Osaka University Knowledge Archive

Title	Class numbers of pure quintic fields
Author(s)	小林, 弘知
Citation	大阪大学, 2016, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/56049
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Class numbers of pure quintic fields

Hirotomo Kobayashi

Abstract. Let m be a fifth power free integer greater than one. Let K be an algebraic number field generated by a fifth root of m over the rational number field. If m has a prime factor p congruent to -1 modulo five, the class number of K is a multiple of five.

1. Introduction

This thesis is a refined version of the paper [**6**]. To study class numbers of algebraic number fields is one of the classical interest in number theory. It is very difficult to grasp the general property for an arbitrary algebraic number field, but it is known that some kind of algebraic number fields have the class numbers acting predictably. Motivation of our study is to find a new one of such knowledge. Let l be a prime, K a pure field of degree l, i.e., $K = \mathbb{Q}(m^{1/l})$ where m is an l-th power free integer greater than one, and L the Galois closure of K over the rational number field $\mathbb{Q}$. There is a question when the class number h_K of K is divisible by l. Genus theory gives an answer in the case $l = 2$. Honda [**3**] solved the cubic case and his method became a model of researches on this subject. Subsequently to Honda's study, Parry [**11**] studied the case $l = 5$ and found the difficulty in this case. He presented the relation formula between the class numbers of K and L:

$$5^5 h_L = c_m h_K^4,$$

where h_L is the class number of L and c_m is a divisor of 5^6. He also gave necessary and sufficient conditions for L to have the class number divisible by 5, and left the six cases unclear whether h_K is divisible by 5 or not (see Theorem IV of [**11**]). For instance, the divisibility remained unclear when m is a prime number p such that $p \equiv -1$

2010 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R20,11R21,11R37.

Key words and phrases. pure quintic fields; class numbers; unit groups.

(mod 5). Iimura [**4**] showed that there are infinitely many fields K with $5 \nmid h_K$ and $5 \mid h_L$. For a general odd prime l, Parry and Walter [**12**] gave necessary and sufficient conditions for L to have the class number divisible by l. They also derived necessary conditions for K to have the class number divisible by l when the class number of the maximal real subfield of the l-th cyclotomic field is not divisible by l.

On the other hand, Ishida [**5**] showed that if l is an odd prime and m has a prime factor p with $p \equiv 1 \pmod{l}$, the class number of K is divisible by l. He showed that the composite field of K and the subfield of degree l of the p-th cyclotomic field is unramified over K, and then the divisibility follows from class field theory. Here, we pose the following conjecture:

Conjecture 1. *Let l be an odd prime greater than three and let p be a prime such that $p \equiv -1 \pmod{l}$. If an l-th power free positive integer m is divisible by p and $K = \mathbb{Q}(m^{1/l})$, then the class number of K is divisible by l.*

It is easy to see that Ishida's method does not work in this case. In this paper we prove this conjecture for $l = 5$, i.e.,

Theorem 1. *Let m be a fifth power free positive integer and let $K = \mathbb{Q}(m^{1/5})$. If m has a prime factor p with $p \equiv -1 \pmod{5}$, then the class number of K is divisible by five.*

As a consequence, we make clear three of the six cases left by Parry. Our method is essentially based on an investigation of the Galois module structure of the unit group of L, but our description is solely devoted to the unit group of the maximal real subfield of L since it is sufficient for our purpose.

We will describe an outline of the proof briefly. Let $K = \mathbb{Q}(m^{1/5})$ where m is a fifth power free integer greater than one, and L the Galois closure of K over the rational number field $\mathbb{Q}$. Let L^+ be the maximal real subfield of L. In general, we show that $5 \mid h_K$ if and only if $5 \mid h_{L^+}$, where h_K and h_{L^+} are the class numbers of K and L^+ respectively. Further assume that $5 \nmid h_{L^+}$. Under this assumption, we determine a set of fundamental units of L^+ and investigate endomorphisms of the unit group of L^+. When m has a prime divisor p congruent to -1 modulo five, applying the investigation to an abstract unit constructed by totally ramified primes in the extension $L^+/\mathbb{Q}(\sqrt{5})$, we encounter a contradiction with our assumption that $5 \nmid h_{L^+}$.

Finally, we touch on the following useful theorem, which is used twice as $n = 1$ in this paper.

THEOREM 2. *Let K be a real algebraic number field and K_+ be the set of positive elements of K. Denote the positive root of the equation $x^s = q^t$ by q^r for $q \in K_+$ and $r = t/s \in \mathbb{Q}$ with $t, s \in \mathbb{Z}$. Let n be a natural number and $q, q_1, \ldots, q_n \in K_+$ and $r, r_1, \ldots, r_n \in \mathbb{Q}$. Then $q^r \in K(q_1^{r_1}, \ldots, q_n^{r_n})$ if and only if*

$$q^r = q_0 q_1^{r_1 e_1} \ldots q_n^{r_n e_n} \text{ with } q_0 \in K \text{ and } e_1, \ldots, e_n \in \mathbb{Z}.$$

We prove this theorem in the appendix, which can be read independently from the other parts of this paper. Besides, it does not require any advanced knowledge.

2. Previous researches

In this chapter, we digest previous researches related to our study roughly. Let $\mathbb{Q}$ denotes the rational number filed. Pure fields mean the algebraic number fields generated by the positive l-th root of m over the rational field when m is an l-th power free positive integer. Our interest is in the class number of pure fields. We restrict ourselves to the case where l is a prime number. Pure fields of degree two over $\mathbb{Q}$ are real quadratic fields. The divisibility of the class number of quadratic fields by two is completely determined as follows;

THEOREM 3. *The quadratic fields with odd class number are the following where p, p_1, p_2 denote primes with $p_1 \neq p_2$:*

(i) $\mathbb{Q}(\sqrt{-1})$,
(ii) $\mathbb{Q}(\sqrt{p})$,
(iii) $\mathbb{Q}(\sqrt{-p})$ *where* $p = 2$ *or* $p \equiv -1$,
(iv) $\mathbb{Q}(\sqrt{p_1 p_2})$ *where* $p_1 \equiv -1$ *and* $p_2 = 2$ *or* $p_2 \equiv -1$.

Here all congruences are modulo 4.

This is one of the results from classical genus theory (see [**2**]). Hereby, it is natural to think that the divisibility of class numbers of pure fields by the degree may act predictably. As pure fields with degree more than two are not abelian over the rational filed, the divisibility might not be so simple. However, Honda obtained the following result and completely determined the divisibility of class numbers of pure cubic fields by three:

THEOREM 4. *Let n be a third power free positive integer and let Ω be the pure field by the cubic root of n over $\mathbb{Q}$. The class numbers of Ω is not a multiple of three if and only if n has one of the following*

forms where p, q are primes with $p \neq q$ and $a, b = 1$ or 2:

$$\begin{aligned}
&\text{(i) } n = 3^a, \\
&\text{(ii) } n = p^a, \ \textit{where } p \equiv -1 \pmod 3, \\
&\text{(iii) } n = 3^a p^b \ \textit{where } p \equiv 2 \textit{ or } 5 \pmod 9, \\
&\text{(iv) } n = p^a q^a, \ \textit{where } p \equiv 2 \textit{ and } q \equiv 5 \pmod 9, \\
&\text{(v) } n = p^2 q, \ \textit{where } p \equiv q \equiv 2 \textit{ or } 5 \pmod 9
\end{aligned}$$

This is taken from [**3**]. Honda's method is roughly explained as follows. Let Ω be as in Theorem 4. Let K be the cubic cyclotomic field, that is, the algebraic number field generated by a primitive cubic root of unity over $\mathbb{Q}$. Let L be the composite field of Ω and K. Let $a_{L/K}$ be the number of ambiguous classes for the cyclic extension L/K. It is known that the ideal class number of L is a multiple of three if and only if $3|a_{L/K}$ (we will prove Proposition 1 which gives this elementary result as a corollary). There is a formula to compute $a_{L/K}$, which is called the ambiguous class number formula (see Theorem 9 later). By this ambiguous class number formula, we see that

$$a_{L/K} = 3^{e-t-1}$$

where e is the number of primes of K which are ramified in L and $t = 0$ or 1 according as a primitive cubic root of unity is in the norm images of L/K or not. It is easy to know the value of e from the number of the prime divisor of n, and t can be evaluated by investigating the Hilbert symbol in K. Moreover, by Brauer-Kuroda relations (see Theorem 13 later), we see that the class number of Ω is a multiple of three if and only if the class number of L is so.

Parry studied the quintic cases after Honda. Let m be a fifth power free positive integer and let Ω be the algebraic number field generated by the real fifth root of m over the rational number field. Let ζ be a primitive fifth root of unity. Further, let k and L be the algebraic number fields generated by ζ over $\mathbb{Q}$ and Ω respectively. We shall denote by h_M the class number of M if M is an algebraic number field. Let $q^* = 0, 1$ or 2 according as none , exactly one or all of

$$\zeta, \ \varepsilon_1 = (1+\sqrt{5})/2, \ \zeta^a \varepsilon_1 \ (a = 1, 2, 3 \text{ or } 4)$$

are in the norm images of L/k. Parry's main result is stated with these notations as follows:

THEOREM 5. *If m has a prime divisor $p \equiv 1 \pmod 5$, then h_Ω and h_L are multiples of five. The class number h_L is not divisible by five if and only if m takes on one of the following values where $a, b = 1, 2, 3$ or*

4 *and* p_1, p_2 *are distinct primes such that* $p_i \equiv \pm 2 \pmod 5$ *for* $i = 1, 2$:

(I) $m = 5^a$,

(II) $m = p_1^a$,

(III) $m = 5^a p_1^b$ *where* $p_1^4 \not\equiv 1 \pmod{25}$,

(IV) $m = p_1^a p_2^b$ *where* $m^2 \equiv 1,\ p_1^4 \not\equiv 1,\ p_2^4 \not\equiv 1 \pmod{25}$.

For each of the above values of m*, the class number* h_Ω *is not a multiple of five. For the following exceptional values of* m*, the class number* h_Ω *may or may not be a multiple of five where* $a, b, c = 1, 2, 3$ *or* 4 *and* p_i, q *are distinct primes each other such that* $p_i \equiv \pm 2 \pmod 5$ *for* $i = 1, 2, 3$ *and that* $q \equiv -1 \pmod 5$:

(i) $m = p_1^a p_2^b$ *where* $m^4, p_2^4 \not\equiv 1 \pmod{25}$,

(ii) $m = p_1^a p_2^b$ *where* $p_1^4 \equiv p_2^4 \equiv 1 \pmod{25}$,

(iii) $m = p_1^a p_2^b p_3^c$ *where* $m^4 \equiv 1,\ p_i^4 \not\equiv 1 \pmod{25}$ *for* $i = 2, 3$,

(iv) $m = 5^a p_1^b$ *where* $p_1^4 \equiv 1 \pmod{25}$,

(v) $m = 5^a p_1^b p_2^c$ *where* $p_2^4 \not\equiv 1 \pmod{25}$,

(vi) $m = q^a$ *where* $q \not\equiv -1 \pmod{25}$,

(vii) $m = p_1^a q^b$ *where* $m^4 \equiv 1,\ p_1^4 \not\equiv 1,\ q \not\equiv -1 \pmod{25}$,

(viii) $m = 5^a q^b$ *where* $q \not\equiv -1 \pmod{25}$,

(ix) $m = q^a$ *where* $q \equiv -1 \pmod{25}$.

For all other values of m*, the class number* h_Ω *is a multiple of five.*

This is taken from [**11**]. Note that the representation of this theorem looks different from Parry's original representation. The nine uncertain cases above is classified into the six uncertain cases in Parry's original representation. Our representation actually follows after that of Iimura. The first half part of this statement is obtained by ambiguous ideal class number formula as in the cubic case. The second half part states that the uncertainty occurs in the listed nine cases. This is because it does not hold that $5|h_L$ if and only if $5|h_\Omega$, though the similar statement holds in the cubic case. This difference occurs as follows. In this quintic case, Brauer-Kuroda relations guarantee that

$$h_L = \frac{(E : \varepsilon)}{5^5} h_\Omega^4$$

where E denotes the full unit group of L, ε denotes the subgroup of E generated by the all conjugates of the units of Ω and $(E : \varepsilon)$ denotes

the index of ε in E. It is not difficult to see that

$$(E : \varepsilon)|5^6.$$

Thus, h_Ω may not be a multiple of 5 even if $5|h_L$, and then $(E : \varepsilon) = 5^6$.

Iimura studied these uncertain cases listed in Theorem 5 and gave a necessary and sufficient condition for h_Ω to be divisible by five in each case, except for Case (ix). He explained that Case (ix) is hard to deal with by means of his method and is excluded from his consideration. We omit to explain his necessary and sufficient conditions in detail here because it is a little bit complicated (see [**4**]). His necessary and sufficient conditions seem difficult to use in many cases, but he showed, using the condition, that there are infinitely many pure quintic fields Ω such that $5 \nmid h_\Omega$ and $5|h_L$, which was not trivial from the Parry's study.

These series of study are considered to start with Honda's idea which combine with ambiguous ideal class number formula and Brauer-Kuroda relations. However, there was a former study about such a class number divisibility of pure fields by Ishida. Ishida studied such a class number divisibility of wider fields by using elementary facts, and he obtained the following result.

THEOREM 6. *Let l be a odd prime and m be a l-th power free positive integer with a prime divisor $p \equiv 1 \pmod{l}$. Then the pure field generated by an l-th root of m over $\mathbb{Q}$ has the class number divisible by l.*

This is taken from [**5**]. We note that this result are contained in theorems stated above when $l = 3$ or 5. Nevertheless, this results seems hard to be covered by the above method derived from Honda, especially for the higher degree cases. This is considered because Brauer-Kuroda relations are harder to compute according as the degree of the pure field becomes higher.

3. Elementary facts

We begin to prove the structure theorem for finitely generated abelian groups for later use. We need the following lemma.

LEMMA 1. *Submodules of finitely generated free $\mathbb{Z}$-modules are also free $\mathbb{Z}$-modules.*

PROOF. Let F be a free $\mathbb{Z}$-module of rank n. We may assume that $n > 0$. If $n = 1$, we may regard $F = \mathbb{Z}$, and then submodules of F are represented in the form $a\mathbb{Z}$ with $a \in \mathbb{Z}$, which shows our assertion in the case where $n = 1$. We shall prove our assertion by the induction

on n. Suppose that $n > 1$. Let N be a submodule of F. If $N = 0$, it is clearly a free $\mathbb{Z}$-module; therefore we may assume that $N \neq 0$. Take a basis $\{f_1, \ldots, f_n\}$ of F and call φ the projection from F onto $\mathbb{Z}$ given by

$$\varphi : \sum_{i=1}^{n} a_i f_i \mapsto a_1.$$

If necessary, we may reorder $f_1, \ldots, f_n$ so that $\varphi(N) \neq 0$. As $\varphi(N)$ is an ideal of $\mathbb{Z}$, it is represented in the form $a\mathbb{Z}$ with $a \in \mathbb{Z}$, and we can take $x \in N$ such that $\varphi(x) = a$. Put $N_1 = \mathrm{Ker}(\varphi) \cap N$. If $y \in N$,

$$y - (\varphi(y)/a)x \in N_1$$

and so

$$N = (\mathbb{Z}x) \oplus N_1. \tag{1}$$

Obviously $\mathrm{Ker}(\varphi)$ is a free $\mathbb{Z}$-module of rank $n-1$, and N_1 is the submodule. Therefore, by the induction assumption, N_1 is a free $\mathbb{Z}$-module, and so N is also a free $\mathbb{Z}$-module by (1). □

If G is a finitely generated abelian group, there is a free $\mathbb{Z}$-module F of finite rank r with a surjective homomorphism $f : F \to G$, and then

$$G \simeq F/N$$

where N is the kernel of f. By means of this, we are able to know sufficient structure information of a finitely generated abelian group from the following theorem.

THEOREM 7. *Let F be a free $\mathbb{Z}$-module of rank $n > 0$ and N be a submodule of F. Then there are a basis $\{f_1, \ldots, f_n\}$ of F and a set of non-negative integers $\{a_1, \ldots, a_n\}$ with $a_i | a_{i+1}$ for $i = 1, \ldots, n-1$ such that $\{a_1 f_1, \ldots, a_n f_n\}$ is a basis of N. Moreover the set $\{a_1, \ldots, a_n\}$ is uniquely determined for N.*

PROOF. We shall prove their existence by induction on n. Suppose that $n = 1$. Take an isomorphism

$$p : \mathbb{Z} \to F; n \mapsto n f_1,$$

where f_1 is a basis of F. Then $p^{-1}(N)$ is an ideal of $\mathbb{Z}$, so that it is represented in the form $a_1\mathbb{Z}$ with some non-negative integer a_1, which shows that N has $a_1 f_1$ as a basis. Suppose that $n > 1$. Consider the following set of ideals of $\mathbb{Z}$

$$\mathcal{X} = \{h(x)\mathbb{Z} | x \in N, h \in \mathrm{Hom}(F, \mathbb{Z})\}.$$

Here, $\mathrm{Hom}(F, \mathbb{Z})$ is the set of all homomorphisms of F into $\mathbb{Z}$. Take $\chi \in N$ and $\eta \in \mathrm{Hom}(F, \mathbb{Z})$ so that $\eta(\chi)\mathbb{Z}$ is the maximal element of

$\mathcal{X}$ with respect to inclusion. We may represent $\eta(F) = s\mathbb{Z}$ with $s \in \mathbb{Z}$ and take $u_1 \in F$ so that $\eta(u_1) = s$. Put $K = \mathrm{Ker}(\eta)$. Then we get the following direct decomposition

$$F = u_1\mathbb{Z} \oplus K \tag{2}$$

because $f - (\eta(f)/s) \cdot u_1 \in K$ and $\eta(f)/s \in \mathbb{Z}$ for any $f \in F$. Since $\eta(N) = \eta(\chi)\mathbb{Z}$, we obtain similarly

$$N = \chi\mathbb{Z} \oplus K_1 \tag{3}$$

where $K_1 = N \cap K$. As K is a free module of rank $n-1$ by Lemma 1, we can apply the induction assumption to the submodule K_1 of K, and so there is a basis $\{f_2, \ldots, f_n\}$ of K and a set of non-negative integers $\{a_2, \ldots, a_n\}$ with $a_i | a_{i+1}$ for $i = 2, \ldots, n-1$ such that $\{a_2 f_2, \ldots, a_n f_n\}$ is a basis of K_1. By the direct decomposition (2), we can take $\eta_1 \in \mathrm{Hom}(F, \mathbb{Z})$ such that $\eta_1(u_1) = 1$ and $\eta_1(K) = 0$, and we may represent

$$\chi = d_1 u_1 + d_2 f_2 + \cdots + d_n f_n$$

with $d_i \in \mathbb{Z}$ for all i because $\{u_1, f_2, \ldots, f_n\}$ is a basis of F. As $\eta_1(\chi)\mathbb{Z} = d_1\mathbb{Z} \in \mathcal{X}$ and $\eta(\chi)\mathbb{Z} = d_1 s\mathbb{Z}$ is taken to be a maximal element of $\mathcal{X}$ with respect to inclusion, we see that $s = \pm 1$. It is obvious that we may take $s = 1$. Let d_{1i} be the greatest common divisor of d_1 and d_i for $i = 2, \ldots, n$. Then there are $c_{1i}, c_i \in \mathbb{Z}$ such that

$$d_{1i} = c_{1i} d_1 + c_i d_i$$

for $i = 2, \ldots, n$. Take a homomorphism $\eta_i \in \mathrm{Hom}(F, \mathbb{Z})$ such that $\eta_i(u_1) = 0$ and $\eta_i(f_j) = \delta_{ij}$ for $i, j = 2, \ldots, n$. Here, δ_{ij} is Kronecker's delta. Then

$$(c_{1i}\eta_1 + c_i\eta_i)(\chi)\mathbb{Z} = (c_{1i} d_1 + c_i d_i)\mathbb{Z} = d_{1i}\mathbb{Z},$$

which shows $d_1 | d_{1i}$ because $d_1\mathbb{Z}$ is a maximal element of $\mathcal{X}$ with respect to inclusion. As d_{1i} is a divisor of d_i, for $i = 2, \ldots, n$, we obtain

$$d_1 | d_i.$$

Put

$$f_1 = u_1 + (d_2/d_1) f_2 + \cdots + (d_n/d_1) f_n.$$

By (2) and (3), we see that $\{f_1, \ldots, f_n\}$ is a basis of F and that $\{d_1 f_1, a_2 f_2, \ldots, a_n f_n\}$ is a basis of N. Let d be the greatest common divisor of d_1 and a_2. There are $p_1, p_2 \in \mathbb{Z}$ such that $d = p_1 d_1 + p_2 a_2$. We can take $\eta_0 \in \mathrm{Hom}(F, \mathbb{Z})$ so that

$$\eta_0(f_1) = p_1, \ \eta_0(f_2) = p_2, \ \eta_0(f_j) = 0$$

for $j = 3, \ldots, n$, and then

$$\eta_0(d_1 f_1 + a_2 f_2) = p_1 d_1 + p_2 a_2 = d.$$

As $d_1 f_1 + a_2 f_2$ is in N, we also see that $d_1 | d$ by the maximality of $d_1\mathbb{Z}$ in $\mathcal{X}$ with respect to inclusion, so that $d_1 | a_2$. Thus, we have shown our assertion except for the uniqueness.

In order to prove the uniqueness of the set $\{a_1, \ldots, a_n\}$ in our assertion, take the quotient group $M = F/N$. Then it is obvious that

$$M \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}. \tag{4}$$

The number of a_i's with $a_i = 0$ is uniquely determined as the rank of the $\mathbb{Q}$-vector space $M \otimes_{\mathbb{Z}} \mathbb{Q}$. Therefore it is sufficient to prove that the set $\{a_1, \ldots, a_n\}$ of positive integers is uniquely determined when M is the finite group represented by (4). We shall prove that the number of minimal generator of M as a $\mathbb{Z}$-module is $n - e$, where e is the number of a_i's with $a_i = 1$. Note that $a_1 = \cdots = a_e = 1$ and $a_{e+1} \neq 1$ then. It is obvious that M has $n - e$ generators. If there is a set $\{x_1, \ldots, x_m\}$ of generators of M whose cardinality m is less than $n - e$, then, for any prime divisor p of a_{e+1}, the quotient group M/pM isomorphic to $\mathbb{F}_p^{n-e}$ has the images of $x_1, \ldots, x_m$ as the generators, but it contradicts with the fact that an $\mathbb{F}_p$-vector space does not have the set of generators whose cardinality is less than its rank. Here $\mathbb{F}_p$ denotes the prime field $\mathbb{Z}/p\mathbb{Z}$. Thus we have shown that the number of a_i's with $a_i = 1$ is uniquely determined in (4), which is denoted by e. Applying the same argument to $a_{e+1}M$, we see that the number of a_i with $a_i = a_{e+1}$ is uniquely determined in (4). Therefore we can prove inductively that the set $\{a_1, \ldots, a_n\}$ of positive integers with $a_i \mid a_{i+1}$ in (4) is uniquely determined for the finite group M, and our assertion is verified completely. □

The structure theorem for finitely abelian groups is usually stated as the following form.

Corollary 1. *Let G be a finitely generated abelian group. Then there is a set of non-negative integers $\{a_1, \ldots, a_n\}$ with $a_i \mid a_{i+1}$ for $i = 1, \ldots, n-1$ such that*

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}.$$

Moreover this set $\{a_1, \ldots, a_n\}$ is uniquely determined for G unless $a_1 = 1$.

Proof. It follows immediately from Theorem 7 and the description preceding that. □

The following theorem is Dirichlet's units theorem. This theorem gives the group structure of the full unit group of an algebraic number field. We will use this theorem without notice later. We refer to Theorem 9 of Chap. IV-4 of [**14**] for the proof.

THEOREM 8. *Let K be an algebraic number field with $r+1$ infinite places and W_K be the group of the roots of unity in K. Then there are units $\epsilon_1, \ldots, \epsilon_r$ of K such that any unit ϵ of K is uniquely represented by*

$$\epsilon = w\epsilon_1^{a_1} \cdots \epsilon_r^{a_r}$$

with $w \in W_K$ and $a_1, \ldots, a_r \in \mathbb{Z}$.

The units $\epsilon_1, \ldots, \epsilon_r$ in this theorem are called fundamental units of K

4. Ambiguous ideals

Our purpose of this chapter is to prove Proposition 1. This chapter presupposes the knowledge of class field theory with idele class group. We will not use results obtained in this chapter later, but these results were elementary in former studies. We note that the material treated in this chapter is mainly taken from [**2**].

Let K be an algebraic number field. Let L/K be a cyclic extension with Galois group $\mathcal{G}$. Take a generator σ of $\mathcal{G}$. We shall denote the ideal class group of L by $\mathrm{Cl}(L)$. We say that an ideal class $\mathfrak{a}$ of $\mathrm{Cl}(L)$ is ambiguous if

$$\mathfrak{a}^\sigma = \mathfrak{a}.$$

It is equivalent to say that $\mathfrak{a}^{1-\sigma}$ is the principal ideal class of $\mathrm{Cl}(L)$. More precisely, if $\mathfrak{a}$ has an ideal a as a representative, then $\mathfrak{a}$ is ambiguous if and only if there is an element c of L such that $a^\sigma = ca$. We shall denote by L^1 the Hilbert class field of L, that is, the maximal abelian extension over L unramified for all places of L. We call the maximal abelian extension of K contained in L^1 the genus field of L/K and denote it by G. The genus group $\mathfrak{G}(L/K)$ is defined as

$$\mathfrak{G}(L/K) = C_L/N_{G/L}(C_G).$$

Here $N_{G/L} : C_G \to C_L$ is the norm map from the idele class group of G to that of L. Class field theory says that $\mathfrak{G}(L/K)$ is isomorphic to the Galois group of G/L.

PROPOSITION 1. *Let L/K be a cyclic extension with Galois group G generated by an element σ. Then*

$$\mathfrak{G}(L/K) = \mathrm{Cl}(L)/\mathrm{Cl}(L)^{1-\sigma}. \tag{5}$$

If moreover the extension degree of L/K is a power of a prime l, then $\mathfrak{G}(L/K)_l$ is trivial if and only if $\mathrm{Cl}(L)_l$ is trivial, where A_l denotes the Sylow l-subgroup of an abelian group A.

Proof. Note that

$$\mathrm{Cl}(L)^{1-\sigma} = \{\mathfrak{a}^{1-\sigma} \mid \mathfrak{a} \in \mathrm{Cl}(L)\}.$$

Let $\Omega = \mathrm{Gal}(L^1/K)$. Here L^1 be the Hilbert class field of L as above. Moreover, put $\Delta = \mathrm{Gal}(L^1/L)$ and take $c \in \Omega$ such that the image of c in $\Omega/\Delta = \mathrm{Gal}(L/K)$ is σ. In the reciprocity isomorphism $r_{L/K} : \mathrm{Cl}(L) \to \Delta$, when $r_{L/K}(\mathfrak{a}) = \tau$, we see that $r_{L/K}(\mathfrak{a}^\sigma) = c^{-1}\tau c$, which is in Δ because Δ is a normal subgroup of Ω, and so $r_{L/K}(\mathfrak{a}^{1-\sigma}) = \tau c^{-1}\tau^{-1}c$. Since Δ is abelian and Ω/Δ is the cyclic group generated by σ, it shows that $r_{L/K}$ maps $\mathrm{Cl}(L)^{1-\sigma}$ onto the subgroup (Δ, Ω) of Ω, which is the subgroup of Ω generated by $aba^{-1}b^{-1}$ for $a \in \Delta, b \in \Omega$. Let $\mathfrak{B}$ be the kernel of the natural projection

$$\mathrm{Cl}(L) \simeq C_L/N_{L^1/L}C_{L^1} \to C_L/N_{G/L}(C_G) = \mathfrak{G}(L/K),$$

where G is the genus field of L/K. By the definition of G, the reciprocity map $r_{L/K}$ maps $\mathfrak{B}$ onto $\Delta \cap (\Omega, \Omega)$, where (Ω, Ω) is the commutator subgroup of Ω. Now, since L/K is abelian, we see that $\Delta \supseteq (\Omega, \Omega)$, and therefore the reciprocity map $r_{L/K}$ maps $\mathfrak{B}$ onto (Ω, Ω). We shall show that $(\Delta, \Omega) = (\Omega, \Omega)$. Since $\Delta \subseteq \Omega$, it is clear that $(\Delta, \Omega) \subseteq (\Omega, \Omega)$. On the other hand, since Ω/Δ is the cyclic group generated by σ, each element a of Ω is of the form $c^i x$ with $i \in \mathbb{Z}, x \in \Delta$. Moreover, for $x \in \Delta$, we may write for $c^i x c^{-i} = x_i$ with $x_i \in \Delta$ uniquely. With this notation, when we represent $a = c^i x$ and $b = c^j y$ with $i, j \in \mathbb{Z}, x, y \in \Delta$ for $a, b \in \Omega$, we have

$$\begin{aligned} aba^{-1}b^{-1} &= c^i x c^j y x^{-1} c^{-i} y^{-1} c^{-j} = x_i c^{i+j} y c^{-i} x_i^{-1} y^{-1} c^{-j} \\ &= x_i c^j y_i x_i^{-1} c^{-i} y_i^{-1} c^{i-j} = x_i (c^j y_i) x_i^{-1} (c^j y_i)^{-1} (c^j y_i) c^{-i} y_i^{-1} c^{i-j} \\ &= \{x_i (c^j y_i) x_i^{-1} (c^j y_i)^{-1}\}\{(c^j y_i) c^{-i} (c^j y_i)^{-1} c^i\} \in (\Delta, \Omega), \end{aligned}$$

which shows that $(\Omega, \Omega) \subseteq (\Delta, \Omega)$. Hence $(\Delta, \Omega) = (\Omega, \Omega)$, so that $\mathrm{Cl}(L)^{1-\sigma} = \mathfrak{B}$, which implies (5).

Next suppose that the extension degree of L/K is a power of l. Let L' be the maximal unramified abelian l-extension of L. Note that $L^1 \supseteq L'$ and L'/K is a Galois extension. Put $\Omega' = \mathrm{Gal}(L'/K)$ and $\Delta' = \mathrm{Gal}(L'/L)$. Assume that $\mathfrak{G}(L/K)_l$ is trivial. Since L/K is abelian, we see that $\Delta' \supseteq (\Omega', \Omega')$. The assumption that $\mathfrak{G}(L/K)_l$ is trivial implies that M/K is not abelian for any field M with $L \subsetneq M \subseteq L'$, so that $\Delta' = (\Omega', \Omega')$. As stated above, since Ω'/Δ' is cyclic, we get

$$(\Omega', \Delta') = (\Omega', \Omega') = \Delta'.$$

This shows that the lower central series of Ω' terminate at $(\Omega', \Delta') = \Delta'$. On the other hand, the finite l-group Ω' is a nilpotent group. It is well known that the lower central series of a nilpotent group terminates at

the trivial subgroup. Hence, Δ' is trivial, which implies that $\mathrm{Cl}(L)_l$ is trivial. The converse is obvious and the proof is completed. $\square$

The following result is called ambiguous class number formula. Although we will not use it in this paper, it is important for the study of the class numbers of pure fields as stated in Chapter 2.

THEOREM 9. *Let L/K be a cyclic extension of prime degree l. Let t be the number of ramified places in L/K and let $\mathrm{Am}(L/K)$ be the subgroup of $\mathrm{Cl}(L)$ consisting of the ambiguous ideal classes. The order of $\mathrm{Am}(L/K)$ is given by*

$$h(K) \cdot \frac{l^{t-1}}{(E_K : E_K \cap N_{L/K} L^\times)},$$

where $h(K)$ is the class number of K, E_K is the unit group of K, $E_K \cap N_{L/K} L^\times$ is the subgroup consisting of norm images of L and $(E_K : E_K \cap N_{L/K} L^\times)$ is the index.

We refer the proof to [**9**].

5. Brauer-Kuroda relations

In this chapter, we will digest the proof of the Brauer-Kuroda relations, which was proved independently by Brauer and Kuroda (see [**1**] and [**7**] respectively).

We start to define the Dedekind zeta function. Let K be an algebraic number field. The Dedekind zeta function is the meromorphic function given for $\mathrm{Re}(s) > 1$ by

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-1}$$

where $\mathfrak{p}$ runs through all prime ideals of K and $\mathfrak{N}(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$ which is the number of elements of the residue field of $\mathfrak{p}$. Put

$$G_1(s) = \pi^{-s/2}\Gamma(s/2), \quad G_2(s) = (2\pi)^{1-s}\Gamma(s),$$

where $\Gamma(s)$ is the gamma function. It is well-known that $\Gamma(s)$ has no zero and has simple poles at non-positive integers. Since $\Gamma(1/2) = \pi^{1/2}$ and $\Gamma(1)$=1, we have

$$G_1(1/2) = 1, \quad G_2(1) = 1.$$

Then we have the following analytic class number formula.

THEOREM 10. *Let K be an algebraic number field with r_1 real places and r_2 imaginary places. Put*

$$\xi_K(s) = G_1(s)^{r_1} G_2(s)^{r_2} \zeta_K(s).$$

Then $\xi_K(s)$ is meromorphic in the entire s-plane, holomorphic except for simple poles at $s = 0$ and $s = 1$, and satisfies the functional equation

$$\xi_K(s) = |D_K|^{\frac{1}{2}-s}\xi_K(1-s),$$

where D_K is the discriminant of K. Its residue at $s = 1$ is

$$\frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K|D_K|^{1/2}}$$

where h_K is the class number of K, R_K is the regulator of K and w_K is the number of roots of unity in K.

The proof is referred to that of Theorem 3 in Chap. VII-6 in [**14**]. The functional equation gives the following corollary.

COROLLARY 2. *$\zeta_K(s)$ has a zero of order r_2 at $s = -1$ and has a zero of order $r_1 + r_2$ at $s = -2$.*

The next deep result is taken from Satz 171 of [**8**].

THEOREM 11. *Let K be an algebraic number field and let T be a positive number. Let $N(T)$ be the number of zeros of $\zeta_K(s)$ in the region* $0 \leq \mathrm{Re(s)} \leq 1, 0 < \mathrm{Im(s)} \leq \mathrm{T}$. *Then*

$$N(T) = \frac{n_K}{2\pi}T\log T + \frac{\log|D_K| - n_K - n_K\log(2\pi)}{2\pi}T + O(\log T),$$

where n_K is the field degree of K over $\mathbb{Q}$ and D_K is the discriminant of K.

Here, note that Landau symbol $O(\log T)$ denotes a function $f(T)$ such that

$$\overline{\lim_{T\to\infty}}\frac{|f(T)|}{\log T} < \infty.$$

We proceed to introduce the Artin L-series. Let K be an algebraic number field again and L/K be a finite Galois extension with the Galois group G. A complex representation of G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, where $\mathrm{GL}(V)$ denotes the automorphism group of a finite dimensional complex vector space V. We shall represent it by the pair (ρ, V). Let $\mathfrak{p}$ be a prime ideal of K and $\mathfrak{P}$ be a prime ideal of L lying above $\mathfrak{p}$. Then the decomposition group $G_{\mathfrak{P}}$ and the inertia group $T_{\mathfrak{P}}$ of $\mathfrak{P}$ are defined as subgroups of G as usual, and the quotient group $G_{\mathfrak{P}}/T_{\mathfrak{P}}$ is the cyclic group generated by the Frobenius automorphism $\varphi_{\mathfrak{P}}$. As $\varphi_{\mathfrak{P}}$ is regarded as an automorphism of the fixed subspace $V^{T_{\mathfrak{P}}}$ of $T_{\mathfrak{P}}$, the characteristic polynomial

$$\det(1 - \varphi_{\mathfrak{P}}t; V^{T_{\mathfrak{P}}}) \tag{6}$$

is defined, where t is an indeterminate and 1 denotes the identity map of $V^{T_{\mathfrak{P}}}$. The polynomial (6) is determined only by $\mathfrak{p}$, that is, independently on the choice of $\mathfrak{P}$ lying above $\mathfrak{p}$. Indeed, if $\mathfrak{P}'$ be another prime ideal of L lying above $\mathfrak{p}$, then there is $\sigma \in G$ such that $\mathfrak{P}' = \mathfrak{P}^{\sigma}$ and

$$G_{\mathfrak{P}'} = \sigma^{-1} G_{\mathfrak{P}} \sigma,\ T_{\mathfrak{P}'} = \sigma^{-1} T_{\mathfrak{P}} \sigma,\ \varphi_{\mathfrak{P}'} = \sigma^{-1} \varphi_{\mathfrak{P}} \sigma,$$

and therefore

$$\begin{aligned} \det(1 - \varphi_{\mathfrak{P}'} t; V^{T_{\mathfrak{P}'}}) &= \det(\sigma^{-1}(1 - \varphi_{\mathfrak{P}} t)\sigma; V^{\sigma^{-1} T_{\mathfrak{P}} \sigma}) \\ &= \det(1 - \varphi_{\mathfrak{P}} t; V^{T_{\mathfrak{P}}}). \end{aligned}$$

It is well-known that two complex representations ρ, ρ' of G are equivalent if and only if their characters $\chi_\rho, \chi_{\rho'}$ are equal. For a representation (ρ, V) of G with character χ, the Artin L-series of ρ (or χ) is defined by

$$\mathcal{L}(s, \chi, L/K) = \prod_{\mathfrak{p}} \frac{1}{\det(1 - \varphi_{\mathfrak{P}} \mathfrak{N}(\mathfrak{p})^{-s}; V^{T_{\mathfrak{P}}})}, \tag{7}$$

where $\mathfrak{p}$ runs through all prime ideals of K. It is not difficult to show that the Artin L-series (7) converges absolutely and uniformly on the half plane $\mathrm{Re}(s) > 1 + \delta$ for any $\delta > 0$.

To state the fundamental properties of Artin L-series, we need the induced character. Let H be a subgroup of a finite group G and (ρ, V) be a complex representation of H with character ψ. Then V may be considered as a $\mathbb{C}[H]$-module where $\mathbb{C}[H]$ denotes a group algebra of H over $\mathbb{C}$, and we put

$$\mathrm{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$$

which is a $\mathbb{C}[G]$-module, and therefore we obtain a complex representation of G

$$\mathrm{Ind}(\rho) : G \to \mathrm{GL}(\mathrm{Ind}_H^G(V)).$$

We denote the character of $\mathrm{Ind}(\rho)$ by χ_ψ and call it the induced character of ψ on G. In particular, we need the induced character χ_{1_H} of 1_H on G. Here, 1_H is the principal character of H, i.e., $1_H(h) = 1$ for any $h \in H$. We also call χ_{1_H} the induced character of G for H.

Lemma 2. *Let G be a finite group and let H be a subgroup of G. If ψ is a character of H , then*

$$\mathrm{Ind}(\psi)(\mathrm{s}) = \frac{1}{|\mathrm{H}|} \sum_{\mathrm{t} \in \mathrm{G}} \psi(\mathrm{tst}^{-1})$$

for $s \in G$. Here $|H|$ is the order of H and $\psi(s) = 0$ if $s \notin H$.

PROOF. Let $\{w_1, \ldots, w_m\}$ be a $\mathbb{C}$-basis of W. Let (σ, W) be a representation with character ψ. Let $\{g_1, \ldots, g_n\}$ be a full set of representatives of left coset modulo H in G. Then $\{g_1^{-1}, \ldots, g_n^{-1}\}$ is a full set of representatives of right coset modulo H in G. Moreover

$$\{g_i^{-1} \otimes w_j | i = 1, \ldots, m,\ j = 1, \ldots, n\}$$

is a $\mathbb{C}$-basis of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$. If $s \in G$, we have

$$s \cdot g_i^{-1} \otimes w_j = (sg_i^{-1}) \otimes w_j = (g_{i(s)}^{-1} s_i) \otimes w_j = g_{i(s)}^{-1} \otimes (s_i w_j),$$

where $i(s) \in \{1, \ldots, n\}, s_i \in H$ such that $sg_i^{-1} = g_{i(s)}^{-1} s_i$. From this, for $s \in G$, we get

$$\begin{aligned} \mathrm{Ind}(\psi)(s) &= \sum_{s=i(s)} \psi(s_i) = \sum_{s=i(s)} \psi(g_i s g_i^{-1}) \\ &= \sum_{i=1}^{n} \psi(g_i s g_i^{-1}) = \frac{1}{|H|} \sum_{t \in G} \psi(tst^{-1}) \end{aligned}$$

when we extend ψ to G so that $\psi(s) = 0$ if $s \notin H$. □

The Artin L-series has the following fundamental properties. We omit the proof and refer to Theorem 4.2 of Chap. V-4 of [**10**].

THEOREM 12. *Let K be an algebraic number field and L/K be a Galois extension.*
(i) $\mathcal{L}(s, 1, L/K) = \zeta_K(s)$ where 1 denotes the principal character of $\mathrm{Gal}(L/K)$.
(ii) If L'/K are also a finite Galois extension such that $L' \supseteq L$, then

$$\mathcal{L}(s, \chi \circ \pi, L'/K) = \mathcal{L}(s, \chi, L/K)$$

where π is the restriction map from $\mathrm{Gal}(L'/K)$ to $\mathrm{Gal}(L/K)$.
(iii) If χ_1, χ_2 are characters of $\mathrm{Gal}(L/K)$, then

$$\mathcal{L}(s, \chi_1 + \chi_2, L/K) = \mathcal{L}(s, \chi_1, L/K) \cdot \mathcal{L}(s, \chi_2, L/K).$$

(iv) If M is an intermediate field of L/K, ψ is a character of $\mathrm{Gal}(L/M)$ and χ_ψ is the induced character of ψ on $\mathrm{Gal}(L/K)$, then

$$\mathcal{L}(s, \chi_\psi, L/K) = \mathcal{L}(s, \psi, L/M).$$

The following theorem is our goal in this chapter.

THEOREM 13. *Let K be a finite Galois extension over $\mathbb{Q}$ with Galois group G. If H is a subgroup of G, we denote $H \leq G$ and the*

corresponding subfield of K by $\Omega(H)$. Suppose that there is a linear relation between the induced characters for the subgroups of G, that is,

$$\sum_{H\leq G} a_H \chi_{1_H} = 0$$

with $a_H \in \mathbb{Z}$. Then

$$\prod_{H\leq G}\left(\frac{R_{\Omega(H)}h_{\Omega(H)}}{w_{\Omega(H)}}\right)^{a_H} = 1. \tag{8}$$

Here R_Ω, h_Ω and w_Ω denote the regulator, the class number and the number of the roots of unity in Ω respectively when Ω is a subfield of K.

Proof. We reproduce Brauer's proof. By (iii) of Theorem 12, our assumption about induced characters gives

$$\prod_{H\leq G} \mathcal{L}(s, \chi_{1_H}, K/\mathbb{Q})^{a_H} = 1$$

and then we get

$$\prod_{H\leq G} \mathcal{L}(s, 1_H, K/\Omega(H))^{a_H} = 1$$

by (iv) of Theorem 12. Moreover, by (i) of Theorem 12, this means

$$\prod_{H\leq G} \zeta_{\Omega(H)}(s)^{a_H} = 1 \tag{9}$$

and, by taking the residue at $s = 1$, we obtain

$$\prod_{H\leq G}\left(\frac{2^{r_1(\Omega(H))}(2\pi)^{r_2(\Omega(H))}h_{\Omega(H)}R_{\Omega(H)}}{w_{\Omega(H)}|D_{\Omega(H)}|^{1/2}}\right)^{a_H} = 1. \tag{10}$$

Here, for any algebraic field number field Ω, we denote the number of the real places and the imaginary places by $r_1(\Omega)$ and $r_2(\Omega)$ respectively, and by D_Ω the discriminant. Applying Theorem 11 to (9), we obtain

$$\sum_{H\leq G} a_H n(\Omega(H)) = 0$$

and

$$\sum_{H\leq G} a_H \log|D_{\Omega(H)}| = 0, \tag{11}$$

where $n(\Omega)$ denotes the degree of Ω over $\mathbb{Q}$ for any algebraic number field Ω. Moreover, by Corollary 2, we also have

$$\sum_{H\leq G} a_H(r_1(\Omega(H))+r_2(\Omega(H)))=0, \tag{12}$$

$$\sum_{H\leq G} a_H r_2(\Omega(H))=0 \tag{13}$$

from (9). These shows that

$$\sum_{H\leq G} a_H r_1(\Omega(H))=0. \tag{14}$$

Substituting (11),(13),(14) for (10), we get the identity (8) in our assertion. □

6. Main Results

We denote by $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ and $\mathbb{R}$ the ring of rational integers, the set of all natural numbers, the rational number field and the real number field respectively. We consider that $0 \notin \mathbb{N}$. Let m be a fifth power free integer greater than one. Denote the real fifth root of m by $m^{1/5}$. Let $k=\mathbb{Q}(\zeta_5), k^+=\mathbb{Q}(\sqrt{5}), K=\mathbb{Q}(m^{1/5}), L=K(\zeta_5)$ and $L^+=K(\sqrt{5})$ where ζ_5 is a primitive fifth root of unity. Note that L^+ is a real algebraic number field. Let h_M and R_M denote the class number and the regulator of an arbitrary algebraic number field M respectively. We denote fundamental units of K by ϵ_1, ϵ_2 and a fundamental unit of k^+ by e. We may assume that $\epsilon_1, \epsilon_2, e>0$. Let $G=\mathrm{Gal}(L/\mathbb{Q})$. Define $\tau, \sigma \in G$ by the following actions respectively:

$$\zeta_5^\tau=\zeta_5^2,\ (m^{1/5})^\tau=m^{1/5},$$
$$\zeta_5^\sigma=\zeta_5,\ (m^{1/5})^\sigma=\zeta_5 m^{1/5}.$$

These actions satisfy the following relations:

$$\sigma\tau=\tau\sigma^2,\ \tau\sigma=\sigma^3\tau.$$

Moreover, it should be noted that τ^2 is the complex conjugate on L. The multiplicative group $L^\times$ of non-zero elements of L will be regarded as a $\mathbb{Z}[G]$-module. Here $\mathbb{Z}[G]$ denotes a group ring of G over $\mathbb{Z}$. In other words, the result of the multiplication of $x \in L^\times$ by $\sum_{\rho\in G} a_\rho \rho \in \mathbb{Z}[G]$ is $x^{\sum_{\rho\in G} a_\rho \rho}=\prod_{\rho\in G}(x^{a_\rho})^\rho$.

Lemma 3. *Let $\{c_1, c_2, c_3\}$ be a coprime set of integers. Then $\epsilon_1^{c_1}\epsilon_2^{c_2}e^{c_3}$ is not a fifth power of a unit of L^+.*

Proof. Suppose that there is a unit u of L^+ such that

$$\epsilon_1^{c_1}\epsilon_2^{c_2}e^{c_3} = u^5. \tag{15}$$

Multiplying (15) by $2(1+\tau)$, we get

$$\epsilon_1^{4c_1}\epsilon_2^{4c_2} = (u^{1+\tau})^{10}. \tag{16}$$

Since $u^{1+\tau}$ is a unit of K and ϵ_1, ϵ_2 are fundamental units of K, we may represent

$$u^{1+\tau} = \pm\epsilon_1^{a_1}\epsilon_2^{a_2}$$

with $a_1, a_2 \in \mathbb{Z}$. We substitute this for (16) and get

$$\epsilon_1^{4c_1}\epsilon_2^{4c_2} = \epsilon_1^{10a_1}\epsilon_2^{10a_2},$$

which shows

$$4c_1 = 10a_1,\ 4c_2 = 10a_2$$

because ϵ_1, ϵ_2 are fundamental units of K. From this, we see that c_1 and c_2 are multiples of five. Therefore, by (15), we get

$$e^{c_3} = v^5 \tag{17}$$

where v is a positive unit of L^+. Multiplying (17) by σ, we obtain

$$e^{c_3} = (v^\sigma)^5. \tag{18}$$

Combining (18) with (17), we have

$$(v^\sigma)^5 = v^5,$$

which shows

$$(v^{\sigma-1})^5 = 1. \tag{19}$$

Since L^+ contains only one fifth power root of unity, i.e., 1, it follows from (19) that

$$v^\sigma = v,$$

and so v is a unit of k^+. Therefore we may represent

$$v = e^b$$

with $b \in \mathbb{Z}$, and we also get

$$e^{c_3} = e^{5b}$$

by (17). Since e is the positive fundamental unit of k^+, it follows that c_3 is a multiple of five. Thus we see that c_1, c_2, c_3 are all multiples of five, and it contradicts with the coprimality of the set $\{c_1, c_2, c_3\}$. Hence our assertion is valid. □

Lemma 4. *There is a set of fundamental units of L^+ which contains $\epsilon_1, \epsilon_2, e$.*

Proof. Suppose that the assertion is false. Applying Theorem 7 to the full positive unit group of L^+ and the subgroup generated by ϵ_1, ϵ_2 and e, we get a positive unit of L^+ such that

$$\epsilon_1^{c_1}\epsilon_2^{c_2}e^{c_3} = u^d, \tag{20}$$

where the set $\{c_1, c_2, c_3\}$ is a coprime integer set and d is an integer greater than one. Multiplying (20) by $2(1+\sigma+\cdots+\sigma^4)$, we get

$$e^{10c_3} = (u^{1+\sigma+\cdots+\sigma^4})^{2d},$$

which implies that $d|5c_3$ since e is a fundamental unit of k^+. Multiplying (20) by $2(1+\tau)$, we get

$$\epsilon_1^{4c_1}\epsilon_2^{4c_2} = (u^{1+\tau})^{2d},$$

which implies that $d|2c_1$ and $d|2c_2$ since ϵ_1, ϵ_2 are fundamental units of K. Since the integer set $\{c_1, c_2, c_3\}$ is coprime, we see that d is a divisor of 10. If $5|d$, we may represent $d = 5d'$ with $d' \in \mathbb{N}$, and by (20), we get

$$\epsilon_1^{c_1}\epsilon_2^{c_2}e^{c_3} = (u^{d'})^5,$$

which contradicts with Lemma 3. Hence $d = 2$. Then c_3 must be even, and so we may represent $c_3 = 2c$ with $c \in \mathbb{Z}$. By (20), we get

$$\epsilon_1^{c_1}\epsilon_2^{c_2} = (ue^{-c})^2. \tag{21}$$

From this, we obtain

$$(\epsilon_1^{c_1}\epsilon_2^{c_2})^{1/2} = ue^{-c} \in L^+ = K(\sqrt{5}). \tag{22}$$

Applying Theorem 15 in the appendix below to (22), we get

$$(\epsilon_1^{c_1}\epsilon_2^{c_2})^{1/2} = \alpha 5^{a/2}, \tag{23}$$

$$(\epsilon_1^{c_1}\epsilon_2^{c_2}) = \alpha^2 5^a, \tag{24}$$

where $\alpha \in K$ and $a \in \mathbb{Z}$. It is easy to see that there is a prime ideal $\mathcal{P}$ of the maximal order of K above the prime ideal $5\mathbb{Z}$ such that $\mathcal{P}$ has an odd ramification index in $K/\mathbb{Q}$. Taking the value of the $\mathcal{P}$-adic exponential valuation at (24), we see that a is even. Hence, by (22) and (23), we see that ue^{-c} is a unit of K. Then it follows from (21) that c_1 and c_2 are even since ϵ_1, ϵ_2 are fundamental units of K. However, it contradicts with the coprimality of the set $\{c_1, c_2, c_3\}$, and therefore the assertion is verified. □

Let ϵ_3, ϵ_4 be positive units such that $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, e$ are fundamental units of L^+.

Proposition 2.

$$\frac{R_{L^+}}{R_K^2 \cdot R_{k^+}} \cdot h_{L^+} = h_K^2.$$

Proof. Recall that $G = \mathrm{Gal}(L/\mathbb{Q})$. For $g \in G$, We denote the conjugacy class of g by $C(g)$. It is easy to see that the set of conjugacy classes of G is

$$\{C(1),\ C(\sigma),\ C(\tau),\ C(\tau^2),\ C(\tau^3)\}.$$

The number of the elements of $C(1)$ is one and that of $C(\sigma)$ is four. The number of the elements of $C(\tau^i)$ is five for $i = 1, 2, 3$. On the other hand, it is easy to see that

$$\mathrm{Gal}(L/L^+) = \{1, \tau^2\}, \quad \mathrm{Gal}(L/k) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\},$$
$$\mathrm{Gal}(L/k^+) = \langle \sigma, \tau^2 \rangle, \quad \mathrm{Gal}(L/K) = \{1, \tau, \tau^2, \tau^3\}.$$

Here, $\langle \sigma, \tau^2 \rangle$ is the subgroup of G generated by σ, τ^2. We denote by χ_M the induced character of G for subgroup $\mathrm{Gal}(L/M)$ where M is an arbitrary subfield of L. Then we get Table 1.

Table 1

	$C(1)$	$C(\sigma)$	$C(\tau)$	$C(\tau^2)$	$C(\tau^3)$
χ_L	20	0	0	0	0
χ_{L^+}	10	0	0	2	0
χ_k	4	4	0	0	0
χ_{k^+}	2	2	0	2	0
χ_K	5	0	1	1	1
$\chi_{\mathbb{Q}}$	1	1	1	1	1

From this table, it is easy to see

$$2(\chi_K - \chi_{\mathbb{Q}}) = \chi_{L^+} - \chi_{k^+}$$

and we obtain the regulator relation by Theorem 13. □

Let E_{L^+} denote the unit group of L^+ and $\mathcal{E}$ the subgroup of E_{L^+} generated by $-1, \epsilon_1, \epsilon_2, \epsilon_1^{\sigma+\sigma^{-1}}, \epsilon_2^{\sigma+\sigma^{-1}}, e$. Note that, for $i = 1, 2$,

$$\epsilon_i^{\sigma+\sigma^{-1}} = (\epsilon_i^{\sigma})^{1+\tau^2} = |\epsilon_i^{\sigma}|^2 > 0$$

because τ^2 is the complex conjugate on L. It is important to consider the index of $\mathcal{E}$ in E_{L^+}.

Lemma 5. *The quotient group $E_{L^+}/\mathcal{E}$ has exponent 5, i.e., $E_{L^+}^5 \subseteq \mathcal{E}$.*

Proof. We shall denote the norm map of L to K^{σ^i} by N_i for $i = 1, 2, 3, 4, 5$. Besides, we denote the norm map of L to k by N_0. Let $\varepsilon \in E_{L^+}$. Since the Galois group of L/K^{σ^i} is $\sigma^{-i}\mathrm{Gal}(L/K)\sigma^i$ and $\mathrm{Gal}(L/K) = \{1, \tau, \tau^2, \tau^3\}$, we obtain

$$\begin{aligned} N_i(\varepsilon) &= \varepsilon^{\sigma^{-i}(1+\tau+\tau^2+\tau^3)\sigma^i} = \varepsilon^{1+\tau\sigma^{i-2i}+\tau^2\sigma^{i-4i}+\tau^3\sigma^{i-8i}} \\ &= \varepsilon^{1+\tau\sigma^{-i}+\tau^2\sigma^{-3i}+\tau^3\sigma^{-2i}}. \end{aligned}$$

Since $\mathrm{Gal}(L/k) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, we obtain

$$N_0(\varepsilon^{\tau^i}) = \varepsilon^{\tau^i(1+\sigma+\sigma^2+\sigma^3+\sigma^4)}.$$

Then

$$\varepsilon^5 = \frac{\varepsilon^{5+(\tau+\tau^2+\tau^3)(1+\sigma+\sigma^2+\sigma^3+\sigma^4)}}{\varepsilon^{(\tau+\tau^2+\tau^3)(1+\sigma+\sigma^2+\sigma^3+\sigma^4)}} = \frac{N_1(\varepsilon)N_2(\varepsilon)N_3(\varepsilon)N_4(\varepsilon)N_5(\varepsilon)}{N_0(\varepsilon^\tau)N_0(\varepsilon^{\tau^2})N_0(\varepsilon^{\tau^3})}. \tag{25}$$

For $i = 1, \ldots, 5$, $N_i(\varepsilon)$ is in the unit group of K^{σ^i}, which is generated by

$$-1, \epsilon_1^{\sigma^i}, \epsilon_2^{\sigma^i},$$

and so $N_i(\varepsilon)$ is represented by

$$N_i(\varepsilon) = \pm\epsilon_1^{a_i\sigma^i}\epsilon_2^{b_i\sigma^i}$$

with $a_i, b_i \in \mathbb{Z}$. Then we obtain

$$\begin{aligned} N_1(\varepsilon)^{\tau^2} &= \varepsilon^{\sigma^{-1}(1+\tau+\tau^2+\tau^3)\sigma\tau^2} = \varepsilon^{\tau^2\sigma^{-4}(1+\tau+\tau^2+\tau^3)\sigma^4} = N_4(\varepsilon) \\ N_2(\varepsilon)^{\tau^2} &= \varepsilon^{\sigma^{-2}(1+\tau+\tau^2+\tau^3)\sigma^2\tau^2} = \varepsilon^{\tau^2\sigma^{-3}(1+\tau+\tau^2+\tau^3)\sigma^3} = N_3(\varepsilon) \end{aligned}$$

because ε is real and τ^2 induces the complex conjugate map on L. Hence, we have

$$\begin{aligned} N_1(\varepsilon)N_4(\varepsilon) &= \epsilon_1^{a_1(\sigma+\sigma^{-1})}\epsilon_2^{b_1(\sigma+\sigma^{-1})} \\ N_2(\varepsilon)N_3(\varepsilon) &= \epsilon_1^{a_2(\sigma^2+\sigma^{-2})}\epsilon_2^{b_2(\sigma^2+\sigma^{-2})} = \pm\epsilon_1^{-a_2(1+\sigma+\sigma^{-1})}\epsilon_2^{-b_2(1+\sigma+\sigma^{-1})} \end{aligned}$$

because $N_0(\epsilon_i) = \epsilon_i^{1+(\sigma+\sigma^{-1})+(\sigma^2+\sigma^{-2})} = \pm 1$ for i =1,2. Thus the numerator of the right side of (25) equals to

$$\pm\epsilon_1^{(a_5-a_2)+(a_1-a_2)(\sigma+\sigma^{-1})}\epsilon_2^{(b_5-b_2)+(b_1-b_2)(\sigma+\sigma^{-1})},$$

which is in $\mathcal{E}$. Moreover the denominator of the right side of (25) is in the unit group of k and

$$\begin{aligned} (N_0(\varepsilon^\tau)N_0(\varepsilon^{\tau^2})N_0(\varepsilon^{\tau^3}))^{\tau^2} &= \varepsilon^{(\tau+\tau^2+\tau^3)(1+\sigma+\sigma^2+\sigma^3+\sigma^4)\tau^2} \\ = \varepsilon^{(\tau^3+1+\tau)(1+\sigma+\sigma^2+\sigma^3+\sigma^4)} &= \varepsilon^{(\tau^3+\tau^2+\tau)(1+\sigma+\sigma^2+\sigma^3+\sigma^4)} \\ &= N_0(\varepsilon^\tau)N_0(\varepsilon^{\tau^2})N_0(\varepsilon^{\tau^3}) \end{aligned}$$

because ε is real and τ^2 induces the complex conjugate map on L. This shows that the denominator of the right side of (25) is in the unit group of k^+ which is generated by $-1, e$, and so it is in $\mathcal{E}$. Thus $\varepsilon^5 \in \mathcal{E}$ and the proof is completed. $\square$

We may represent

$$(\log\epsilon_1, \log\epsilon_2, \log\epsilon_1^{\sigma+\sigma^{-1}}, \log\epsilon_2^{\sigma+\sigma^{-1}}, \log e) = (\log\epsilon_1, \log\epsilon_2, \log\epsilon_3, \log\epsilon_4, \log e)P \tag{26}$$

by an integer matrix P.

Proposition 3.

$$\frac{h_K^2}{h_{L^+}} = \frac{R_{L^+}}{R_K^2 \cdot R_{k^+}} = \frac{5^2}{|\det(P)|} \in \mathbb{N}.$$

Proof. The first equality follows directly by Proposition 2. We shall show the second equality. From (26), we obtain a regulator relation as follows: $|\det(P)| \cdot R_{L^+} =$

$$\left|\det\begin{pmatrix} \log\epsilon_1 & 2\log|\epsilon_1^{\sigma}| & 2\log|\epsilon_1^{\sigma^2}| & 2\log|\epsilon_1^{\sigma}| & 2\log|\epsilon_1^{\sigma^2}| \\ \log\epsilon_2 & 2\log|\epsilon_2^{\sigma}| & 2\log|\epsilon_2^{\sigma^2}| & 2\log|\epsilon_2^{\sigma}| & 2\log|\epsilon_2^{\sigma^2}| \\ \log\epsilon_1^{\sigma+\sigma^{-1}} & 2\log|\epsilon_1^{\sigma^2+1}| & 2\log|\epsilon_1^{\sigma^3+\sigma}| & 2\log|\epsilon_1^{\sigma^3+\sigma^{-1}}| & 2\log|\epsilon_1^{\sigma^4+1}| \\ \log\epsilon_2^{\sigma+\sigma^{-1}} & 2\log|\epsilon_2^{\sigma^2+1}| & 2\log|\epsilon_2^{\sigma^3+\sigma}| & 2\log|\epsilon_2^{\sigma^3+\sigma^{-1}}| & 2\log|\epsilon_2^{\sigma^4+1}| \\ \log e & 2\log e & 2\log e & -2\log e & -2\log e \end{pmatrix}\right| =$$

$$\left|\det\begin{pmatrix} 0 & 2\log|\epsilon_1^{\sigma}| & 2\log|\epsilon_1^{\sigma^2}| & 0 & 0 \\ 0 & 2\log|\epsilon_2^{\sigma}| & 2\log|\epsilon_2^{\sigma^2}| & 0 & 0 \\ 0 & 2\log|\epsilon_1^{\sigma^2+1}| & 2\log|\epsilon_1^{\sigma^3+\sigma}| & 2\log|\epsilon_1^{\sigma^3+\sigma^4-\sigma^2-1}| & 2\log|\epsilon_1^{\sigma^4+1-\sigma^3-\sigma}| \\ 0 & 2\log|\epsilon_2^{\sigma^2+1}| & 2\log|\epsilon_2^{\sigma^3+\sigma}| & 2\log|\epsilon_2^{\sigma^3+\sigma^4-\sigma^2-1}| & 2\log|\epsilon_2^{\sigma^4+1-\sigma^3-\sigma}| \\ 5\log e & 2\log e & 2\log e & -4\log e & -4\log e \end{pmatrix}\right|$$

$$= \left|5\log e \cdot \det\begin{pmatrix} 2\log|\epsilon_1^{\sigma}| & 2\log|\epsilon_1^{\sigma^2}| \\ 2\log|\epsilon_2^{\sigma}| & 2\log|\epsilon_2^{\sigma^2}| \end{pmatrix} \cdot \det\begin{pmatrix} 2\log|\epsilon_1^{\sigma-1}| & 2\log|\epsilon_1^{1-\sigma^2}| \\ 2\log|\epsilon_2^{\sigma-1}| & 2\log|\epsilon_2^{1-\sigma^2}| \end{pmatrix}\right|$$

$$= \left|5\log e \cdot \det\begin{pmatrix} \log\epsilon_1 & 2\log|\epsilon_1^{\sigma^2}| \\ \log\epsilon_2 & 2\log|\epsilon_2^{\sigma^2}| \end{pmatrix} \cdot \det\begin{pmatrix} 5\log\epsilon_1 & 2\log|\epsilon_1^{1-\sigma^2}| \\ 5\log\epsilon_2 & 2\log|\epsilon_2^{1-\sigma^2}| \end{pmatrix}\right|$$

$$= 5^2 \cdot R_{k^+} \cdot {R_K}^2.$$

Thus the second equality of our assertion is verified. It is rest to prove that $5^2/|\det(P)| \in \mathbb{N}$. By Lemma 5, we see that $\epsilon_3^5, \epsilon_4^5 \in \mathcal{E}$, and therefore there is an integer matrix Q such as

$$(\log\epsilon_1, \log\epsilon_2, \log\epsilon_3^5, \log\epsilon_4^5, \log e) = (\log\epsilon_1, \log\epsilon_2, \log\epsilon_1^{\sigma+\sigma^{-1}}, \log\epsilon_2^{\sigma+\sigma^{-1}}, \log e)Q.$$

Then we have

$$\begin{aligned}(\log\epsilon_1, \log\epsilon_2, \log\epsilon_3, \log\epsilon_4, \log e)A &= (\log\epsilon_1, \log\epsilon_2, \log\epsilon_3^5, \log\epsilon_4^5, \log e)\\ &= (\log\epsilon_1, \log\epsilon_2, \log\epsilon_1^{\sigma+\sigma^{-1}}, \log\epsilon_2^{\sigma+\sigma^{-1}}, \log e)Q\\ &= (\log\epsilon_1, \log\epsilon_2, \log\epsilon_3, \log\epsilon_4, \log e)PQ,\end{aligned}$$

where $A = (a_{ij})$ is a five-by-five diagonal matrix with $a_{11} = a_{22} = a_{55} = 1$ and $a_{33} = a_{44} = 5$. Since $A = PQ$, we get $|\det(Q)| = 5^2/|\det(P)|$. Moreover, as Q is an integer matrix, we see that $5^2/|\det(P)| \in \mathbb{N}$, which completes our proof. □

Corollary 3. *The class number h_K is a multiple of five if $|\det(P)| \neq 5^2$.*

Proof. It follows from Proposition 3 that $|\det(P)|$ is a divisor of 5^2, and so h_K^2/h_{L^+} is a multiple of five if $|\det(P)| \neq 5^2$, which implies that $5|h_K$. □

Corollary 4. *The class number h_K is a multiple of five if and only if h_{L^+} is a multiple of five.*

Proof. There is a prime ideal P of the maximal order of K above $5\mathbb{Z}$ whose ramification index is odd. Since the prime ideal of k^+ above $5\mathbb{Z}$ has an even ramification index, the prime ideal P is ramified in L^+. Therefore the quadratic extension L^+/K is ramified, and so it follows from Theorem 10.1 of [**13**] that $5|h_{L^+}$ if $5|h_K$. Conversely, suppose that $5|h_{L^+}$. If $|\det(P)| \neq 5^2$, the class number of K is a multiple of five by Corollary 3. If $|\det(P)| = 5^2$, it follows from Proposition 3 that $h_{L^+} = h_K^2$, which shows that $5|h_K$. Thus, our assertion is completely verified. □

Assume

$$|\det(P)| = 5^2 \tag{27}$$

from now on.

Proposition 4. *There are units $u_1, u_2 \in E_{L^+}$ such that $\epsilon_i^{\sigma+\sigma^{-1}-2} = u_i^5$ for $i = 1, 2$.*

Proof. From (27) and Lemma 5, there are units $v_1, v_2 \in E_{L^+}$ such that

$$\epsilon_1^{b_{i1}+b_{i2}(\sigma+\sigma^{-1})}\epsilon_2^{b_{i3}+b_{i4}(\sigma+\sigma^{-1})}e^{b_{i5}} = v_i^5 \tag{28}$$

for $i = 1, 2$, where the integer matrix

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15}\\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25}\end{pmatrix}$$

has rank 2 after reduction modulo 5. Further, we see that the matrix

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \end{pmatrix} \tag{29}$$

has rank 2 after reduction modulo 5. Indeed, if not so, we may consider that $b_{21} = \cdots = b_{24} = 0$ and $b_{25} = 1$, and then (28) implies that e is a fifth power element of some unit in L^+, which contradicts with Lemma 4. Multiplying (28) by $2(\sigma + \sigma^{-1}) + 1$, we obtain

$$(\epsilon_1^{b_{i2}-2b_{i1}}\epsilon_2^{b_{i4}-2b_{i3}})^{\sigma+\sigma^{-1}-2} = (\epsilon_1^{b_{i1}}\epsilon_2^{b_{i3}}e^{b_{i5}}v_i^{-(2\sigma+2\sigma^{-1}+1)})^5 \tag{30}$$

for $i = 1, 2$. If the integer matrix

$$\begin{pmatrix} b_{12} - 2b_{11} & b_{14} - 2b_{13} \\ b_{22} - 2b_{21} & b_{24} - 2b_{23} \end{pmatrix} \tag{31}$$

is regular modulo 5, the assertion follows from (30) immediately. Therefore we may suppose that the matrix (31) has rank less than two.

Assume that the rank of the matrix (31) is zero. Then, it follows from (28) that there are units $\nu_1, \nu_2 \in E_{L^+}$ such that

$$\epsilon_1^{b_{i2}(\sigma+\sigma^{-1}-2)}\epsilon_2^{b_{i4}(\sigma+\sigma^{-1}-2)}e^{b_{i5}} = \nu_i^5 \tag{32}$$

for $i = 1, 2$. Take $c_1, c_2 \in \mathbb{Z}$ such that $c_1b_{15} + c_2b_{25} \equiv 0 \pmod 5$ and $(c_1, c_2) \not\equiv (0, 0) \pmod 5$. As the matrices (29) and (31) have rank two and zero after reduction modulo 5 respectively, it is easy to see that the matrix

$$\begin{pmatrix} b_{12} & b_{14} \\ b_{22} & b_{24} \end{pmatrix}$$

has rank two after reduction modulo 5, and so the matrix

$$(d_1, d_2) = \begin{pmatrix} c_1b_{12} + c_2b_{22} & c_1b_{14} + c_2b_{24} \end{pmatrix}$$

has rank one after reduction modulo 5. Hence, without loss of generality, we may assume that $d_1 \equiv 1 \pmod 5$ by retaking suitable c_i for $i = 1, 2$ and exchanging the indices of ϵ_1, ϵ_2 if necessary. Then, by (32), we see that there is a unit $\nu \in E_{L^+}$ such that

$$\varepsilon_1^{\sigma+\sigma^{-1}-2} = \nu^5, \tag{33}$$

where $\varepsilon_1 = \epsilon_1\epsilon_2^{d_2}$. It is obvious that $\varepsilon_1, \epsilon_2$ are fundamental units of K. Note that Lemma 4 holds even if we replace ϵ_1 by ε_1. Moreover, we

have

$$\begin{aligned}&(\log\varepsilon_1,\log\epsilon_2,\log\varepsilon_1^{\sigma+\sigma^{-1}},\log\epsilon_2^{\sigma+\sigma^{-1}},\log e)\\=&(\log\epsilon_1,\log\epsilon_2,\log\epsilon_1^{\sigma+\sigma^{-1}},\log\epsilon_2^{\sigma+\sigma^{-1}},\log e)B\\=&(\log\epsilon_1,\log\epsilon_2,\log\epsilon_3,\log\epsilon_4,\log e)PB\\=&(\log\varepsilon_1,\log\epsilon_2,\log\epsilon_3,\log\epsilon_4,\log e)D^{-1}PB\end{aligned}$$

where

$$B=\begin{pmatrix}1&0&0&0&0\\d_2&1&0&0&0\\0&0&1&0&0\\0&0&d_2&1&0\\0&0&0&0&1\end{pmatrix},\ D=\begin{pmatrix}1&0&0&0&0\\d_2&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}.$$

Since

$$|\det(D^{-1}PB)|=5^2 \tag{34}$$

by (27), our assumption (27) also holds even if we replace ϵ_1 by ε_1. Hence, by (33), (34) and Lemma 5, there are units $\eta_1,\eta_2\in E_{L^+}$ such that

$$\varepsilon_1^{\beta_{i1}}\epsilon_2^{\beta_{i3}+\beta_{i4}(\sigma+\sigma^{-1})}e^{\beta_{i5}}=\eta_i^5 \tag{35}$$

for $i=1,2$, where the integer matrix

$$\begin{pmatrix}\beta_{11}&\beta_{13}&\beta_{14}&\beta_{15}\\\beta_{21}&\beta_{23}&\beta_{24}&\beta_{25}\end{pmatrix} \tag{36}$$

has rank 2 after reduction modulo 5. Obviously, we may assume that $\beta_{21}=0$. Then, multiplying (35) by $1+\tau$, we have

$$\varepsilon_1^{2\beta_{11}}\epsilon_2^{2\beta_{13}-\beta_{14}}=(\eta_1e^{\beta_{15}})^{5(1+\tau)}, \tag{37}$$

$$\epsilon_2^{2\beta_{23}-\beta_{24}}=(\eta_2e^{\beta_{25}})^{5(1+\tau)}, \tag{38}$$

because $e^{\beta_{i5}(1+\tau)}=(-1)^{\beta_{i5}}=e^{5\beta_{i5}(1+\tau)}$ for $i=1,2$. From Lemma 4, the equation (38) implies that

$$2\beta_{23}\equiv\beta_{24}\pmod 5.$$

Moreover, multiplying (37) by $\sigma+\sigma^{-1}-2$, we obtain

$$\epsilon_2^{(2\beta_{13}-\beta_{14})(\sigma+\sigma^{-1}-2)}=\left(\eta_1^{(1+\tau)(\sigma+\sigma^{-1}-2)}\nu^{-2\beta_{11}}\right)^5 \tag{39}$$

by (33). Assume that $2\beta_{13}\equiv\beta_{14}\pmod 5$. Then it follows from (37) and Lemma 4 that $\beta_{11}\equiv 0\pmod 5$. Since the matrix (36) has rank

two, we now see that the matrix

$$\begin{pmatrix} \beta_{14} & \beta_{15} \\ \beta_{24} & \beta_{25} \end{pmatrix} \tag{40}$$

is regular modulo 5. By (35), we have

$$\epsilon_2^{\beta_{i4}(\sigma+\sigma^{-1}-2)} e^{\beta_{i5}} = \eta_i^5 \varepsilon_1^{-\beta_{i1}} \epsilon_2^{-\beta_{i3}-2\beta_{i4}} \tag{41}$$

for $i = 1, 2$. The right side of (41) is a fifth power element of a unit of L^+ because $\beta_{i1} \equiv \beta_{i3} + 2\beta_{i4} \equiv 0 \pmod 5$ for $i = 1, 2$. As the matrix (40) is regular modulo 5, it follows from (41) that e is a fifth power element of a unit of L^+, which contradicts with Lemma 4. Thus we get $2\beta_{13} \not\equiv \beta_{14} \pmod 5$, and then it follows from (39) that there is a unit u_2 of L^+ such that $\epsilon_2^{\sigma+\sigma^{-1}-2} = u_2^5$. As $\varepsilon_1 = \epsilon_1 \epsilon_2^{d_2}$, our assertion follows from (33).

Assume that the rank of the matrix (31) is one. We may suppose that the matrix

$$(d_1, d_2) = \begin{pmatrix} b_{12} - 2b_{11} & b_{14} - 2b_{13} \end{pmatrix}$$

has rank one after reduction modulo 5 and $d_1 \not\equiv 0 \pmod 5$ by exchanging the indices of ϵ_1, ϵ_2 if necessary. Obviously, we may further assume that $d_1 \equiv 1 \pmod 5$. Then, by (30), there is a unit $\nu \in E_{L^+}$ such that

$$\varepsilon_1^{\sigma+\sigma^{-1}-2} = \nu^5,$$

where $\varepsilon_1 = \epsilon_1 \epsilon_2^{d_2}$. Thus we reach (33) of the rank zero case, and it is easy to see that the rest of the proof for the rank zero case is also valid for the rank one case. Therefore our assertion is true for this case, and hence the whole proof is completed. □

It follows from (26) and (27) that $\mathcal{E}$ is a subgroup of E_{L^+} with index 5^2. Denote E_0 by the subgroup of E_{L^+} generated by $-1, \epsilon_1, \epsilon_2, u_1, u_2, e$, where u_1, u_2 are taken as in Proposition 4. It follows from Proposition 4 that $\mathcal{E}$ is a subgroup of E_0 with index 5^2. Hence, we see that $E_0 = E_{L^+}$, i.e., $\epsilon_1, \epsilon_2, u_1, u_2, e$ are fundamental units of L^+. We set $\epsilon_3 = u_1$ and $\epsilon_4 = u_2$ from now on.

Proposition 5. *$\epsilon_{i+2}^{1+\tau} = \epsilon_i^{-1}$ and $\epsilon_{i+2}^{\sigma+\sigma^{-1}-2} = \epsilon_i^{-1}\epsilon_{i+2}^{-5}$ for $i = 1, 2$.*

Proof. For $i = 1, 2$, multiplying the equation $\epsilon_{i+2}^5 = \epsilon_i^{\sigma+\sigma^{-1}-2}$ by $1 + \tau$ and $\sigma + \sigma^{-1} - 2$, we obtain

$$\epsilon_{i+2}^{5(1+\tau)} = \epsilon_i^{(\sigma+\sigma^{-1}-2)(1+\tau)} = \epsilon_i^{(\sigma+\sigma^{-1}+\sigma^2+\sigma^{-2}-4)} = \epsilon_i^{-5}, \tag{42}$$

$$\begin{aligned} \epsilon_{i+2}^{5(\sigma+\sigma^{-1}-2)} = \epsilon_i^{(\sigma+\sigma^{-1}-2)^2} &= \epsilon_i^{(\sigma+\sigma^{-1})^2-4(\sigma+\sigma^{-1})+4} = \epsilon_i^{5-5(\sigma+\sigma^{-1})} \\ &= (\epsilon_i^{-1} \cdot \epsilon_i^{2-\sigma-\sigma^{-1}})^5 = (\epsilon_i^{-1} \cdot \epsilon_{i+2}^{-5})^5 \end{aligned} \tag{43}$$

respectively, because $\epsilon_i^{1+\sigma+\sigma^{-1}+\sigma^2+\sigma^{-2}} = 1$. Moreover,

$$\epsilon_{i+2}^{1+\tau},\ \epsilon_i^{-1},\ \epsilon_{i+2}^{\sigma+\sigma^{-1}-2},\ \epsilon_i^{-1}\epsilon_{i+2}^{-5} \in E_{L^+} \text{ for } i = 1, 2,$$

because they are invariant under τ^2. Therefore the assertion follows immediately from (42) and (43) since L^+ is a real algebraic number field. □

Corollary 5. *The kernel of the norm homomorphism $1+\tau$ between the unit groups of L^+ and K is generated by $-1, \epsilon_1\epsilon_3^2, \epsilon_2\epsilon_4^2$ and e^2.*

Proof. It is obvious that -1 and e^2 are in the kernel. Since $\epsilon_{i+2}^{1+\tau} = \epsilon_i^{-1}$ for $i = 1, 2$, the kernel also contains $\epsilon_1\epsilon_3^2$ and $\epsilon_2\epsilon_4^2$. Conversely, take $\iota \in E_{L^+}$ such that $\iota^{1+\tau} = 1$. We may represent

$$\iota = \delta\epsilon_1^{a_1}\epsilon_2^{a_2}\epsilon_3^{a_3}\epsilon_4^{a_4}e^{a_5},$$

where $\delta = \pm 1$ and $a_i \in \mathbb{Z}$ for $i = 1, \ldots, 5$. Since $\iota^{1+\tau} = 1$, we have

$$\iota^{1+\tau} = \epsilon_1^{2a_1}\epsilon_2^{2a_2}\epsilon_3^{a_3(1+\tau)}\epsilon_4^{a_4(1+\tau)}(e^{1+\tau})^{a_5} = \epsilon_1^{2a_1-a_3}\epsilon_2^{2a_2-a_4}(-1)^{a_5} = 1,$$

which shows that a_5 is even and $a_{i+2} = 2a_i$ for $i = 1, 2$. Thus the assertion is proved. □

Lemma 6. *Let p be a prime divisor of m. Then the prime ideal $p\mathbb{Z}$ is totally ramified in K.*

Proof. Denote the maximal order of K by $\mathcal{O}_K$. We use the following ideal decomposition in $\mathcal{O}_K$:

$$m\mathcal{O}_K = (m^{1/5}\mathcal{O}_K)^5. \tag{44}$$

Take a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above $p\mathbb{Z}$. Taking the value of the $\mathfrak{p}$-adic exponential valuation at (44), we see that the ramification index of $\mathfrak{p}$ in $K/\mathbb{Q}$ is a multiple of five since m is a fifth power free. This shows that $p\mathbb{Z}$ is totally ramified in K. □

Theorem 14. *Suppose that m has a prime factor p with $p \equiv -1 \pmod 5$. Then the class number h_K of K is a multiple of five.*

Proof. In this proof, we shall denote h_{L^+} by h simply. Assume that h_K is not a multiple of 5. Then it follows from Corollary 4 that the class number h of L^+ is neither. It also follows from Corollary 3 that the condition (27) holds, and therefore we may take a set of fundamental units $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, e$ of L^+ as above. Since the prime ideal $p\mathbb{Z}$ totally ramifies in K by Lemma 6 and splits in k^+, there are two prime ideals $\mathfrak{P}_1, \mathfrak{P}_2$ of L^+ over $p\mathbb{Z}$ whose ramification indices over k^+ are five. Denote by $\mathcal{O}_M$ the maximal order of an arbitrary field M. We may represent $\mathfrak{P}_1^h = x_1\mathcal{O}_{L^+}$ with $x_1 \in \mathcal{O}_{L^+}$. Let $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}_{k^+}$ for

$i = 1, 2$. Similarly we may represent $\mathfrak{p}_1^h = y_1\mathcal{O}_{k^+}$ with $y_1 \in \mathcal{O}_{k^+}$. Set $x_2 = x_1^\tau, y_2 = y_1^\tau$ and $z_i = y_i/x_i^5$ for $i = 1, 2$. Since e/e^τ is negative, we may assume that

$$y_1/y_2 > 0, \tag{45}$$

replacing y_1 by ey_1 if necessary. For $i = 1, 2$, as the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}_i$ is five, we have

$$y_i\mathcal{O}_{L^+} = \mathfrak{p}_i^h\mathcal{O}_{L^+} = \mathfrak{P}_i^{5h} = (x_i\mathcal{O}_{L^+})^5 = x_i^5\mathcal{O}_{L^+},$$

which shows that z_i is a unit of L^+. Therefore z_1/z_2 is also a unit of L^+, and moreover we have

$$(z_1/z_2)^{1+\tau} = (z_1/z_2) \cdot (z_1^\tau/z_2^\tau) = (z_1/z_2) \cdot (z_2/z_1) = 1$$

because τ^2 is the identity on L^+. Hence, by Corollary 5, we may represent

$$z_1/z_2 = \pm(\epsilon_1\epsilon_3^2)^a(\epsilon_2\epsilon_4^2)^b e^{2c}, \tag{46}$$

where $a, b, c \in \mathbb{Z}$. Multiplying z_1/z_2 by $\sigma + \sigma^{-1} - 2$, we have

$$(z_1/z_2)^{\sigma+\sigma^{-1}-2} = (x_1/x_2)^{-5(\sigma+\sigma^{-1}-2)} \tag{47}$$

since σ is the identity on k^+. Multiplying the right side of (46) by $\sigma + \sigma^{-1} - 2$, we get

$$\begin{aligned}(\pm(\epsilon_1\epsilon_3^2)^a(\epsilon_2\epsilon_4^2)^b e^{2c})^{\sigma+\sigma^{-1}-2} &= (\epsilon_3^5 \cdot \epsilon_1^{-2}\epsilon_3^{-10})^a(\epsilon_4^5 \cdot \epsilon_2^{-2}\epsilon_4^{-10})^b \\ &= (\epsilon_1^{2a}\epsilon_3^{5a}\epsilon_2^{2b}\epsilon_4^{5b})^{-1}\end{aligned} \tag{48}$$

by Propositions 4 and 5, where we note that u_i in the statement of Proposition 4 is denoted by ϵ_{i+2} for $i = 1, 2$ now. Hence, multiplying (46) by $\sigma + \sigma^{-1} - 2$, we have

$$(x_1/x_2)^{5(\sigma+\sigma^{-1}-2)} = \epsilon_1^{2a}\epsilon_3^{5a}\epsilon_2^{2b}\epsilon_4^{5b}$$

by (47) and (48), and so

$$\epsilon_1^{2a}\epsilon_2^{2b} = ((x_1/x_2)^{\sigma+\sigma^{-1}-2} \cdot \epsilon_3^{-a}\epsilon_4^{-b})^5,$$

which implies that $5 \mid a$ and $5 \mid b$. Since the left side of (46) is also represented by $(y_1/y_2) \cdot (x_2/x_1)^5$, the equation (46) implies that

$$e^{-2c}(y_1/y_2) = \pm(\epsilon_1\epsilon_3^2)^a(\epsilon_2\epsilon_4^2)^b(x_1/x_2)^5,$$

which shows that

$$(e^{-2c}(y_1/y_2))^{1/5} \in L^+ = k^+(m^{1/5}). \tag{49}$$

by the fact that a and b are multiples of 5. Since the fundamental unit e of k^+ is taken to be positive, it follows from (45) that $e^{-2c}(y_1/y_2)$ is also positive. Besides, recall that m is defined to be greater than one

and hence positive. Applying Theorem 15 in the appendix below to (49), we get

$$e^{-2c}(y_1/y_2) = y^5 \cdot m^s, \tag{50}$$

where $y \in k^+$ and $s \in \mathbb{Z}$. Taking the value of the $\mathfrak{p}_1$-adic exponential valuation at (50), we obtain

$$h \equiv \mu s \pmod 5,$$

where μ is the value of the p-adic exponential valuation at m, i.e., $\mu = 1, 2, 3$ or 4. Taking the value of the $\mathfrak{p}_2$-adic exponential valuation at (50), we obtain

$$-h \equiv \mu s \pmod 5.$$

These congruence equations lead to $5 \mid h$. It is a contradiction. □

Remark 1. Our proof of Theorem 14 is valid as long as m has a prime divisor p which splits in k^+. Since the prime number p splits in k^+ if and only if $p \equiv \pm 1 \pmod 5$, we also see that the class number of $\mathbb{Q}(m^{1/5})$ is a multiple of five if m has a prime divisor p such that $p \equiv 1 \pmod 5$. This result is already obtained by Ishida [**5**], but his proof is based on more class field theoretical arguments.

Corollary 6. *Suppose that m has a prime factor p with $p^2 \equiv 1 \pmod 5$. Then the class number of L is divisible by* 25.

Proof. It follows from Theorem 1 of [**5**] (or Remark 1 above) and Theorem V of [**11**]. □

7. Appendix

In this appendix, we study more general objects than in the previous chapters. The purpose of this appendix is to prove Theorem 15 below, which is used in the proofs of Lemma 4 and Theorem 14 above. We prove it for all $n \in \mathbb{N}$, but we use it in this paper only as $n = 1$. One can read this appendix independently from the other parts of this paper.

Let K be a real algebraic number field. We denote by K_+ the set of positive elements of K. For $\alpha \in K_+$ and $r = m/n \in \mathbb{Q}$ with $m, n \in \mathbb{Z}$, we denote by α^r the positive root of the equation $x^n = \alpha^m$. We also denote by $\mathrm{Tr}_{L/K}$ the trace from L to K for any finite algebraic extension L/K.

Lemma 7. *Let K be a real algebraic number field. Let $n \in \mathbb{N}$ and $\alpha \in K_+$. Then $\alpha^{1/n} \notin K$ if and only if $\mathrm{Tr}_{L/K}(\alpha^{1/n}) = 0$ for all finite algebraic extensions $L/K(\alpha^{1/n})$.*

Proof. Obviously it is sufficient to prove that $\mathrm{Tr}_{K(\alpha^{1/n})/K}(\alpha^{1/n}) = 0$ when $\alpha^{1/n} \notin K$. Let $\alpha^{1/n} \notin K$ and m be the smallest natural number such that $\alpha^{m/n} \in K$. Then the polynomial $x^m - \alpha^{m/n}$ is irreducible over K. Indeed, if the polynomial is reducible, the constant terms of the proper factors are represented by $\zeta\alpha^{l/n} \in K$ with $l < m$ and $\zeta^m = 1$, and hence $\zeta = \pm 1$ because ζ is a real root of unity by the fact that $\zeta \in K(\alpha^{1/n}) \subseteq \mathbb{R}$, so that $\alpha^{l/n} \in K$, which contradicts the definition of m. Thus the algebraic extension $K(\alpha^{1/n})/K$ has the degree m. Then $1, \alpha^{1/n}, \ldots, \alpha^{(m-1)/n}$ is a basis of $K(\alpha^{1/n})$ over K. Therefore we have

$$\alpha^{1/n}(1, \alpha^{1/n}, \ldots, \alpha^{(m-1)/n}) = (1, \alpha^{1/n}, \ldots, \alpha^{(m-1)/n}) \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha^{m/n} \\ 1 & 0 & \cdots & 0 & 0 \\ & & \cdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

This shows $\mathrm{Tr}_{K(\alpha^{1/n})/K}(\alpha^{1/n}) = 0$. □

Corollary 7. *Let $\alpha \in K_+$ and $r \in \mathbb{Q}$. If $\alpha^r \notin K$, then $\mathrm{Tr}_{L/K}(\alpha^r) = 0$ for any finite algebraic extension $L/K(\alpha^r)$.*

Proof. We may represent $r = k/l$ with $k \in \mathbb{Z}$ and $l \in \mathbb{N}$. Since $\alpha^k \in K_+$ and $\alpha^r = (\alpha^k)^{1/l} \notin K$, we obtain the assertion. □

Corollary 8. *Let $\alpha_1, \alpha_2 \in K_+$ and $r_1, r_2 \in \mathbb{Q}$ such that $\alpha_1^{r_1}\alpha_2^{r_2} \notin K$. Then $\mathrm{Tr}_{L/K}(\alpha_1^{r_1}\alpha_2^{r_2}) = 0$ for any finite algebraic extension $L/K(\alpha_1^{r_1}\alpha_2^{r_2})$.*

Proof. We may represent $r_i = k_i/l$ with $l \in \mathbb{N}$ and $k_i \in \mathbb{Z}$ for $i = 1, 2$. Since $\alpha_1^{k_1}\alpha_2^{k_2} \in K_+$ and $\alpha_1^{r_1}\alpha_2^{r_2} = (\alpha_1^{k_1}\alpha_2^{k_2})^{1/l} \notin K$, the assertion follows. □

Theorem 15. *Let $n \in \mathbb{N}$. Let K be a real algebraic number field. Let $q, q_1, \ldots, q_n \in K_+$ and $r, r_1, \ldots, r_n \in \mathbb{Q}$. Then $q^r \in K(q_1^{r_1}, \ldots, q_n^{r_n})$ if and only if*

$$q^r = q_0 \cdot q_1^{r_1 e_1} \cdots q_n^{r_n e_n}$$

with $q_0 \in K$ and $e_1, \ldots, e_n \in \mathbb{Z}$.

Proof. The "if" part is clear. We shall prove the "only if" part by induction on $n \in \mathbb{N}$. Let $q^r \in K(q_1^{r_1})$. Assume that

$$q^r \cdot q_1^{r_1 j} \notin K \text{ for all } j \in \mathbb{Z}. \tag{51}$$

Let e be the smallest natural number such that $q_1^{r_1 e} \in K$. As $q^r \in K(q_1^{r_1})$, we may represent

$$q^r = a_0 + a_1 q_1^{r_1} + \cdots + a_{e-1} q_1^{r_1(e-1)} \tag{52}$$

with $a_i \in K$ for $i = 0, \ldots, e-1$. Denote by d the degree of algebraic extension $K(q_1^{r_1})/K$. Taking the trace of (52) in $K(q_1^{r_1})/K$, we obtain

$0 = d \cdot a_0$ by Corollary 7 because $q^r, q_1^{r_1 i} \notin K$ for $i = 1, \ldots, e-1$. Hence $a_0 = 0$. Suppose that $a_0 = \cdots = a_l = 0$ with some $0 \le l < e-1$. Dividing (52) by $q_1^{r_1(l+1)}$, we have

$$q^r \cdot q_1^{-r_1(l+1)} = a_{l+1} + a_{l+2} q_1^{r_1} + \cdots + a_{e-1} q_1^{r_1(e-l-2)}. \tag{53}$$

Taking the trace of (53) in $K(q_1^{r_1})/K$, we obtain $a_{l+1} = 0$ by Corollaries 7 and 8 because the left side of (53) is not in K by our assumption (51). Thus we obtain inductively that $a_i = 0$ for all $0 \le i < e$, and therefore $q^r = 0$, i.e., $q = 0$, which is absurd. Therefore our assertion is verified for $n = 1$. Suppose that our assertion is valid for $n \le k$ with some $k \in \mathbb{N}$. Let $q^r \in K(q_1^{r_1}, \ldots, q_{k+1}^{r_{k+1}})$. Assume that

$$q^r \cdot q_1^{r_1 j_1} \cdots q_{k+1}^{r_{k+1} j_{k+1}} \notin K \text{ for all } j_1, \ldots, j_{k+1} \in \mathbb{Z}. \tag{54}$$

Take e as the smallest natural number such that

$$q_{k+1}^{r_{k+1} e} \in K(q_1^{r_1}, \ldots, q_k^{r_k}).$$

Then we may represent

$$q^r = a_0 + a_1 q_{k+1}^{r_{k+1}} + \cdots + a_{e-1} q_{k+1}^{r_{k+1}(e-1)} \tag{55}$$

where $a_i = a_i(q_1^{r_1}, \ldots, q_k^{r_k}) \in K(q_1^{r_1}, \ldots, q_k^{r_k})$ for $i = 0, 1, \ldots, e-1$. Put $a_{-1} = 0$. We prove that $a_i = 0$ for $i = -1, 0, \ldots, e-1$ inductively as follows. Suppose that

$$a_{-1} = a_0 = \cdots = a_l = 0 \text{ with some } -1 \le l < e-1.$$

Then, dividing (55) by $q_{k+1}^{r_{k+1}(l+1)}$, we have

$$q^r \cdot q_{k+1}^{-r_{k+1}(l+1)} = a_{l+1} + a_{l+2} q_{k+1}^{r_{k+1}} + \cdots + a_{e-1} q_{k+1}^{r_{k+1}(e-l-2)}. \tag{56}$$

By (54), we have

$$(q^r \cdot q_{k+1}^{-r_{k+1}(l+1)}) \cdot q_1^{r_1 j_1} \ldots q_k^{r_k j_k} \notin K \text{ for all } j_1, \ldots, j_k \in \mathbb{Z},$$

and hence, by our assertion for $n = k$, we get

$$q^r \cdot q_{k+1}^{-r_{k+1}(l+1)} \notin K(q_1^{r_1}, \ldots, q_k^{r_k})$$

because we may represent

$$q^r \cdot q_{k+1}^{-r_{k+1}(l+1)} = (q^s \cdot q_{k+1}^{-t(l+1)})^{1/u} \text{ and then } q^s \cdot q_{k+1}^{-t(l+1)} \in K_+$$

if $r = s/u$ and $r_{k+1} = t/u$ with some $s, t, u \in \mathbb{Z}$. On the other hand, by the definition of e, we get

$$q_{k+1}^{r_{k+1} i} \notin K(q_1^{r_1}, \ldots, q_k^{r_k}) \text{ for } i = 1, \ldots, e-l-2$$

because $e - l - 2 < e$. Taking the trace of (56) in

$$K(q_1^{r_1}, \ldots, q_{k+1}^{r_{k+1}})/K(q_1^{r_1}, \ldots, q_k^{r_k}),$$

we obtain

$$a_{l+1} = 0$$

by Corollaries 7 and 8. Thus we have shown that $a_i = 0$ for $i = -1, 0, \ldots, e-1$, which implies $q^r = 0$ by (55). It contradicts with $q \in K_+$. Therefore the assumption (54) is denied, and so our assertion is also valid for $n = k+1$. Hence, the proof is completed. □

Acknowledgments

The author would like to thank Professor Kazuhiro Konno for helpful advice, encouragement and a big heart.

References

[1] R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, Math. Nachr. **4** (1951), 158-174.
[2] A. Fröhlich, Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, Contemp. Math., vol. 24, 1983.
[3] T. Honda, Pure cubic fields whose class numbers are multiples of three, Journal of Number Theory **3** (1971), 7-12.
[4] K. Iimura, A criterion for the class number of a pure quintic field to be divisible by 5, Journal für die reine und angewandte Mathematik **292** (1977), 201-210.
[5] M. Ishida, Class numbers of algebraic number fields of Eisenstein type, Journal of Number Theory **2** (1970), 404-413.
[6] H. Kobayashi, Class numbers of pure quintic fields, Journal of Number Theory **160** (2016), 463-477.
[7] S. Kuroda, Über die Klassenzahlen algebraischer Zahlkörper, Nagoya Math. J. **1** (1950), 1-10.
[8] E. Landau, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, Leipzig, 1918.
[9] F. Lemmermeyer, The ambiguous class number formula revisited, J. of the Ramanujan Math. Soc. **28**(4) (2013), 415-421.
[10] J. Neukirch, Class Field Theory, Grundlehren der mathematischen Wissenschaften, Vol. 280, Springer Verlag, 1986.
[11] C. Parry, Class number relations in pure quintic fields, Symposia Mathematica. **15** (1975), 475-485.
[12] C. Parry and C. Walter, The class number of pure fields of prime degree, Mathematika **23** (1976), 220-226; **24** (1977), 133.
[13] L. C. Washington, Introduction to Cyclotomic Fields, Springer, New York/Berlin, 1997.
[14] A. Weil, Basic Number Theory, Springer, Berlin/Heidelberg, 1974.