\omega_i\omega_j')\right) = \left(\sigma_k(\omega_i)\sigma_l'(\omega_j')\right).$$

Since we can regard M as a $n' \times n'$-matrix whose (j,l)-element is $n \times n$-matrix $Q\sigma_l'(\omega_j')$ with $Q := (\sigma_k(\omega_i))$, we have

$$M = \begin{pmatrix} Q & O_n & \cdots & O_n \\ O_n & Q & \cdots & O_n \\ \vdots & \ddots & \ddots & \vdots \\ O_n & \cdots & O_n & Q \end{pmatrix} \begin{pmatrix} E_n\sigma_1'(\omega_1') & E_n\sigma_2(\omega_1') & \cdots & E_n\sigma_{n'}(\omega_1') \\ E_n\sigma_1'(\omega_2') & E_n\sigma_2'(\omega_2') & \cdots & E_n\sigma_{n'}'(\omega_2') \\ \vdots & \ddots & \ddots & \vdots \\ E_n\sigma_1'(\omega_{n'}') & E_n\sigma_2'(\omega_{n'}') & \cdots & E_n\sigma_{n'}'(\omega_{n'}') \end{pmatrix},$$

where O_n is the $n \times n$-zero matrix and E_n is the $n \times n$-unit matrix. Therefore, we have

$$\det(M) = \det(Q)^{n'}\det(\sigma_l'(\omega_j'))^n = d(K)^{n'}d(K')^n,$$

which completes the proof. □

1.3 Root Discriminants of Algebraic Number Fields

For an algebraic number field K with degree n over $\mathbb{Q}$, the root discriminant $\mathrm{rd}(K)$ of K is defined by

$$\mathrm{rd}(K) := |d(K)|^{1/n}, \tag{1.3.1}$$

that is, the positive real number whose n-th power is equal to the absolute value of $d(K)$. Then Masley [25] proved the following proposition:

Proposition 1.8 (Masley). *Let L/K be an extension of algebraic number fields with finite degrees over $\mathbb{Q}$. Then we have $\mathrm{rd}(K) \leq \mathrm{rd}(L)$. Moreover, the equality holds if and only if L/K is an unramified extension at all finite primes.*

Proof. Let $d(L/K)$ be the absolute norm of the relative discriminant ideal for L/K. Then we have

$$|d(L)| = d(L/K)|d(K)|^{[L:K]}.$$

It is true that $d(L/K) \geq 1$ and the equality holds if and only if L/K is an unramified extension at all finite primes. This completes the proof. □

Proposition 1.8 implies that for an algebraic number field K and its Hilbert class field $H(K)$, we have

$$\mathrm{rd}(H(K)) = \mathrm{rd}(K). \tag{1.3.2}$$

Using the equation (1.3.2), we can establish an upper bound of the class number $h(K)$ of a totally real algebraic number field K with small root discriminant, which is used in Masley [25] or Linden [24]:

Proposition 1.9. *Let K be a totally real field with degree n and (A, E) a pairing of real numbers which appears in the table of Odlyzko* [39]*. If $\mathrm{rd}(K) < A$, then we have*

$$h(K) < \frac{E}{n(\log A - \log \mathrm{rd}(K))}. \tag{1.3.3}$$

Proof. Since K is totally real, the Hilbert class field $H(K)$ of K is also totally real. By theorem 1.6, we have

$$d(H(K)) > A^{h(K)n} \mathrm{e}^{-E}$$

for each pairing in the table of Odlyzko [39]. By the equation (1.3.2), we have

$$d(H(K)) = \mathrm{rd}(H(K))^{h(K)n} = \mathrm{rd}(K)^{h(K)n}.$$

Therefore, we have

$$h(K)n(\log A - \log \mathrm{rd}(K)) < E.$$

If $\mathrm{rd}(K) < A$, then we obtain $\log A - \log \mathrm{rd}(K) > 0$. Therefore, we have

$$h(K) < \frac{E}{n(\log A - \log \mathrm{rd}(K))},$$

which completes the proof. □

Remark 1.10. The maximal of A in the table of Odlyzko [39] is 60.704 (cf. tabel 1.1). Therefore, if the root discriminant of an algebraic number field K exceeds 60.704, then we cannot use the class number upper bound given in (1.3.3).

In order to calculate root discriminants, we have the following lemma by proposition 1.7:

Lemma 1.11. *Let K and K' be algebraic number fields given in proposition* 1.7*. Then we have*

$$\mathrm{rd}(KK') = \mathrm{rd}(K)\mathrm{rd}(K').$$

1.4 Cyclotomic $\mathbb{Z}_p$-extensions of Algebraic Number Fields

We recall that ζ_m is a primitive m-th root of unity in $\mathbb{C}$ for a positive integer m. By Galois theory, the extension $\mathbb{Q}(\zeta_{2p^{n+1}})/\mathbb{Q}$ has an unique real extension $\mathbb{B}_{p,n}$ with degree p^n over $\mathbb{Q}$ for a prime integer p and a non-negative integer n. Since $\mathbb{B}_{p,n} \subset \mathbb{B}_{p,n+1}$ for each non-negative integer n,

$$\mathbb{B}_{p,\infty} := \bigcup_{n=0}^{\infty} \mathbb{B}_{p,n}$$

is a field, which is called *the cyclotomic $\mathbb{Z}_p$-extension of* $\mathbb{Q}$. We note that $\mathbb{B}_{p,\infty}/\mathbb{Q}$ is a Galois extension and the Galois group of $\mathbb{B}_{p,\infty}/\mathbb{Q}$ is isomorphic to $\mathbb{Z}_p$ as topological groups.

For an arbitrary algebraic number field K, We put $K_{p,\infty} := K\mathbb{B}_{p,\infty}$. Then $K_{p,\infty}/K$ is a Galois extension and

$$\mathrm{Gal}(K_{p,\infty}/K) \cong \mathrm{Gal}(\mathbb{B}_{p,\infty}/\mathbb{B}_{p,\infty} \cap K) \cong \mathbb{Z}_p$$

as topological groups. We call $K_{p,\infty}$ *the cyclotomic $\mathbb{Z}_p$-extension of K.*

By Galois theory, there exists an unique intermediate field $K_{p,n}$ of $K_{p,\infty}/K$ with degree p^n over K for each non-negative integer n, which is called *the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of K.*

In the case of $p = 2$ and $K = \mathbb{Q}(\sqrt{5})$, we have

$$K_{2,n} = K_n$$

for each non-negative integer n, where K_n is defined in (0.0.1). Using the upper bound given in (1.3.3), Linden [24] proved the following:

Theorem 1.12 (cf. Linden)**.** *The class numbers of K_1, K_2 and K_3 are 1.*

Since lemma 1.11 implies that

$$\mathrm{rd}(K_n) = \mathrm{rd}(\mathbb{Q}(\sqrt{5}))\mathrm{rd}(\mathbb{B}_n)$$

for each positive integer n, we have

$$\mathrm{rd}(K_n) = \sqrt{5}\cdot 2^{(n+1)-\frac{1}{2^n}} > 68.520$$

for $n \geq 4$. So we cannot use the class number upper bound given in (1.3.3) for K_n with $n \geq 4$.

Then we are interested in ℓ-divisibility of h_n, the class number of K_n, for a prime number ℓ. In the case of $\ell = 2$, since the class number of K_0 is 1, we have the following by applying the result of Iwasawa [23]:

Theorem 1.13 (cf. Iwasawa)**.** *The prime number 2 does not divide h_n for any positive integer n.*

In the case of $\ell \neq 2$, we can apply the result of Washington [41]:

Theorem 1.14 (cf. Washington)**.** *For an odd prime number ℓ, let ℓ^{e_n} be the exact power of ℓ dividing h_n. Then e_n is bounded as n tends to ∞.*

Chapter 2

Explicit Bound of ℓ-indivisibility

In this chapter, we shall recall theorem 0.4 and prove the theorem. For each odd prime number ℓ, theorem 0.4 gives an explicit bound m_ℓ of Washington's theorem for the cyclotomic $\mathbb{Z}_2$-extension for $\mathbb{Q}(\sqrt{5})$. Since $\ell = 5$ divides the discriminant of $\mathbb{Q}(\sqrt{5})$, we deal with the case of $\ell = 5$ separately.

We recall our notations. For an odd prime number ℓ, let δ_ℓ be 0 or 1 according as $\ell \equiv 1 \pmod 4$ or not and 2^{c_ℓ} the exact power of 2 dividing $\ell^{\delta_\ell+1} - 1$. For a real number x, we denote by $\lfloor x \rfloor$ the greatest integer not exceeding x. Then we prove the following:

Theorem 2.1 (Theorem 0.4)**.** *Let ℓ be an odd prime. Put*

$$m_\ell := \begin{cases} 2c_\ell + \lfloor \log_2(5\ell - 1) \rfloor - \delta_\ell - 2 & \text{if } \ell \neq 5, \\ 4 & \text{if } \ell = 5. \end{cases}$$

Then ℓ does not divide h_n/h_{m_ℓ} for any $n \geq m_\ell$.

Remark 2.2. For $\ell = 5$, m_ℓ is derived from

$$m_\ell = 2c_\ell + \lfloor \log_2(\ell - 1) \rfloor - \delta_\ell - 2.$$

Remark 2.3. Since the prime ideal of K_0 lying above 2 is totally ramified in K_n/K_0 for any positive integer n, we have h_n/h_{n-1} is a rational integer.

2.1 The ℓ-parts of the generalized Bernoulli Numbers

Toward the theorem 2.1, we first study the ℓ-parts of the generalized Bernoulli numbers. For an odd prime number ℓ, let v_ℓ be the additive ℓ-adic valuation normalized by $v_\ell(\ell) = 1$. For a non-negative integer n, we put $K'_n := K_n(\zeta_\ell)$. We denote by G_n and G'_n the Galois group of $K_n/\mathbb{Q}$ and $K'_n/\mathbb{Q}$, respectively. We also denote by Δ_ℓ the Galois group of $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$. We define the character $\omega_\ell : \Delta_\ell \to \mathbb{Z}_\ell$ by $\zeta_\ell^\delta = \zeta_\ell^{\omega_\ell(\delta)}$ for all $\delta \in \Delta_\ell$, which is called the Teichimüller character. Then ω_5^2 generates the character group of $\mathrm{Gal}(K_0/\mathbb{Q})$. We remark that there are canonical isomorphisms

$$G'_n \cong \begin{cases} G_n \times \Delta_\ell & \text{if } \ell \neq 5, \qquad (2.1.1) \\ \Gamma_n \times \Delta_\ell & \text{if } \ell = 5, \qquad (2.1.2) \end{cases}$$

where Γ_n denotes the Galois group of $\mathbb{B}_n/\mathbb{Q}$. We denote by ψ_n a character modulo 2^{n+2} whose order is 2^n.

Let f_ℓ be 5 or 5ℓ according as $\ell = 5$ or not and χ a character modulo f_ℓ with $\chi(-1) = -1$. Then we define the generalized Bernoulli number $B_{1,\chi\psi_n}$ by

$$B_{1,\chi\psi_n} = \frac{1}{f_\ell \cdot 2^{n+2}} \sum_{b=1}^{f_\ell \cdot 2^{n+2}} \chi\psi_n(b)b.$$

We remark that we can regard $\chi\psi_n$ as a character $\chi\psi_n : G'_n \to \mathbb{Z}_\ell$. Then we can define the idempotent $e_{\chi\psi_n}$ by

$$e_{\chi\psi_n} := \frac{1}{|G'_n|} \sum_{\sigma \in G'_n} \mathrm{Tr}(\chi^{-1}\psi_n^{-1}(\sigma))\sigma \in \mathbb{Z}_\ell[G'_n],$$

where Tr is the trace mapping from $\mathbb{Q}_\ell(\chi\psi_n(G_n))$ to $\mathbb{Q}_\ell$. Since we can act $e_{\chi\psi_n}$ on A'_n, we put $A'_{n,\chi\psi_n} = e_{\chi\psi_n} A'_n$. The following theorem is a direct consequence of Mazur and Wiles [26, p.216, Theorem 2]:

Theorem 2.4 (Mazur and Wiles). *We have*

$$v_\ell(|A'_{n,\chi\psi_n}|) = (\mathbb{Z}_\ell[\chi\psi_n(G'_n)] : \mathbb{Z}_\ell) v_\ell(B_{1,\chi^{-1}\psi_n^{-1}}). \qquad (2.1.3)$$

Theorem 2.4 implies that $v_\ell(B_{1,\chi\psi_n}) \geq 0$ for each χ. For χ, we also define $f_{1,\chi}(T) \in \mathbb{Q}_\ell(T)$ by

$$f_{1,\chi}(T) := \left(\sum_{\substack{b \equiv 1 \pmod{2^{c_\ell}} \\ 0<b<f_\ell \cdot 2^{c_\ell+1}}} \chi^{-1}(b) T^b \right) \left(T^{f_\ell \cdot 2^{c_\ell+1}} - 1 \right)^{-1}. \tag{2.1.4}$$

Then we have the following by [42, pp.386-387]:

Lemma 2.5. *Let $n \geq 2c_\ell - 1$. If $f_{1,\chi}(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbb{Q}}_\ell$, then $B_{1,\chi^{-1}\psi_n^{-j}} \not\equiv 0 \pmod{\overline{\ell}}$ for any odd integer j, where $\overline{\ell}$ is the ideal of $\mathbb{Z}_\ell[\eta]$ generated by ℓ.*

Lemma 2.6. *If $n \geq m_\ell + 1$, then $f_{1,\chi}(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbb{Q}}_\ell$.*

Proof. We put

$$g(T) = f_{1,\chi}(T)(T^{f_\ell \cdot 2^{c_\ell}} - 1)T^{-1}. \tag{2.1.5}$$

Since χ is a character modulo f_ℓ, we have

$$g(T) = \sum_{\substack{b \equiv 1 \pmod{2^{c_\ell}} \\ 0<b\leq 1+(f_\ell-1)\cdot 2^{c_\ell}}} \chi^{-1}(b) T^{b-1} \in \mathbb{Z}_\ell[T].$$

We denote by $\deg(g)$ the degree of $g(T)$. For all $n \geq m_\ell+1$ and any primitive 2^{n+2}-th root of unity η in $\overline{\mathbb{Q}}_\ell$, we have

$$\begin{aligned} [\mathbb{Q}_\ell(\eta) : \mathbb{Q}_\ell] &= 2^{n+2-c_\ell+\delta_\ell} \\ &\geq 2^{c_\ell + \lfloor \log_2(f_\ell - 1) \rfloor + 1} \\ &> 2^{c_\ell}(f_\ell - 1) \geq \deg(g). \end{aligned}$$

Hence we have $g(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbb{Q}}_\ell$. Thus we have $f_{1,\chi}(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any η. □

Therefore, we obtain the following proposition by lemmas 2.5 and 2.6:

Proposition 2.7. *If $n \geq m_\ell + 1$, then we have $v_\ell(B_{1,\chi^{-1}\psi_n^{-j}}) = 0$ for all odd integer j with $0 \leq j \leq 2^n - 1$.*

2.2 Isomorphisms between $\mathbb{Z}_\ell[\Delta_\ell]$-modules

This section is devoted to the proof of proposition 2.8, which is proved uniformly for the cases of $\ell \neq 5$ and $\ell = 5$. Proposition 2.8 plays an important role for our proof of theorem 2.1.

For an integer i with $0 \leq i \leq \ell - 2$, we define the idempotent e_i by

$$e_i := \frac{1}{\ell - 1} \sum_{\delta \in \Delta_\ell} \omega_\ell^{-i}(\delta)\delta \in \mathbb{Z}_\ell[\Delta_\ell]. \tag{2.2.1}$$

Let A_n and A'_n be the ℓ-Sylow subgroup of $Cl(K_n)$ and $Cl(K'_n)$, respectively. Since natural mappings $A_{n-1} \to A_n$ and $A'_{n-1} \to A'_n$ are injective by lemma 1.2, we can regard A_{n-1} and A'_{n-1} as G_n-submodule of A_n and G'_n-submodule of A'_n, respectively. Let D_n and D'_n be the kernels of the norm mappings $A_n \to A_{n-1}$ and $A'_n \to A'_{n-1}$, respectively. Then we have $A_n = A_{n-1} \oplus D_n$ and $A'_n = A'_{n-1} \oplus D'_n$ again by lemma 1.2.

Let L'_n be the maximal unramified elementary abelian ℓ-extension of K'_n, that is, the maximal unramified abelian extension over K'_n whose Galois group over K'_n is isomorphic to a direct sum of $\mathbb{Z}/\ell\mathbb{Z}$. Note that $L'_n/\mathbb{Q}$ is a Galois extension since $K'_n/\mathbb{Q}$ is a Galois extension. Since $\mathrm{Gal}(L'_n/K'_n)$ is a normal abelian subgroup of $\mathrm{Gal}(L'_n/\mathbb{Q})$, we can act G'_n on $\mathrm{Gal}(L'_n/K'_n)$ by

$$\sigma^g := \tilde{g}\sigma\tilde{g}^{-1},$$

where $\sigma \in \mathrm{Gal}(L'_n/K'_n)$ and $\tilde{g} \in \mathrm{Gal}(L'_n/\mathbb{Q})$ such that the restriction of $\tilde{g}$ to K'_n is equal to g. Therefore, $\mathrm{Gal}(L'_n/K'_n)$ is isomorphic to $A'_n/\ell A'_n$ as G'_n-module by the Artin mapping. By class field theory, we have $\mathrm{Gal}(L'_n/L'_{n-1}K'_n) \cong D'_n/\ell D'_n$. Since

$$\mathrm{Gal}(L'_n/K'_n) \cong A'_n/\ell A'_n \cong A'_{n-1}/\ell A'_{n-1} \oplus D'_n/\ell D'_n,$$

there exists an intermediate field M'_n of L'_n/K'_n such that $\mathrm{Gal}(L'_n/M'_n) \cong A'_{n-1}/\ell A'_{n-1}$ by the Artin mapping. Note that D'_n is a G'_n-submodule of A'_n. Then we have the following:

$$L'_n = M'_n L'_{n-1}, \tag{2.2.2}$$

$$L'_{n-1}K'_n \cap M'_n = K'_n, \tag{2.2.3}$$

$$\mathrm{Gal}(M'_n/K'_n) \cong D'_n/\ell D'_n, \tag{2.2.4}$$

$$M'_n/\mathbb{Q} \text{ is a Galois extension.} \tag{2.2.5}$$

Since $\zeta_\ell \in K'_n$, M'_n/K'_n is a Kummer extension. Then there exists a subgroup V of $K_n'^\times/(K_n'^\times)^\ell$ such that $M'_n = K'_n(\sqrt[\ell]{V})$ in the obvious notation. Since $M'_n/\mathbb{Q}$ is a Galois extension, we can act G'_n on V by

$$\tilde{b}^g = g(b)(K_n'^\times)^\ell,$$

where $\tilde{b} = b(K_n'^\times)^\ell$ for $b \in K_n'^\times$. Let W be the subgroup in $\mathbb{C}^\times$ generated by ζ_ℓ. Then there is a non-degenerate pairing

$$\mathrm{Gal}(M'_n/K'_n) \times V \to W; (h, \tilde{b}) \mapsto \langle h, \tilde{b} \rangle,$$

which is defined by

$$\langle h, \tilde{b} \rangle := \frac{h(\sqrt[\ell]{b})}{\sqrt[\ell]{b}}$$

for all $h \in \mathrm{Gal}(M'_n/K'_n)$ and $\tilde{b} = b(K_n'^\times)^\ell$ and satisfies $\langle h^g, \tilde{b}^g \rangle = \langle h, \tilde{b} \rangle^g$ for all $g \in G'_n$. Then the reflection theorem (cf. Gras [11, pp.18-19]) says the following:

Proposition 2.8. *As abelian groups, we have*

$$e_j V \cong e_i \mathrm{Gal}(M'_n/K'_n) \tag{2.2.6}$$

for integers i, j with $i + j \equiv 1 \pmod{\ell - 1}$.

2.3 The case of $\ell \neq 5$

For $\ell \neq 5$, we prove the following:

Lemma 2.9. *If $e_1(A'_n/A'_{n-1}) = 0$, then $A_n = A_{n-1}$.*

Proof. By (2.2.6), we have

$$\begin{aligned} e_1 V &\cong e_0 \mathrm{Gal}(M'_n/K'_n) \\ &\cong e_0 \left(D'_n/\ell D'_n\right) \\ &= D_n/\ell D_n \cong (A_n/A_{n-1})/\ell(A_n/A_{n-1}). \end{aligned} \tag{2.3.1}$$

We assume that $A_n \neq A_{n-1}$. Then $e_1 V$ is not trivial by (2.3.1). Therefore, there exists $b(K_n'^{\times})^\ell \in e_1 V$ such that the extension $K_n'(\sqrt[\ell]{b})/K_n'$ is non-trivial. Since $K_n'(\sqrt[\ell]{b}) \subset M_n'$, we have

$$L_{n-1}' K_n' \cap K_n'(\sqrt[\ell]{b}) = K_n'. \tag{2.3.2}$$

by (2.2.3). Then there exists an ideal $\mathfrak{b}$ of K_n' whose ideal class belongs to $e_1 V$ and satisfying $\mathfrak{b}^\ell = (b)$, the ideal generated by b in K_n'. Since $e_1(A_n'/A_{n-1}') = e_1 A_n'/e_1 A_{n-1}'$, there exists $d \in K_{n-1}'$ such that $\mathfrak{b}^\ell = (d)$. Hence there exists a unit u of K_n' satisfying $b = du$. This implies that

$$b(K_n'^{\times})^\ell = e_1(b(K_n'^{\times})^\ell) = (e_1(d(K_n'^{\times})^\ell))(e_1(u(K_n'^{\times})^\ell)).$$

Since $e_1(u(K_n'^{\times})^\ell) = \zeta(K_n'^{\times})^\ell$ for some $\zeta \in W$, we have $K_n'(\sqrt[\ell]{b}) \subset L_{n-1}' K_n'$. Therefore, by (2.3.2), we have $K_n'(\sqrt[\ell]{b}) = K_n'$, which contradicts to the choice of $b(K_n'^{\times})^\ell$. □

Then we study $e_1(A_n'/A_{n-1}') \cong e_1 A_n'/e_1 A_{n-1}'$. By (2.1.3) and decomposing $e_1 A_n'$ using ψ_n^j and $\omega_5^2 \psi_n^j$ (cf. Gras [11, Section 3 in Chaper 2]), we can describe the difference between the ℓ-parts of $|e_1 A_n'|$ and $|e_1 A_{n-1}'|$ as follows:

Proposition 2.10. *We have*

$$v_\ell(|e_1 A_n'|) - v_\ell(|e_1 A_{n-1}'|) = \sum_{j=1:\mathrm{odd}}^{2^n-1} \left(v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) + v_\ell(B_{1,\omega_\ell^{-1}\omega_5^{-2}\psi_n^{-j}}) \right).$$

So we study the ℓ-parts of $B_{1,\omega_\ell^{-1}\psi_n^{-j}}$ and $B_{1,\omega_\ell^{-1}\omega_5^{-2}\psi_n^{-j}}$ for odd integer j with $1 \leq j \leq 2^n - 1$. We can obtain the following condition for vanishing the ℓ-parts of $B_{1,\omega_\ell^{-1}\psi_n^{-j}}$ (cf. Fukuda and Komatsu [7, Section 4]):

Proposition 2.11 (Fukuda and Komatsu)**.** *Let $n \geq 2c_\ell + \lfloor \frac{1}{2}\log_2 \ell \rfloor$. Then we have $v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) = 0$ for all odd integer j with $1 \leq j \leq 2^n - 1$.*

We remark that since $m_\ell + 1 \geq 2c_\ell + \lfloor \frac{1}{2}\log_2 \ell \rfloor$ for all odd prime mumber ℓ, proposition 2.11 implies that if $n \geq m_\ell + 1$, we have $v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) = 0$ for all odd integer j with $1 \leq j \leq 2^n - 1$.

By putting $\chi = \omega_\ell \omega_5^2$, proposition 2.7 is reformulated as follows:

Proposition 2.12. *If $n \geq m_\ell + 1$, then we have $v_\ell(B_{1,\omega_\ell^{-1}\omega_5^{-2}\psi_n^{-j}}) = 0$ for all odd integer j with $0 \leq j \leq 2^n - 1$.*

Then the following proposition is immediately obtained by propositions 2.10 thorough 2.12:

Proposition 2.13. *If $n \geq m_\ell + 1$, then we have $e_1 A'_n = e_1 A'_{n-1}$.*

We assume that $n \geq m_\ell$. Then we have $e_1 A'_n = e_1 A'_{n-1} = \cdots = e_1 A'_{m_\ell}$ by proposition 2.13. Therefore, lemma 2.9 says that $A_n = A_{n-1} = \cdots = A_{m_\ell}$. This completes the proof of theorem 2.1 for the case of $\ell \neq 5$.

2.4 The Case of $\ell = 5$

In the case of $\ell = 5$, we cannot obtain the isomorphism (2.3.1) because we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathrm{Gal}(K'_n/\mathbb{B}_n).$$

In order to obtain an isomorphism similar to (2.3.1), we use e_2. Let $\alpha \in A'_n$. Since the 5-part of $Cl(\mathbb{B}_n)$ is trivial for all positive integer n (cf. K. Horie [16, Proposition 3] or Fukuda and Komatsu [7, Corollary 1.3]), we have

$$\begin{aligned} e_2(\alpha) &= \frac{1}{4}\left(\sum_{\sigma \in \mathrm{Gal}(K'_n/K_n)} \sigma - \sum_{\tau \in \mathrm{Gal}(K'_n/\mathbb{B}_n) \setminus \mathrm{Gal}(K'_n/K_n)} \tau\right)\alpha \\ &= \frac{1}{2}\left(\sum_{\sigma \in \mathrm{Gal}(K'_n/K_n)} \sigma\right)\alpha \end{aligned}$$

for all $\alpha \in A'_n$. Therefore, we can regard e_2 as the norm map from A'_n to A_n and (2.2.6) says that

$$\begin{aligned} e_3 V &\cong e_2 \mathrm{Gal}(M'_n/K'_n) \\ &\cong e_2(D'_n/\ell D'_n) \\ &= D_n/\ell D_n \cong (A_n/A_{n-1})/\ell(A_n/A_{n-1}), \end{aligned}$$

which allows us to prove the following by a similar argument in the proof of lemma 2.9:

Lemma 2.14. *If* $e_3(A'_n/A'_{n-1}) = 0$*, then* $A_n = A_{n-1}$.

To describe the difference between the 5-parts of $|e_3A'_n|$ and $|e_3A'_{n-1}|$, we repeat a similar argument in the proof of proposition 2.12:

Proposition 2.15. *We have*

$$v_5(|e_3A'_n|) - v_5(|e_3A'_{n-1}|) = \sum_{j=1:\mathrm{odd}}^{2^n-1} v_5(B_{1,\omega_5^{-3}\psi_n^{-j}}).$$

By putting $\chi = \omega_5^3$, proposition 2.7 is reformulated as follows:

Proposition 2.16. *If* $n \geq m_\ell + 1$*, then we have* $v_5(B_{1,\omega_5^{-3}\psi_n^{-j}}) = 0$ *for all odd integer* j *with* $0 \leq j \leq 2^n - 1$.

Propositions 2.15 and 2.16 allow us to obtain the following:

Proposition 2.17. *If* $n \geq m_\ell + 1$*, then we have* $e_3A'_n = e_3A'_{n-1}$.

By proposition 2.17 and lemma 2.14, we have $A_n = A_{n-1} = \cdots = A_{m_\ell}$ for $n \geq m_\ell$, which completes the proof of theorem 2.1 for the case of $\ell = 5$.

Chapter 3

Numerical Result

In this chapter, we shall recall theorem 0.5. This theorem is derived from theorem 2.1 by a computer calculation. So we give the algorithm to calculate ℓ-indivisibility of h_n.

We recall our result:

Theorem 3.1 (Theorem 0.5). *Let ℓ be an odd prime number less than $6 \cdot 10^4$. Then ℓ does not divide h_n for any positive integer n.*

3.1 General Setting

Let ℓ be an odd prime number less than 10^9. For a character $\chi : G_n \to \mathbb{Z}_\ell$, we define the idempotent e_χ by

$$e_\chi := \frac{1}{|G_n|} \sum_{\sigma \in G_n} \mathrm{Tr}(\chi^{-1}(\sigma))\sigma \in \mathbb{Z}_\ell[G_n], \tag{3.1.1}$$

where Tr is the trace mapping from $\mathbb{Q}_\ell(\chi(G_n))$ to $\mathbb{Q}_\ell$. Since we can act e_χ on A_n, we put $A_{n,\chi} := e_\chi A_n$, which is called the χ-part of A_n. Then we have

$$A_n = \bigoplus_{\chi'} A_{n,\chi'}, \tag{3.1.2}$$

where χ' runs over all representatives of $\mathbb{Q}_\ell$-conjugacy classes of the character group of G_n. Let K_χ be the subfield of K_n corresponding to Kerχ and A_χ the

χ-part of the ℓ-Sylow subgroup of $Cl(K_\chi)$. Then there is a canonical group isomorphism

$$A_{n,\chi} \cong A_\chi. \tag{3.1.3}$$

We rewrite (3.1.2) more concretely. Let ρ be the generator of Γ_n induced by $\zeta_{2^{n+2}} \mapsto \zeta_{2^{n+2}}^5$, σ the generator of $\mathrm{Gal}(K/\mathbb{Q})$ induced by $\zeta_5 \mapsto \zeta_5^2$, and ψ the generator of the character group of Γ_n. We abbreviate ω_5 as ω. We put $F_n = K_n^{\mathrm{Ker}\omega^2\psi}$ and $H_n = \mathrm{Gal}(F_n/\mathbb{Q})$. We define $X \subset \mathbb{Z}$ to make $\{\psi^j | j \in X\}$ be a set of representatives of injective characters of Γ_n. Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of injective characters of H_n.

Noting the isomorphism (3.1.3), we can rewrite (3.1.2) as follows:

$$A_n = A_{n-1} \oplus \bigoplus_{j\in X} A_{n,\psi^j} \oplus \bigoplus_{j\in X} A_{n,\omega^2\psi^j}. \tag{3.1.4}$$

For each $j \in X$, we have $|A_{n,\psi^j}| = 1$ if $\ell < 10^9$ by [9]. Therefore, if it is true that $|A_{n,\omega^2\psi^j}| = 1$ for all $j \in X$, we have $A_n = A_{n-1}$, which implies that ℓ does not divide h_n/h_{n-1}. Since $h_1 = 1$, we may assume that $n \geq 2$.

In order to prove that ℓ does not divide

$$h_{m_\ell} = h_1 \prod_{n=2}^{m_\ell} \frac{h_n}{h_{n-1}},$$

we define a cyclotomic unit ξ_n of K_n. For non-negative integer n, let $\zeta_{5\cdot 2^{n+2}}$ be a primitive $5 \cdot 2^{n+2}$-th root of unity in $\mathbb{C}$. We put $\zeta_{2^{n+2}} = \zeta_{5\cdot 2^{n+2}}^5$ and $\zeta_5 = \zeta_{5\cdot 2^{n+2}}^{2^{n+2}}$. We also put

$$\xi_n = (\zeta_5\zeta_{2^{n+2}} - 1)(\zeta_5\zeta_{2^{n+2}}^{-1} - 1)(\zeta_5^{-1}\zeta_{2^{n+2}} - 1)(\zeta_5^{-1}\zeta_{2^{n+2}}^{-1} - 1) \in K_n.$$

For $\chi = \omega^2\psi^j$ with $j \in X$, we define a truncation $e_{\chi,\ell} \in \mathbb{Z}[G_n]$ of e_χ by

$$e_{\chi,\ell} \equiv e_\chi \pmod{\ell}.$$

Then we can act $e_{\chi,\ell}$ on ξ_n. The following is the special case of [2, Lemma 1]:

Lemma 3.2. *If there exists a prime number p congruent to 1 modulo $5\ell\cdot 2^{n+2}$ and satisfies*

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{\mathfrak{p}} \tag{3.1.5}$$

for some prime ideal $\mathfrak{p}$ of K_n lying above p, then we have $|A_{n,\chi}| = 1$.

Let $s = c_\ell - \delta_\ell$. Then 2^s is the exact power of 2 dividing $\ell - 1$ or $\ell + 1$ according as $\ell \equiv 1 \pmod 4$ or not.

Owing to Lemma 3.2, we may regard χ as a character of G_n into $\overline{\mathbb{F}}_\ell$, where $\overline{\mathbb{F}}_\ell$ is the algebraic closure of $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. Let η_n be a primitive 2^n-th root of unity in $\overline{\mathbb{F}}_\ell$ and

$$L = \mathbb{F}_\ell(\eta_n).$$

We may also define e_χ to be an element of $\mathbb{F}_\ell[G_n]$ and assume that $\psi(\rho) = \eta_n^{-1}$. Then we have

$$e_{\omega^2\psi^j} = \frac{1}{2^{n+1}} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^{ij}) \left(\rho^i - \sigma\rho^i\right). \tag{3.1.6}$$

Now, let p be a prime number satisfying $p \equiv 1 \pmod{5\ell \cdot 2^{n+2}}$ and g_p a primitive root modulo p. Since p is totally decomposed in $\mathbb{Q}(\zeta_{5\cdot 2^{n+2}})/\mathbb{Q}$, there exists a prime ideal $\mathfrak{P}$ in $\mathbb{Q}(\zeta_{5\cdot 2^{n+2}})$ lying above p which satisfies

$$\zeta_{5\cdot 2^{n+2}} \equiv g_p^{\frac{p-1}{5\cdot 2^{n+2}}} \pmod{\mathfrak{P}}.$$

To consider (3.1.5), we can ignore $1/2^{n+1}$ in (3.1.6). Therefore, we put $2^{n+1} e_{\omega^2\psi^j,\ell} = \sum_{i=0}^{2^n-1} a_{ij}(\rho^i - \sigma\rho^i)$, that is,

$$a_{ij} \equiv \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^{ij}).$$

We fix non-negative integers z_1, z_2, z_3, z_4 satisfying

$$\begin{aligned} z_1 &\equiv g_p^{\frac{p-1}{5}} \pmod p, z_2 z_1 \equiv 1 \pmod p, \\ z_3 &\equiv g_p^{\frac{p-1}{2^{n+2}}} \pmod p, z_4 z_3 \equiv 1 \pmod p. \end{aligned}$$

Then we have

$$\begin{aligned} \xi_n^{2^{n+1} e_{\omega^2\psi^j,\ell}} &= \prod_{i=0}^{2^n-1} \left(\frac{(\zeta_5 \zeta_{2^{n+2}}^{5^i} - 1)(\zeta_5 \zeta_{2^{n+2}}^{-5^i} - 1)(\zeta_5^{-1} \zeta_{2^{n+2}}^{5^i} - 1)(\zeta_5^{-1} \zeta_{2^{n+2}}^{-5^i} - 1)}{(\zeta_5^2 \zeta_{2^{n+2}}^{5^i} - 1)(\zeta_5^2 \zeta_{2^{n+2}}^{-5^i} - 1)(\zeta_5^{-2} \zeta_{2^{n+2}}^{5^i} - 1)(\zeta_5^{-2} \zeta_{2^{n+2}}^{-5^i} - 1)} \right)^{a_{ij}} \\ &\equiv \prod_{i=0}^{2^n-1} \left(\frac{(z_1 z_3^{5^i} - 1)(z_1 z_4^{5^i} - 1)(z_2 z_3^{5^i} - 1)(z_2 z_4^{5^i} - 1)}{(z_1^2 z_3^{5^i} - 1)(z_1^2 z_4^{5^i} - 1)(z_2^2 z_3^{5^i} - 1)(z_2^2 z_4^{5^i} - 1)} \right)^{a_{ij}} \pmod{\mathfrak{p}} \end{aligned}$$

with $\mathfrak{p} = \mathfrak{P} \cap K_n$. For convenience, we fix $\zeta(b^i) \in \mathbb{Z}$ satisfying $0 \leq \zeta(b^i) \leq p-1$ and

$$\zeta(b^i) \equiv \frac{(z_1 z_3^{b^i} - 1)(z_1 z_4^{b^i} - 1)(z_2 z_3^{b^i} - 1)(z_2 z_4^{b^i} - 1)}{(z_1^2 z_3^{b^i} - 1)(z_1^2 z_4^{b^i} - 1)(z_2^2 z_3^{b^i} - 1)(z_2^2 z_4^{b^i} - 1)} \pmod{p}$$

for each integer $b \geq 1$ and $i \geq 0$.

We need to determine X, a_{ij} for each positive integer i and $j \in X$ and b explicitly. We treat 4 cases for this purpose.

3.2 The case $\ell \equiv 1 \pmod 4$ and $2 \leq n \leq s$

In this case, we have $L = \mathbb{F}_\ell$. Hence $\mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n) = \eta_n$. Since the choice of η_n is arbitrary, we may assume that

$$\eta_n \equiv g_\ell^{\frac{\ell-1}{2^n}} \pmod{\ell},$$

where g_ℓ is a primitive root modulo ℓ. Since there are 2^{n-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are also 2^{n-1} $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbb{Z} | 1 \leq j \leq 2^n - 1, j \text{ is odd}\}.$$

Then $\{\omega^2 \psi^j | j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s by

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{2^n} ij} \pmod{\ell}$$

for each $0 \leq i \leq 2^n - 1$ and $j \in X$. Then we have the following criterion:

Lemma 3.3. *If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying*

$$\left(\prod_{i=0}^{2^n-1} \zeta(5^i)^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p},$$

then ℓ does not divide h_n/h_{n-1}.

3.3 The case $\ell \equiv 1 \pmod 4$ and $s+1 \leq n$.

In this case, we have $[L : \mathbb{F}_\ell] = 2^{n-s}$. So the minimal polynomial of η_n over $\mathbb{F}_\ell$ is

$$T^{2^{n-s}} - \eta_n^{2^{n-s}}.$$

Therefore, if 2^{n-s} does not divide i, then $\mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^i) = 0$. So we have

$$\begin{aligned} e_{\omega^2\psi^j} &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^{2^{n-s}ij}) \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right) \\ &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_s^{ij}) \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right) \\ &= \frac{1}{2^{s+1}} \sum_{i=0}^{2^s-1} \eta_s^{ij} \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right). \end{aligned}$$

Since there are 2^{s-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are also 2^{s-1} $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbb{Z} | 1 \leq j \leq 2^s - 1, j \text{ is odd}\}.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv g_\ell^{\frac{p-1}{2^s}ij} \pmod \ell$$

for each $0 \leq i \leq 2^s - 1$ and $j \in X$. Then we have the following criterion:

Lemma 3.4. *If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying*

$$\left(\prod_{i=0}^{2^s-1} \zeta(5^{2^{n-s}i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p,$$

then ℓ does not divide h_n/h_{n-1}.

3.4 The case $\ell \equiv 3 \pmod 4$ and $2 \le n \le s$

In this case, we have $[L : \mathbb{F}_\ell] = 2$. Hence we obtain

$$\mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n) = \eta_n + \eta_n^\ell.$$

Since there are 2^{n-2} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are also 2^{n-2} $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbb{Z} | 1 \le j \le 2^{n-1} - 1, j \text{ is odd}\}.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv t_{2^{s+1-n}ij} \pmod \ell$$

for each $0 \le i \le 2^n - 1$ and $j \in X$, where t_i's are elements in $\mathbb{F}_\ell$ defined in (3.5.1) in section 3.5. Then we have the following criterion:

Lemma 3.5. *If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying*

$$\left(\prod_{i=0}^{2^n-1} \zeta(5^i)^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p,$$

then ℓ does not divide h_n/h_{n-1}.

3.5 The case $\ell \equiv 3 \pmod 4$ and $s + 1 \le n$

In this case, we have $[L : \mathbb{F}_\ell] = 2^{n-s}$. Let

$$T^2 - aT - 1$$

be the minimal polynomial of η_{s+1} over $\mathbb{F}_\ell$. Then the minimal polynomial of η_n over $\mathbb{F}_\ell$ is

$$T^{2^{n-s}} - aT^{2^{n-s-1}} - 1.$$

Thus if 2^{n-s-1} does not divide i, then $\mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^i) = 0$. Therefore, we have

$$\begin{aligned} e_{\omega^2\psi^j} &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_n^{2^{n-s-1}ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right) \\ &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{L/\mathbb{F}_\ell}(\eta_{s+1}^{ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right) \\ &= \frac{1}{2^{s+2}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right). \end{aligned}$$

We put

$$t_i = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i). \tag{3.5.1}$$

We need to calculate t_i's. Fukuda and Komatsu showed the following two lemmas in [7, Lemmas 3.3 and 3.6]:

Lemma 3.6 (Fukuda and Komatsu)**.** *Put $a_2 = 0 \in \mathbb{F}_\ell$ and define $a_i \in \mathbb{F}_\ell$ for all $3 \le i \le s+1$ by the recursive formula*

$$\begin{aligned} a_i &= \sqrt{2 + a_{i-1}} \quad (3 \le i \le s), \\ a_{s+1} &= \sqrt{-2 + a_s}. \end{aligned}$$

Then we have $t_1 = a_{s+1}$.

Proof. We recall that

$$t_i = \eta_{s+1}^i + \eta_{s+1}^{i\ell}$$

for all integer i. Noting that $\eta_{s+1}^{\ell+1} = -1$, we obtain

$$\begin{aligned} t_2 &= \eta_{s+1}^2 + \eta_{s+1}^{2\ell} \\ &= (\eta_{s+1} + \eta_{s+1}^\ell)^2 - 2\eta_{s+1}^{(\ell+1)} \\ &= (\eta_{s+1} + \eta_{s+1}^\ell)^2 + 2 \\ &= t_1^2 + 2 \end{aligned}$$

and

$$\begin{aligned}t_{2^k} &= \eta_{s+1}^{2^k} + \eta_{s+1}^{2^k\ell}\\ &= (\eta_{s+1}^{2^{k-1}} + \eta_{s+1}^{2^{k-1}\ell})^2 - 2\eta_{s+1}^{2^{k-1}(\ell+1)}\\ &= (\eta_{s+1}^{2^{k-1}} + \eta_{s+1}^{2^{k-1}\ell})^2 - 2\\ &= t_{2^{k-1}}^2 - 2\end{aligned}$$

for all integer k with $2 \leq k \leq s-1$. Since

$$t_{2^{s-1}} = t_{2^{s-2}}^2 - 2 = 0,$$

we obtain the lemma by reversing the above procedure. □

Remark 3.7. For each step, we have two square roots. So we have just 2^{s-1} instances of t_1. Since they correspond to the 2^{s-1} non-conjugate primitive 2^{s+1}-th roots of unity in $\overline{\mathbb{F}}_\ell$, we fix an arbitrary one.

Lemma 3.8 (Fukuda and Komatsu)**.** *We have* $t_{i+2} = t_1 t_{i+1} + t_i$ *for all* $i \geq 0$.

Proof. A straightforward calculation gives

$$\begin{aligned}t_1 t_{i+1} &= (\eta_{s+1} + \eta_{s+1}^{\ell})(\eta_{s+1}^{i+1} + \eta_{s+1}^{(i+1)\ell})\\ &= (\eta_{s+1}^{i+2} + \eta_{s+1}^{(i+2)\ell}) + \eta_{s+1}^{\ell+1}(\eta_{s+1}^{i} + \eta_{s+1}^{i\ell})\\ &= t_{i+2} - t_i,\end{aligned}$$

which completes the proof. □

Since there are 2^{s-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are also 2^{s-1} $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbb{Z} : \text{odd} | 1 \leq j \leq 2^{s-1} \text{ or } 2^s + 1 \leq j \leq 2^s + 2^{s-1} - 1\}.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv t_{ij} \pmod{\ell}$$

for each $0 \leq i \leq 2^{s+1} - 1$ and $j \in X$. Then we have the following criterion:

Lemma 3.9. *If for each* $j \in X$*, there exists a prime number* p *congruent to 1 modulo* $5\ell \cdot 2^{n+2}$ *satisfying*

$$\left(\prod_{i=0}^{2^{s+1}-1} \zeta(5^{2^{n-s-1}i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p},$$

then ℓ *does not divide* h_n/h_{n-1}.

3.6 The Logarithmic Algorithm

It takes too much time to verify that an odd prime number ℓ with large s does not divide h_{m_ℓ} with the previous criteria. For example, it takes more than 3 weeks with a computer calculation by Mathematica 9 to verify that $6143 = 3 \cdot 2^{11} - 1$ does not divide h_{35}.

To obtain theorem 3.1, we need to verify that $8191 = 2^{13} - 1$ does not divide h_{40}. Thus we are led to a logarithmic version of the previous criteria (cf. Aoki [1, Theorem 13]).

For $x \in \mathbb{F}_p^\times$, let $\nu_p(x)$ be the unique non-negative integer less than p satisfying

$$x = g_p^{\nu_p(x)}.$$

The calculation of $\nu_p(x)$ is considered hard for large p. But $\nu_p(x)$ modulo ℓ is enough for our purpose. Let $\nu_p(x) = i + j\ell$ with $0 \leq i < \ell$. Then we can determine i by

$$x^{\frac{p-1}{\ell}} = \left(g_p^{i+j\ell}\right)^{\frac{p-1}{\ell}} = \left(g_p^{\frac{p-1}{\ell}}\right)^i.$$

Hence we can fix $x_i \in \mathbb{Z}$ satisfying $0 \leq x_i < \ell$ and

$$x_i \equiv \nu_p(\zeta(b^i)) \pmod{\ell},$$

where b is defined by

$$b = \begin{cases} 5 & \text{if } 2 \leq n \leq s, \\ 5^{2^{n-c_\ell}} & \text{if } s+1 \leq n. \end{cases}$$

We also put r by

$$r = \begin{cases} n & \text{if } 2 \leq n \leq s, \\ c_\ell & \text{if } s+1 \leq n. \end{cases}$$

Then we obtain the following criterion as the logarithmic version of lemmas 3.3 through 3.5 and 3.9:

Lemma 3.10. *If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying*

$$\sum_{i=0}^{2^r-1} a_{ij} x_i \not\equiv 0 \pmod{\ell},$$

then ℓ does not divide h_n/h_{n-1}.

Lemma 3.10 allows us to verify that if an odd prime number ℓ satisfies that $\ell = 8191$ or $10^4 < \ell < 6 \cdot 10^4$, then ℓ does not divide h_n for any positive integer n.

Chapter 4

Establishing an Upper Bound of Class numbers

In this chapter, we explain Miller's method in [28] to establish an upper bound of class numbers of totally real algebraic number fields with large root discriminants. The root discriminant of an algebraic number field is defined by (1.3.1). Without knowledge of prime ideals or non-trivial zeros of the Dedekind zeta functions, we cannot obtain any upper bound of class numbers of algebraic number fields with large root discriminants. In order to establish an upper bound of class numbers of those algebraic number fields, we need to study prime ideals of totally real algebraic number fields.

4.1 Another Unconditional Upper Bound of Class Numbers

In this section, we shall show another upper bound of class numbers of totally real number fields except that given in section 1.3. Let K be an algebraic number field with degree n and r_1 real embeddings into $\mathbb{C}$. We denote by N_K the absolute norm map of the ideal group of K. We define γ by

$$\gamma = \lim_{m\to\infty}\left(\sum_{k=1}^{m}\frac{1}{k} - \log m\right),$$

the Euler constant. Then we have the following by Poitou [40]:

Theorem 4.1 (Poitou)**.** *Let $F : \mathbb{R} \to \mathbb{R}$ be a Schwarz function satisfying $F(0) = 1$ and $F(-x) = F(x)$ for all $x \in \mathbb{R}$. For each $s \in \mathbb{C}$, the transformation Φ of F is defined by*

$$\Phi(s) := \int_{-\infty}^{\infty} F(x) \mathrm{e}^{(s-\frac{1}{2})x} dx.$$

Then we have

$$\begin{aligned} \log |d(K)| = r_1 \frac{\pi}{2} + n(\gamma + \log 8\pi) - n \int_0^\infty \frac{1 - F(x)}{2 \sinh \frac{x}{2}} dx \\ -r_1 \int_0^\infty \frac{1 - F(x)}{2 \cosh \frac{x}{2}} dx - 4 \int_0^\infty F(x) \cosh \frac{x}{2} dx \\ + \sum_\rho \Phi(\rho) + 2 \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{\log N_K \mathfrak{p}}{N_K \mathfrak{p}^{m/2}} F(m \log N_K \mathfrak{p}), \end{aligned} \tag{4.1.1}$$

where ρ runs over all non-trivial zeros of the Dedekind zeta function of K which satisfies that $0 < \mathrm{Re}(\rho) < 1$ and $\mathfrak{p}$ runs over all finite prime ideals of K.

Remark 4.2. In theorem 4.1, the choice of F does not depend on a totally real field K.

First, following Miller [28], we shall establish an unconditional upper bound of class numbers of totally real algebraic number fields:

Proposition 4.3 (Miller)**.** *Let K be a totally real number field with degree n. We define $F_c : \mathbb{R} \to \mathbb{R}$ by*

$$F_c(x) := \frac{\mathrm{e}^{-(x/c)^2}}{\cosh \frac{x}{2}} \tag{4.1.2}$$

for each $c \in \mathbb{R}_{>0}$. We put

$$\mathfrak{C} = \frac{\pi}{2} + \gamma + \log 8\pi, \tag{4.1.3}$$

$$\mathfrak{g}(c) = \int_0^\infty \frac{1 - F_c(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx. \tag{4.1.4}$$

If it is true that

$$\mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K) > 0, \tag{4.1.5}$$

then we have

$$h(K) < \frac{2c\sqrt{\pi}}{n\left(\mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K)\right)}.$$

Proof. For a totally real field K with degree n, we note that $d(K) > 0$. Then the equation (4.1.1) is rewritten as follows:

$$\begin{aligned}\log d(K) = n\mathfrak{C} - n\int_0^\infty \frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}} + \frac{1}{\cosh\frac{x}{2}}\right)dx \\ -4\int_0^\infty F(x)\cosh\frac{x}{2}dx + \sum_\rho \Phi(\rho) \\ +2\sum_{\mathfrak{p}}\sum_{m=1}^\infty \frac{\log N_K\mathfrak{p}}{N_K\mathfrak{p}^{m/2}}F(m\log N_K\mathfrak{p}).\end{aligned} \tag{4.1.6}$$

Let $H(K)$ be the Hilbert class field of K. Since K is totally real, $H(K)$ is also totally real. Putting $F = F_c$ with positive real number c, we have

$$\int_0^\infty F_c(x)\cosh\frac{x}{2}dx = \int_0^\infty \mathrm{e}^{-(x/c)^2}dx = \frac{c\sqrt{\pi}}{2}.$$

Then we obtain

$$\begin{aligned}\log d(H(K)) = h(K)n\mathfrak{C} - h(K)n\mathfrak{g}(c) - 2c\sqrt{\pi} + \sum_{\rho'}\Phi(\rho') \\ +2\sum_{\mathfrak{P}}\sum_{m=1}^\infty \frac{\log N_{H(K)}\mathfrak{P}}{N_{H(K)}\mathfrak{P}^{m/2}}F(m\log N_{H(K)}\mathfrak{P}),\end{aligned} \tag{4.1.7}$$

where ρ' runs over all non-trivial zeros of the Dedekind zeta function of $H(K)$ which satisfies that $0 < \mathrm{Re}(\rho') < 1$ and $\mathfrak{P}$ runs over all finite prime ideals of $H(K)$. By (1.3.2), we obtain

$$\log d(H(K)) = h(K)n\log \mathrm{rd}(K).$$

Since

$$\sum_{\rho'}\Phi(\rho') > 0 \text{ and } 2\sum_{\mathfrak{P}}\sum_{m=1}^\infty \frac{\log N_{H(K)}\mathfrak{P}}{N_{H(K)}\mathfrak{P}^{m/2}}F_c(m\log N_{H(K)}\mathfrak{P}) > 0$$

for $F = F_c$, we have an inequality

$$h(K)n\left(\mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K)\right) < 2c\sqrt{\pi}$$

If the inequality (4.1.5) holds, then we have

$$h(K) < \frac{2c\sqrt{\pi}}{n\left(\mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K)\right)},$$

which completes the proof. □

Remark 4.4. If a totally real field K has the root discriminant greater than $4\pi e^{\gamma+1} = 60.839$, then we cannot establish an upper bound of the class number of K by proposition 4.3.

4.2 Miller's Upper Bound of Class Numbers

As we mentioned in section 1.4, the root discriminant of K_n is greater than 68.520 if $n \geq 4$. So we cannot establish an upper bound of the class numbers of either K_4 or K_5 by proposition 4.3.

To establish an upper bound of class numbers of algebraic number fields with large discriminant, we shall follow Miller's work in [28] to study

$$2\sum_{\mathfrak{P}}\sum_{m=1}^{\infty} \frac{\log N_{H(K)}\mathfrak{P}}{N_{H(K)}\mathfrak{P}^{m/2}} F_c(m \log N_{H(K)}\mathfrak{P}) \tag{4.2.1}$$

more precisely.

Let K be a totally real field with degree n. We denote by $S(K)$ the set of all prime numbers each of which splits completely into a product of principal prime ideals of K. By class field theory, we have following:

Proposition 4.5. *Let $H(K)$ be the Hilbert class field of K. A prime ideal $\mathfrak{p}$ of K splits completely in $H(K)/K$ if and only if $\mathfrak{p}$ is a principal ideal.*

We assume that $q \in S(K)$. Then q splits completely in $H(K)/\mathbb{Q}$ by proposition 4.5, which implies that the number of prime ideals in $H(K)$ lying above q is $h(K)n$. Since we have

$$N_{H(K)}\mathfrak{Q} = q$$

for each prime ideal $\mathfrak{Q}$ in $H(K)$ lying above q, we obtain

$$\begin{aligned}
&2\sum_{\mathfrak{P}}\sum_{m=1}^{\infty}\frac{\log N_{H(K)}\mathfrak{P}}{N_{H(K)}\mathfrak{P}^{m/2}}F_c(m\log N_{H(K)}\mathfrak{P})\\
&\geq 2\sum_{q\in S(K)}\sum_{\mathfrak{Q}|q}\sum_{m=1}^{\infty}\frac{\log q}{q^{m/2}}F_c(m\log q)\\
&=2h(K)n\sum_{q\in S(K)}\sum_{m=1}^{\infty}\frac{\log q}{q^{m/2}}F_c(m\log q).
\end{aligned}$$

Using the above inequality, we obtain a generalization of proposition 4.3 as follows:

Proposition 4.6 (Miller)**.** *Let K be a totally real algebraic number field with degree n. For a subset T of $S(K)$ and real number c, we put*

$$B(c,T)=\mathfrak{C}-\mathfrak{g}(c)-\log\mathrm{rd}(K)+2\sum_{q\in T}\sum_{m=1}^{\infty}\frac{\log q}{q^{m/2}}F_c(m\log q). \tag{4.2.2}$$

If it is true that

$$B(c,T)>0 \tag{4.2.3}$$

for some c and T, then we have

$$h(K)<\frac{2c\sqrt{\pi}}{B(c,T)}. \tag{4.2.4}$$

Chapter 5

An Upper bound of the Class number of K_5

In this chapter, we shall establish an upper bound for the class number of K_5 using Miller's method introduced in the previous chapter.

We recall our results:

Theorem 5.1 (Theorem 0.6). *The class number of K_5 is at most 133.*

Considering that h_5 has no prime factor ℓ less than 60000 by theorem 3.1, we have $h_5 = 1$. Moreover, remark 2.3 says that $h_5 = 1$ implies $h_4 = 1$. Thus we obtain the following result:

Theorem 5.2 (Theorem 0.7). *The class numbers of K_4 and K_5 are 1.*

In section 5.2, we shall prove that h_4 is at most 518 without the knowledge of theorem 5.1.

5.1 Integral Bases of K_n

In order to prove theorem 5.1, we need to construct a subset of $S(K_n)$ which contains many small prime numbers. We recall that $S(K_n)$ is the set of all prime numbers each of which splits completely into a product of principal prime ideals of K_n . To verify whether a prime number p is in $S(K_n)$, we use the following lemma:

Lemma 5.3. *A prime number p is contained in $S(K_n)$ if and only if there exists an algebraic integer α of K_n which satisfies that*

$$p = |N_{K_n/\mathbb{Q}}(\alpha)|, \tag{5.1.1}$$

the absolute value of the norm map of α form K_n to $\mathbb{Q}$.

Proof. Let $p \in S(K_n)$ and $\mathfrak{p}$ a prime ideal in K_n lying above p. Then there exists an algebraic integer α of K_n satisfying

$$\mathfrak{p} = (\alpha).$$

Therefore, we have

$$|N_{K_n/\mathbb{Q}}(\alpha)| = N_{K_n}\mathfrak{p} = p.$$

Conversely, we assume that there exists an algebraic integer α in K_n which satisfies (5.1.1) for a prime number p. Then the ideal $\mathfrak{p} = (\alpha)$ is a prime ideal of K_n lying above p. Since $K_n/\mathbb{Q}$ is a Galois extension, all prime ideals of K_n lying above p is principal. For $p = 2$ or $p = 5$, it is not possible to satisfy the equation (5.1.1) for any algebraic integer α. Thus p is unramified in $K_n/\mathbb{Q}$.

Therefore, p spilts completely into a product of principal prime ideals of K_n, which implies that $p \in S(K_n)$. This completes the proof. □

In order to apply lemma 5.3, we need to give an integral basis of K_n. We put

$$\omega = \frac{1+\sqrt{5}}{2}.$$

Then $\{1, \omega\}$ is an integral basis of $\mathbb{Q}(\sqrt{5})$ (cf. example 1.3). Since $K_n = \mathbb{B}_n \cdot \mathbb{Q}(\sqrt{5})$ and the discriminants of $\mathbb{B}_n$ and $\mathbb{Q}(\sqrt{5})$ are coprime, we obtain an integral basis of K_n by propositions 1.5 and 1.7 as follows:

Lemma 5.4. *For each rational integer j with $0 \leq j \leq 2^{n+1} - 1$, we put*

$$u_j = \begin{cases} \left(2\cos\frac{2\pi}{2^{n+2}}\right)^j & \text{if } 0 \leq j < 2^n, \\ \omega u_{j-2^n} & \text{if } 2^n \leq j < 2^{n+1}. \end{cases}$$

Then the set

$$\mathfrak{B}_1 := \{u_0, u_1, u_2, \cdots, u_{2^{n+1}-1}\} \tag{5.1.2}$$

forms an integral basis of K_n.

Though we obtain an integral basis of K_n, $\mathfrak{B}_1$ is not enough for our purpose. We recall that we need to establish a subset T of $S(K_n)$ which satisifies that

$$B(c,T) = \mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K_n) + 2\sum_{q\in T}\sum_{m=1}^{\infty} \frac{\log q}{q^{m/2}} F_c(m\log q) > 0$$

with some real number c. Since F_c is a Schwarz function, we need T to contain many small prime numbers. If we obtain an algebraic integer α of K_n by

$$\alpha = a_0u_0 + a_1u_1 + \cdots + a_{2^{n+1}-1}u_{2^{n+1}-1}$$

with rational integers a_i's each of which satisfies that $|a_i| \leq 2$, then it is very hard to find α with small absolute value of $N_{K_n/\mathbb{Q}}(\alpha)$.

In order to find an algebraic integer α of K_n with small absolute value of $N_{K_n/\mathbb{Q}}(\alpha)$, we cite Cerri's work in [4]:

Theorem 5.5 (Cerri). *Let n be a positive integer. For each rational integer j with $0 \leq j < 2^n$, we put*

$$e_j = \begin{cases} 1 & \text{if } j = 0, \\ 2\cos\frac{2j\pi}{2^{n+2}} & \text{if } 1 \leq j < 2^n. \end{cases}$$

Then

$$\{e_0, e_1, \cdots, e_{2^n-1}\}$$

is an integral basis of $\mathbb{B}_n$ and satisfies the follwing;

(i) $\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_0) = \mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_0^2) = 2^n$ *and* $\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_j) = 0$ *for* $j \neq 0$.

(ii) $\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_j^2) = 2^{n+1}$ *for* $j \neq 0$ *and* $\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_ie_j) = 0$ *for* $i \neq j$.

Proof. For convenience, we put

$$\zeta = \zeta_{2^{n+2}}.$$

Then we recall that

$$\{1, \zeta+\zeta^{-1}, (\zeta+\zeta^{-1})^2, \cdots, (\zeta+\zeta^{-1})^{2^n-1}\}$$

is an integral basis of $\mathbb{B}_n$ by proposition 1.5. Since

$$e_j = \zeta^j + \zeta^{-j}$$

for each integer $1 \leq j \leq 2^n - 1$, we have

$$w_j := (\zeta + \zeta^{-1})^j = \sum_{k=0}^{j} \binom{j}{k} \zeta^{2k-j} = \sum_{k=0}^{\lfloor \frac{j}{2} \rfloor} \binom{j}{k} e_{j-2k}.$$

Therefore, there exists a $2^n \times 2^n$-matrix M such that

$$\begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_{2^n-1} \end{pmatrix} = M \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{2^n-1} \end{pmatrix}$$

and whose all components are rational integers. Since M is a lower triangular matrix and each diagonal component of M is 1, we have $M \in \mathrm{GL}(2^n, \mathbb{Z})$. Thus

$$\{e_0, e_1, \cdots, e_{2^n-1}\}$$

is an integral basis of $\mathbb{B}_n$.

(i) Trivially, we have

$$\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_0) = \mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_0^2) = \mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(1) = 2^n$$

We assume that $j \neq 0$. We denote by Γ_n the Galois group of $\mathbb{B}_n/\mathbb{Q}$. Then we have

$$\begin{aligned} \mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_j) &= \sum_{\sigma \in \Gamma_n} \sigma(e_j) = \sum_{k=0}^{2^n-1} (\zeta^{j(2k+1)} - \zeta^{-j(2k+1)}) \\ &= 2 \sum_{k=0}^{2^n-1} \mathrm{Re}(\zeta^{j(2k+1)}) = 2\mathrm{Re}\left(\zeta^j \sum_{k=0}^{2^n-1} \zeta^{2jk}\right) \\ &= 2\mathrm{Re}\left(\zeta^j \frac{1-\zeta^{2^{n+1}j}}{1-\zeta^{2j}}\right) = 2\mathrm{Re}\left(\frac{1-\zeta^{2^{n+1}j}}{\zeta^{-j}-\zeta^j}\right). \end{aligned}$$

If j is even, we have

$$\frac{1-\zeta^{2^{n+1}j}}{\zeta^{-j}-\zeta^{j}}=0.$$

If j is odd, we have

$$\frac{1-\zeta^{2^{n+1}j}}{\zeta^{-j}-\zeta^{j}}=\frac{2}{\zeta^{-j}-\zeta^{j}},$$

which is a pure imaginary number. Therefore, we have $\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_j)=0$.

(ii) We assume that $j=0$ and $i\neq 0$. Then the property of (ii) is obvious by (i). So we assume that $ij\neq 0$. Then we have

$$e_ie_j=(\zeta^{i+j}+\zeta^{-(i+j)})+(\zeta^{i-j}+\zeta^{-(i-j)}).$$

We remark that $2\leq i+j<2^{n+1}$. If $i+j=2^n$, then we have $\zeta^{i+j}+\zeta^{-(i+j)}=0$. By a similar argument in (i), we can show

$$\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(\zeta^{i+j}+\zeta^{-(i+j)})=0$$

for each i and j with $1\leq i,j\leq 2^n-1$. If $i\neq j$, we have

$$\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(\zeta^{i-j}+\zeta^{-(i-j)})=0$$

again by (i). If $i=j$, we have $\zeta^{i-j}+\zeta^{-(i-j)}=2$ and

$$\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(e_j^2)=\mathrm{Tr}_{\mathbb{B}_n/\mathbb{Q}}(2)=2^{n+1}.$$

This completes the proof. □

Remark 5.6. The properties of the integral basis of $\mathbb{B}_n$ given in theorem 5.5 are important to calculate the discriminant of $\mathbb{B}_n$. As a cororally of theorem 5.5, we have the following (cf. Cerri [4] or equation (1.2.1)):

$$d(\mathbb{B}_n)=2^{(n+1)2^n-1}.$$

We put

$$v_j=\begin{cases}e_j & \text{if } 0\leq j<2^n,\\ \omega e_{j-2^n} & \text{if } 2^n\leq j<2^{n+1}.\end{cases}$$

Then we have another integral basis of K_n except that given in lemma 5.4:

Lemma 5.7. *The following subset of K_n is an integral basis of K_n ;*

$$\mathfrak{B} := \{v_0, v_1, v_2, \cdots, v_{2^{n+1}-1}\}.$$

Remark 5.8. For each element v of $\mathfrak{B}$, there exists a element v' of $\mathfrak{B}$ such that v and v' are Galois conjugate. An integral basis of $\mathfrak{B}_1$ does not have such a property. Owing to this property, an algebraic integer obtained by a linear combination of $\mathfrak{B}$ over $\mathbb{Z}$ tends to have small absolute value of the norm.

5.2 Construction of a Subset of $S(K_4)$

As an easy example, we calculate norms of algebraic integers of K_4 and construct an upper bound of the class number of K_4 without the knowledge of theorem 5.1. The integral basis of K_4 given in lemma 5.7 is as follows:

$$v_j = \begin{cases} 1 & (j = 0), \\ \zeta_{64}^{j} + \zeta_{64}^{-j} = 2\cos(\frac{2j\pi}{64}) & (1 \le j < 16), \\ \omega v_{j-16} & (16 \le j < 32). \end{cases}$$

Using a computer, we can verify the following:

Lemma 5.9. *Put*

$$\gamma_1 := v_1 + v_3 + v_5 + v_9 - v_{16},$$
$$\gamma_2 := v_5 + v_{15} - v_{16}.$$

Then we have

$$|N_{K_4/\mathbb{Q}}(\gamma_1)| = 191,$$
$$|N_{K_4/\mathbb{Q}}(\gamma_2)| = 449.$$

Remark 5.10. 191 and 449 are the first two smallest prime numbers each of which splits completely in K_4.

We put $T := \{191, 449\}$ and $c = 210$. Then we have

$$2\sum_{p\in T}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F_{210}(m\log p) > 0.1643.$$

Therefore, we have

$$\begin{aligned}\mathfrak{C} - \mathfrak{g}(c) - \log \mathrm{rd}(K_4) + 2\sum_{p\in T}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F_{210}(m\log p) &> 0.1643 - 0.1193 \\ &= 0.0449,\end{aligned}$$

which implies that

$$h(K_4) \leq \left\lfloor \frac{420\sqrt{\pi}}{32\cdot 0.0449} \right\rfloor = 518 \tag{5.2.1}$$

by lemma 4.6. Therefore, we have the following:

Proposition 5.11. *The class number of K_4 is at most* 518.

5.3 Construction of a Subset of $S(K_5)$

To establish an upper bound of the class number of K_5, we construct a subset T_0 of $S(K_5)$ to apply lemma 4.6. The case of K_5 is much more complicated than that of K_4 because we need to verify that a large number of small prime numbers are in $S(K_5)$ for our result. For each rational integer j with $0 \leq j < 64$, we put

$$v_j := \begin{cases} 1 & (j = 0), \\ \zeta_{128}^{j} + \zeta_{128}^{-j} = 2\cos(\frac{2j\pi}{128}) & (1 \leq j < 32), \\ \omega v_{j-32} & (32 \leq j < 64). \end{cases}$$

Then

$$\{v_j \mid j \text{ is an integer with } 0 \leq j < 64\}$$

is an integral basis of K_5 by lemma 5.7.

We consider an algebraic integer α in K_5 of the form

$$\alpha = \sum_{k=1}^{8} a_k v_{j_k}, \tag{5.3.1}$$

where j_k's are integers with $0 \leq j_1 < \cdots < j_6 < 32 \leq j_7 < j_8 < 64$ and a_k's are integers with $-2 \leq a_k \leq 2$. We denote by A the set of $\alpha \in \mathfrak{O}_{K_5}$ of the form (5.3.1). For convenience, we put

$$N(\alpha) := |N_{K_5/\mathbb{Q}}(\alpha)|$$

for all algebraic integer α in K_5. We also put

$$\begin{aligned} U &:= \{N(\alpha) \mid \alpha \in A\}, \\ U_1 &:= \left\{m \in U \mid \text{all prime factors of } m \text{ are less than } 10^9\right\}, \\ T_1 &:= \{p \in U_1 \mid p \text{ is a prime number}\}. \end{aligned}$$

Then we have $T_1 \subset S(K_5)$. However, T_1 is not enough to give an upper bound of $h(K_5)$. So we use the following lemma.

Lemma 5.12. *Let p, q be distinct prime numbers and assume that $p \in S(K_5)$. If there exists an algebraic integer α in K_5 satisfying $N(\alpha) = pq$, then it is also true that $q \in S(K_5)$.*

Proof. We denote the prime ideal factorization of (α) in K_5 by

$$(\alpha) = \mathfrak{p}\mathfrak{q},$$

where $\mathfrak{p}$ is a prime ideal lying above p and $\mathfrak{q}$ is a prime ideal lying above q. Since $p \in S(K_5)$, there exists an algebraic integer β in K_5 such that $\mathfrak{p} = (\beta)$. Therefore we have

$$(\alpha/\beta) = \mathfrak{q}.$$

Since α/β is an algebraic integer in K_5 satisfying

$$N(\alpha/\beta) = N_{K_5}\mathfrak{q} = q,$$

we conclude $q \in S(K_5)$ by lemma 5.3. $\square$

We define U_{n+1} and T_{n+1} recursively by

$$U_{n+1} := \left\{ \frac{m}{p} \mid m \in \bigcup_{k=1}^{n} U_k,\ p \in \bigcup_{k=1}^{n} T_k \text{ and } \frac{m}{p} \text{ is an integer} \right\},$$
$$T_{n+1} := \{ q \in U_{n+1} \mid q \text{ is a prime} \}$$

for all positive integer n. Lemma 5.12 implies that $T_n \subset S(K_5)$ for all positive integer n.

We define T_0 by

$$T_0 := \bigcup_{k=1}^{\infty} T_k. \tag{5.3.2}$$

This T_0 is what we want to obtain the upper bound given in theorem 5.1.

Remark 5.13. Since A is a finite set, there exists some integer M which satisfies that $T_n = \emptyset$ for all integer $n \geq M$. In our case, we have $T_n = \emptyset$ if $n \geq 5$.

5.4 Proof of Theorem 5.1

We prove theorem 5.1 using the subset T_0 of $S(K_5)$ constructed in section 5.3. For $c = 210$, we have

$$\mathfrak{C} - \mathfrak{g}(210) - \log \operatorname{rd}(K_5) > -0.8341$$

and

$$2 \sum_{p \in T_0} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F_{210}(m \log p) > 0.9212.$$

Therefore we have

$$\begin{aligned} \mathfrak{C} - \mathfrak{g}(210) - \log \operatorname{rd}(K_5) + 2 \sum_{p \in T_0} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F_{210}(m \log p) &> -0.8341 + 0.9212 \\ &= 0.0871. \end{aligned}$$

Proposition 4.6 says that

$$h(K_5) \leq \left\lfloor \frac{420\sqrt{\pi}}{64 \cdot 0.0871} \right\rfloor = 133.$$

This completes the proof of theorem 5.1.

5.5 Examples of the Elements of T_0

Finally, we give several examples of prime numbers contained in T_0. The set of the ten smallest primes which split completely in $K_5/\mathbb{Q}$ is

$$P := \{641, 769, 1151, 1279, 1409, 2689, 3329, 4481, 5119, 6271\}.$$

We can verify that $P \subset T_0$. For positive integer i with $i \leq 10$, we define an algebraic integer α_i in K_5 by

$$\begin{aligned}
\alpha_1 &:= -v_{13} - v_{14} + v_{16} + v_{17} + v_{32},\\
\alpha_2 &:= v_7 + v_8 - v_{10} - v_{11} + v_{13} + v_{14} + v_{32},\\
\alpha_3 &:= v_4 + v_5 + v_9 + v_{32},\\
\alpha_4 &:= -v_{21} + v_{22} + v_{23} - v_{24} + v_{26} + v_{32},\\
\alpha_5 &:= v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{32},\\
\alpha_6 &:= v_{12} + v_{13} + v_{32},\\
\alpha_7 &:= v_{25} - v_{26} + v_{27} - v_{28} + v_{29} - v_{30} + v_{32},\\
\alpha_8 &:= -v_4 - v_5 + v_9 + v_{32},\\
\alpha_9 &:= v_{10} - v_{12} + v_{13} + v_{32},\\
\alpha_{10} &:= v_{19} + v_{21} + v_{32}.
\end{aligned}$$

Then we have

$$\begin{aligned}
&N(\alpha_1) = 641, \quad N(\alpha_2) = 769, \quad N(\alpha_3) = 1279,\\
&N(\alpha_4) = 3329, \quad N(\alpha_5) = 4481, \quad N(\alpha_6) = 5119,\\
&N(\alpha_7) = 2689 \cdot 3329, \quad N(\alpha_8) = 1151 \cdot 2689,\\
&N(\alpha_9) = 1151 \cdot 1409, \quad N(\alpha_{10}) = 641 \cdot 6271.
\end{aligned}$$

The above equations imply that there exist algebraic integers $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ of K_5 which satisfy that

$$N(\gamma_1) = 6271, \tag{5.5.1}$$
$$N(\gamma_2) = 2689, \tag{5.5.2}$$
$$N(\gamma_3) = 1151, \tag{5.5.3}$$
$$N(\gamma_4) = 1409 \tag{5.5.4}$$

by lemma 5.12. Indeed, we can determine γ_j's which satisfy the equations (5.5.1) through (5.5.4) explicitly as follows.

We assume that for distinct prime numbers p and q, there exist algebraic integers α, β in K_5 which satisfy that $N(\alpha) = pq$ and $N(\beta) = p$. Let σ be the generator of the Galois group of $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ induced by $\zeta_5 \mapsto \zeta_5^2$ and ρ a generator of the Galois group of $\mathbb{B}_5/\mathbb{Q}$ induced by $\zeta_{128} \mapsto \zeta_{128}^5$. Then for all $\tau \in \mathrm{Gal}(K_5/\mathbb{Q})$, there exist some rational integers k, l which satisfy

$$\tau = \sigma^k \rho^l.$$

For integer $0 \le i < 64$, we chose rational integers i_1, i_2 which satisfy

$$i = 32 i_1 + i_2$$

with $0 \le i_2 < 32$. Then we put $\tau_i := \sigma^{i_1}\rho^{i_2}$. We also put

$$V = \begin{pmatrix} \tau_0(v_0) & \tau_0(v_1) & \cdots & \tau_0(v_{63}) \\ \tau_1(v_0) & \tau_1(v_1) & \cdots & \tau_1(v_{63}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{63}(v_0) & \tau_{63}(v_1) & \cdots & \tau_{63}(v_{63}) \end{pmatrix}.$$

Then $\det(V)^2 = d(K_5)$, which implies that $V \in \mathrm{GL}(64, K_5)$. For each integer $0 \le k < 64$, we put $\gamma_k = \alpha/\beta^{\tau_k}$. Then there exist rationals $x_j^{(k)}$ which satisfy that

$$x_0^{(k)} v_0 + x_1^{(k)} v_1 + \cdots + x_{63}^{(k)} v_{63} = \gamma_k.$$

Operating τ_i for each integer $0 \le i < 64$, we have

$$x_0^{(k)} \tau_i(v_0) + x_1^{(k)} \tau_i(v_1) + \cdots + x_{63}^{(k)} \tau_i(v_{63}) = \tau_i(\gamma_k).$$

Therefore we have the following equation:

$$V \begin{pmatrix} x_0^{(k)} \\ x_1^{(k)} \\ \vdots \\ x_{63}^{(k)} \end{pmatrix} = \begin{pmatrix} \tau_0(\gamma_k) \\ \tau_1(\gamma_k) \\ \vdots \\ \tau_{63}(\gamma_k) \end{pmatrix},$$

which implies

$$\begin{pmatrix} x_0^{(k)} \\ x_1^{(k)} \\ \vdots \\ x_{63}^{(k)} \end{pmatrix} = V^{-1} \begin{pmatrix} \tau_0(\gamma_k) \\ \tau_1(\gamma_k) \\ \vdots \\ \tau_{63}(\gamma_k) \end{pmatrix}. \tag{5.5.5}$$

Thus we have the following:

Lemma 5.14. *For some k_0, if it is true that $x_j^{(k_0)}$ given in equation* (5.5.5) *is rational integer for all $0 \le j < 64$, then we can conclude that γ_{k_0} is an algebraic integer of K_5 which satisfies that $N(\gamma_{k_0}) = q$.*

Using lemma 5.14, we can give algebraic integers $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ in K_5 which satisfy equations (5.5.1) through (5.5.4) explicitly. For convenience, we denote $\gamma = \sum_{j=0}^{63} x_j v_j$ by $\gamma = [x_0, x_1, \cdots, x_{63}]$.

Example 5.15.

1. The following γ_1 satisfies that $N(\gamma_1) = 6271$:

   $\gamma_1 = [93, -38, -55, 90, -17, -70, 81, 6, -82, 67, 28, -90, 50, 47, -93, 31, 61, -87, 7, 74, -76, -17, 85, -63, -37, 90, -45, -55, 89, -24, -69, 81, -57, 21, 34, -55, 8, 46, -51, -3, 53, -43, -13, 54, -30, -27, 54, -16, -41, 54, -4, -50, 50, 7, -52, 40, 21, -52, 26, 36, -53, 13, 46, -51]$.

2. The following γ_2 satisfies that $N(\gamma_2) = 2689$:

   $\gamma_2 = [-17, 14, -10, 6, 1, -3, 7, -7, 6, -6, 3, -3, 4, -4, 9, -10, 12, -12, 9, -4, -3, 10, -15, 19, -19, 16, -13, 8, -3, 1, 2, -1, 15, -12, 12, -7, 3, -1, -2, 3, -2, 3, -2, 3, -3, 5, -6, 9, -10, 11, -8, 6, -2, -3, 5, -7, 8, -7, 5, -1, 0, 2, -2, 1]$.

3. The following γ_3 satisfies that $N(\gamma_3) = 1151$:

   $\gamma_3 = [27, 25, 20, 20, 23, 25, 22, 22, 20, 21, 22, 22, 16, 16, 19, 20, 18, 15, 11, 11, 15, 15, 10, 8, 9, 10, 8, 5, 1, 3, 5, 4, -12, -13, -16, -20, -12, -7, -12, -17, -17, -14, -9, -8, -15, -17, -11, -8, -7, -11, -13, -10, -2, -4, -9, -10, -8, -4, 0, -2, -8, -3, 3, 3]$.

4. The following γ_4 satisfies that $N(\gamma_4) = 1409$:

$$\gamma_4 = [-2, 2, -11, 20, 8, -39, 23, 7, -8, 15, -30, 11, 24, -21, -3, 8, 2, -11, 20, -5, -34, 42, -3, -24, 23, -26, 19, 21, -42, 11, 17, -11, 1, 0, 7, -13, -4, 26, -15, -5, 7, -9, 18, -6, -14, 12, 2, -3, -1, 5, -11, 4, 20, -26, 3, 14, -14, 18, -14, -13, 28, -7, -13, 9].$$

Furthermore, we can also verify that $\gamma_1 = \alpha_{10}/\alpha_1^{\tau_{40}}$, $\gamma_2 = \alpha_7/\alpha_4^{\tau_{62}}$, $\gamma_3 = \alpha_8/\gamma_2^{\tau_{63}}$ and $\gamma_4 = \alpha_9/\gamma_3^{\tau_{41}}$.

The subset T_0 of $S(K_5)$ we construct consists of 741,766 elements.

Chapter 6

Perspectives of the Research

In this chapter, we shall describe perspectives of our research by comparing to known results on Weber's class number problem.

6.1 Lower Bounds for ℓ-indivisibility

An explicit lower bounds for ℓ-indivisibility of $h_{p,n}$ plays a very important role. Let p, ℓ be distinct prime numbers, q be 4 or p according as $p = 2$ or not, $f_p(\ell)$ the order of ℓ modulo q and $s_p(\ell)$ the exact power of p dividing $\ell^{f_p(\ell)-1}$. Then for a prime number p and positive rational integers s, f, the set of prime numbers $D(p, s, f)$ is defined by

$$D(p, s, f) := \{\ell \neq p \mid f_p(\ell) = f, s_p(\ell) = s\}.$$

As an improved version of K. Horie and M. Horie [20], Morisawa and Okazaki [34] proved the following:

Theorem 6.1 (Morisawa and Okazaki). *Let p, ℓ be distinct prime numbers, q be 4 or p according as $p = 2$ or not, s a positive integer and f a positive divisor of $\phi(q)$ with the Euler function ϕ. We put $c = (p-1)p^{s-1}$ and*

$$G(p, s, f) = \begin{cases} \left(2\left(\frac{\sqrt{\pi}}{\sqrt{2}\log(2+\sqrt{5})}\right)^{c} \frac{c+2}{2}!\right)^{1/f} & \text{if } p = 2, \\ \left(\left(\frac{\sqrt{2\pi}}{3^{3/4}\log((3^{40/81}+\sqrt{3^{80/81}+4})/2)}\right)^{c} \frac{c+2}{2}!\right)^{1/f} & \text{if } p = 3. \end{cases}$$

If $\ell \in D(p, s, f)$ and $\ell > G(p, s, f)$, then ℓ does not divide $h_{p,n}$ for any non-negative integer n.

Remark 6.2. They also provided the constant $G(p, f, s)$ for general prime number $p \geq 5$.

As a corollary of theorem 6.1, we have following:

Theorem 6.3 (Morisawa and Okazaki)**.** *If a prime number ℓ satisfies that $\ell \not\equiv \pm 1 \pmod{64}$, then ℓ does not divide $h_{2,n}$ for any positive integer n.*

So the following is a natural question:

Problem. Can we provide an explicit lower bound for ℓ-indivisibility of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{5})$?

6.2 The $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension

In order to approach the conjecture of Coates, it is natural to study the $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension with distinct prime numbers $p_1, \cdots, p_s$. K. Horie [17] and Morisawa [32] also gave explicit lower bounds for ℓ-indivisibility of the class numbers of the $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension of $\mathbb{Q}$.

On the other hand, K. Horie [12] found examples of prime numbers which divide class numbers of intermediate fields of $\mathbb{Z}_p \times \mathbb{Z}_q$-extension. We denote by $h(p^n \cdot q^m)$ the class number of $\mathbb{B}_{p,n}\mathbb{B}_{q,m}$ for distinct prime numbers p, q and positive integers n, m. We shall cite some of known results:

Example 6.4.

(i) 31 divides $h(2 \cdot 31)$ (proved by K. Horie [12]).

(ii) 1546463 divides $h(2 \cdot 1546463)$ (proved by Fukuda and Komatsu, cf. [10]).

(iii) 114689 divides $h(2^{10} \cdot 114689)$ (proved by Fukuda, Komatsu and Morisawa [10]).

(iv) 107 divides $h(2 \cdot 53)$ (proved by Fukuda; cf. [2] and [10]).

So the following is an interesting question:

Problem. Fix a prime number ℓ. Does there exist an intermediate field F of $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension of $\mathbb{Q}(\sqrt{5})$ such that the class number of F is divisible by F ?

Bibliography

[1] M. Aoki, *Notes on the Structure of the Ideal Class Groups of the Algebraic Number Fields*, Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), No. 5, 69-74.

[2] M. Aoki and T. Fukuda, *An Algorithm for Computing p-Class Groups of Abelian Number Fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, (2006), 56-71.

[3] H. Bauer, *Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper*, J. Number Theory 1 (1969), 161-162.

[4] J.-P. Cerri, *De l'euclidianité de* $\mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$ *et* $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ *pour la norme*, J. Théor. Nombres de Bordeaux, tome 12, No. 1 (2000), 103-126.

[5] J. Coates, *The enigmatic Tate-Shafarevich group*, Fifth International Congress of Chinese Mathematicians, Part 1, AMS/IP Stud. Adv. Math. 51, Amer. Math. Soc., Providence RI(2012), 43-50.

[6] H. Cohn, *A Numerical Study of Weber's Real Class Number Caluculation Part I*, Numer. Math. 2 (1960), 347-362 .

[7] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic* $\mathbb{Z}_2$*-extension of* $\mathbb{Q}$, Experiment. Math. 18(2009), No. 2, 213-222.

[8] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic* $\mathbb{Z}_2$*-extension of* $\mathbb{Q}$*,* II, J. Théor. Nombres Bordeaux 22(2010), No. 2, 359-368.

[9] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic* $\mathbb{Z}_2$*-Extension of* $\mathbb{Q}$*,* III, Int. J. Number Theory Vol.7, No.6 (2011) 1627-1635.

[10] T. Fukuda, K. Komatsu and T. Morisawa, *Weber's Class Number One Problem. Iwasawa theory 2012*, 221-226, Contrib. Math. Comput. Sci., 7, Springer, Heidelberg, 2014.

[11] G. Gras, *Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés*, Ann. Inst. Fourier 27-1(1977), 1-66.

[12] K. Horie, *A Note on the* $\mathbb{Z}_p \times \mathbb{Z}_q$*-extension over* $\mathbb{Q}$, Proc. Japan Acad. Ser. A Math. Sci. 77(2001), No.6, 84-86

[13] K. Horie, *Ideal Class Groups of Iwasawa-theoretical Abelian Extensions over the Rational Fields*, J. London Math. Soc. (2) 66(2002), No.2, 257-275.

[14] K. Horie, *Primary Components of the Ideal Class Group of the* $\mathbb{Z}_p$*-extension over* $\mathbb{Q}$ *for Typical Inert Primes*, Proc. Japan Acad. A Math. Sci. 81(2005), No.3, 40-43.

[15] K. Horie, *The Ideal Class Group of the Basic* $\mathbb{Z}_p$*-extension over an imaginary quadratic field*, Tohoku Math. J. (2) 57(2005), No.3, 375-394.

[16] K. Horie, *Certain Primary Components of the Ideal Class Group of the* $\mathbb{Z}_p$*-extension over the Rationals*, Tohoku Math. J. (2) 59(2007), 259-291.

[17] K. Horie, *Primary Components of the Ideal Class Group of an Iwasawa-theoretical Abelian Number Field*, J. Math. Soc. Japan 59(2007),No.3, 811-824.

[18] K. Horie and M. Horie, *The Narrow Class Groups of Some* $\mathbb{Z}_p$*-extensions over the Rationals*, Acta Arith. 135(2008), No.2, 159-180.

[19] K. Horie and M. Horie, *The Ideal Class Group of the* $\mathbb{Z}_{23}$*-extension over the rational field*, Proc. Japan Acad. A Math. Sci. 85(2009), No.2, 155-159.

[20] K. Horie and M. Horie, *The Ideal Class Groups of the* $\mathbb{Z}_p$*-extension over the Rationals*, Tohoku Math. J. (2) 61(2009), No.4, 551-570.

[21] K. Horie and M. Horie, *The Narrow Class Groups of the $\mathbb{Z}_{17}$- and $\mathbb{Z}_{19}$-extensions over the Rational Field*, Abh. Math. Semin. Univ. Hambg. 80(2010), No.1, 47-57.

[22] K. Horie and M. Horie, *The l-class Group of the $\mathbb{Z}_p$-extension of the Rational Field*, J. Math. Soc. Japan 64(2012), No.4, 1071-1089.

[23] K. Iwasawa, *A Note on Class Numbers of Algebraic Number Fields*, Abh. Math. Sem. der Univ. Hamburg 20 (1956), 257-258.

[24] F. J. van der Linden, *Class Number Computations of Real Abelian Number Fields*, Math. Comp. Vol. 39, No. 160 (1982), 693-707.

[25] J. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math. 37, No. 3(1978), 297-319.

[26] B. Mazur and A. Wiles, *Class Fields of Abelian Extension of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179-330.

[27] J. C. Miller, *Class numbers of real cyclotomic fields of composite conductor*, LMS J. Comput. Math. 17, Special Issue A(2014), 404-417.

[28] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. no.4 (2014), 381-397.

[29] J. C. Miller, *Class Numbers in Cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory 150(2015),47-73.

[30] T. Morisawa, *A Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of* $\mathbb{Q}$, Tokyo J. Math. 32(2009), No.2, 549-558.

[31] T. Morisawa, *Mahler Measure of the Horie Unit and Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of* $\mathbb{Q}$, Acta Arith. 153(2012), No.1, 35-49.

[32] T. Morisawa, *On the ℓ-part of the $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension of* $\mathbb{Q}$, J. Number Theory 133(2013), 1814-1826.

[33] T. Morisawa and R. Okazaki, *Mahler Measure and Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for odd prime number p*, Tohoku Math. J. (2) 65(2013), No.2, 253-272.

[34] T. Morisawa and R. Okazaki, *Height and Weber's Class Number Problem*, J. Théor. Nombres Bordeaux 28(2016), No. 3, 811-828.

[35] J. Neukirch, *Algebraic number theory*, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder, Grundlehen Math. Wiss. [Fundamental principles of Mathematical Science], 332, Springer-Verlag, Berlin, 1992.

[36] A. M. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. 29(1976), No. 3, 275-297.

[37] A. M. Odlyzko, *Lower bounds for discriminants of number fields.* II, Tohoku Math. J. 29(1977), No. 2, 209-216.

[38] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results*, Sém. Théor. des Nombres, Bordeaux 2 (1990), 199-141.

[39] A. M. Odlyzko, *Table4: Unconditional Bounds for Discriminants*, unpublished, 1976,

http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table4.

[40] G. Poitou, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, No.1 (1976-1977), exp. No.6, 1-17.

[41] L. C. Washington, *The Non-p-Part of the Class Number in a Cyclotomic* $\mathbb{Z}_p$*-Extension*, Invent. Math. 49(1978), no.1 87-97.

[42] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Vol. 83, 2nd edition (Springer-Verlag, Berlin, 1997).

[43] H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Math. 8(1886), 193-263.

List of Original Papers

1. T. Aoki, A class number problem for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$, Tokyo J. Math., Vol. 39(1), 2016, 69-81.

2. T. Aoki, A class number calculation of the 5^{th} layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{5})$, to appear in Funct. Approx. Comment. Math.