# Abstract

## English

This thesis studies the group of circular units $C$ of a compositum of quadratic fields $k = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, where $d_1, \ldots, d_s$ are square-free odd integers and $d_1 \equiv 3 \pmod 4$. In the main part (Chapter 2) we construct a basis of $C$, compute the index of $C$ in the full group of units of $k$ and derive a lower bound for the divisibility of this index by a power of 2. These results give a lower bound for the divisibility of the class number of the maximal real subfield of $k$ by a power of 2 if the ramification index $e$ at 2 is equal to 1 or 2.

In Chapter 3 we describe the group $C$ in the last case that has not been covered yet, namely in the case when the ramification index $e$ of 2 equals 4. Let $W$ be the group of roots of unity in $k$ and let $G = \mathrm{Gal}(k/\mathbb{Q})$. The key property of the group $C$ allowing to solve the case $e \leq 2$ is that for any $\varepsilon \in C$ and any $\sigma \in G$ there is $\rho \in W$ and $\eta \in C$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$. But this key property is not satisfied in the mentioned case $e = 4$ and so we cannot use the same approach. Nevertheless, using the three maximal subfields of $k$ whose ramification index at 2 is 2, we are able to describe an explicit maximal independent system of units in $C$. Let $\tilde{C}$ be the group generated by $W$ and by this system. Then we can compute the index $[E : \tilde{C}]$ and give a reasonable upper bound for the index $[C : \tilde{C}]$.

# Česky

Tato práce se zabývá studiem grupy kruhových jednotek $C$ v kompozitu kvadratických těles $k = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, kde $d_1, \ldots, d_s$ jsou lichá celá čísla nedělitelná druhou mocninou prvočísla a zároveň $d_1 \equiv 3 \pmod 4$. V hlavní části práce (kapitola 2) zkonstruujeme bázi grupy $C$, spočítáme index této grupy v grupě všech jednotek tělesa $k$ a získáme odhad pro dělitelnost tohoto indexu mocninou prvočísla 2. Na základě těchto výsledků navíc můžeme získat odhad dělitelnosti počtu tříd ideálů maximálního reálného podtělesa tělesa $k$ mocninou 2, jestliže index $e$ větvení dvojky v $k/\mathbb{Q}$ je roven 1 nebo 2.

V kapitole 3 se zabýváme studiem grupy $C$ v posledním možném případě, tedy pokud index větvení $e$ v 2 je roven 4. Označme $W$ grupu všech odmocnin z jedné tělesa $k$ a $G = \mathrm{Gal}(k/\mathbb{Q})$. Klíčová vlastnost grupy $C$ umožňující řešit případ $e \leq 2$ je, že pro každé $\varepsilon \in C$ a $\sigma \in G$ existuje $\eta \in C$ a $\rho \in W$ tak, že $\varepsilon^{1-\sigma} = \rho\eta^2$. Avšak tato klíčová vlastnost není splněna ve zmíněném případě $e = 4$. I přesto lze popsat maximální nezávislý systém jednotek v $C$ využitím tří maximálních podtěles $k$, jejichž index větvení v 2 je 2. Jestliže označíme $\tilde{C}$ grupu generovanou tímto maximální systémem jednotek a grupou všech odmocnin z jedné, bude možné spočítat index $[E : \tilde{C}]$ a dát horní odhad dělitelnosti indexu $[C : \tilde{C}]$ mocninou 2.

# Contents

# Introduction

The principal concern of this thesis is to deal with some aspects of class number of composita of quadratic fields. The main attention is focused on the group of circular units $C$ and to the description of this group by means of a basis modulo roots of unity. The main goal of the thesis is to compute the index of $C$ in the group $E$ of all units of a compositum of quadratic field.

At first, we start with a brief historical overview concerning circular units in cyclotomic, and more generally abelian fields. By an abelian field we have in mind a Galois extension of $\mathbb{Q}$ which is finite and whose Galois group is abelian. The well-known Kronecker-Weber theorem states that any abelian field is a subfield of a cyclotomic field. As we explain, in the case of an abelian field it is not so clear how to define the group of circular units.

In the middle of 19th century E. Kummer studied the $p$-th cyclotomic field $\mathbb{Q}(\zeta_p)$, where $p$ is an odd prime and $\zeta_p = e^{2\pi i/p}$ is a $p$-th root of unity. He noticed that the regulator of $\frac{1-\zeta_p^a}{1-\zeta_p}$, where $a = 2, \dots \frac{p-1}{2}$, is equal to $R \cdot h^+$; here $R$ is the regulator of $\mathbb{Q}(\zeta_p)$ and $h^+$ is the class number of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of $\mathbb{Q}(\zeta_p)$. By today language we can say that these numbers together with $\zeta_p$ generate a subgroup $C$ of circular units, which has index $h^+$ in the full group of units $E$.

In 1953, H. W. Leopoldt in [16] studied units of a real abelian field $k$ and defined "group of formal circular units". He showed that his group is of finite index in the full group $E$ of units of $k$ and that this index is equal to the class number $h$ of $k$ multiplied by an explicit factor. Later on, this result was improved by R. Gillard in [5].

The numbers $\frac{1-\zeta_n^a}{1-\zeta_n}$, where $n$ is a positive integer, $\zeta_n = e^{2\pi i/n}$ and $a \in \mathbb{Z}$, $1 < a < \frac{n}{2}, (a, n) = 1$, were studied also by algebraic topologists: John Milnor asked whether these numbers are multiplicatively independent for any of $n$. The negative answer to this question was given by K. Ramachandra who showed that they can be dependent. Moreover in [20] he gave a new explicit construction of a maximal independent system of units of the $n$-th cyclotomic field $\mathbb{Q}(\zeta_n)$.

This construction can be used to obtain a maximal independent system

of units in any abelian field $k$ (see [28], Theorem 8.2). Let us mention that the subgroup of units generated by the Ramachandra units has a finite index in the full group of units and that this index is an explicit multiple of the class number of maximal real subfield $k^+$ of $k$.

An important progress was made by Sinnott who gave in [22] and [23] a new definition of the group $C$ of circular units of an abelian field $k$. Sinnott group of circular units can be described by means of explicit generators and, roughly speaking, contains all previously defined groups. These two pieces of paper of Sinnott are devoted not only to circular units but also to Stickelberger ideal.

The starting point for this investigation of the Stickelberger ideal $S$ was the result of Iwasawa. Let us denote $R^- = (1-j)\,\mathbb{Z}[G]$ where $G = \mathrm{Gal}(k/\mathbb{Q})$ and $j$ is the complex conjugation. In [8] Iwasawa has computed for $k = \mathbb{Q}(\zeta_{p^m})$ that the index $[R^- : R^- \cap S]$ is equal to the relative class number $h^-$ of $k$. An elementary proof of this result of Iwasawa was obtained by Skula in [24] (for a detailed study of the matrices made by means of bases of the Sickelberger ideal, see also [9], [25] and [26]). Following Sinnott, let us define the Stickelberger ideal $S$ of the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$:

For any $a \in \mathbb{Z}$ let

$$\theta(a) = \sum_{0<r<n,\,(r,n)=1} \left\langle -\frac{ar}{n} \right\rangle \sigma_r^{-1} \in \mathbb{Q}[G],$$

where $\langle x \rangle$ is the fractional part of $x$, $G$ denotes the Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $\sigma_r \in G$ is the automorphism determined by $\sigma_r(\zeta_n) = \zeta_n^r$. Then $\theta(a)$ is called the Stickelberger element. Let $S'$ be the $\mathbb{Z}$-module generated in the rational group ring $\mathbb{Q}[G]$ by the set $\{\theta(a);\, a \in \mathbb{Z}\}$. The Stickelberger ideal of $\mathbb{Q}(\zeta_n)$ is the intersection $S = S' \cap \mathbb{Z}[G]$.

Now we shall try to mention some reasons why these two very different notions - group of circular units and Stickelberger ideal are studied together.

**The first interrelation - universal ordinary distributions:** The group of circular units as well as the Stickelberger ideal can be described by means of the module generated by values of an odd (Stickelberger ideal) and even (the circular units) Kubert's universal ordinary distribution (for more details, see [10]). Using the results of [10] we can obtain a system of independent generators of the group of circular units and a basis of the Stickelberger ideal as $\mathbb{Z}$-module for a general case of a cyclotomic field (see [11]; Theorem 6.1 and 6.2) or a compositum of quadratic fields (see [12]).

**The second interrelation - the class number:** Let $k$ be an abelian field, $G = \mathrm{Gal}(k/\mathbb{Q})$, $S$ is the Stickelberger ideal of $k$ (to keep this introduction simple we have defined $S$ only for cyclotomic field, the general case of an

abelian field is similar but much more technical) and $A = \{\alpha \in \mathbb{Z}[G];\ \forall \sigma \in G:\ (1-\sigma)(1+j)\alpha = 0\}$, where $j$ is the complex conjugation. Sinnott has shown in [23] that the index of $S$ in $A$ is in the form

$$[A : S] = h^- \cdot c_k^-$$

where $h^-$ is the relative class number of $k$ and $c_k^-$ is the rational number whose definition does not involve the class number $h^-$. Similarly, Sinnott has also found the index $[E : C]$ in the form

$$[E : C] = h^+ \cdot c_k^+$$

where $h^+$ is the class number of $k^+$ and $c_k^+$ is the rational number whose definition does not involve the class number $h^+$. Both $c_k^-$ and $c_k^+$ can be expressed in terms involving a so-called Sinnott module $U$.

**The third interrelation – annihilators of the ideal class group:** The elements of the Stickelberger ideal are annihilators of the ideal class group of the field $k$. The main step in the proof of this result is the following theorem (Stickelberger relation).

If $n \not\equiv 2 \pmod 4$ is a positive integer and $\zeta_n = e^{2\pi i/n}$ a primitive $n$th root of unity then $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$. Let $P$ be a prime ideal of $\mathbb{Z}[\zeta_n]$ not containing $n$ and $F = \mathbb{Z}[\zeta_n]/P$ the residue class field. Let $\chi$ be the $n$th power residue symbol on $\mathbb{Z}[\zeta_n]$ and $\psi$ the additive character on $F$ determined by the trace. Let $g(P) = \sum_{a \in F} \chi^{-1}(a)\psi(a)$ be the corresponding Gauss sum. Then $g(P)^n \in \mathbb{Z}[\zeta_n]$ and we have the following classical factorization of the principal ideal $(g(P)^n)$ generated by $g(P)^n$:

**Theorem 1.** *(The Stickelberger Relation)*

$$(g(P)^n) = \prod_t P^{t\sigma_t^{-1}} = P^{\sum_t t\sigma_t^{-1}}$$

*where the product and the sum are taken over all* $1 \le t < n$ *which are relatively prime to* $n$ *and* $\sigma_t$ *is the element of* $\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})$ *determined by* $\sigma_t(\zeta_n) = \zeta_n^t$.

*Proof.* See [7; Theorem 2 on page 209] □

Since the exponent $\sum_t t\sigma_t^{-1}$ does not depend on $P$ and since each class of ideals in the ideal class group contains such ideal $P$, one obtains that $\sum_t t\sigma_t^{-1}$ annihilates the ideal class group of $\mathbb{Q}(\zeta_n)$.

Sinnott has proved that for any abelian field $k$ any element of the Stickelberger ideal (defined by him) is an annihilator of the ideal class group of $k$.

Let us mention that this result is important for imaginary abelian fields while for a real abelian field it says only a trivial fact because in this case any element of the Stickelberger ideal is a multiple of the absolute norm.

Thaine in [27] showed a method to obtain annihilators of the ideal class group $Cl(k)$ of a real abelian field $k$. If an odd prime $p$ does not divide the degree $[k:\mathbb{Q}]$ then Sinnott formula implies that the $p$-Sylow subgroups $Cl(k)_p$ of $Cl(k)$ and $(E/C)_p$ of $E/C$ are of the same order: $|Cl(k)_p| = |(E/C)_p|$. Thaine proved the following statement:

**Theorem 2.** *Let $k$ be a totally real abelian number field, $G = \mathrm{Gal}(k/\mathbb{Q})$, let $C$ be the group of circular units defined as above, and let $Cl(k)$ be the class group of $k$. Let $p$ be an odd prime not dividing $[k:\mathbb{Q}]$. If $\theta \in \mathbb{Z}[G]$ annihilates $(E/C)_p$ then $\theta$ annihilates $Cl(k)_p$.*

Moreover, Thaine proved more since his theorem covers also the case $p = 2$: if $2 \nmid [k:\mathbb{Q}]$ and $\theta \in \mathbb{Z}[G]$ annihilates $(E/C)_2$ then $2\theta$ annihilates $Cl(k)_2$.

Thaine used in [27] different definition of the group of circular units than Sinnott but Lettl in [17] has shown that these two definitions are equivalent.

Thaine's method has been generalized by Rubin in [21] to any abelian extension of number fields (instead of an abelian extension of $\mathbb{Q}$) and any prime $p$ (allowing $p$ to divide the degree of the extension).

Now let us introduce the main ideas of this thesis. The aim of this paper can be understood as a counterpart of Kučera's results about the compositum of quadratic fields. In [12] Kučera studied a compositum $k$ of quadratic fields such that $-1$ is not a square in the genus field $K$ of $k$ in narrow sense. He has constructed bases of the Stickelberger ideal and the group of circular units and computed indices of these modules. This paper is the motivation of my work.

This thesis consists of three parts. In the first part (Chapter 1) we introduce some basic definitions and statements that we will use later. At first, we mention a brief overview about the circular units in cyclotomic fields and also in abelian fields. We recall some known results and theorems preceding the results of this thesis.

The main part of this thesis are Chapters 2 and 3 where we study the compositum $k$ of quadratic fields such that $-1$ is a square in the genus field $K$ of $k$ in the narrow sense. Then the ramification index of 2 in $k$ is equal to 2 or 4. Chapter 2 is devoted to the former case (when 2 is not a square in $K$) while Chapter 3 covers the latter case (when 2 is a square in $K$). In both

cases we construct a group $C$ of circular units of $k$, which is slightly larger than the Sinnott's group given in [23], we find a basis of $C$ and compute the index of $C$ in the group $E$ of all units of $k$. The case studied in Chapter 3 is much more difficult and we are not able to construct an explicit basis of $C$ here. So instead of that we describe only an explicit maximal independent system of units here and give a reasonable upper bound for the index of the subgroup generated by this system.

Thus these two chapters contain the results of the papers [18], [19] which together with [12] cover all composita of quadratic fields. Moreover, these results give a lower bound for the divisibility of the class number of the maximal real subfield of k by a power of 2.

This thesis and presented results have been achieved under the support of the Grant Agency of the Czech Republic by the projects 201/04/381 and 201/07/0191.

# Chapter 1

# Preliminaries

At first, let us mention some basic definitions we will use later on: *An algebraic number field* $K$ is a finite extension of the rationals $\mathbb{Q}$. *An algebraic integer* is a root of a monic polynomial with integral coefficients. The set of all algebraic integers in $k$ forms *the ring $R$ of algebraic integers* of the field $k$. Recall that $R$ is a Dedekind domain, so every nonzero ideal of $R$ can be uniquely written as a product of nonzero prime ideals of $R$.

*Dirichlet's unit theorem* gives the structure of the group $E$ of all units of the ring $R$. The theorem states that the group of units is finitely generated and has rank (maximal number of multiplicatively independent generators of the non-torsional part) equal to $r = r_1 + r_2 - 1$ where $r_1$ is the number of real embeddings and $r_2$ the number of conjugate pairs of complex embeddings of $k$, e.g. the group of units is isomorphic to its torsion subgroup multiplied with $r$ copies of $\mathbb{Z}$ (and $n = r_1 + 2r_2$ is the degree of the extension $k$ over $\mathbb{Q}$).

If we want to describe the multiplicative structure of the ring of algebraic integers $R$ of $K$ we will use fractional ideals. A fractional ideal is a nonzero finitely generated $R$-submodule of $K$. In other words, such an ideal can be written in the form $\alpha a$ where $\alpha \in K$, $\alpha \neq 0$ and $a$ is a nonzero ideal of $R$. Consequently, we can denote $I(K)$ the group of all fractional ideals of $K$. A fractional ideal is called principal if it is equal to $\alpha R$ for a suitable $\alpha \in K$, $\alpha \neq 0$. Since the principal ideals form the subgroup $P(K)$ of $I(K)$ we define *ideal class group* (class group in brief) $Cl$ of $R$ as the quotient group $Cl = I(K)/P(K)$.

Dirichlet theorem states that the group $E$ of units of $R$ is finitely generated. Moreover the class group $Cl$ of $R$ is finite. The order of $Cl$ (the size of the class group) is given by the *class number* $h = |Cl|$. In order to understand the arithmetic of $R$ it is useful to know the explicit generators of $E$ and a structure of the class group $Cl$ (or at least the class number $h$). The relation between the class number $h$ of $K$ and the arithmetic of $R$ is

following:

- $h = 1$ if and only if $R$ is a unique factorization domain
- $h = 2$ if and only if factorization in $R$ is not unique in general but any two factorizations of a given element of $R$ have the same number of factors (this result is given by L. Carlitz in [3])

All cyclotomic fields of class number $h = 1$ are described in [28] (see Theorem 11.1).

## 1.1 Circular units in cyclotomic fields

The most natural situation where one can consider circular units is in the case of cyclotomic fields. Let $n$ be a positive integer such that $n \not\equiv 2 \pmod 4$ and $\zeta_n$ be a primitive $n$th root of unity, i.e. $\zeta_n = e^{2\pi i/n}$. Then we call $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ to be the $n$th cyclotomic field. In general, we don't know the explicit generators of the full group of units in the ring of algebraic integers $\mathbb{Z}[\zeta_n]$ of $\mathbb{Q}^{(n)}$. However, for cyclotomic fields, we are able to find explicitly a special group of units, called the circular units. The group of circular units $C(\mathbb{Q}^{(n)})$ can be defined as the intersection of the subgroup of the multiplicative group $\mathbb{Q}^{(n)\times}$ generated by $1-\zeta_n, 1-\zeta_n^2, \ldots, 1-\zeta_n^{n-1}$ and the group of all units $E(\mathbb{Q}^{(n)})$ as follows

$$C(\mathbb{Q}^{(n)}) = \langle \{1-\zeta_n^a;\, a \in \mathbb{Z}, 1 \le a \le n-1\} \rangle \cap E(\mathbb{Q}^{(n)}).$$

An important property of the circular units is the fact that the group $C(\mathbb{Q}^{(n)})$ is of finite index in the full group of units $E(\mathbb{Q}^{(n)})$. Moreover, this index is closely connected to the class number $h^+$ of the maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{R} \cap \mathbb{Q}^{(n)}$ of the $n$th cyclotomic field. Sinnott proved in [22] that

$$[E(\mathbb{Q}^{(n)}) : C(\mathbb{Q}^{(n)})] = 2^c \cdot h^+_{\mathbb{Q}^{(n)}},$$

where $h^+_{\mathbb{Q}^{(n)}}$ is the class number of the maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of $\mathbb{Q}^{(n)}$ and $c$ is given explicitly by the number $s$ of ramified primes in $\mathbb{Q}^{(n)}$ (i.e. the primes dividing $n$) as follows

$$c = \begin{cases} 0, & \text{if } s = 1, \\ 2^{s-2} + 1 - s, & \text{if } s > 1. \end{cases}$$

Since the real units multiplied by roots of unity are of index 1 or 2 in the full group of units (see Theorem 4.12 in [28]) then it is sufficient to work

with real units. If $n$ is a prime power it is not so difficult to find a basis of $C(\mathbb{Q}^{(n)})$. The cyclotomic units of $C(\mathbb{Q}^{(n)})$ are generated by $-1$ and the units

$$\frac{1-\zeta_n^a}{1-\zeta_n}, \qquad 1 < a < \frac{n}{2},\ (a,n) = 1.$$

In general case, the situation is much more complicated since the relations among the generators are more difficult with the increasing number of prime divisors of $n$. It is not so easy to construct such a basis, especially to find the set of generators which will be suitable. Such a basis of the group of circular units of the $n$th cyclotomic field was found by Gold, Kim in [6] and independently by Kučera in [11].

## 1.2 Circular units in abelian fields

In contrast to a cyclotomic field it is not so clear how to construct the group $C$ of circular units of an abelian number field $k$. Let $n$ be the conductor of $k$, i.e. $n$ is the least positive integer satisfying $k \subseteq \mathbb{Q}^{(n)}$. As mentioned before we have several possibilities how to define the group $C$. We recall the best known of them. Since we want to find explicit generators of $C$ and to compute the index of this group in the full group of units we want to use Sinnott's definition. Sinnott group $C_S(k)$ of circular units of $k$ can be defined by the intersection

$$C_S(k) = \langle \{ \mathrm{N}_{\mathbb{Q}^{(r)}/\mathbb{Q}^{(r)}\cap k}(1-\zeta_r^a);\ 1 < r \,|\, n,\ (a,r) = 1\} \cup \{-1\} \rangle \cap E(k).$$

Sinnott's class number formula states that

$$[E(k) : C_S(k)] = h_k^+ \, Q \, \frac{\prod_{p|n}[k_p : \mathbb{Q}]}{[k : \mathbb{Q}]} \, 2^{-g}(e^+\mathbb{Z}[G] : e^+U) \qquad (*)$$

where $h_k^+$ is the class number of $k^+$, $Q = [E : E^+W]$ is the Hasse unit index ($Q = 1$ if $k$ is real), $k_p$ is the maximal subfield of $k$ ramified only at $p$ and the integer $g = 1 - [k : \mathbb{Q}]$ if $k$ is real. If $k$ is imaginary then we only know that $g$ is between the number of primes $p \,|\, n$ with $k_p$ imaginary and the number of them with $[k_p : \mathbb{Q}]$ even. One approach how to avoid problems with the integer $g$ was described by Kučera who enlarged the set of generators of $C_S(k)$ by adding $\sqrt{p}$ for each $p \,|\, n$ such that $\sqrt{p} \in k$ to the generators. Then we obtain slightly bigger group whose index is given by a formula which differs from (*) only at one point: $g$ is replaced by the number of primes $p \,|\, n$ with $[k_p : \mathbb{Q}]$ even.

The most serious problem is to describe the Sinnott module $U$ and to determine the index $(e^+\mathbb{Z}[G] : e^+U)$. Sinnott proved that this index is an integer that can be divisible only by primes dividing the degree $[k : \mathbb{Q}]$ and also by 2 if $k$ is imaginary. The precise value of this index is known only in some special cases. For example, if $k$ is ramified at most at two finite primes, or if the degree of $k$ is the square of an odd prime, or if $k$ is real and $G$ is cyclic, or if $K$ is a compositum of quadratic fields. The latter case was investigated by Kučera in [12] where he found the basis of the group of circular units and its index in the group of all units of the compositum of quadratic fields $k$ such that $-1$ is not a square in the genus field of $k$ in the narrow sense.

The second, well-known definition of circular units is mentioned in the Washington's monograph on cyclotomic fields ([28]) as the intersection $C_W(k) = k \cap C(\mathbb{Q}^{(n)})$. So we call $C_W(k)$ as Washington group of circular units. It is easy to see that $C_S(k) \subseteq C_W(k)$. Generally we don't have the same properties as in Sinnott definition. We know neither the explicit generators nor the index of the group of circular units in the full group of units as in the case of $C_S(k)$. As a comparison between Sinnott and Washington groups of circular units we can consider the following theorem.

**Theorem 1.** *Let $K$ be the genus field of an abelian field $k$ in narrow sense. Let $p$ be an odd prime such that $p\,|[C_W(k) : C_S(k)]$. Then $p\,|[K : k]$.*

Let us mention that if $p \mid [K : k]$ then $p \mid [k : \mathbb{Q}]$. For the proof of this theorem, other definitions of circular units and more details see [13].

The natural question arises how to determine the set of abelian fields having the property $C_W(k) = C_S(k)$. Kučera has partially succeeded in this problem in [13] by the following way:

**Theorem 2.** *Let $k$ be a compositum of any finite number of imaginary abelian fields, each of them being ramified at one prime. Then $C_S(k) = C_W(k)$.*

## 1.3 Circular units in a compositum of quadratic fields

In this part, let us mention some of the results determining the precise value of the index $(e^+\mathbb{Z}[G] : e^+U)$ of Sinnott module $U$ in the integral group ring of the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$, especially in case of the compositum of quadratic fields. The results introduced in this part were obtained by Kučera in [12].

Let $k$ be the compositum of quadratic fields such that $-1$ is not a square in the genus field $K$ of $k$ in the narrow sense. In such a field the Sinnott module $U$ corresponding to $K$ satisfies the inclusion $IU \subseteq 2U$ where $I$ is the augmentation ideal. Consequently we change slightly the definition of the group of circular units $C$ of $k$. This group contains Sinnott's group of circular units of $k$ but it can be slightly bigger (by adding a $\sqrt{p}$ to the generators where $p$ divides the conductor of $k$ and $\sqrt{p} \in k$). The precise definition of $C$ can be found in Chapter 2. The reason why to define the group $C$ as an enlargement of Sinnott's group is that the Galois group $G$ acts trivially on $C/(\pm C^2)$. In other words, the action of augmentation ideal on $C/W$ gives squares in $C/W$, where $W$ is the group of roots of unity in $k$. The following lemma gives this key property:

**Lemma 3.** *For any $\varepsilon \in C$ and any $\sigma \in G$ there is $\rho \in W$ and $\eta \in C$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$.*

*Proof.* See [12; Lemma 2]. □

Now the previous Lemma gives us the nice tool how to construct bases and mainly how to compute the index of $C$ in the group of all units $E$ of the field $k$, as follows

**Theorem 4.** *Let $X$ be the group of all Dirichlet characters corresponding to $k^+$. For any $\xi \in X$ let $k_\xi$ be the maximal subfield of $k$ ramified only at primes dividing the conductor of $\xi$. Then*

$$[E : C] = \left( \prod_{\xi \in X,\, \xi \neq 1} \frac{2 \cdot [k : k_\xi]}{[k : k^+]} \right) \cdot (\#X)^{-\frac{1}{2}(\#X)} \cdot Qh^+,$$

*where $Q$ is the Hasse unit index and $h^+$ is the class number of $k^+$.*

*Proof.* See [12; Theorem 1]. □

Consequently, we have obtained the formula for Sinnott index $(e^+Z[G] : e^+U)$

**Proposition 5.** *Let $R = \mathbb{Z}[\mathrm{Gal}(k/\mathbb{Q})], e^+ = \frac{1}{2}(1 + j)$ where $j$ is the complex conjugation. Then*

$$(e^+\mathbb{Z}[G] : e^+U) = [\, k^+ : \mathbb{Q}\,]^{-(1/2)[k^+:\mathbb{Q}]} \cdot \prod_{\xi \in X} [\, k : k_\xi\,]$$

*Proof.* See [12; Proposition 1]. □

As an application of these results let us mention the divisibility of the class number of some real fields by a power of 2. Let $n$ be the number of primes ramifying in $k$.

**Theorem 6.** *Let* $2^l = [k : \mathbb{Q}]$.

*i) If* $k$ *is real then*

$$2^{2^l-1-l-n-\binom{l}{2}} \mid [E : C],$$

*ii) if* $k$ *is imaginary then*

$$2^{2^{l-1}-l-n-\binom{l}{2}} \mid [E : C],$$

*Proof.* See [12; Theorem 2]. □

**Corollary 7.** *Let* $k$ *be equal to its genus field* $K$ *in narrow sense. If* $k/\mathbb{Q}$ *is ramified at least at two primes congruent to* 3 *modulo* 4 *then*

$$2^{2^{n-2}-n-\binom{n}{2}-1} \mid h^+.$$

*Proof.* See [12; Example on page 156] □

## 1.4 Other applications

Another example of applications of these results can be found in the computation of the parity of the class number of biquadratic fields. Conner and Hurrelbrink in [4] determine the parity of the class number of any biquadratic field up to the cases $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p, q$ are different primes such that $p \equiv q \equiv 1 \pmod 4$ and the Legendre symbol $(p/q) = 1$ and $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ where $p$ is a prime, $p \equiv 1 \pmod 8$.

Kučera has extended these results in [14] where he has obtained the criterion for the parity of the class number of these biquadratic fields in general, especially if $p \equiv q \equiv 1 \pmod 4$ or $p \equiv 1 \pmod 4$ and $q = 2$ (for more details see [14; Theorem 1 and Theorem 2]). Later, Bulant has used his methods to determine the parity of the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, where $p, q, r$ are primes congruent to 1 mod 4 as follows

**Theorem 8.** *Let* $p, q$ *and* $r$ *be different primes such that* $p, q, r \equiv 1 \pmod 4$ *Let* $h$ *denote the class number of* $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$
*1. If* $(p/q) = (p/r) = (q/r) = -1$, *fix* $u_{pq}, u_{pr}, u_{qr} \in \mathbb{Z}$ *satisfying* $u_{pq}^2 \equiv pq \pmod r, u_{pr}^2 \equiv pr \pmod q, u_{qr}^2 \equiv qr \pmod p$. *Then* $h$ *is even if and only if*

$(u_{pq}/r)(u_{pr}/q)(u_{qr}/p) = -1$.
*2. If* $(p/q) = 1, (p/r) = (q/r) = -1$, *then the parity of* $h$ *is the same as the parity of the class number of the biquadratic field* $\mathbb{Q}(\sqrt{p}, \sqrt{q})$
*3. If* $(p/q) = (q/r) = 1, (p/r) = -1$, *then* $h$ *is even.*
*4. If* $(p/q) = (p/r) = (q/r) = 1$, *then* $h$ *is even. (Moreover, if we denote by* $v_{pq}, v_{pr}, v_{qr}, v_{pqr}$ *the highest exponents of* 2 *dividing the class number of* $\mathbb{Q}(\sqrt{p}, \sqrt{q}), \mathbb{Q}(\sqrt{p}, \sqrt{r}), \mathbb{Q}(\sqrt{q}, \sqrt{r}), \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, *respectively, then* $v_{pqr} > 1 + v_{pq} + v_{pr} + v_{qr}$.)

Similarly he proved this statement in case $p = 2$ (see [1]; Theorem 2). Finally, Bulant has tried to find an integer $n$ such that any compositum of $n$ quadratic fields has to have an even class number. He was successful and was able to prove this is really true for $n = 5$ (see [2]).

# Chapter 2

# The ramification index of 2 being 2

This chapter deals with the compositum $k$ of a finite number of quadratic fields such that $-1$ is a square in $K$ but 2 is not a square in $K$, where $K$ is the genus field of $k$ in narrow sense.

The aim of this chapter is to construct a group $C$ of circular units of $k$, which is slightly larger than the Sinnott's group given in [23]. We find a basis of $C$ and compute the index of $C$ in the group $E$ of all units of $k$ (see Proposition 4). The main result of this paper is a lower bound for the divisibility of $[E : C]$ by a power of 2 (see Theorem 25). These results give a lower bound for the divisibility of the class number of the maximal real subfield of $k$ by a power of 2.

## 2.1 Definition of C

Let $k$ be a compositum of quadratic fields and let $K$ be the genus field of $k$ in narrow sense. We assume that $\sqrt{-1} \in K$ and $\sqrt{2} \notin K$. We define a set $J$ of signed primes ramifying in $k$ as follows

$$J = \{p \in \mathbb{Z}\,; p \equiv 1 \,(\mathrm{mod}\, 4),\ |p| \text{ is a prime ramifying in } k\} \cup \{-2\}.$$

For any $p \in J$, let us define

$$n_{\{p\}} = \begin{cases} |p| & \text{if } p \text{ is odd,} \\ 4 & \text{if } p = -2, \end{cases} \qquad K_{\{p\}} = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \text{ is odd,} \\ \mathbb{Q}(\sqrt{-1}) & \text{if } p = -2. \end{cases}$$

For any $L \subseteq J$ let us denote $n_L = \prod_{p \in L} n_{\{p\}}$, $K_L = \prod_{p \in L} K_{\{p\}}$ if $L \neq \emptyset$ and $K_\emptyset = \mathbb{Q}$, and finally $\mathbb{Q}^L = \mathbb{Q}(\zeta_L)$, where $\zeta_L = e^{2\pi i/n_L}$ is a primitive $n_L$th root of unity. It is easy to see that $K_J$ equals $K$.

For any $L \subseteq J$ let us now define

$$\varepsilon_L = \begin{cases} 1 & \text{if } L = \emptyset, \\ \frac{1}{\sqrt{p}} \mathrm{N}_{\mathbb{Q}^L/K_L}(1-\zeta_L) & \text{if } L = \{p\}, p \neq -2, \\ i & \text{if } L = \{-2\}, \\ \mathrm{N}_{\mathbb{Q}^L/K_L}(1-\zeta_L) & \text{if } \#L > 1, \end{cases}$$

and $\eta_L = \mathrm{N}_{K_L/k_L}(\varepsilon_L)$ where $k_L = k \cap K_L$. It is easy to see that all $\varepsilon_L$ are units of $K_L$.

For any $p \in J$ let $\sigma_p$ be the generator of $\mathrm{Gal}(K_J/K_{J\setminus\{p\}})$. Then we denote $G = \mathrm{Gal}(K_J/\mathbb{Q})$.

**Lemma 1.** *Let $p \in L \subseteq J$. Then*

$$\mathrm{N}_{K_L/K_{L\setminus\{p\}}}(\varepsilon_L) = \begin{cases} -\operatorname{sgn} p & \text{if } L = \{p\}, \\ t_{p,q} \cdot \varepsilon_{\{q\}}^{1-\mathrm{Frob}(|p|,K_{\{q\}})} & \text{if } L = \{p,q\},\ p \neq q,\ q \neq -2, \\ 1 & \text{if } L = \{p,-2\},\ |p| \equiv 1 \,(\mathrm{mod}\, 4), \\ -i & \text{if } L = \{p,-2\},\ |p| \equiv 3 \,(\mathrm{mod}\, 4), \\ \varepsilon_{L\setminus\{p\}}^{1-\mathrm{Frob}(|p|,K_{L\setminus\{p\}})} & \text{if } \#L > 2, \end{cases}$$

*where* $\operatorname{sgn} p$ *means the sign of* $p$, $\mathrm{Frob}(|p|, K_{L\setminus\{p\}})$ *is the Frobenius automorphism of* $|p|$ *in* $K_{L\setminus\{p\}}/\mathbb{Q}$ *and* $t_{p,q}$ *is defined by means of the Legendre symbol as follows:*

$$t_{p,q} = \left(\frac{|p|}{|q|}\right).$$

*Proof.* At first, let us suppose $\#L > 1$. Then

$$\begin{aligned} \mathrm{N}_{K_L/K_{L\setminus\{p\}}}(\varepsilon_L) &= \mathrm{N}_{\mathbb{Q}^{L\setminus\{p\}}/K_{L\setminus\{p\}}}(\mathrm{N}_{\mathbb{Q}^L/\mathbb{Q}^{L\setminus\{p\}}}(1-\zeta_L)) \\ &= \mathrm{N}_{\mathbb{Q}^{L\setminus\{p\}}/K_{L\setminus\{p\}}}((1-\zeta_{L\setminus\{p\}})^{1-\mathrm{Frob}^{-1}(|p|,\,\mathbb{Q}^{L\setminus\{p\}})}) \\ &= \mathrm{N}_{\mathbb{Q}^{L\setminus\{p\}}/K_{L\setminus\{p\}}}(1-\zeta_{L\setminus\{p\}})^{1-\mathrm{Frob}(|p|,\,K_{L\setminus\{p\}})}, \end{aligned}$$

because $\mathrm{Frob}^2(|p|, K_{L\setminus\{p\}})$ is the identity. So the lemma is proved if $\#L > 2$. If $L = \{p, -2\}$ then

$$\mathrm{N}_{\mathbb{Q}^{\{-2\}}/K_{\{-2\}}}(1-\zeta_{\{-2\}}) = 1 - i$$

and the third and fourth case of the lemma follows from

$$(1-i)^{1-\mathrm{Frob}(|p|,\,K_{\{-2\}})} = \begin{cases} 1 & \text{if } |p| \equiv 1 \,(\mathrm{mod}\, 4) \\ -i & \text{if } |p| \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

Similarly by using $(\sqrt{q})^{1-\mathrm{Frob}(|p|,K_{\{q\}})} = t_{p,\,q}$ we prove the second case. If $L = \{p\}$ the lemma follows easily. □

**Lemma 2.** *Let $L \subseteq J$, $\sigma \in G$. Then*

$$\varepsilon_L^{1-\sigma} = \varrho \prod_{S \subseteq L} \varepsilon_S^{2a_S}$$

*for suitable $a_S \in \mathbb{Z}$, where $\varrho \in \{1, -1, i, -i\}$ depends on the choice of $L$ and $\sigma$.*

*Proof.* This can be proved in the same way as Lemma 2 of [12]. □

**Lemma 3.** *Let $L \subseteq J$, $\sigma \in G$. Then*

$$\eta_L^{1-\sigma} = \varrho \prod_{S \subseteq L} \eta_S^{2a_S},$$

*for suitable $a_S \in \mathbb{Z}$, where $\varrho \in \{1, -1, i, -i\} \cap k$ depends on the choice of $L$ and $\sigma$.*

*Proof.* This is a corollary of Lemma 2 and of the fact that $\eta_S \in k$ implies $\varrho \in k$. □

Now let us denote $W$ the group of roots of unity of $k$. Since $k$ is a compositum of quadratic fields then it is not difficult to prove that $\#\, W \mid 24$. Moreover, we assume that $\sqrt{2} \notin K_J$ and so $\#\, W \mid 12$. Further, we need to define the set $X$ as follows:

$$X = \{\xi \in \hat{G};\, \xi(\sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(K_J/k^+)\},$$

where $\hat{G}$ is the group of characters of $G$. Then $X$ can be viewed as the group of all Dirichlet characters corresponding to the maximal real subfield $k^+$ of $k$. For any $\xi \in X$ define

$$L_\xi = \{p \in J;\, \xi(\sigma_p) = -1\}.$$

Finally, let $C$ denote the group generated by $W$ and by $\{\eta_L^\sigma;\, L \subseteq J,\, \sigma \in G\}$ and let $E$ denote the full group of units of $k$. Notice that $C$ contains Sinnott's group of circular units defined in [23]. It can be shown that these two groups do not coincide in general.

**Proposition 4.** *Let $B = \{\eta_{L_\xi};\, \xi \in X,\, \xi \neq 1\}$. Then $B$ is a basis of non-torsion part of $C$ and moreover*

$$[E : C] = \left( \prod_{\xi \in X,\, \xi \neq 1} \frac{2 \cdot [k : k_{L_\xi}]}{[k : k^+]} \right) \cdot (\#X)^{-\frac{1}{2}(\#X)} \cdot Q h^+,$$

*where $Q = [E : E^+W]$ is the Hasse unit index ($Q = 1$ if $k$ is real) and $h^+$ is the class number of $k^+$.*

*Proof.* This can be proved in the same way as Theorem 1 and Lemma 5 of [12]. □

## 2.2 Circular Units that are Squares in K

For any $\varepsilon \in C$ and any $\sigma \in G$ Lemma 2 implies that $\varepsilon^{1-\sigma}$ is up to a root of unity the square of a unit in $C$. But $\#W \mid 12$ and so any $\rho \in W$ can be uniquely written in the form $\rho = \Delta \cdot (\delta \cdot \varphi)^2$, where $\Delta, \delta \in \{1, i\}$ and $\varphi^3 = 1$. Moreover, if $\#W \mid 4$ then $\varphi = 1$ and if $\#W \mid 6$ then $\Delta = 1$. Therefore we have the identity

$$\varepsilon^{1-\sigma} = \Delta(\sigma, \varepsilon) \cdot (\delta(\sigma, \varepsilon) \cdot \varphi(\sigma, \varepsilon) \cdot \psi(\sigma, \varepsilon))^2,$$

where $\Delta(\sigma, \varepsilon), \delta(\sigma, \varepsilon) \in \{1, i\}, \varphi(\sigma, \varepsilon) \in \{1, \zeta_3, \zeta_3^2\}$ and $\psi(\sigma, \varepsilon)$ belongs to the group generated by the set $B$. Moreover $\Delta(\sigma, \varepsilon), \delta(\sigma, \varepsilon), \varphi(\sigma, \varepsilon)$ and $\psi(\sigma, \varepsilon)$ are uniquely determined by the previous identity.

**Lemma 5.** *Let $\sigma \in G$. Then $\Delta(\sigma, \cdot)^2$ and $\psi(\sigma, \cdot)$ are homomorphisms, i.e., for any $\varepsilon, \eta \in C$,*

$$\Delta(\sigma, \varepsilon\eta)^2 = (\Delta(\sigma, \varepsilon)\, \Delta(\sigma, \eta))^2,$$
$$\psi(\sigma, \varepsilon\eta) = \psi(\sigma, \varepsilon)\, \psi(\sigma, \eta).$$

*Proof.* The lemma follows from the identity $(\varepsilon\eta)^{1-\sigma} = \varepsilon^{1-\sigma}\eta^{1-\sigma}$ and from the definition of $\varepsilon^{1-\sigma}$ in the form as above. □

**Lemma 6.** *Let* $\sigma, \tau \in G$ *and* $\varepsilon \in C$. *Then*

$$\Delta(\sigma\tau, \varepsilon)^2 = (\Delta(\sigma, \varepsilon)\, \Delta(\tau, \varepsilon))^2$$

*Proof.* From the relation

$$1 = \frac{\varepsilon^{1-\sigma} \cdot (\varepsilon^{1-\tau})^{\sigma}}{\varepsilon^{1-\sigma\tau}}$$

and by decomposing $\varepsilon^{1-\sigma}$ as at the beginning of this chapter it is easy to see that $\Delta(\sigma, \varepsilon)\Delta(\tau, \varepsilon)^{\sigma}/\Delta(\sigma\tau, \varepsilon) \in \{\pm 1, \pm i\}$ is a square in $k$. The identity follows because $\pm i$ is not a square in $k$ and $\Delta(\tau, \varepsilon)^{\sigma} = \pm\Delta(\tau, \varepsilon)$. □

**Proposition 7.** *Let* $\varepsilon \in E$ *be such that there exists a function* $f : G \to K_J$ *satisfying* $\varepsilon^{1-\sigma} = f(\sigma)^2$ *for any* $\sigma \in G$. *If there exists a function* $g : G \to \{-1, 1\}$ *such that* $fg$ *is a crossed homomorphism, i.e., for all* $\sigma, \tau \in G$

$$f(\sigma\tau)g(\sigma\tau) = f(\sigma)g(\sigma)(f(\tau)g(\tau))^{\sigma},$$

*then* $\varepsilon$ *or* $2\varepsilon$ *is a square in* $K_J$.

*Proof.* Similarly as in [12], Proposition 2, we can show that there is $\alpha \in K_J^*$ and $b \in \mathbb{Q}^*$ such that $b = \varepsilon\alpha^2$ and that $\pm b = c^2 \prod_{p \in L} p$ for a suitable $c \in \mathbb{Q}^*$ and $L \subseteq J$. The proposition follows from the fact that $\sqrt{-1} \in K_J$ and $\sqrt{p} \in K_J$ for all $p \in J, p \neq -2$. □

**Remark 8.** The sufficient condition of Proposition 7 is also necessary. If $\varepsilon = \eta^2$ or $2\varepsilon = \eta^2$ for a suitable $\eta \in K_J$ then $f(\sigma) = \eta^{1-\sigma}$ satisfies $\varepsilon^{1-\sigma} = f(\sigma)^2$ and for any $f : G \to K_J$ with $f(\sigma)^2 = \varepsilon^{1-\sigma}$ we have the function $g : G \to \{-1, 1\}$ determined by $g(\sigma) = \eta^{1-\sigma}/f(\sigma)$, such that $fg$ is a crossed homomorphism.

Now let us denote for any $\sigma, \tau \in G$ and for any $\varepsilon \in C$

$$\langle \sigma, \tau \rangle_{\varepsilon} = \Delta(\sigma, \psi(\tau, \varepsilon))^2.$$

**Lemma 9.** *Let* $\sigma, \tau \in G$ *and* $\varepsilon \in C$. *Then*

$$\langle \sigma, \tau \rangle_{\varepsilon\eta} = \langle \sigma, \tau \rangle_{\varepsilon} \langle \sigma, \tau \rangle_{\eta}$$

*Proof.* The lemma follows immediately from Lemma 5. □

**Proposition 10.** *Let $\varepsilon \in C$. Then $\varepsilon$ or $2\varepsilon$ is a square in $K_J$ if and only if the following conditions are satisfied for any $\sigma, \tau \in G$:*

*(C1)* $(\Delta(\sigma,\varepsilon))^2 = 1$,

*(C2)* $\langle \sigma, \sigma \rangle_\varepsilon = 1$,

*(C3)* $\langle \sigma, \tau \rangle_\varepsilon = \langle \tau, \sigma \rangle_\varepsilon$

*(C4)* $\delta(\sigma,\varepsilon)^{\tau-1} \cdot \delta(\tau, \psi(\sigma,\varepsilon))^2 = \delta(\tau,\varepsilon)^{\sigma-1} \cdot \delta(\sigma, \psi(\tau,\varepsilon))^2$

*(C5)* $(\delta(\sigma,\varepsilon))^{\sigma+1} \cdot \delta(\sigma, \psi(\sigma,\varepsilon))^2 = 1$

*Proof.* At first, let us suppose that there is $\gamma \in K_J$ such that $\varepsilon = \gamma^2$ or $\varepsilon = 2\gamma^2$. Then

$$(\gamma^{1-\sigma})^2 = \varepsilon^{1-\sigma} = \Delta(\sigma,\varepsilon) \cdot (\delta(\sigma,\varepsilon) \cdot \varphi(\sigma,\varepsilon) \cdot \psi(\sigma,\varepsilon))^2, \tag{1}$$

and easily $\Delta(\sigma,\varepsilon)$ is a square in $K_J$. It follows immediately that we have the condition (C1) because $i$ is not a square in $K_J$. Therefore (1) implies

$$\gamma^{1-\sigma} = \pm\delta(\sigma,\varepsilon) \cdot \varphi(\sigma,\varepsilon) \cdot \psi(\sigma,\varepsilon). \tag{2}$$

It is easy to see that

$$(\delta(\sigma,\varepsilon))^{1-\tau} = \begin{cases} \delta(\sigma,\varepsilon)^2 & \text{if } i^\tau = -i, \\ 1 & \text{otherwise} \end{cases}$$

and that $\varphi(\sigma,\varepsilon)^{1-\tau}$ is a third root of unity, so a square in $K_J$. Then substituting

$$\psi(\sigma,\varepsilon)^{1-\tau} = \Delta(\tau,\psi(\sigma,\varepsilon)) \cdot (\delta(\tau,\psi(\sigma,\varepsilon)) \cdot \varphi(\tau,\psi(\sigma,\varepsilon)) \cdot \psi(\tau,\psi(\sigma,\varepsilon)))^2 \tag{3}$$

for $\tau = \sigma$ to the identity obtained from (2) by the application of $1-\sigma$, we deduce that $\Delta(\sigma,\psi(\sigma,\varepsilon))$ is a square in $K_J$ but $i$ is not a square in $K_J$. So the condition (C2) follows. Similarly we substitute (3) to the identity $\gamma^{(1-\sigma)(1-\tau)} = \gamma^{(1-\tau)(1-\sigma)}$. Since $\varphi(\cdot,\cdot)$ is a third root of unity then

$$\frac{\varphi(\sigma,\varepsilon)^{1-\tau} \cdot \varphi(\tau,\psi(\sigma,\varepsilon))^2}{\varphi(\tau,\varepsilon)^{1-\sigma} \cdot \varphi(\sigma,\psi(\tau,\varepsilon))^2} = 1$$

and consequently

$$\frac{\delta(\sigma,\varepsilon)^{1-\tau}\cdot\Delta(\tau,\psi(\sigma,\varepsilon))\cdot(\delta(\tau,\psi(\sigma,\varepsilon))\cdot\psi(\tau,\psi(\sigma,\varepsilon)))^2}{\delta(\tau,\varepsilon)^{1-\sigma}\cdot\Delta(\sigma,\psi(\tau,\varepsilon))\cdot(\delta(\sigma,\psi(\tau,\varepsilon))\cdot\psi(\sigma,\psi(\tau,\varepsilon)))^2}=1.$$

By using the same arguments as above we deduce

$$\frac{\Delta(\tau,\psi(\sigma,\varepsilon))}{\Delta(\sigma,\psi(\tau,\varepsilon))}=1$$

because this is a square in $K_J$. So the condition (C3) follows.

By the same way the identity $\gamma^{(1-\sigma)(1-\tau)}=\gamma^{(1-\tau)(1-\sigma)}$ gives that

$$\left(\frac{\psi(\tau,\psi(\sigma,\varepsilon))}{\psi(\sigma,\psi(\tau,\varepsilon))}\right)^2\in W.$$

Since $\psi(\cdot,\cdot)$ belongs to the non-torsion group generated by $B$ then

$$\frac{\psi(\tau,\psi(\sigma,\varepsilon))}{\psi(\sigma,\psi(\tau,\varepsilon))}=1.$$

Moreover, as $\delta(\cdot,\cdot)$ is a fourth root of unity, then

$$\frac{\delta(\sigma,\varepsilon)^{1-\tau}\cdot\delta(\tau,\psi(\sigma,\varepsilon))^2}{\delta(\tau,\varepsilon)^{1-\sigma}\cdot\delta(\sigma,\psi(\tau,\varepsilon))^2}=1$$

which implies (C4). To prove the last condition compare (1) and

$$\begin{aligned}\gamma^{(1-\sigma)^2}&=\delta(\sigma,\varepsilon)^{1-\sigma}\cdot\varphi(\sigma,\varepsilon)^{1-\sigma}\cdot(\delta(\sigma,\psi(\sigma,\varepsilon))\cdot\varphi(\sigma,\psi(\sigma,\varepsilon))\\&\quad\cdot\psi(\sigma,\psi(\sigma,\varepsilon)))^2.\end{aligned}$$

Hence using the same facts as in proving the previous condition we have the last one.

On the other hand, suppose that the conditions (C1)-(C5) are satisfied. Let us denote $f(\sigma)=\delta(\sigma,\varepsilon)\,\varphi(\sigma,\varepsilon)\,\psi(\sigma,\varepsilon)$ for any $\sigma\in G$. Hence, the condition (C1) implies $\varepsilon^{1-\sigma}=f(\sigma)^2$. Then

$$1=\frac{\varepsilon^{1-\sigma\tau}}{\varepsilon^{1-\sigma}(\varepsilon^{1-\tau})^\sigma}=\left(\frac{f(\sigma\tau)}{f(\sigma)(f(\tau))^\sigma}\right)^2.$$

Let us denote $\chi_\varepsilon(\sigma,\tau)=\frac{f(\sigma\tau)}{f(\sigma)(f(\tau))^\sigma}$. The previous identity implies $\chi_\varepsilon(\sigma,\tau)=\pm1$. By substituting

$$\psi(\tau,\varepsilon)^{1-\sigma}=\Delta(\sigma,\psi(\tau,\varepsilon))\cdot(\delta(\sigma,\psi(\tau,\varepsilon))\cdot\varphi(\sigma,\psi(\tau,\varepsilon))\cdot\psi(\sigma,\psi(\tau,\varepsilon)))^2\quad(4)$$

to the identity $\chi_\varepsilon(\sigma,\tau) = \frac{f(\sigma\tau)f(\tau)^{1-\sigma}}{f(\sigma)f(\tau)}$ and using the facts that $\varphi(\sigma,\varepsilon)$ is a third root of unity and $\psi(\sigma,\varepsilon)$ belongs to a non-torsion group, we deduce that

$$\chi_\varepsilon(\sigma,\tau) = \delta(\sigma\tau,\varepsilon)\cdot\delta(\tau,\varepsilon)^{-\sigma}\cdot\delta(\sigma,\varepsilon)^{-1}\cdot\delta(\sigma,\psi(\tau,\varepsilon))^2\cdot\Delta(\sigma,\psi(\tau,\varepsilon)).$$

The conditions (C2) and (C5) imply $\chi_\varepsilon(\sigma,\sigma)=1$. Since the conditions (C3) and (C4) are satisfied we have $\chi_\varepsilon(\sigma,\tau)=\chi_\varepsilon(\tau,\sigma)$. This identity states that $f(\sigma)^\tau\cdot f(\tau) = f(\tau)^\sigma\cdot f(\sigma)$ for any $\sigma,\tau\in G$. Hence for any $\rho\in G$

$$\begin{aligned}\chi_\varepsilon(\sigma\rho,\tau)\cdot\chi_\varepsilon(\sigma,\rho) &= \frac{f(\sigma\rho\tau)}{f(\sigma\rho)f(\tau)^{\sigma\rho}}\cdot\frac{f(\sigma\rho)}{f(\sigma)^\rho f(\rho)} = \frac{f(\sigma\rho\tau)}{(f(\tau)^\sigma f(\sigma))^\rho f(\rho)}\\ &= \frac{f(\sigma\rho\tau)}{(f(\tau)f(\sigma)^\tau)^\rho f(\rho)} = \frac{f(\sigma\rho\tau)}{f(\tau\rho)f(\sigma)^{\rho\tau}}\cdot\frac{f(\rho\tau)}{f(\tau)^\rho f(\rho)}\\ &= \chi_\varepsilon(\rho\tau,\sigma)\cdot\chi_\varepsilon(\rho,\tau).\end{aligned}\tag{5}$$

Let us fix a basis $\sigma_1,\ldots,\sigma_l$ of $G$. So for any $\sigma\in G$ there is a unique $V_\sigma\subseteq\{1,\ldots,n\}$ such that $\sigma=\prod\limits_{i\in V}\sigma_i$. We define the mapping $g: G\to\{-1,1\}$ by

$$g(\sigma)=\prod_{i\in V_\sigma}\chi_\varepsilon\left(\prod_{j\in V_\sigma,\, j<i}\sigma_j,\,\sigma_i\right).$$

Let us show that for any linear ordering $\prec$ on $\{\sigma_1,\ldots,\sigma_l\}$ we have

$$g(\sigma)=\prod_{i\in V_\sigma}\chi_\varepsilon\left(\prod_{j\in V_\sigma,\,\sigma_j\prec\sigma_i}\sigma_j,\,\sigma_i\right).\tag{6}$$

Indeed, any linear ordering can be obtained from the initial ordering $\sigma_1\prec\ldots\prec\sigma_n$ by a finite number of interchanges of neighbors. If two orderings $\prec$ and $\ll$ differ just by the interchange of the couple of neighbors $\sigma_i,\sigma_j$ (i.e. $\sigma_i\prec\sigma_j$ but $\sigma_i\gg\sigma_j$ and for all $\{\sigma_k,\sigma_l\}\neq\{\sigma_i,\sigma_j\}$ we have $\sigma_k\prec\sigma_l$ if and only if $\sigma_k\ll\sigma_l$) then the right hand sides of (6) are different for $\prec$ and $\ll$ only if both $i,j\in V_\sigma$ in which case the corresponding products differ just in two factors: the former has factors $\chi_\varepsilon(\tau,\sigma_i)\cdot\chi_\varepsilon(\tau\sigma_i,\sigma_j)$ while the latter has $\chi_\varepsilon(\tau,\sigma_j)\cdot\chi_\varepsilon(\tau\sigma_j,\sigma_i)$, where $\tau=\prod\limits_{k\in V_\sigma,\,\sigma_k<\sigma_i,\,\sigma_k<\sigma_j}\sigma_k$. But these products are the same (see (5)).

We shall show that for any $\sigma,\tau\in G$ we have

$$\chi_\varepsilon(\sigma,\tau)=g(\sigma)g(\tau)g(\sigma\tau).\tag{7}$$

We shall use the induction with respect to $|V_\tau|$. If $V_\tau = \emptyset$ then $\tau = 1$ and $\chi_\varepsilon(\sigma, 1) = 1 = g(\sigma)^2$. So let us assume that $|V_\tau| = m > 0$ and that the result has been proved for all $\tau$ with $|V_\tau| < m$. Let us choose $i \in V_\tau$ and write $\tau = \sigma_i\tau'$, so $|V'_\tau| = m - 1$. Using (5), the induction hypothesis for $\tau'$, $g(\sigma_i) = 1$ given by (6), we obtain

$$\begin{aligned}\chi_\varepsilon(\sigma, \tau) &= \chi_\varepsilon(\sigma, \sigma_i\tau') = \chi_\varepsilon(\sigma_i, \tau') \cdot \chi_\varepsilon(\sigma\sigma_i, \tau') \cdot \chi_\varepsilon(\sigma, \sigma_i) \\ &= \chi_\varepsilon(\sigma_i, \tau') \cdot g(\sigma\sigma_i) \cdot g(\tau') \cdot g(\sigma\tau) \cdot \chi_\varepsilon(\sigma, \sigma_i) \\ &= g(\tau) \cdot g(\sigma\tau) \cdot g(\sigma\sigma_i) \cdot \chi_\varepsilon(\sigma_i, \sigma).\end{aligned}$$

So we need to show that $g(\sigma) = g(\sigma\sigma_i) \cdot \chi_\varepsilon(\sigma_i, \sigma)$. On one hand, if $i \notin V_\sigma$ this easily follows from the definition of $g$. On the other hand, if $i \in V_\sigma$ then for $\sigma' = \sigma\sigma_i$ we have $V_{\sigma'} = V_\sigma - \{i\}$ and $g(\sigma) = g(\sigma') \cdot \chi_\varepsilon(\sigma_i, \sigma')$. Using (5) and $\chi_\varepsilon(\sigma_i, \sigma_i) = 1$ we have

$$\chi_\varepsilon(\sigma, \sigma_i) = \chi_\varepsilon(\sigma'\sigma_i, \sigma_i) = \chi_\varepsilon(\sigma', \sigma_i) \cdot \chi_\varepsilon(\sigma', \sigma_i^2) \cdot \chi_\varepsilon(\sigma_i, \sigma_i) = \chi_\varepsilon(\sigma', \sigma_i).$$

The definition of $\chi_\varepsilon(\sigma, \tau)$ and (7) give that $fg$ is a crossed homomorphism and Proposition 7 gives that $\varepsilon$ or $2\varepsilon$ is a square in $K_J$. The proposition is proved. □

## 2.3 The Index of $[\mathbf{C} : \mathbf{D}'']$

In this chapter we study the set $D''$ of all units $\varepsilon \in C$ that satisfy all conditions (C1)-(C5) of Proposition 10. Our aim is to show that $D''$ is a subgroup of $C$ and to compute its index.

**Lemma 11.** *Let $\varepsilon \in C$ and let $\sigma, \tau \in G$. Then*

$$\begin{aligned}\langle \cdot, \tau \rangle_\varepsilon &: G \to \{-1, 1\} \\ \langle \sigma, \cdot \rangle_\varepsilon &: G \to \{-1, 1\}\end{aligned}$$

*are homomorphisms.*

*Proof.* The first identity follows from Lemma 6. The identity $\varepsilon^{1-\rho\tau} = \varepsilon^{1-\rho}(\varepsilon^{1-\tau})^\rho$ gives that $\psi(\rho\tau, \varepsilon)^{-2}\psi(\rho, \varepsilon)^2\psi(\tau, \varepsilon)^{2\rho} \in W$. Then by substituting

$$\psi(\tau, \varepsilon)^{1-\rho} = \Delta(\rho, \psi(\tau, \varepsilon))(\delta(\rho, \psi(\tau, \varepsilon)) \cdot \varphi(\rho, \psi(\tau, \varepsilon)) \cdot \psi(\rho, \psi(\tau, \varepsilon)))^2.$$

to the latter identity we have

$$\left(\frac{\psi(\rho, \varepsilon)\,\psi(\tau, \varepsilon)}{\psi(\rho\tau, \varepsilon)}\right)^2 \cdot \psi(\rho, \psi(\tau, \varepsilon)^{-4} \in W$$

Since the group generated by $B$ has no torsion then

$$\frac{\psi(\rho,\varepsilon)\,\psi(\tau,\varepsilon)}{\psi(\rho\tau,\varepsilon)}\cdot\psi(\rho,\psi(\tau,\varepsilon)^{-2}=1$$

and by applying $\Delta(\sigma,\cdot)^2$ to this relation, Lemma 5 gives the second identity. □

**Lemma 12.** *Let us denote* $r_{\sigma,\tau}(\varepsilon)=\langle\sigma,\tau\rangle_\varepsilon\langle\tau,\sigma\rangle_\varepsilon$. *Then*

$$\begin{aligned} r_{\sigma,\tau}(\varepsilon\eta) &= r_{\sigma,\tau}(\varepsilon)r_{\sigma,\tau}(\eta),\\ r_{\rho\sigma,\tau}(\varepsilon) &= r_{\rho,\tau}(\varepsilon)r_{\sigma,\tau}(\varepsilon),\\ r_{\rho,\sigma\tau}(\varepsilon) &= r_{\rho,\sigma}(\varepsilon)r_{\rho,\tau}(\varepsilon)\end{aligned}$$

*for all* $\sigma,\rho,\tau\in G$ *and for all* $\varepsilon,\eta\in C$.

*Proof.* The first identity follows from Lemma 9. The second and the third ones are easy corollaries of Lemma 11. □

Let us now define a subgroup of the group of circular units $C$. Recall that Lemma 5, Lemma 9 and Lemma 12 state that $\Delta(\sigma,\cdot)^2$, $\langle\sigma,\sigma\rangle_\cdot, r_{\sigma,\tau}(\cdot)$ are homomorphisms $C\to\{-1,1\}$.

**Definition 13.** Let $D$ be the intersection of the kernels of the following homomorphisms $C\to\{-1,1\}:\Delta(\sigma,\cdot)^2,\langle\sigma,\sigma\rangle_\cdot$ for all $\sigma\in G$ and $r_{\sigma,\tau}(\cdot)$ for all $\sigma,\tau\in G$.

**Remark 14.** Notice that $D$ is the subgroup of all units in $C$ satisfying the conditions (C1), (C2), (C3) of Proposition 10.

**Lemma 15.** *Let* $2^l=[k:\mathbb{Q}]$. *Then*

$$[C:D]=2^a,$$

*where* $a\le 2l+\binom{l}{2}-1$ *if* $\sqrt{-1}\in k$, $a\le l+\binom{l}{2}-1$ *if* $\sqrt{-1}\notin k$ *and* $k$ *is imaginary, and* $a\le l+\binom{l}{2}$ *if* $k$ *is real.*

*Proof.* Let $\tau_1,\dots,\tau_l\in G$ be such that their restrictions to $k$ are generators of $\mathrm{Gal}(k/\mathbb{Q})$. If the restrictions of $\sigma,\tau\in G$ to $k$ coincide then $\Delta(\sigma,\varepsilon)=\Delta(\tau,\varepsilon)$ and $\psi(\sigma,\varepsilon)=\psi(\tau,\varepsilon)$ for any $\varepsilon\in C$. So $D$ is the intersection of the kernels $\Delta(\sigma,\cdot)^2,\langle\sigma,\sigma\rangle_\cdot$ and $r_{\sigma,\tau}(\cdot)$, where $\sigma,\tau$ runs over the subgroup of $G$ generated by $\tau_1,\dots,\tau_l$. Moreover, using Lemma 6, Lemma 12 and Lemma 11 we obtain that $D$ is the intersection of the kernels of $\Delta(\tau_i,\cdot)^2,\langle\tau_i,\tau_i\rangle_\cdot$ for $1\le i\le l$ and $r_{\tau_i,\tau_j}(\cdot)$, for $1\le i<j\le l$. If $\sqrt{-1}\notin k$ then $\Delta(\tau_i,\cdot)=1$. The lemma follows from observation that if $k$ is imaginary and $\tau_1$ is the complex conjugation then $\psi(\tau_1,\varepsilon)=1$ and so $\langle\tau_1,\tau_1\rangle_\varepsilon=1$ for all $\varepsilon\in C$. □

**Lemma 16.** *Let us denote*

$$s_{\sigma,\tau}(\varepsilon) = \delta(\tau,\varepsilon)^{\sigma-1} \cdot \delta(\sigma,\psi(\tau,\varepsilon))^2 \cdot \delta(\sigma,\varepsilon)^{\tau-1} \cdot \delta(\tau,\psi(\sigma,\varepsilon))^2.$$

*Then*

$$\begin{aligned} s_{\sigma,\tau}(\varepsilon\eta) &= s_{\sigma,\tau}(\varepsilon)s_{\sigma,\tau}(\eta), \\ s_{\rho\sigma,\tau}(\varepsilon) &= s_{\rho,\tau}(\varepsilon)s_{\sigma,\tau}(\varepsilon), \\ s_{\rho,\sigma\tau}(\varepsilon) &= s_{\rho,\sigma}(\varepsilon)s_{\rho,\tau}(\varepsilon) \end{aligned}$$

*for any $\sigma, \tau, \rho \in G$ and $\varepsilon, \eta \in D$.*

*Proof.* It is easy to see that

$$\delta(\sigma,\varepsilon)^{\tau-1} = \begin{cases} \delta(\sigma,\varepsilon)^2 & \text{if } i^\tau = -i, \\ 1 & \text{otherwise.} \end{cases}$$

We deduce from the relation $(\varepsilon\eta)^{1-\sigma} = \varepsilon^{1-\sigma}\eta^{1-\sigma}$ that

$$\Delta(\sigma,\varepsilon\eta)\delta(\sigma,\varepsilon\eta)^2 = \Delta(\sigma,\varepsilon)\delta(\sigma,\varepsilon)^2\Delta(\sigma,\eta)\delta(\sigma,\eta)^2.$$

Since $\Delta(\sigma,\varepsilon) = 1$ for all $\varepsilon \in D$ then $\delta(\sigma,\varepsilon\eta)^2 = \delta(\sigma,\varepsilon)^2\delta(\sigma,\eta)^2$, hence $\delta(\sigma,\varepsilon\eta)^{1-\tau} = \delta(\sigma,\varepsilon)^{1-\tau}\delta(\sigma,\eta)^{1-\tau}$. Interchanging $\sigma$ and $\tau$ gives $\delta(\tau,\varepsilon\eta)^{1-\sigma} = \delta(\tau,\varepsilon)^{1-\sigma}\delta(\tau,\eta)^{1-\sigma}$.

Moreover, Lemma 6 states that $\psi(\tau,\varepsilon\eta)^{1-\sigma} = \psi(\tau,\varepsilon)^{1-\sigma}\psi(\tau,\varepsilon)^{1-\sigma}$ and consequently we deduce from this relation that

$$\begin{aligned} \Delta(\sigma,\psi(\tau,\varepsilon\eta))\delta(\sigma,\psi(\tau,\varepsilon\eta))^2 = \Delta(\sigma,\psi(\tau,\varepsilon))\delta(\sigma,\psi(\tau,\varepsilon))^2\Delta(\sigma,\psi(\tau,\eta)) \\ \cdot \delta(\sigma,\psi(\tau,\eta))^2. \end{aligned}$$

Similarly, interchanging $\sigma$ and $\tau$,

$$\begin{aligned} \Delta(\tau,\psi(\sigma,\varepsilon\eta))\delta(\tau,\psi(\sigma,\varepsilon\eta))^2 = \Delta(\tau,\psi(\sigma,\varepsilon))\delta(\tau,\psi(\sigma,\varepsilon))^2\Delta(\tau,\psi(\sigma,\varepsilon)) \\ \cdot \delta(\tau,\psi(\sigma,\varepsilon))^2. \end{aligned}$$

Since $\varepsilon \in D$ we have $r_{\sigma,\tau}(\varepsilon) = 1$ which means

$$\Delta(\sigma,\psi(\tau,\varepsilon)) = \Delta(\tau,\psi(\sigma,\varepsilon)).$$

Similarly $\eta \in D$ gives

$$\Delta(\sigma,\psi(\tau,\eta)) = \Delta(\tau,\psi(\sigma,\eta))$$

and $\varepsilon\eta \in D$ gives

$$\Delta(\sigma, \psi(\tau, \varepsilon\eta)) = \Delta(\tau, \psi(\sigma, \varepsilon\eta)).$$

Putting things together we obtain

$$\frac{\delta(\sigma, \psi(\tau, \varepsilon\eta))^2}{\delta(\tau, \psi(\sigma, \varepsilon\eta))^2} = \frac{\delta(\sigma, \psi(\tau, \varepsilon))^2}{\delta(\tau, \psi(\sigma, \varepsilon))^2} \cdot \frac{\delta(\sigma, \psi(\tau, \eta)^2}{\delta(\tau, \psi(\sigma, \eta))^2}.$$

The first identity follows.

Since $\sigma\rho - 1 = \sigma - 1 + (\rho - 1)\sigma$ then

$$\delta(\tau, \varepsilon)^{\sigma\rho - 1} = \delta(\tau, \varepsilon)^{\sigma - 1} \delta(\tau, \varepsilon)^{\rho - 1}. \tag{i}$$

Further, we use the identity

$$1 = \frac{\varepsilon^{1-\sigma} \cdot \left(\varepsilon^{1-\rho}\right)^{(\sigma-1)} \cdot \varepsilon^{1-\rho}}{\varepsilon^{1-\sigma\rho}}. \tag{8}$$

At first, we express

$$\left(\varepsilon^{1-\rho}\right)^{(\sigma-1)} = \Delta(\rho, \varepsilon)^{\sigma-1} \cdot \varphi(\rho, \varepsilon)^{2(\sigma-1)} \cdot \psi(\rho, \varepsilon)^{2(\sigma-1)}$$

and consequently we substitute $\psi(\rho, \varepsilon)^{2(1-\sigma)}$ in the relation (8) by the identity

$$\left(\psi(\rho, \varepsilon)^{1-\sigma}\right)^2 = \left(\Delta(\sigma, \psi(\rho, \varepsilon)) \cdot \left(\varphi(\sigma, \psi(\rho, \varepsilon)) \cdot \psi(\sigma, \psi(\rho, \varepsilon))\right)^2\right)^2.$$

Since $\varphi(\cdot, \cdot)$ is a third root of unity, $\Delta(\sigma, \varepsilon) = \Delta(\rho, \varepsilon) = \Delta(\sigma\rho, \varepsilon) = 1$ as $\varepsilon \in D$, and $\psi(\cdot, \cdot)$ belongs to the non-torsion group then we obtain from (8) the identity

$$\delta(\sigma\rho, \varepsilon)^2 = \delta(\sigma, \varepsilon)^2 \delta(\rho, \varepsilon)^2 \Delta(\sigma, \psi(\rho, \varepsilon))^2. \tag{9}$$

In both cases, independently whether $i^\tau = -i$ or $i^\tau = i$, this gives

$$\delta(\sigma\rho, \varepsilon)^{\tau - 1} = \delta(\sigma, \varepsilon)^{\tau - 1} \delta(\rho, \varepsilon)^{\tau - 1} \Delta(\sigma, \psi(\rho, \varepsilon))^{\tau - 1}. \tag{ii}$$

By putting $\psi(\tau, \varepsilon)$ instead of $\varepsilon$ in the relation (8) we obtain the identity

$$1 = \frac{\psi(\tau, \varepsilon)^{1-\sigma} \cdot \left(\psi(\tau, \varepsilon)^{1-\rho}\right)^{(\sigma-1)} \cdot \psi(\tau, \varepsilon)^{1-\rho}}{\psi(\tau, \varepsilon)^{1-\sigma\rho}}. \tag{10}$$

As before, we express

$$\begin{aligned}\left(\psi(\tau, \varepsilon)^{1-\rho}\right)^{(\sigma-1)} = \Delta(\rho, \psi(\tau, \varepsilon))^{\sigma-1} \cdot \varphi(\rho, \psi(\tau, \varepsilon))^{2(\sigma-1)} \\ \cdot \psi(\rho, \psi(\tau, \varepsilon))^{2(\sigma-1)}.\end{aligned}$$

Hence, substituting

$$(\psi(\rho,\psi(\tau,\varepsilon))^{1-\sigma})^2 = \Delta(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^2 \cdot \varphi(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^4 \cdot \psi(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^4$$

to the identity (10) similarly as in previous case we obtain

$$\delta(\sigma\rho,\psi(\tau,\varepsilon))^2 = \delta(\sigma,\psi(\tau,\varepsilon))^2\delta(\rho,\psi(\tau,\varepsilon))^2 \cdot \Delta(\rho,\psi(\tau,\varepsilon))^{\sigma-1} \cdot \frac{\Delta(\sigma,\psi(\tau,\varepsilon))\Delta(\rho,\psi(\tau,\varepsilon))}{\Delta(\sigma\rho,\psi(\tau,\varepsilon))} \cdot \Delta(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^2. \quad \text{(iii)}$$

Finally, we express $\psi(\sigma,\psi(\rho,\varepsilon))$ and $\psi(\cdot,\varepsilon)$ in the relation

$$\left(\frac{\psi(\sigma,\varepsilon)\psi(\rho,\varepsilon)}{\psi(\sigma\rho,\varepsilon)}\right)^{1-\tau} = \psi(\sigma,\psi(\rho,\varepsilon))^{-2(1-\tau)}$$

which was obtained in the proof of Lemma 6. Since again $\psi(\cdot,\cdot)$ belongs to the non-torsion group and $\varphi(\cdot,\cdot)$ is a third root of unity then we have

$$\delta(\tau,\psi(\sigma\rho,\varepsilon))^2 = \delta(\tau,\psi(\sigma,\varepsilon))^2\delta(\tau,\psi(\rho,\varepsilon))^2 \cdot \frac{\Delta(\tau,\psi(\sigma,\varepsilon))\Delta(\tau,\psi(\rho,\varepsilon))}{\Delta(\tau,\psi(\sigma\rho,\varepsilon))} \cdot \Delta(\tau,\psi(\sigma,\psi(\rho,\varepsilon)))^2. \quad \text{(iv)}$$

Since $\varepsilon$ is in the kernel of the homomorphism $r_{\sigma,\tau}(\cdot)$ for all $\sigma,\tau \in G$ then it is easy to see that $\Delta(\sigma,\psi(\tau,\varepsilon)) = \Delta(\tau,\psi(\sigma,\varepsilon))$. In order to prove the identity $s_{\rho\sigma,\tau}(\varepsilon) = s_{\rho,\tau}(\varepsilon)s_{\sigma,\tau}(\varepsilon)$ we multiply the identities (i), (ii), (iii), (iv) and use Lemma 6. Therefore we have to show that

$$1 = \Delta(\rho,\psi(\tau,\varepsilon))^{\sigma-1} \cdot \Delta(\sigma,\psi(\rho,\varepsilon))^{\tau-1} \cdot \Delta(\tau,\psi(\sigma,\psi(\rho,\varepsilon)))^2 \cdot \Delta(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^2. \quad (11)$$

At first, expressing the relation $\psi(\rho,\varepsilon)^{(1-\tau)(\sigma-1)} = \psi(\rho,\varepsilon)^{(1-\sigma)(\tau-1)}$ as before we deduce that

$$\frac{\Delta(\tau,\psi(\rho,\varepsilon))^{\sigma-1} \cdot \Delta(\sigma,\psi(\tau,\psi(\rho,\varepsilon)))^{-2}}{\Delta(\sigma,\psi(\rho,\varepsilon))^{\tau-1} \cdot \Delta(\tau,\psi(\sigma,\psi(\rho,\varepsilon)))^{-2}} = 1.$$

Since $\Delta(\tau,\psi(\rho,\varepsilon))^{\sigma-1} = \Delta(\rho,\psi(\tau,\varepsilon))^{\sigma-1}$ as $\varepsilon \in D$, we obtain that the identity (11) is equivalent to

$$\Delta(\sigma,\psi(\tau,\psi(\rho,\varepsilon)))^2 \cdot \Delta(\sigma,\psi(\rho,\psi(\tau,\varepsilon)))^{-2} = 1.$$

Hence, using the relation $\varepsilon^{(1-\rho)(1-\tau)} = \varepsilon^{(1-\tau)(1-\rho)}$ it is easy to see that $\psi(\tau,\psi(\rho,\varepsilon)) = \psi(\rho,\psi(\tau,\varepsilon))$ which gives exactly what we need. The second identity of the lemma follows. The third one is a consequence of the second one using the symmetry $s_{\sigma,\tau}(\varepsilon) = s_{\tau,\sigma}(\varepsilon)$. □

Now we need to define another subgroup of $C$. Recall that Lemma 16 states that $s_{\sigma,\tau}(\cdot)$ is a homomorphism $D \to \{-1,1\}$ for each $\sigma,\tau \in G$.

**Definition 17.** Let $D'$ be the intersection of the kernels of the homomorphisms $s_{\sigma,\tau}(\cdot) : D \to \{-1,1\}$ for all $\sigma,\tau \in G$.

**Remark 18.** Notice that $D'$ is the subgroup of all units in $C$ satisfying the conditions (C1), (C2), (C3), (C4) of Proposition 10.

**Lemma 19.** *Let* $2^l = [k : \mathbb{Q}]$. *Then*

$$[D : D^{'}] = 2^b,$$

*where* $b \leq \binom{l}{2}$ *if* $\sqrt{-1} \in k$ *and* $b \leq \binom{l+1}{2}$ *otherwise.*

*Proof.* If the restrictions of $\sigma,\tau \in G$ to $k(i)$ coincide then $s_{\sigma,\rho}(\varepsilon) = s_{\tau,\rho}(\varepsilon)$ for any $\rho \in G$ and $\varepsilon \in D$. Let $\tau_1,\ldots,\tau_m \in G$ be such that their restrictions to $k(i)$ form a basis of $\mathrm{Gal}(k(i)/\mathbb{Q})$. Lemma 16 implies that $D'$ is the intersection of the kernels of $s_{\tau_i,\tau_j}(\cdot)$ for $1 \leq i < j \leq m$. The lemma follows. □

**Lemma 20.** *Let us denote* $t_\sigma(\varepsilon) = \delta(\sigma,\varepsilon)^{\sigma+1}\delta(\sigma,\psi(\sigma,\varepsilon))^2$. *Then*

$$t_\sigma(\varepsilon\eta) = t_\sigma(\varepsilon)t_\sigma(\eta),$$
$$t_{\sigma\tau}(\varepsilon) = t_\sigma(\varepsilon)t_\tau(\varepsilon)$$

*for all* $\varepsilon,\eta \in D^{'}$ *and for all* $\sigma,\tau \in G$.

*Proof.* It follows easily that

$$\delta(\sigma,\varepsilon)^{1+\sigma} = \begin{cases} \delta(\sigma,\varepsilon)^2 & \text{if } i^\sigma = i, \\ 1 & \text{otherwise.} \end{cases}$$

The relation $(\varepsilon\eta)^{1-\sigma} = \varepsilon^{1-\sigma}\eta^{1-\sigma}$ gives that $\Delta(\sigma,\cdot)\delta(\sigma,\cdot)^2$ is a homomorphism for all $\varepsilon,\eta \in C$. Therefore using the definition of $D$ (namely the condition (C1) of Proposition 10) we have $\delta(\sigma,\cdot)^2 : D \to \{-1,1\}$ is a homomorphism for any $\sigma \in G$. Similarly, the identity $\psi(\sigma,\varepsilon\eta)^{1-\sigma} = \psi(\sigma,\varepsilon)^{1-\sigma}\psi(\sigma,\eta)^{1-\sigma}$ (see Lemma 5) states that $\Delta(\sigma,\psi(\sigma,\cdot))\delta(\sigma,\psi(\sigma,\cdot))^2 : C \to \{-1,1\}$ is a homomorphism for any $\sigma \in G$. Hence, the definition of $D$ (namely the condition (C2) of Proposition 10) gives that $\delta(\sigma,\psi(\sigma,\cdot))^2 : D \to \{-1,1\}$ is a homomorphism for any $\sigma \in G$. The first identity follows.

Since $\sigma\tau + 1 = (\sigma+1)\tau + (\tau+1)(-1) + 2$ then

$$\delta(\sigma\tau,\varepsilon)^{\sigma\tau+1} = \delta(\sigma\tau,\varepsilon)^{\sigma+1} \cdot \delta(\sigma\tau,\varepsilon)^{\tau+1} \cdot \delta(\sigma\tau,\varepsilon)^2. \tag{12}$$

Moreover, for $\rho = \sigma$ or $\rho = \tau$ independently whether $i^\rho = -i$ or $i^\rho = i$, the identity $\delta(\sigma\tau,\varepsilon)^2 = \delta(\sigma,\varepsilon)^2\delta(\tau,\varepsilon)^2\Delta(\sigma,\psi(\tau,\varepsilon))^2$ obtained in the proof of Lemma 16 (see the identity (11)), gives that

$$\delta(\sigma\tau,\varepsilon)^{\rho+1} = \delta(\sigma,\varepsilon)^{\rho+1}\delta(\tau,\varepsilon)^{\rho+1}\Delta(\sigma,\psi(\tau,\varepsilon))^{\rho+1}. \tag{13}$$

Therefore, putting (12) and (13) together we obtain

$$\begin{aligned}\delta(\sigma\tau,\varepsilon)^{\sigma\tau+1} = {} & \delta(\sigma,\varepsilon)^{\sigma+1}\cdot\delta(\tau,\varepsilon)^{\sigma+1}\cdot\Delta(\sigma,\psi(\tau,\varepsilon))^{\sigma+1}\cdot\delta(\tau,\varepsilon)^{\tau+1}\\ & \cdot\delta(\sigma,\varepsilon)^{\tau+1}\cdot\Delta(\tau,\psi(\sigma,\varepsilon))^{\tau+1}\cdot\delta(\sigma,\varepsilon)^2\cdot\delta(\tau,\varepsilon)^2\\ & \cdot\Delta(\sigma,\psi(\tau,\varepsilon))^2.\end{aligned} \tag{14}$$

As $\Delta(\sigma,\psi(\tau,\varepsilon))^2 = \Delta(\sigma,\psi(\tau,\varepsilon))^{-2}$ and since $\delta(\sigma,\varepsilon)^2 = \delta(\sigma,\varepsilon)^{-2}$ we have

$$\begin{aligned}\delta(\sigma\tau,\varepsilon)^{\sigma\tau+1} = {} & \delta(\sigma,\varepsilon)^{\sigma+1}\cdot\delta(\tau,\varepsilon)^{\tau+1}\cdot\delta(\sigma,\varepsilon)^{\tau-1}\cdot\delta(\tau,\varepsilon)^{\sigma-1}\\ & \cdot\Delta(\sigma,\psi(\tau,\varepsilon))^{\sigma-1}\cdot\Delta(\tau,\psi(\sigma,\varepsilon))^{\tau+1}.\end{aligned} \tag{15}$$

Now we use the identity (iv) obtained in the proof of Lemma 16. Hence, changing $\rho$ to $\tau$ and $\tau$ to $\sigma\tau$ we obtain

$$\begin{aligned}\delta(\sigma\tau,\psi(\sigma\tau,\varepsilon))^2 = {} & \delta(\sigma\tau,\psi(\sigma,\varepsilon))^2\cdot\delta(\sigma\tau,\psi(\tau,\varepsilon))^2\cdot\Delta(\sigma\tau,\psi(\sigma,\psi(\tau,\varepsilon)))^2\\ & \cdot\frac{\Delta(\sigma\tau,\psi(\sigma,\varepsilon))\Delta(\sigma\tau,\psi(\tau,\varepsilon))}{\Delta(\sigma\tau,\psi(\sigma\tau,\varepsilon))}.\end{aligned} \tag{16}$$

Further, we substitute $\delta(\sigma\tau,\psi(\sigma,\varepsilon))^2$ and $\delta(\sigma\tau,\psi(\tau,\varepsilon))^2$ in this relation by the identity (iii) obtained in the proof of Lemma 16 where we change $\rho$ to $\tau$ (and eventually $\tau$ to $\sigma$). Then the condition (C2) of Proposition 10 gives

$$\begin{aligned}\delta(\sigma\tau,\psi(\sigma\tau,\varepsilon))^2 = {} & \delta(\sigma,\psi(\sigma,\varepsilon))^2\cdot\delta(\tau,\psi(\tau,\varepsilon))^2\cdot\delta(\sigma,\psi(\tau,\varepsilon))^2\\ & \cdot\delta(\tau,\psi(\sigma,\varepsilon))^2\cdot\Delta(\tau,\psi(\sigma,\varepsilon))\cdot\Delta(\sigma,\psi(\tau,\varepsilon))\\ & \cdot\Delta(\tau,\psi(\sigma,\varepsilon))^{\sigma-1}\cdot\Delta(\sigma,\psi(\tau,\psi(\tau,\varepsilon)))^{-2}\\ & \cdot\Delta(\sigma,\psi(\tau,\psi(\sigma,\varepsilon)))^{-2}\cdot\Delta(\sigma\tau,\psi(\sigma,\psi(\tau,\varepsilon)))^2.\end{aligned} \tag{17}$$

If we use the condition (C3) of Proposition 10 and the identity

$$s_{\sigma,\tau}(\varepsilon) = \delta(\tau,\varepsilon)^{\sigma-1}\cdot\delta(\sigma,\psi(\tau,\varepsilon))^2\cdot\delta(\sigma,\varepsilon)^{\tau-1}\cdot\delta(\tau,\psi(\sigma,\varepsilon))^2 = 1$$

resulting from the definition of $D'$, then multiplying (15) and (17) we obtain

$$\begin{aligned}t_{\sigma\tau}(\varepsilon) = {} & t_\sigma(\varepsilon)\cdot t_\tau(\varepsilon)\cdot\Delta(\sigma,\psi(\tau,\varepsilon))^{\sigma-1}\cdot\Delta(\tau,\psi(\sigma,\varepsilon))^{\sigma-1}\\ & \cdot\Delta(\tau,\psi(\sigma,\varepsilon))^{\tau-1}\cdot\Delta(\sigma,\psi(\tau,\psi(\tau,\varepsilon)))^{-2}\cdot\Delta(\sigma,\psi(\tau,\psi(\sigma,\varepsilon)))^{-2}\\ & \cdot\Delta(\sigma\tau,\psi(\sigma,\psi(\tau,\varepsilon)))^2.\end{aligned} \tag{18}$$

It follows from Lemma 6 that

$$\Delta(\sigma\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2.$$

Hence, we have to show that

$$\begin{aligned}&\Delta(\tau, \psi(\sigma, \varepsilon))^{\sigma-1} \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{\sigma-1} \cdot \Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \\ &\cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^{-2} \cdot \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \\ &\cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.\end{aligned}$$

Similarly as in the proof of Lemma 16 we deduce easily from the relation $\varepsilon^{(1-\sigma)(1-\tau)} = \varepsilon^{(1-\tau)(1-\sigma)}$ that

$$\psi(\tau, \psi(\sigma, \varepsilon)) = \psi(\sigma, \psi(\tau, \varepsilon))$$

and so we have

$$\Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^{-2} \cdot \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$

Further, it is easy to see that $\Delta(\sigma, \psi(\tau, \varepsilon))^{\sigma-1} \cdot \Delta(\tau, \psi(\sigma, \varepsilon))^{\sigma-1} = 1$ and we only need to show that

$$\Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$

The relation $\psi(\tau, \varepsilon)^{(1-\tau)(1-\sigma)} = \psi(\tau, \varepsilon)^{(1-\sigma)(1-\tau)}$ implies that

$$\frac{\Delta(\tau, \psi(\tau, \varepsilon))^{1-\sigma} \cdot \varphi(\tau, \psi(\tau, \varepsilon))^{2(1-\sigma)} \cdot \psi(\tau, \psi(\tau, \varepsilon))^{2(1-\sigma)}}{\Delta(\sigma, \psi(\tau, \varepsilon))^{1-\tau} \cdot \varphi(\sigma, \psi(\tau, \varepsilon))^{2(1-\tau)} \cdot \psi(\sigma, \psi(\tau, \varepsilon))^{2(1-\tau)}} = 1.$$

At first, we express

$$\begin{aligned}\psi(\tau, \psi(\tau, \varepsilon))^{2(1-\sigma)} = &\Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2 \cdot \varphi(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^4 \\ &\cdot \psi(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^4.\end{aligned}$$

Similarly we have

$$\begin{aligned}\psi(\sigma, \psi(\tau, \varepsilon))^{2(1-\tau)} = &\Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \varphi(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^4 \\ &\cdot \psi(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^4.\end{aligned}$$

Putting things together and using that $\varphi(\cdot, \cdot)$ is a third root of unity and $\psi(\cdot, \cdot)$ belongs to the non-torsion group generated by $B$ we obtain

$$\frac{\Delta(\tau, \psi(\tau, \varepsilon))^{1-\sigma} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2}{\Delta(\sigma, \psi(\tau, \varepsilon))^{1-\tau} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2} = 1.$$

Recall that $\Delta(\tau, \psi(\tau, \varepsilon)) = 1$. Hence, the identity $\Delta(\sigma, \psi(\tau, \varepsilon))^{1-\tau} = \Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1}$ gives

$$\Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$

The lemma follows immediately. □

Now we define another subgroup of $C$. Recall that Lemma 20 states that $t_\sigma(\cdot)$ is a homomorphism $D' \to \{-1, 1\}$ for every $\sigma \in G$.

**Definition 21.** Let $D''$ be the intersection of the kernels of the homomorphisms $t_\sigma(\cdot) : D' \to \{-1, 1\}$ for all $\sigma \in G$.

**Remark 22.** Notice that $D''$ is the subgroup of all units in $C$ satisfying all conditions of Proposition 10, in other words $D'' = C \cap (K_J^2 \cup 2K_J^2)$.

**Lemma 23.** *Let $2^l = [k : \mathbb{Q}]$. Then*

$$[D^{'} : D^{''}] = 2^c,$$

*where $c \leq l - 1$ if $\sqrt{-1} \in k$, $c \leq l$ if $\sqrt{-1} \notin k$ and $k$ is imaginary, and $c \leq l + 1$ if $k$ is real.*

*Proof.* This follows from Lemma 20 similarly as Lemma 15 and Lemma 19 using the observation that if $k$ is imaginary and $\tau_1$ is the complex conjugation then $t_{\tau_1}(\varepsilon) = 1$ for all $\varepsilon \in C$. □

## 2.4 The Divisibility of $[\mathbf{E} : \mathbf{C}]$ by a Power of 2

In this chapter we introduce the main results of this text.

**Lemma 24.** *Let $\varepsilon \in C$. If there is $\gamma \in K_J$ such that $\varepsilon = \gamma^2$ or $\varepsilon = 2\gamma^2$, then $\xi_\varepsilon$ defined by $\xi_\varepsilon(\sigma) = \gamma^{1-\sigma}$ is a character on $\mathrm{Gal}(K_J/k)$, i.e., $\xi_\varepsilon : \mathrm{Gal}(K_J/k) \to \{-1, 1\}$ is a homomorphism, and $\gamma \in k$ if and only if $\xi_\varepsilon$ is the principal character. Moreover*

$$\tilde{\xi} : C \cap ({K_J}^2 \cup 2{K_J}^2) \to \widehat{\mathrm{Gal}(K_J/k)},$$

*where $\tilde{\xi}(\varepsilon) = \xi_\varepsilon$, is a homomorphism, i.e., $\xi_{\varepsilon\eta}(\sigma) = \xi_\varepsilon(\sigma)\xi_\eta(\sigma)$ for all $\varepsilon, \eta \in C \cap ({K_J}^2 \cup 2{K_J}^2)$ and for any $\sigma \in G$.*

*Proof.* The lemma follows immediately from $1 - \sigma\tau = (1 - \sigma) + (1 - \tau)\sigma$. □

**Theorem 25.** *Let $n = \#J$ and $2^l = [k : \mathbb{Q}]$.*

*i) If $k$ is real then*

$$2^{2^l - n - l^2 - l - 3} \mid [E : C],$$

*ii) If $k$ is imaginary and $\sqrt{-1} \notin k$ then*

$$2^{2^{l-1} - n - l^2 - l - 1} \mid [E : C],$$

*iii) If* $\sqrt{-1} \in k$ *then*

$$2^{2^{l-1}-n-l^2-l} \mid [E : C].$$

*Proof.* Let $D''' = C \cap (k^2 \cup 2k^2)$, i. e. $D'''$ consists of all $\varepsilon \in C$ of the form $\varepsilon = \eta^2$ or $\varepsilon = 2\eta^2$ for a suitable $\eta \in k$. Recall that from Lemma 24 and the definitions of $D''$ and $D'''$ it follows that $[D'' : D'''] = 2^d$, where $d \leq n - l$. Moreover, using Lemma 15, Lemma 19 and Lemma 23 we know that $[C : D'''] = [C : D] \cdot [D : D'] \cdot [D' : D''] \cdot [D'' : D'''] = 2^{a+b+c+d}$, where

$$a + b + c + d \leq \begin{cases} l^2 + n + l + 1 & \text{if } k \text{ is real} \\ l^2 + n + l - 1 & \text{if } k \text{ is imaginary and } \sqrt{-1} \notin k \\ l^2 + n + l - 2 & \text{if } \sqrt{-1} \in k. \end{cases}$$

From the definition of $E$ and $D'''$ we know that $\operatorname{rank} E = \operatorname{rank} D'''$. Each unit in $D'''$ is of the form $\eta^2$ or $2\eta^2$ for a suitable $\eta \in k$. Since $(2\eta^2) \cdot (2\vartheta^2) = (2\eta\vartheta)^2$ is again a square, there is a basis of $D'''$ where all elements but at most one are squares. Therefore we have $2^{2^l-2} \mid [E : D''']$ if $k$ is real and $2^{2^{l-1}-2} \mid [E : D''']$ if $k$ is imaginary. The theorem follows using $[E : C] = \frac{[E:D''']}{[C:D''']}$. □

Putting together Proposition 4 and Theorem 25 we obtain a lower bound for the divisibility of the class number $h^+$ by a power of 2. A very explicit special case of this result is given by the following example.

**Example 26.** Let us denote $n = \#J$. Let us suppose $k = K_J$ and $\#\{p \in J;\ p < 0\} > 1$. Then

$$[E : C] = 2^{2^{n-2}-n} \cdot Qh^+,$$

which can be obtained in the same way as in [12] (see Theorem 1 and Remark below its proof). Then Theorem 25 gives

$$2^{2^{n-1}-2n-n^2} \mid [E : C]$$

and consequently

$$2^{2^{n-2}-n-n^2-1} \mid h^+$$

because $Q \mid 2$.

# Chapter 3

# The ramification index of 2 being 4

The aim of this chapter is to describe the group of circular units $C$ of a compositum $k$ of quadratic fields in the last case that has not been covered yet, namely in the case when the ramification index $e$ of 2 equals 4. It is easy to see that $e$ divides 4. If $e = 1$ or $e = 2$ we already know a basis of $C$ and an explicit formula for the index of $C$ in the full group of units $E$ (see [12] and [18]). The main ingredience for these results was the observation that the action of the augmentation ideal of $\mathbb{Z}[G]$, where $G = \mathrm{Gal}(k/\mathbb{Q})$, on the quotient $C/W$, where $W$ is the group of all roots of unity in $k$, gives squares in $C/W$. In other words, for any $\varepsilon \in C$ and any $\sigma \in G$ there is $\rho \in W$ and $\eta \in C$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$. Unfortunately this key property of the group of circular units of a compositum of quadratic field is not satisfied in the mentioned case $e = 4$ (see Example 8 for $k = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$ below). Therefore if $e = 4$ we cannot use the same approach for $k$. Nevertheless, using the three maximal subfields of $k$ whose ramification index at 2 is 2, we are able to describe an explicit maximal independent system of units in $C$. Let $\tilde{C}$ be the group generated by $W$ and by this system. Then we can compute the index $[E : \tilde{C}]$ and give a reasonable upper bound for the index $[C : \tilde{C}]$ (see Theorem 7 and Proposition 5).

## 3.1 Definitions and basic results

Let $k$ be a compositum of quadratic fields and let $K$ be the genus field of $k$ in narrow sense. We assume that both $-1$ and 2 are squares in $K$. We put

$$J = \{-1, -2, 2\} \cup \{p \in \mathbb{Z};\ p \equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } k\}.$$

For any $p \in J$, let

$$n_{\{p\}} = \begin{cases} |p| & \text{if } p \notin \{-1, -2, 2\}, \\ 4 & \text{if } p = -1, \\ 8 & \text{if } p = \pm 2. \end{cases}$$

For any $L \subseteq J$ let $n_L$ be the smallest common multiple of $n_{\{p\}}$ for all $p \in L$ (by convention $n_\emptyset = 1$), moreover similarly as in previous Chapter 2 let us denote

$$\zeta_S = e^{2\pi i/n_S}, \quad \mathbb{Q}^S = \mathbb{Q}(\zeta_S), \quad K_S = \mathbb{Q}(\sqrt{p};\, p \in S), \quad k_S = k \cap K_S.$$

We call a subset $L \subseteq J$ *admissible* if $L$ contains at most one of the numbers $-1$, 2, and $-2$. For any admissible set $L \subseteq J$ we define

$$\varepsilon_L = \begin{cases} 1 & \text{if } L = \emptyset, \\ i & \text{if } L = \{-1\}, \\ \frac{1}{\sqrt{p}}\, \mathrm{N}_{\mathbb{Q}^L/K_L}(1 - \zeta_L) & \text{if } L = \{p\},\ p \neq -1, \\ \mathrm{N}_{\mathbb{Q}^L/K_L}(1 - \zeta_L) & \text{if } \#L > 1, \end{cases}$$

and $\eta_L = \mathrm{N}_{K_L/k_L}(\varepsilon_L)$.

Let $\chi_2$ and $\chi_{-2}$ be the unique even and odd Dirichlet character of conductor 8, respectively. For each $p \in J - \{2, -2\}$ let $\chi_p$ be the unique Dirichlet character of conductor $n_{\{p\}}$, so $\chi_p$ is odd if and only if $p < 0$.

Let $X$ be the group of all even Dirichlet characters corresponding to $k$. Each $\chi \in X$ can be written in the form $\chi = \prod_{p \in L_\chi} \chi_p$ for a unique admissible set $L_\chi \subseteq J$. Then the conductor of $\chi$ is equal to $n_{L_\chi}$.

It is easy to see that, for any admissible set $L \subseteq J$, a character $\chi \in X$ belongs to the set of Dirichlet characters corresponding to the field $k_L$ if and only if $L_\chi \subseteq L$.

Let $C$ be the group of circular units of $k$ defined in [12]. This group contains the Sinnott's group of circular units of $k$ but it can be slightly bigger. Similarly, for any $S \subseteq J$ let $C_S$ be the group of circular units of $k_L$ defined in [12]. If $L$ is admissible then the ramification index of 2 in $k_L$ is not equal to 4 and so we know the following basis of $C_L$:

**Lemma 1.** *If $L \subseteq J$ is admissible then a basis of $C_L$ is formed by the set of all $\eta_{L_\chi}$ where $\chi \in X$ is non-trivial and satisfies $L_\chi \subseteq S$.*

*Proof.* If $-1 \notin L$ see see [12, Lemma 5], otherwise see [18, Proposition 1.4]. □

Let $W$ be the group of all roots of unity in $k$. Let $\tilde{C}$ be the subgroup of the multiplicative group $k^\times$ generated by $W$ and by all conjugates of $\eta_L$ for all admissible sets $L \subseteq J$. Let $G = \mathrm{Gal}(k/\mathbb{Q})$ be the Galois group of $k$.

**Lemma 2.** *For any $\varepsilon \in \tilde{C}$ and any $\sigma \in G$ there is $\rho \in W$ and $\eta \in \tilde{C}$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$.*

*Proof.* Consider a conjugate of $\eta_L$ for an admissible set $L \subseteq J$. If $-1 \notin L$ use [12, Lemma 2], otherwise use [18, Lemma 1.2]. □

**Lemma 3.** *The set $W \cup \{\eta_{L_\chi};\ \chi \in X,\ \chi \neq 1\}$ generates the group $\tilde{C}$.*

*Proof.* Lemma 2 gives that $\tilde{C}$ is as a group generated by $W$ and by $\eta_L$ for all admissible sets $L \subseteq J$. For any admissible set $L \subseteq J$ we can show that if $L \neq L_\chi$ for all $\chi \in X$ then $\eta_L$ can be written as a multiplicative $\mathbb{Z}$-linear combination of $\eta_L$ for $L \subsetneq L$ (modulo roots of unity). If $-1 \notin L$ use [12, Lemma 5], otherwise use [18, pp. 1077]. □

## 3.2 The index of $\tilde{C}$ in $C$

**Proposition 4.** *The group $C$ of circular units of $k$ is generated by $\tilde{C}$ and by all conjugates of $\mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$, where $L \subseteq J$ is not admissible, $L \neq \{-1, 2, -2\}$, and the ramification index of $k_L$ at 2 is 4.*

*Proof.* Let $E$ be the full group of units of $k$. By definition (see [15]), $C$ is the intersection of $E$ and a group $D$, where $D$ is generated by $-1$, by $\sqrt{p}$ for all $p \in J$ such that $p > 0$ and $\sqrt{p} \in k$, and by all conjugates of $\mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$ for all non-empty $L \subseteq J$.

For a non-empty $L \subseteq J$, it is well-known that $\mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$ is a unit if and only if $n_L$ is not a prime-power. Moreover, if $p \in J$ and $p < 0$ then all units of $k_{\{p\}}$ are roots of unity. Therefore $\tilde{C}$ is the intersection of $E$ and a group $\tilde{D}$, where $\tilde{D}$ is generated by $-1$, by $\sqrt{p}$ for all $p \in J$ such that $p > 0$ and $\sqrt{p} \in k$, and by all conjugates of $\mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$ for all *admissible* non-empty $L \subseteq J$.

If $L$ is not admissible and the ramification index of $k_L$ at 2 is not 4 then $k_L = k_{L'}$ for a suitable admissible $L' \subseteq L$. Hence $D$ is generated by $\tilde{D}$ and by $\mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$ for all non-admissible $L \subseteq J$ such that the ramification index of $k_L$ at 2 is 4. This norm is a unit unless $L = \{-1, 2, -2\}$ and $\sqrt{-1}, \sqrt{2} \in k$, in which case $k_L = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ is the eighth cyclotomic field. But the group of all units of the eighth cyclotomic field is generated by $\zeta_8$ and by

$$\eta = \zeta_8^{-1} \cdot \frac{1-\zeta_8^3}{1-\zeta_8} = 1 + \zeta_8 + \zeta_8^{-1} = 1 + \sqrt{2}.$$

We have

$$\eta_{\{2\}} = \frac{1}{\sqrt{2}} \mathrm{N}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2})}(1-\zeta_8) = \sqrt{2}-1 = \eta^{-1}$$

and the proposition follows. □

**Proposition 5.** *The group $\tilde{C}$ is of finite index in $C$ and $[C:\tilde{C}] \leq 2^n$, where $n$ is the number of all $L \subseteq J$ such that $\{-1,2,-2\} \subsetneq L$ and the ramification index of $k_L$ at 2 is 4. Moreover, the Galois action of $G$ on $C/\tilde{C}$ is trivial.*

*Proof.* Let $T = J - \{-1,2,-2\}$. For any $x \in \{-1,2,-2\}$ let $\rho_x$ be the generator of $\mathrm{Gal}(K/K_{T\cup\{x\}})$. For any $S \subseteq T$ we put $L = S \cup \{-1,2,-2\}$ and $\varepsilon = \mathrm{N}_{\mathbb{Q}^L/k_L}(1-\zeta_L)$. Then

$$\varepsilon^2 = \varepsilon^{1+\rho_{-1}} \cdot \varepsilon^{1+\rho_{-2}} \cdot \left(\varepsilon^{1+\rho_2}\right)^{-\rho_{-1}}.$$

For any $x \in \{-1,2,-2\}$ we have

$$\varepsilon^{1+\rho_x} = \mathrm{N}_{\mathbb{Q}^L/k_{T\cup\{x\}}}(1-\zeta_L) = \eta_{T\cup\{x\}}$$

because $\mathrm{N}_{\mathbb{Q}^L/\mathbb{Q}^{T\cup\{x\}}}(1-\zeta_L) = 1-\zeta_{T\cup\{x\}}$. We have obtained $\varepsilon^2 \in \tilde{C}$ and for any $\sigma \in G$ Lemma 2 gives $\varepsilon^{2(1-\sigma)} \in W \cdot \tilde{C}^2$, which implies $\varepsilon^{1-\sigma} \in \tilde{C}$. The proposition follows by means of Proposition 4. □

## 3.3 A basis of $\tilde{C}$ and the index of $\tilde{C}$ in $E$

**Theorem 6.** *The set $\{\eta_{L_\chi};\ \chi \in X,\ \chi \neq 1\}$ is a $\mathbb{Z}$-basis of $\tilde{C}$, i.e. elements of this set are multiplicatively independent and together with $W$ generate $\tilde{C}$.*

*Proof.* Proposition 5 gives that $\tilde{C}$ and $C$ has the same $\mathbb{Z}$-rank. As the index $[E:C]$ is finite, $\tilde{C}$ and $E$ has the same $\mathbb{Z}$-rank and the $\mathbb{Z}$-rank of $E$ is equal to the number of elements of the given set. The theorem follows from Lemma 3. □

Having a $\mathbb{Z}$-basis allows us to compute the index:

**Theorem 7.** *We have*

$$[E:\tilde{C}] = \left(\prod_{\chi\in X,\,\chi\neq 1} \frac{2\cdot[k:k_{L_\chi}]}{[k:k^+]}\right) \cdot |X|^{-|X|/2} \cdot Qh^+,$$

*where $k^+$ is the maximal real subfield of $k$, $|X|$ means the number of characters in $X$, $Q = [E : W\cdot(E\cap k^+)]$ is the Hasse unit index of $k$ and $h^+$ is the class number of $k^+$.*

*Proof.* This can be proved in the same way as Theorem 1 in [12]. □

The following example shows that the estimate of the index $[C : \tilde{C}]$ can be precise. It seems to be an interesting question whether this holds true in general.

**Example 8.** Let $k = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$. Then $k$ is the 24th cyclotomic field. Sinnott's formula for the index of the group of circular units of a cyclotomic field (see Theorem 4.1 in [22]) gives that (for the field $k$) the Sinnott's group of circular units of $k$ equals $E$ and so we also have $C = E$. Then Theorem 6.1 in [11] gives the following $\mathbb{Z}$-basis of $C$: $\alpha = 1 - \zeta$, $\beta = 1 - \zeta^{19}$, $\gamma = \frac{1-\zeta^9}{1-\zeta^3}$. As $\beta$ is a conjugate of $\alpha$, we see that we obtain $\alpha \cdot \beta^{-1}$ by an action of the augmentation ideal on $\alpha$. As both $\alpha$ and $\beta$ belong to a basis we see that $\alpha \cdot \beta^{-1}$ is not a square modulo roots of unity in $E$. Theorem 6 states that $\eta_{\{2\}}$, $\eta_{\{-1,-3\}}$ and $\eta_{\{-2,-3\}}$ form a $\mathbb{Z}$-basis of $\tilde{C}$. We have

$$\begin{aligned} \eta_{\{2\}} &= (1+\sqrt{2})^{-1} = \zeta^3 \cdot \gamma, \\ \eta_{\{-1,-3\}} &= 1 - \zeta^2 = \zeta \cdot \alpha \cdot \beta^{-1} \cdot \gamma, \\ \eta_{\{-2,-3\}} &= \alpha \cdot \beta. \end{aligned}$$

The determinant of the transition matrix gives the index $[C : \tilde{C}] = 2$ for $k$, which equals the upper bound given by Proposition 5.

# Bibliography


[1] M. BULANT, Class Number Parity of a Compositum of Quadratic Fields, Ph.D. thesis, Faculty of science MU Brno (2002)

[2] M. BULANT, Class number parity of a compositum of five quadratic fields. Acta Mathematica et Informatica Universitatis Ostraviensis (2002), 25 - 34.

[3] L. CARLITZ, A characterization of algebraic number fields with class number two. Proc. Am. Math. Soc. 11 (1960), 391-392.

[4] P. E. CONNER and J. HURRELBRINK, Class number parity. Number 8 in Ser. Pure Math. World Sei., Singapore, 1988.

[5] R. GILLARD, Remarques sur les unités cyclotmiques et les unités elliptiques, J. Number Theory 11 (1979), 21-48.

[6] R. GOLD and J. KIM, Bases for cyclotomic fields, Compositio Math. 71 (1989), 13-27.

[7] K. IRELAND and S. ROSEN, A classical introduction to modern number theory, Springer (1992).

[8] K. IWASAWA, A class number formula for cyclotomic fields, Ann. of Math. 76 (1) (1962), 171-179.

[9] R. KUČERA, Formulae for the relative class number of an imaginary abelian field in the form of a determinant, Nagoya Math. J. 163 (2001), 167-191.

[10] R. KUČERA, On bases of odd and even universal ordinary distributions, J. Number Theory 40 (1992), 264-283.

[11] R. KUČERA, On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field, J. Number Theory 40 (1992), 284-316.

[12] R. KUČERA, On the Stickelberger ideal and circular units of a compositum of quadratic fields, J. Number Theory 56 (1996), 139-166.

[13] R. KUČERA, Circular units and class groups of abelian fields, Ann. Sci. Math. Québec 28 (2004), 121 - 136.

[14] R. KUČERA, On the parity of the class number of a biquadratic field, J. Number Theory 52 (1995), 43-52.

[15] R. KUČERA, A note on Sinnott's definition of circular units of an abelian field, J. Number Theory 63 (1997), 403-407.

[16] H. W. LEOPOLDT, Über die Einheitengruppe und Klassenzahl reeller Abelscher Zahlkörper, Abh. Deutsch. Akad. Wiss. Berlin, Math.-Naturw. Kl. 1953, No. 2, 1-48.

[17] G. LETTL, A note on Thaine's circular units, J. Number Theory 35 (1990), 224-226.

[18] Z. POLICKÝ, On the index of circular units in the full group of units of a compositum of quadratic fields, J. Number Theory 128/4 (2008), 1074-1090.

[19] Z. POLICKÝ, On the group of circular units of any compositum of quadratic fields, to appear in Acta Arithmetica.

[20] K. RAMACHANDRA, On the units of cyclotomic fields, Acta Arith. 12 (1966), 165-173.

[21] K. RUBIN, Global units and ideal class groups, Invent. Math. 89 (1987), 511-526.

[22] W. SINNOTT, On the Stickelberger ideal and circular units of a cyclotomic field, Ann. of Math. 108 (1978), 107-134.

[23] W. SINNOTT, On the Stickelberger ideal and circular units of an abelian field, Invent. Math. 62 (1980), 181-234.

[24] L. SKULA, Another proof of Iwasawa's class number formula, Acta Arith. 39 (1981), 1-6.

[25] L. SKULA, Some basis of the Sticklberger ideal, Math. Slovaca 43 (1993), 541-571.

[26] L. SKULA, The orders of solutions of the Kummer system of congruences, Trans. Am. Math. Soc. 343, (1994), 587-607.

[27] F. THAINE, On the ideal class groups of real abelian number fields, Ann. of Math. 128 (1988), 1-18.

[28] L. C. WASHINGTON, Introduction to Cyclotomic Fields, Grad. Texts in Math. 83, Springer, New York, NY, 1997.