2002

Exotic integral witt equivalence of algebraic number fields

Changheon Kang
Louisiana State University and Agricultural and Mechanical College

EXOTIC INTEGRAL WITT EQUIVALENCE OF ALGEBRAIC NUMBER FIELDS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Changheon Kang
B.S., Korea University, 1990
M.S., Korea University, 1994
M.S., Louisiana State University, 1997
August 2002

Acknowledgments

I would like to thank my major professor, Dr. Robert V. Perlis, for directing this dissertation, as well as much of my mathematical education. His help, guidance, advice, and endless patience have been greatly appreciated.

I am grateful to Dr. Pierre E. Conner for sharing his insight and suggestions which led to the topic of this dissertation.

I would like to express my appreciation to the Department of Mathematics at Louisiana State University for giving me the opportunity to pursue my interest in the field of algebraic number theory. I also thank all my professors in the Department of Mathematics at Korea University for helping me build a solid mathematical background.

I am deeply indebted to my wife, Yeonhee, and to my son, Hosung, for all their patience and support.

Finally, I must thank my parents, Gyehoon and Soonja, for their love, and for encouraging me constantly to improve my knowledge.

Table of Contents

Acknowledgments ..... **ii**

Abstract ..... **iv**

Introduction **1**

1. Preliminaries **4**
1.1 The Witt Ring $W(K)$ 4
1.2 Invariants of $W(K)$ 6
1.3 The Symbols of K 12

2. The Integral Witt Ring $W(\mathcal{O}_K)$ **15**
2.1 The Integral Witt Ring $W(\mathcal{O}_K)$ 15
2.2 The Knebusch Exact Sequence 16
2.3 The Symbols of $\mathcal{O}_K$ 17
2.4 The Symbols and the Integral Witt Ring 23
2.5 The Ideals of the Integral Witt Ring 27

3. The Main Results **36**

4. The Class $\mathcal{K}_0$ **43**
4.1 Exotic Integral Witt Equivalence in $\mathcal{K}_0$ 43
4.2 An Exotic Example 44

5. The Class $\mathcal{K}_1$ **49**

6. CM Extensions in $\mathcal{K}_0$ or $\mathcal{K}_1$ **55**

7. Conclusions **63**

References **64**

Vita **65**

Abstract

Two algebraic number fields K and L are said to be *exotically integrally Witt equivalent* if there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ between the Witt rings of the number rings $\mathcal{O}_K$ and $\mathcal{O}_L$ of K and L, respectively. This dissertation studies exotic integral Witt equivalence for totally complex number fields and gives necessary and sufficient conditions for exotic integral equivalence in two special classes of totally complex number fields.

Introduction

An algebraic number field K is of the form $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is a root of a polynomial with rational coefficients. In a number field K there is the ring $\mathcal{O}_K$ of integers of K.

This dissertation will associate two rings to a number field K:

(1) $W(K)$, the Witt ring of K

(2) $W(\mathcal{O}_K)$, the integral Witt ring.

These two rings are related by the Knebusch exact sequence [M-H, 3.3, p.93]:

$$0 \longrightarrow W(\mathcal{O}_K) \longrightarrow W(K) \xrightarrow{\partial} \bigoplus_{\mathfrak{p}} W(\mathcal{O}_K/\mathfrak{p})$$

where the direct sum extends over all non-zero prime ideals of $\mathcal{O}_K$. Since the structure of $W(K)$ is well-studied, we can use this sequence to describe $W(\mathcal{O}_K)$.

Two fields K and L are called *Witt equivalent* if there exists a ring isomorphism $W(K) \cong W(L)$. In 1994, Perlis, Szymiczek, Conner, and Litherland studied Witt equivalence for number fields and gave necessary and sufficient conditions for two number fields to be Witt equivalent (see [P-S-C-L]).

Shastri [Sh] has given the structure of the additive group of $W(\mathcal{O}_K)$ in terms of arithmetical invariants of K. Czogała [Cz] defined two number fields K and L to be *integrally Witt equivalent* if there exists a ring isomorphism $W(K) \cong W(L)$ which induces a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$. He also gave a finite set of necessary and sufficient conditions for integral Witt equivalence.

Note that integral Witt equivalence is *more* than the ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$; such an isomorphism is required to be induced by a ring isomorphism $W(K) \cong W(L)$. An interesting question arises for number fields K and L:

Q. Can we have a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$
while $W(K) \ncong W(L)$?

The answer to the question **Q** is yes by the example given in Section 4.2. In this dissertation we define two number fields K and L to be *exotically integrally Witt equivalent* if there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$, but no assumption is made on $W(K)$ or $W(L)$.

Note that integral Witt equivalence implies exotic integral Witt equivalence. The positive answer to the question **Q** tells that exotic integral Witt equivalence does not imply integral Witt equivalence.

This dissertation studies exotic integral Witt equivalence for totally complex number fields. We discuss two special classes $\mathcal{K}_0$ and $\mathcal{K}_1$ of totally complex number fields in Chapter 4 and in Chapter 5, respectively. Although the definitions of these two classes are technical, we can see that the class $\mathcal{K}_0$ contains at least all totally complex number fields having only one dyadic prime, and that every fields in the class $\mathcal{K}_1$ has at least 2 dyadic primes. We give finite sets of necessary and sufficient conditions for a pair of fields in either of these special classes to be exotically integrally Witt equivalent. Here are the results:

Theorem 4.2. *For $K,\ L \in \mathcal{K}_0$, there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ iff we have*

(1) $level K = level L$,

(2) $c_K + g_2(K) + 2\text{-}rk\, \mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\, \mathcal{C}_L$.

Theorem 5.5. *For $K,\ L \in \mathcal{K}_1$, there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ iff we have*

(1) $level K = level L$,

(2) $c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L$,

(3) Either -1 *lies in both* Δ_K *and* Δ_L*, or it lies in neither one,*

(4) $2\text{-}rk(E_K/\Delta_K) = 2\text{-}rk(E_L/\Delta_L)$.

For a general pair of number fields K and L not assumed to be in either $\mathcal{K}_0$ or in $\mathcal{K}_1$, necessary and sufficient conditions for exotic integral Witt equivalence are not known.

In Section 4.2, we give an example of two algebraic number fields

$$K = \mathbb{Q}(\alpha) \quad \text{and} \quad L = \mathbb{Q}(\sqrt{-5})$$

where $\alpha \in \mathbb{C}$ is a root of the polynomial $x^4 + x^3 + 2x^2 - 4x + 3$. Their degrees are

$$[K\colon \mathbb{Q}] = 4 \quad \text{and} \quad [L\colon \mathbb{Q}] = 2$$

which implies $W(K) \ncong W(L)$.

On the other hand, for the number field K, we have

$$c_K = 2, \quad g_2(K) = 1, \quad 2\text{-}rk\mathcal{C}_K = 0, \quad \text{and} \quad levelK = 2.$$

For the number field L, we have

$$c_L = 1, \quad g_2(L) = 1, \quad 2\text{-}rk\mathcal{C}_L = 1, \quad \text{and} \quad levelL = 2.$$

Since K and L are totally complex number fields with one dyadic prime, they are in the class $\mathcal{K}_0$. Then since we have

$$\begin{aligned} levelK &= 2 &&= levelL \\ c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K &= 3 &&= c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L \end{aligned}$$

we have $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ by Theorem 4.2. Thus K and L give a positive answer to the question **Q** posed earlier in this introduction.

1. Preliminaries

In this chapter we introduce the basic concepts and results. References are given, but no attempt is made to prove the material presented here.

1.1 The Witt Ring $W(K)$

Let K be a field of characteristic not equal to 2.

Definition 1.1. An inner product space over K is a pair (V, β) in which V is a non-zero finite dimensional K-vector space and

$$\beta \colon V \times V \to K$$

is a symmetric K-bilinear form which is non-degenerate in the sense that the adjoint

$$\mathsf{Ad}_\beta \colon V \to \mathrm{Hom}_K(V, K)$$

$$x \;\mapsto\; \beta(\_, x)$$

is an isomorphism.

We call such a non-degenerate symmetric bilinear form an *inner product*.

Definition 1.2. Two inner product spaces (V, β) and (V', β') over K are said to be *isometric* ($V \simeq V'$) if there is an K-linear bijection

$$L \colon V \to V'$$

such that

$$\beta'(L(u), L(v)) = \beta(u, v) \quad \text{for all} \;\; u, v \in V.$$

Addition and multiplication of two K-inner product spaces (V_1, β_1) and (V_2, β_2) are defined as follows.

Definition 1.3. The *orthogonal sum* $(V_1, \beta_1) \oplus (V_2, \beta_2)$ is defined to be the pair $(V_1 \oplus V_2, \beta_1 \oplus \beta_2)$ where $V_1 \oplus V_2$ is the direct sum of K-vector spaces V_1 and V_2, and $\beta_1 \oplus \beta_2$ is given by

$$(\beta_1 \oplus \beta_2)(u_1 \oplus u_2, v_1 \oplus v_2) = \beta_1(u_1, v_1) + \beta_2(u_2, v_2)$$

(where $u_1 \oplus u_2$ is just the pair (u_1, u_2)). And the *tensor product* $(V_1, \beta_1) \otimes (V_2, \beta_2)$ is defined to be the pair $(V_1 \otimes V_2, \beta_1 \otimes \beta_2)$ where $V_1 \otimes V_2$ is the tensor product of K-vector spaces V_1 and V_2, and $\beta_1 \otimes \beta_2$ is given by

$$(\beta_1 \otimes \beta_2)(u_1 \otimes u_2, v_1 \otimes v_2) = \beta_1(u_1, v_1)\beta_2(u_2, v_2).$$

Let (V, β) be a K-inner product space and W a subspace of V.

Definition 1.4. The *orthogonal complement*, $W^\perp$, of W is the subspace of V defined by

$$W^\perp = \{v \in V \mid \beta(v, W) = 0\}.$$

Note that the restriction β_W of β to W need not be an inner product.

Definition 1.5. A subspace W of V is called a *metabolizer* of (V, β) if $W = W^\perp$. In this case, (V, β) is called to be *metabolic*.

To each $d \in K^*$ we associate $< d >$, the 1-dimensional inner product structure on K itself with the inner product β defined by $\beta(u, v) = duv$. Then

Theorem 1.6. *If (V, β) is any n-dimensional inner product space over K, then there exist $d_1, \ldots, d_n \in K^*$ such that*

$$V \simeq < d_1 > \oplus \cdots \oplus < d_n > .$$

Proof. Corollary 2.4, p.10 in [Lam]. □

Notation. We will abbreviate $< d_1 > \oplus \cdots \oplus < d_n >$ by $< d_1, \ldots, d_n >$, and the n-dimensional space $< d, \ldots, d >$ by $n < d >$.

Definition 1.7. Two inner product spaces (V_1, β_1) and (V_2, β_2) over K are said to be *Witt equivalent* if there exist metabolic inner product spaces (V_1', β_1') and (V_2', β_2') such that

$$(V_1, \beta_1) \oplus (V_1', \beta_1') \simeq (V_2, \beta_2) \oplus (V_2', \beta_2').$$

Witt equivalence forms an equivalence relation on the set of all isometry classes of inner product spaces. The equivalence class of (V, β) will be denoted by $\langle V, \beta \rangle$ and referred to as the *Witt class* of (V, β). And $\langle d \rangle$ denotes the Witt class of the 1-dimensional space $< d >$. The collection of all Witt classes is a commutative ring with identity, which we call the *Witt ring* $W(K)$ of K:

- Addition: $\langle V, \beta \rangle + \langle V', \beta' \rangle = \langle V \oplus V', \beta \oplus \beta \rangle$
- Additive identity: $\langle V, \beta \rangle$ where (V, β) contains a metabolizer
- Additive inverse: $-\langle V, \beta \rangle = \langle V, -\beta \rangle$
- Multiplication: $\langle V, \beta \rangle \langle V', \beta' \rangle = \langle V \otimes V', \beta \otimes \beta' \rangle$
- Multiplicative identity: $\langle 1_K \rangle$.

Note that, for $a,\ b \in K^*$, we have $\langle ab^2 \rangle = \langle a \rangle$ in $W(K)$. Thus we have a group homomorphism

$$K^*/K^{*2} \longrightarrow W(K)^*$$

from the square class group K^*/K^{*2} into the group of units in $W(K)$, which is in fact an embedding. And $W(K)$ is additively generated by the classes $\langle a \rangle$ for all $a \in K^*$ [M-H, Lemma 3.1, p.65].

1.2 Invariants of $W(K)$

Let K be an algebraic number field with its Witt ring $W(K)$. We will discuss the following invariants:

A. the rank modulo 2,

B. the discriminant modulo squares,

C. the total signature,

D. the Hasse-Witt invariants.

It is known by Hasse that these four invariants form a complete set of invariants of the Witt ring $W(K)$ of a number field K, meaning: two K-inner product spaces (V_1, β_1) and (V_2, β_2) are in the same Witt class in $W(K)$ *iff* they have the same rank mod 2, the same discriminant mod squares, the same total signature, and the same Hasse-Witt invariants (See Theorem I.2.2, p.16 in [C-P]). Moreover, two K-inner product spaces (V_1, β_1) and (V_2, β_2) are isometric *iff* they are in the same Witt class and have the same rank in $\mathbb{Z}$ (See Theorem I.2.1, p.11 in [C-P]).

A. The rank modulo 2

The first invariant of a K-inner product space (V, β) is the dimension $\dim_K V$ of V over K, called the *rank* of (V, β).

Definition 1.8. We define the *rank* of $\langle V, \beta \rangle$ to be the rank of any representative, modulo 2:

$$rk_2\langle V, \beta \rangle = \dim_K V \pmod 2 .$$

This is a Witt-class invariant, and produces a ring homomorphism

$$rk_2 \colon W(K) \to \mathbb{Z}/2\mathbb{Z}$$

$$\langle V, \beta \rangle \mapsto \dim_K V \pmod 2 .$$

Lemma 1.9. *For any field K, there is one and only one ideal I in $W(K)$ such that*

$$W(K)/I \cong \mathbb{Z}/2\mathbb{Z} .$$

Hence, we have the exact sequence

$$0 \to I \to W(K) \to \mathbb{Z}/2\mathbb{Z} \to 0 \ .$$

Proof. See Lemma 3.3, p.66 in [M-H]. □

In fact, the isomorphism will be $rk_2 \colon W(K)/I \cong \mathbb{Z}/2\mathbb{Z}$. The ideal $I = I(K)$ is called the *fundamental ideal* of $W(K)$, and consists of all Witt classes of even rank.

Remark 1.10. For the fundamental ideal I of $W(K)$, we have the following (see [M-H, p.66]):

(1) $\langle 1 \rangle \equiv \langle -1 \rangle \mod I$

(2) $\langle a \rangle \equiv \langle 1 \rangle \mod I$ for every $a \in K^*$

(3) I is additively generated by $\langle a, 1 \rangle$ for all $a \in K^*$.

B. The discriminant

Let B be the associated matrix of the n-dimensional K-inner product space (V, β) with respect to a fixed basis $e_1, \ldots, e_n$ for V over K:

$$B = \Big(\ \beta(e_i, e_j) \ \Big) \, .$$

Note that if two matrices A and B are congruent, say $A = T^t B T$, then we have

$$\det(A) = \det(T^t B T) = \det(T) \det(B) \det(T)$$

which is the same as $\det(B)$ up to squares, i.e.,

$$\det(A) = \det(T^t B T) \ \text{ in } K^*/K^{*2}$$

so that we can denote $\det(V) = \det(B)$ in K^*/K^{*2}.

Definition 1.11. The *discriminant* of $\langle V, \beta \rangle$ is defined to be

$$disc\langle V, \beta \rangle = (-1)^{\frac{n(n-1)}{2}} \det(V) \in K^*/K^{*2}$$

where n is the rank of V.

The factor $(-1)^{\frac{n(n-1)}{2}}$ is needed to insure that the discriminant is Witt-class invariant.

Lemma 1.12. *The restriction of the discriminant to the fundamental ideal I of $W(K)$ induces an isomorphism from I/I^2 to K^*/K^{*2}.*

Proof. See Theorem 5.2, p.76 in [M-H]. □

There are formulae which relate the discriminant to the algebraic operations on $W(K)$:

Remark 1.13. For any two Witt classes $X,\ Y \in W(K)$ with $e_1 = rk_2(X),\ e_2 = rk_2(Y) \in \mathbb{Z}/2\mathbb{Z}$. Then

(1) $disc(X+Y) = (-1)^{e_1 e_2} disc(X) disc(Y) \in K^*/K^{*2}$

(2) $disc(XY) = (disc\, X)^{e_2} (disc\, Y)^{e_1} \in K^*/K^{*2}$.

With these formulae we can define a ring structure on $\mathbb{Z}/2\mathbb{Z} \times K^*/K^{*2}$:

- Addition : $(e_1, x) + (e_2, y) = (e_1 + e_2, (-1)^{e_1 e_2} xy)$
- Multiplication : $(e_1, x)(e_2, y) = (e_1 e_2, x^{e_2} y^{e_1})$

so that these two invariants above can be combined to form a ring homomorphism

$$\begin{aligned} W(K) &\rightarrow \mathbb{Z}/2\mathbb{Z} \times K^*/K^{*2} \\ X &\mapsto (rk_2(X), discX). \end{aligned}$$

Then we have the following exact sequence

$$0 \to I^2 \to W(K) \to \mathbb{Z}/2\mathbb{Z} \times K^*/K^{*2} \to 0 \ .$$

Remark 1.14.

(1) The ideal $I^2 \subset W(K)$ is additively generated by the four dimensional Witt classes

$$\langle a, 1\rangle\langle b, 1\rangle = \langle ab, a, b, 1\rangle \ \ (a,\ b \in K^*)$$

each of which has trivial discriminant.

(2) $\langle a, b\rangle \equiv \langle -1, -ab\rangle \mod I^2$ and $\langle -1, -1, -1\rangle \equiv \langle 1\rangle \mod I^2$.

(3) For any Witt class $X \in I$, we have $X \equiv \langle discX, -1\rangle \mod I^2$.

C. The total signature

First, let us introduce the ordering of a field.

Definition 1.15. An *ordering* of a field F is a subset $P \subset F^*$ which is closed under addition and multiplication, and satisfies

$$P \cup (-P) = F^*.$$

The elements of P are called *positive*, and one writes $x > y$ if $x - y \in P$. A field F together with an ordering is called an *ordered field*.

Note that these two subsets P and $-P$ are necessarily disjoint and that, in an ordered field, every non-zero square is positive.

Lemma 1.16 (Artin-Schreier Theorem). *A field F possesses an ordering iff -1 is not a sum of squares in F.*

Proof. See Theorem 2.2, p.60 in [M-H] □

If F does not admit an ordering, then signatures are not defined. Suppose that F has at least one ordering. Then to each ordering of F we associate a signature to an F-inner product space (V, β), which is an invariant lying in $\mathbb{Z}$.

Definition 1.17. Let P be a fixed ordering of F and choose an orthogonal basis $e_1, \ldots, e_n$ for (V, β), that is, $\beta(e_i, e_j) = 0$ for $i \neq j$. Let n^+ be the number of the basis elements satisfying $\beta(e_i, e_i) > 0$. Then the *signature* of (V, β) for the ordering P is defined as

$$\mathrm{sgn}_P(V, \beta) = n^+ - (n - n^+) = 2n^+ - n \in \mathbb{Z}.$$

For a 1-dimensional inner product space $< a >$, the signature $\mathrm{sgn}_P < a >$ is just what usually called the *sign* of the field element $a \in F^*$ at the ordering P.

Now, an algebraic number field K might contain real infinite primes each of which corresponds to a specific real embedding of K, thus to an ordering of K, and hence to a signature of K. Thus there is a *total signature*

$$\mathrm{Sgn}\colon W(K) \to \mathbb{Z}^r$$

assigning to each Witt class X an r-tuple of integers, where r is the number of real infinite primes of K.

D. The Hasse-Witt invariants

First, recall that, in an algebraic number field K,

- a *finite prime* means a prime ideal in the ring $\mathcal{O}_K$ of algebraic integers of K,
- a *real infinite prime* means a real embedding of K,

- a *complex infinite prime* means a pair of complex conjugate embeddings of K.

At each prime of K, we have the Hasse-Witt invariant of a Witt class $\langle V, \beta \rangle$ defined in terms of the Hasse symbol of a representative inner product space.

Definition 1.18. Let $\mathfrak{p}$ be a prime of K, finite or infinite. Let $e_1, \ldots, e_n$ be an orthogonal basis for an inner product space (V, β) over K and set $d_i = \beta(e_i, e_i)$. The *Hasse symbol* of (V, β) at $\mathfrak{p}$ is defined by

$$\mathrm{c}_{\mathfrak{p}}(V, \beta) = \prod_{i<j} (d_i, d_j)_{\mathfrak{p}}$$

where $(d_i, d_j)_{\mathfrak{p}}$ is the *Hilbert symbol*, that is, for any c, $d \in K_{\mathfrak{p}}$,

$$(c, d)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } cx^2 + dy^2 \text{ represents 1 in the completion } K_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

If $\dim_K V = 1$, then we set $\mathrm{c}_{\mathfrak{p}}(V, \beta) = 1$.

Now we have to choose this representative appropriately to obtain an invariant of the entire Witt class:

- if $\langle V, \beta \rangle$ is a Witt class of a 1-dimensional inner product space, then we set $\mathrm{c}_{\mathfrak{p}} \langle V, \beta \rangle = 1$ for all primes $\mathfrak{p}$;

- otherwise, choose a representative (V, β) with $\dim_K V \equiv 0$ or $1 \pmod 8$, and let $\mathrm{c}_{\mathfrak{p}} \langle V, \beta \rangle$ be defined as the Hasse symbol of (V, β) at $\mathfrak{p}$.

1.3 The Symbols of K

We continue in the context of the previous section.

Let $G = G(K)$ be the set of all functions $f \colon \Omega \to \mathbb{Z}^*$ where $\Omega = \Omega(K)$ is the set of all primes $\mathfrak{p}$ of K, satisfying the following:

(1) $f(\mathfrak{p}) = 1$ for almost all primes,

(2) $f(\mathfrak{p}) = 1$ for all complex primes,

(3) $\prod_{\mathfrak{p}\in\Omega} f(\mathfrak{p}) = 1$ (called the *reciprocity law*).

For elements x, $y \in K^*/K^{*2}$ we denote by $[x, y] \in G$ the function which to each prime $\mathfrak{p} \in \Omega$ assigns the value $(x, y)_{\mathfrak{p}}$:

$$[x, y]\colon \mathfrak{p} \mapsto (x, y)_{\mathfrak{p}}.$$

This yields a symmetric bi-multiplicative pairing of $K^*/K^{*2} \times K^*/K^{*2}$ into G. The realization theorem for Hilbert symbols (see Theorem 10.1, p.43 in [C-H]) states that, for any $f \in G$, there is a pair x, $y \in K^*/K^{*2}$ for which

$$[x, y] = f.$$

Now, we define $\mathrm{c}\colon W(K) \to G$ by $\langle V, \beta\rangle \mapsto \mathrm{c}\langle V, \beta\rangle$ where $\mathrm{c}\langle V, \beta\rangle$ is the function assigning to each prime $\mathfrak{p}$ the value of the Hasse-Witt invariant $\mathrm{c}_{\mathfrak{p}}\langle V, \beta\rangle$ of the Witt class $\langle V, \beta\rangle \in W(K)$. It is a well-defined invariant which is called the *Hasse-Minkowski* invariant (see [Co, Lemma 1.4, p.123]). The relation of this invariant to the algebraic operations on $W(K)$ can be given as follows:

Lemma 1.19. *For any two Witt classes X, Y in $W(K)$ with $rk_2(X) = s$ and $rk_2(Y) = t$, we have*

(1) $\mathrm{c}(X + Y) = [(-1)^{st}, -discX\, discY][discX, discY]\mathrm{c}(X)\mathrm{c}(Y)$

(2) $\mathrm{c}(XY) = [discX, discY]^{st+1}\mathrm{c}(X)^t\mathrm{c}(Y)^s$.

Proof. See Lemma 1.5, p.123 in [Co]. □

Now, we introduce the *symbols* of K,

$$\mathrm{Symb}(K) = \mathbb{F}_2 \times K^*/K^{*2} \times G$$

which is a ring with the following algebraic properties:

- Addition:

$$(e_1, d_1, f_1) + (e_2, d_2, f_2) = (e_1 + e_2,\ (-1)^{e_1 e_2} d_1 d_2,\ [(-1)^{e_1 e_2}, -d_1 d_2][d_1, d_2] f_1 f_2)$$

- Multiplication:

$$(e_1, d_1, f_1) \cdot (e_2, d_2, f_2) = (e_1 e_2,\ d_1^{e_2} d_2^{e_1},\ [d_1, d_2]^{e_1 e_2 + 1} f_1^{e_2} f_2^{e_1})$$

- Additive identity: $(0, 1, \mathbf{1})$

- Multiplicative identity: $(1, 1, \mathbf{1})$

  where $\mathbf{1}$ is the trivial function in G.

Theorem 1.20. *For any algebraic number field K, the ring homomorphism $X \mapsto (rk_2(X), disc(X), \mathrm{c}(X))$ yields a short exact sequence*

$$0 \to I^3 \to W(K) \to \mathrm{Symb}(K) \to 0.$$

If K is totally complex, then $W(K) \cong \mathrm{Symb}(K)$.

Proof. See Theorem 1.8, p.127 in [Co]. □

2. The Integral Witt Ring $W(\mathcal{O}_K)$

2.1 The Integral Witt Ring $W(\mathcal{O}_K)$

Let K be an algebraic number field with its ring $\mathcal{O}_K$ of algebraic integers. We simply call K a number field and $\mathcal{O}_K$ the number ring of K. The definition of the integral Witt ring $W(\mathcal{O}_K)$ of K can be made entirely by analogy with the definition of $W(K)$.

Definition 2.1. An inner product space over $\mathcal{O}_K$ is a pair (X, β) in which X is a finitely generated projective $\mathcal{O}_K$-module and

$$\beta\colon X \times X \to \mathcal{O}_K$$

is a symmetric $\mathcal{O}_K$-bilinear form which is non-degenerate in the sense that the adjoint

$$\mathsf{Ad}_\beta\colon X \to \mathrm{Hom}_{\mathcal{O}_K}(X, \mathcal{O}_K)$$

$$x \;\mapsto\; \beta(\_, x)$$

is an isomorphism.

Definition 2.2. Two inner product spaces (X, β) and (X', β') over $\mathcal{O}_K$ are said to be *isometric* ($X \simeq X'$) if there is an $\mathcal{O}_K$-linear bijection

$$L\colon X \to X'$$

such that

$$\beta'(L(x), L(y)) = \beta(x, y) \quad \text{for all} \;\; x, y \in X\ .$$

We can define the addition and multiplication of inner product spaces over $\mathcal{O}_K$ via the *orthogonal sum* and the *tensor product* defined in Definition 1.3 on page 5.

Definition 2.3. An inner product space (X, β) over $\mathcal{O}_K$ is *split* (or *metabolic*) if there exists a submodule N of X such that N is a direct summand of X and $N = N^{\perp}$.

By abuse of notation we will use X for an inner product space (X, β), whenever there's no danger of confusion.

Definition 2.4. Two inner product spaces X_1 and X_2 over $\mathcal{O}_K$ are said to be *Witt equivalent* if there exist split inner product spaces N_1 and N_2 such that

$$X_1 \oplus N_1 \simeq X_2 \oplus N_2.$$

This is an equivalence relation. We call such an equivalence class a Witt class. And again, X denotes both the inner product space and the Witt class of the space. The context will always make it clear which is meant. The *integral Witt ring* $W(\mathcal{O}_K)$ of K is defined to be the collection of all Witt classes of inner produce spaces over $\mathcal{O}_K$.

2.2 The Knebusch Exact Sequence

Let K be a number field with its number ring $\mathcal{O}_K$. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the residue class field $\overline{K}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ is finite. For a fixed local uniformizer π of the prime ideal $\mathfrak{p}$, there is a homomorphism of additive groups

$$\partial_{\mathfrak{p}} \colon W(K) \to W(\overline{K}_{\mathfrak{p}})$$

$$\langle \pi^i u \rangle \mapsto \begin{cases} \langle u \rangle & \text{if } i \text{ is odd} \\ 0 & \text{if } i \text{ is even.} \end{cases}$$

It is well-defined additive homomorphism, and is called the *second residue homomorphism* [M-H, p.85]. Note that $\partial_{\mathfrak{p}}$ depends on the choice of the local uniformizer π. And the extension of scalars gives us the injective ring homomorphism $W(\mathcal{O}_K) \to W(K)$.

Since $\partial_{\mathfrak{p}}(X) = 0$ for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, we have an additive homomorphism

$$\partial\colon W(K) \to \bigoplus W(\overline{K}_{\mathfrak{p}})$$

where the direct sum extends over all non-zero prime ideals of $\mathcal{O}_K$. This homomorphism ∂ produces the *Knebusch exact sequence* [M-H, p.93, 3.3]

$$0 \longrightarrow W(\mathcal{O}_K) \longrightarrow W(K) \xrightarrow{\partial} \bigoplus W(\overline{K}_{\mathfrak{p}}).$$

Note that although each homomorphism $\partial_{\mathfrak{p}}$ depends on the choice of the local uniformizer at $\mathfrak{p}$, the kernel $\mathrm{Ker}\partial_{\mathfrak{p}}$ does not depend on that choice. Hence the kernel of the homomorphism ∂ does not depend on the choice of local uniformizers.

We can consider $W(\mathcal{O}_K)$ as the kernel of ∂, which enables us to use the classical theories of inner product spaces over a number field to determine the ring structure of $W(\mathcal{O}_K)$.

2.3 The Symbols of $\mathcal{O}_K$

Let K be a number field with its number ring $\mathcal{O}_K$. Let r_K be the number of real embeddings of K and c_K the number of pairs of complex conjugate embeddings of K. Recall that we have $[K\colon \mathbb{Q}] = r_K + 2c_K$.

We will introduce two elementary abelian 2-groups which will form the main framework of $\mathrm{Symb}(\mathcal{O}_K)$, the *symbols* of the number ring $\mathcal{O}_K$, together with $\mathbb{F}_2$. First let K_{ev} be the group of elements in K^* with even order at all prime ideals of $\mathcal{O}_K$, that is,

$$K_{ev} = \{d \in K^* \mid ord_{\mathfrak{p}}\, d \equiv 0 \pmod 2, \text{ for all prime ideals } \mathfrak{p} \subset \mathcal{O}_K\}\,.$$

Then we set the first elementary abelian 2-group E as

$$E = K_{ev}/K^{*2}.$$

We will write an element $\bar{d}$ of E where $d \in K_{ev}$ is a coset representative. Then

Lemma 2.5. *There is a natural short exact sequence*

$$1 \to \mathcal{O}_K^*/\mathcal{O}_K^{*2} \to E \to {}_2\mathcal{C}_K \to 1$$

and hence

$$2\text{-}rk E = 2\text{-}rk \mathcal{O}_K^*/\mathcal{O}_K^{*2} + 2\text{-}rk\, \mathcal{C}_K$$

where ${}_2\mathcal{C}_K \subset \mathcal{C}_K$ is the finite elementary abelian 2-group of all ideal classes with order ≤ 2.

Proof. If a unit in $\mathcal{O}_K$ is the square of an element in K^*, then it is the square of a unit in $\mathcal{O}_K$. For that reason there is an embedding

$$1 \to \mathcal{O}_K^*/\mathcal{O}_K^{*2} \to E.$$

Now let $\bar{d} \in E$, then $d \in K^*$ with $ord_{\mathfrak{p}}\, d \equiv 0 \pmod 2$ for all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$. Thus we can decompose the principal ideal (d) as

$$(d) = d\mathcal{O}_K = \prod_{i=1}^{s} \mathfrak{p}_i^{2e_i}$$

where each $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$ and each e_i is an integer. Putting $A = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$, we have $A^2 = (d)$, and hence the square of the ideal class of A is trivial in the ideal class group $\mathcal{C}_K$ of K. So, the ideal class of A is of order 1 or 2. Send d to the ideal class of A in ${}_2\mathcal{C}_K \subset \mathcal{C}_K$. If we also have $B^2 = (d)$ for some fractional $\mathcal{O}_K$-ideal B, then $(AB^{-1})^2 = (1) = \mathcal{O}_K$ so that A and B are in the same ideal class. If d is replaced by dd_1^2, then A is replaced by $d_1 A$. Thus we have a well-defined epimorphism

$$E \to {}_2\mathcal{C}_K \to 1.$$

Note that if $A^2 = (x)$ and $A = (y)$, then, for some unit $u \in \mathcal{O}_K^*$, we have

$$uy^2 = x. \quad \square$$

Since $2\text{-}rk(\mathcal{O}_K^*/\mathcal{O}_K^{*2}) = r_K + c_K$ for any number field K, we have $2\text{-}rkE = c_K + 2\text{-}rk\mathcal{C}_K$ if K is totally complex. .

Now, let $G_2 = G_2(K)$ be the multiplicative elementary abelian 2-group of all functions $f\colon \Omega_2 \to \mathbb{Z}^*$ for which

$$\prod_{D\in\Omega_2} f(D) = +1$$

where $\Omega_2 = \Omega_2(K)$ is the set of all dyadic prime ideals $D \subset \mathcal{O}_K$. Set $g_2(K) = \#\Omega_2$, the number of all dyadic prime ideals. Then $1 \le g_2(K) \le 2c_K$. And we have

$$2\text{-}rk\, G_2 = g_2(K) - 1$$

and hence G_2 is trivial if and only if $g_2(K) = 1$.

Lemma 2.6. *If $d,\ d_1 \in E$, then $(d, d_1)_{\mathfrak{p}} = +1$ for any non-dyadic prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.*

Proof. Fix a non-dyadic prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, and let $d,\ d_1 \in E$. Then since $ord_{\mathfrak{p}}d$ and $ord_{\mathfrak{p}}d_1$ are both even, we can write

$$d = u\pi_{\mathfrak{p}}^{2s}, \qquad d_1 = u_1\pi_{\mathfrak{p}}^{2t}$$

where $u,\ u_1$ are units at $\mathfrak{p}$, $\pi_{\mathfrak{p}}$ a local uniformizer for $\mathfrak{p}$, and $s,\ t$ integers. Thus,

$$(d, d_1)_{\mathfrak{p}} = (u\pi_{\mathfrak{p}}^{2s}, u_1\pi_{\mathfrak{p}}^{2t})_{\mathfrak{p}} = (u, u_1)_{\mathfrak{p}} = 1. \quad \square$$

Then, by Hilbert Reciprocity, we have

$$\prod_{D\in\Omega_2} (d, d_1)_D = +1 \quad \text{for } d,\ d_1 \in E.$$

So, to each pair $d,\ d_1 \in E$ we associate $[d, d_1] \in G_2$, the function which to each $D \in \Omega_2$ assigns the value $(d, d_1)_D = \pm 1$. Then, for $d,\ d_1 \in E$, the following are equivalent (see [C-H, p.41]):

(1) $[d, d_1] = \mathbf{1} \in G_2$ where $\mathbf{1}$ is the identity in G_2

(2) d_1 is a norm from $K(\sqrt{d})$ over K

(3) d is a norm from $K(\sqrt{d_1})$ over K.

We have two interesting subgroups of E. First, let R be the elementary abelian 2-group of all global square classes $d \in K^*/K^{*2}$ for which $K(\sqrt{d})$ is unramified over K:

$$R = \{d \in K^*/K^{*2} \mid K(\sqrt{d}) \text{ is unramified over } K\}.$$

Lemma 2.7. *Under the same notations above we have*

(1) $R \subset E$.

(2) $2\text{-}rk(R) = 2\text{-}rk(\mathcal{C}_K)$.

(3) If $d \in R$ *and* $d_1 \in E$, *then* $[d, d_1] = \mathbf{1} \in G_2$.

Proof. (1) Let $d \in R$, then $K(\sqrt{d})$ is unramified over K. Let $\mathfrak{p}$ be a finite prime of K. Suppose $ord_{\mathfrak{p}} d \equiv 1 \pmod 2$. Then, in $K_{\mathfrak{p}}$, we can write $d = u\pi^{2s}\pi$ where u is a local unit at $\mathfrak{p}$, π a local uniformizer for $\mathfrak{p}$. Then $\sqrt{d} = \pi^s\sqrt{u\pi}$ and hence $K_{\mathfrak{p}}(\sqrt{d}) = K_{\mathfrak{p}}(\sqrt{u\pi}) = K_{\mathfrak{p}}(\sqrt{\pi_1})$ where $\pi_1 = u\pi$ is another prime element in $K_{\mathfrak{p}}$. Setting $K_{\mathfrak{p}}(\sqrt{\pi_1}) = L$, we have $(\pi_1) = \pi_1\mathcal{O}_L = (\sqrt{\pi_1})^2$ in $\mathcal{O}_L$. Thus $\mathfrak{p}$ is ramified in $L = K_{\mathfrak{p}}(\sqrt{\pi_1})$ which is a contradiction. Hence, $ord_{\mathfrak{p}} d \equiv 0 \pmod 2$ for all finite primes of K. Therefore, $d \in E$.

(2) Class field theory gives us that, for the Hilbert class field $\mathcal{H}_K$ of K, which is the largest abelian unramified extension of K, the Galois group of $\mathcal{H}_K$ over K is isomorphic to the ideal class group $\mathcal{C}_K$ of K:

$$\mathrm{Gal}\,(\mathcal{H}_K/K) \cong \mathcal{C}_K.$$

Let $\mathcal{G} = \mathrm{Gal}\,(\mathcal{H}_K/K)$. then we have $\mathcal{G}/\mathcal{G}^2 \cong \mathcal{C}_K/\mathcal{C}_K^2$, and hence $2\text{-}rk(\mathcal{G}) = 2\text{-}rk(\mathcal{C}_K)$. Note that $\mathcal{G}/\mathcal{G}^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$, a direct sum of $2\text{-}rk(\mathcal{G})$ copies of $\mathbb{Z}/2\mathbb{Z}$, and that to each $\mathbb{Z}/2\mathbb{Z}$ corresponds distinct quadratic extension $K(\sqrt{d})$ of K as a fixed field of each $\mathbb{Z}/2\mathbb{Z}$. Since each of these quadratic extensions is a subfield of the Hilbert class field $\mathcal{H}_K$ which is the largest unramified extension of K, each $K(\sqrt{d})$ must be unramified, and these are all the unramified quadratic extensions of K. Thus we have $2\text{-}rk(R) = 2\text{-}rk(\mathcal{G}) = 2\text{-}rk(\mathcal{C}_K)$.

(3) For $d \in R$ and $d_1 \in E$, it is enough to show that d_1 is a local norm from $K_{\mathfrak{p}}(\sqrt{d})$ for a fixed finite prime $\mathfrak{p}$ of K. Since $K(\sqrt{d})$ is unramified over K, $\mathfrak{p}$ remains prime in $K_{\mathfrak{p}}(\sqrt{d})$. Write $\mathfrak{p} = \mathfrak{P}$ in $K_{\mathfrak{p}}(\sqrt{d})$. Since $ord_{\mathfrak{p}} d_1$ is even, we can write $d_1 = u\pi^{2s}$ where u is a local unit at $\mathfrak{p}$, π a local uniformizer for $\mathfrak{p}$. Since $\mathfrak{p} = (\pi)$ remains prime in $K_{\mathfrak{p}}(\sqrt{d})$, π^{2s} is a norm from $K_{\mathfrak{p}}(\sqrt{d})$. Note that a unit u at $\mathfrak{p}$ is a norm of a unit at $\mathfrak{P}$. Therefore, d_1 is a norm from $K_{\mathfrak{p}}(\sqrt{d})$. □

However, it is conceivable that $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap R \subset E$ can be non-trivial.

We introduce another subgroup of E. We define $\Delta \subset E$ to be the subgroup of E such that

$$\Delta = \{d \in E \mid [d, d_1] = \mathbf{1} \in G_2,\ \forall\, d_1 \in E\}\ .$$

By Lemma 2.7 we have $R \subset \Delta \subset E$ and hence we have

$$2\text{-}rk\, R = 2\text{-}rk\, \mathcal{C}_K \leqslant 2\text{-}rk\, \Delta \leqslant 2\text{-}rk\, E\ .$$

We are particularly interested in the quotient E/Δ noting

$$0 \leqslant 2\text{-}rk(E/\Delta) \leqslant c_K\ .$$

If $g_2(K) = 1$, then G_2 is trivial and $\Delta = E$. We will discuss the example with $\Delta = E$ in Chapter 4 and the example with $\Delta = R$ in Chapter 6.

Now, we always have $-1 \in E$. Consider the quotient homomorphism $\nu\colon E \to E/\Delta$. Let us define

$$\gamma = \nu(-1) \in E/\Delta.$$

Remark 2.8.

(1) Obviously, $\gamma = e \in E/\Delta \iff -1 \in \Delta$ where $e \in E/\Delta$ is the identity.

(2) For every $d \in E$, we have $[d, d] = [-1, d] \in G_2$.

Then we have the following.

Lemma 2.9. *The element $\gamma \in E/\Delta$ is trivial iff every non-trivial element of E has pythagoras number 2. In that case, $levelK = 1$ or 2, and γ is always trivial if $levelK = 1$.*

Proof. From Remark 2.8 we have

$$\gamma = e \in E/\Delta \Leftrightarrow [d, d] = [-1, d] = \mathbf{1} \in G_2$$

if and only if d is a norm from $K(\sqrt{-1})$ over K, that is,

$$d = (x + y\sqrt{-1})(x - y\sqrt{-1}) = x^2 + y^2$$

for some $x,\ y \in K$.

If $levelK = 4$, then $-1 \in E$ is a sum of four non-zero squares in K. And if $levelK = 1$, then $-1 \in E$ is a square in K and hence $[-1, d] = \mathbf{1}$ which implies that γ is trivial. □

By analogy with $\mathrm{Symb}(K)$, we introduce the ring

$$\mathrm{Symb}(\mathcal{O}_K) = \mathbb{F}_2 \times E \times G_2$$

with the same algebraic properties on page 14.

2.4 The Symbols and the Integral Witt Ring

From Section 2.2, the integral Witt ring $W(\mathcal{O}_K)$ can be regarded as the kernel of ∂ in the Knebusch exact sequence

$$0 \to W(\mathcal{O}_K) \to W(K) \xrightarrow{\partial} \bigoplus_{\mathfrak{p}} W(\mathcal{O}_K/\mathfrak{p}).$$

We will begin with the description of the image of $\partial_\mathfrak{p}$ for each prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.

Lemma 2.10. *For $X \in W(K)$, put $t = ord_\mathfrak{p} disc\, X$. Then*

$$\partial_\mathfrak{p}(X) = t \quad in\ \mathbb{Z}/2\mathbb{Z} \cong W(\mathcal{O}_K/\mathfrak{p})$$

if $\mathfrak{p}$ is dyadic. If $\mathfrak{p}$ is non-dyadic, then

$$\partial_\mathfrak{p}(X) = (t, (\pi_\mathfrak{p}, -disc\, X)_\mathfrak{p}^t \mathrm{c}_\mathfrak{p}(X)) \quad in\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^* \cong W(\mathcal{O}_K/\mathfrak{p})$$

where $\pi_\mathfrak{p}$ is the local uniformizer at $\mathfrak{p}$.

Proof. See Theorem II.4.2, p.82 in [C-P]. □

Thus, if $X \in W(K)$ is in the kernel of $\partial_\mathfrak{p}$, then $ord_\mathfrak{p} disc\, X = 0$ at all prime ideals, and $(\pi_\mathfrak{p}, -disc\, X)_\mathfrak{p}^t \mathrm{c}_\mathfrak{p}(X) = 1$ at all non-dyadic prime ideals. Since $t = ord_\mathfrak{p} disc\, X$ is even at all prime ideals, we have $(\pi_\mathfrak{p}, -disc\, X)_\mathfrak{p}^t = 1$. Thus we have $\mathrm{c}_\mathfrak{p}(X) = 1$ at all non-dyadic prime ideals. Then regarding $W(\mathcal{O}_K)$ as the kernel of ∂ we can characterize $W(\mathcal{O}_K)$.

Characterization 2.11. Let $X \in W(K)$. Then

$$X \in W(\mathcal{O}_K) \Leftrightarrow \begin{cases} ord_\mathfrak{p}(disc X) \equiv 0 \pmod 2 \text{ at all prime ideals } \mathfrak{p} \subset \mathcal{O}_K \\ \mathrm{c}_\mathfrak{p}(X) = +1 \text{ at all non-dyadic prime ideals } \mathfrak{p} \subset \mathcal{O}_K \end{cases}$$

Since, if $X \in W(\mathcal{O}_K)$, then $\mathrm{c}_\mathfrak{p}(X) = +1$ at all non-dyadic prime ideals $\mathfrak{p} \subset \mathcal{O}_K$, we have

$$\prod_{D \in \Omega_2} \mathrm{c}_D(X) = +1.$$

So, for $X \in W(\mathcal{O}_K)$, the Hasse-Minkowski invariant $\mathrm{c}(X) \in G_2$ will assign each $D \in \Omega_2$ the value $\mathrm{c}_D(X) = \pm 1$.

For the rest of this dissertation, we will restrict attention to the totally complex number field K.

Proposition 2.12. *If K is a totally complex number field, then there is a canonical ring-isomorphism*

$$\Phi \colon W(\mathcal{O}_K) \cong \mathrm{Symb}(\mathcal{O}_K) = \mathbb{F}_2 \times E \times G$$

given by

$$X \mapsto (rk_2(X), discX, \mathrm{c}(X)).$$

Proof. From Theorem 1.20 we have $W(K) \cong \mathrm{Symb}(K)$ if K is totally complex. Then Characterization 2.11 tells us that Φ is a well-defined ring epimorphism. Now, for $X \in W(\mathcal{O}_K)$, if $\Phi(X)$ is trivial in $\mathrm{Symb}(\mathcal{O}_K)$, then it is trivial in $\mathrm{Symb}(K)$. So, X must be trivial in $W(K)$. Thus X is trivial in $W(\mathcal{O}_K)$ and hence ϕ is injective. □

The immediate corollary is

Corollary 2.13. *For a totally complex number field K,*
the Witt ring $W(\mathcal{O}_K)$ is finite with order

$$\#W(\mathcal{O}_K) = 2^{c_K + g_2(K) + 2\text{-}rk\, \mathcal{C}_K}.$$

Proof. In Section 2.3, we have

$$2\text{-}rk\, E = c_K + 2\text{-}rk\, \mathcal{C}_K \text{ and } 2\text{-}rk\, G_2 = g_2(K) - 1.$$

Clearly, $2\text{-}rk\, \mathbb{F}_2 = 1$. By Proposition 2.12, we get the order of $W(\mathcal{O}_K)$. □

Next we may ask for the $2\text{-}rk(W(\mathcal{O}_K),+)$ and the $4\text{-}rk(W(\mathcal{O}_K),+)$.

Let us introduce the homomorphism

$$\eta\colon E \to G_2$$

given by $\eta(d) = [-1, d]$ for all $d \in E$. Note that the kernel of η is the subgroup of elements in E with pythagoras number at most 2.

Proposition 2.14. *Let K be a totally complex number field.*

(1) If $levelK = 1$ then

$(W(\mathcal{O}_K),+)$ *is an elementary abelian 2-group with 2-rank*

$$2\text{-}rk(W(\mathcal{O}_K),+) = c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K.$$

(2) If $levelK = 2$ then

$$2\text{-}rk(W(\mathcal{O}_K),+) = g_2(K) - 1 + 2\text{-}rk(\mathrm{Ker}(\eta))$$
$$4\text{-}rk(W(\mathcal{O}_K),+) = 2\text{-}rk(\mathrm{Im}(\eta)) + 1.$$

(3) If $levelK = 4$ then

$$2\text{-}rk(W(\mathcal{O}_K),+) = g_2(K) - 1 + 2\text{-}rk(\mathrm{Ker}(\eta))$$
$$4\text{-}rk(W(\mathcal{O}_K),+) = 2\text{-}rk(\mathrm{Im}(\eta)) > 0$$
$$8\text{-}rk(W(\mathcal{O}_K),+) = 1.$$

Proof. Note that a Witt class $X \in W(\mathcal{O}_K)$ corresponds to an element (e, d, f) in $\mathrm{Symb}(\mathcal{O}_K)$ under $W(\mathcal{O}_K) \cong \mathrm{Symb}(\mathcal{O}_K)$. And it is easy to calculate that

$$(\dagger)\begin{cases} 2(e,d,f) = (0, (-1)^{e^2}, [(-1)^{e^2}, -1][d,d]) = (0, (-1)^{e^2}, [(-1)^{e^2}, -1][-1,d]) \\ 4(e,d,f) = (0, 1, [(-1)^{e^2}, (-1)^{e^2}]) = (0, 1, [-1, (-1)^{e^2}]) \\ 8(e,d,f) = (0, 1, \mathbf{1}) \end{cases}$$

(1) If $levelK = 1$, then $\langle 1_K \rangle \in W(\mathcal{O}_K)$ has additive order 2. Thus every element in $W(\mathcal{O}_K)$ is at most 2-torsion. Therefore,

$$2\text{-}rk(W(\mathcal{O}_K), +) = c_K + g_2(K) + 2\text{-}rk\, \mathcal{C}_K.$$

(2) If $levelK = 2$, then $\langle 1_K \rangle \in W(\mathcal{O}_K)$ has additive order 4. Thus every element in $W(\mathcal{O}_K)$ is at most 4-torsion. Since, from (†), any 2-torsion element in $\mathrm{Symb}(\mathcal{O}_K)$ is of the form $(0, d, f)$ with $d \in \mathrm{Ker}(\eta)$, we have

$$2\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk\, G_2 + 2\text{-}rk(\mathrm{Ker}(\eta)) = g_2(K) - 1 + 2\text{-}rk(\mathrm{Ker}(\eta)).$$

Noting that $2\text{-}rk\, E = 2\text{-}rk(\mathrm{Ker}(\eta)) + 2\text{-}rk(\mathrm{Im}(\eta))$ and that $\#W(\mathcal{O}_K) = 2^{g_2(K)+2\text{-}rk\, E}$, we have

$$4\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk(\mathrm{Im}(\eta)) + 1.$$

(3) If $levelK = 4$, then $\langle 1_K \rangle \in W(\mathcal{O}_K)$ has additive order 8. Thus every element in $W(\mathcal{O}_K)$ is at most 8-torsion. With the same argument as in (2), we have

$$2\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk\, G_2 + 2\text{-}rk(\mathrm{Ker}(\eta)) = g_2(K) - 1 + 2\text{-}rk(\mathrm{Ker}(\eta)).$$

Again, from (†), any 4-torsion element in $\mathrm{Symb}(\mathcal{O}_K)$ is of the form $(0, d, f)$ whose number is $2^{2\text{-}rk\, G + 2\text{-}rk\, E}$. Noting that the number of 4-torsion elements of a 2-group H is equal to $2^{2\text{-}rk\, H + 4\text{-}rk\, H}$, we have

$$\begin{aligned} & 2\text{-}rk(W(\mathcal{O}_K), +) + 4\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk\, G_2 + 2\text{-}rk\, E \\ \Rightarrow \quad & 4\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk\, G_2 + 2\text{-}rk\, E - 2\text{-}rk(W(\mathcal{O}_K), +) \\ \Rightarrow \quad & 4\text{-}rk(W(\mathcal{O}_K), +) = 2\text{-}rk(\mathrm{Im}(\eta)) \end{aligned}$$

and

$$8\text{-}rk(W(\mathcal{O}_K), +) = 1.$$

Note that, from Lemma 2.9, only when $levelK = 1, 2$, we have $[-1, d] = \mathbf{1}$ for all $d \in E$. So $\mathrm{Im}(\eta)$ is not trivial in this case. Thus $2\text{-}rk(\mathrm{Im}(\eta)) > 0$. □

2.5 The Ideals of the Integral Witt Ring

Assume that K is totally complex. Let $\mathfrak{M} = I \cap W(\mathcal{O}_K) \subset W(\mathcal{O}_K)$, the ideal of all Witt classes $X \in W(\mathcal{O}_K)$ with $rk_2(X) = 0$, that is,

$$\mathfrak{M} = \{X \in W(\mathcal{O}_K) \mid rk_2(X) = 0\}.$$

Remark 2.15.

(1) $\mathfrak{M}$ corresponds to $\{0\} \times E \times G_2$ under $W(\mathcal{O}_K) \cong \mathrm{Symb}(\mathcal{O}_K)$.

(2) Using the fact that $I^3 = \{0\}$ since K is totally complex, we see $X^3 = 0$ for every $X \in \mathfrak{M}$.

Proposition 2.16. *Let K be a totally complex number field.*

(1) If $X \in W(\mathcal{O}_K)$, then

$$X \text{ is a unit in } W(\mathcal{O}_K) \text{ iff } rk_2(X) \equiv 1 \pmod 2 .$$

(2) $W(\mathcal{O}_K)$ is a local ring whose unique maximal ideal is $\mathfrak{M} = I \cap W(\mathcal{O}_K)$.

Proof. Since $W(\mathcal{O}_K) \cong \mathrm{Symb}(\mathcal{O}_K)$, X is a unit in $W(\mathcal{O}_K)$ *iff* the image of X in $\mathrm{Symb}(\mathcal{O}_K)$ is a unit. Note that we have $(1, d, f)(1, d, f) = (1, 1, \mathbf{1})$ for $(1, d, f) \in \mathrm{Symb}(\mathcal{O}_K)$, and $(0, d_1, f_1)(e, d, f) \neq (1, 1, \mathbf{1})$ for $(0, d_1, f_1)$, $(e, d, f) \in \mathrm{Symb}(\mathcal{O}_K)$. Hence units in $\mathrm{Symb}(\mathcal{O}_K)$ are of the form $(1, d, f)$ with $d \in E$ and $f \in G_2$. Therefore, X is a unit in $W(\mathcal{O}_K)$ *iff* $rk_2(X) \equiv 1 \pmod 2$. Hence $\mathfrak{M}$ contains all non-units in $W(\mathcal{O}_K)$ which implies (2). □

Before we discuss $\mathfrak{M}^2$, let us look at the ideal $I^2 \cap W(\mathcal{O}_K)$ of $W(\mathcal{O}_K)$.

Remark 2.17.

(1) If $X \in W(\mathcal{O}_K)$, then

$$X \in I^2 \cap W(\mathcal{O}_K) \text{ iff } rk_2(X) \equiv 0 \pmod 2 \text{ and } discX = 1 \in E\ .$$

(2) Thus, $I^2 \cap W(\mathcal{O}_K)$ corresponds to $\{0\} \times \{1\} \times G_2 \subset \mathrm{Symb}(\mathcal{O}_K)$.

(3) Simply, we can see

$$(I^2 \cap W(\mathcal{O}_K), +) \cong (G_2, \cdot) \quad \text{by} \quad X \mapsto \mathrm{c}(X).$$

(4) For $X \in I^2 \cap W(\mathcal{O}_K)$, we have $2X = 0$, and $YX = 0$ for all $Y \in \mathfrak{M}$.

Since we have $4\langle 1_K\rangle = 2^2\langle 1_K\rangle \in I^2 \cap W(\mathcal{O}_K)$, $rk_2(2^2\langle 1_K\rangle) \equiv 0 \pmod 2$, and $disc(2^2\langle 1_K\rangle) = 2^2 = 1$ in E, we may note $4X = 0$ for all $X \in \mathfrak{M}$.

However, while $\mathfrak{M}^2 \subset I^2 \cap W(\mathcal{O}_K)$, we do not claim an equality.

Lemma 2.18.

(1) $(\mathfrak{M}^2, +)$ is isomorphic to a multiplicative subgroup of $(G_2, \cdot)$.

(2) In particular, $\mathfrak{M}^2 = \{0\} \Leftrightarrow \Delta = E$.

(3) If K is a totally complex field with $g_2(K) = 1$, then $\mathfrak{M}^2 = \{0\} = I^2 \cap W(\mathcal{O}_K)$.

Proof. (1) Note that the ideal $\mathfrak{M}^2$ is additively generated by all products XY with $X,\ Y \in \mathfrak{M}$. For $X,\ Y \in \mathfrak{M}$, we can write

$$X = \langle discX, -1\rangle + X_1, \quad Y = \langle discY, -1\rangle + Y_1,$$

where $X_1,\ \ Y_1 \in I^2 \cap W(\mathcal{O}_K)$. Then we have $\mathrm{c}(X) = \mathrm{c}(X_1),\ \mathrm{c}(Y) = \mathrm{c}(Y_1)$, and $\mathrm{c}\langle discX, -1\rangle = \mathrm{c}\langle discY, -1\rangle = \mathbf{1} \in G_2$. Thus we have

$$XY = \langle discX, -1\rangle\langle discY, -1\rangle \in \mathfrak{M}^2$$

with

$$\mathrm{c}(XY) = [discX, discY] \in G_2.$$

Hence $(\mathfrak{M}^2, +)$ is isomorphic to a multiplicative subgroup of $(G_2, \cdot)$.

(2) $\mathfrak{M}^2 = \{0\} \Leftrightarrow [d, d_1] = \mathbf{1} \in G_2 \ \ \forall\, d, d_1 \in E$. Then, by the definition, $\Delta = E$.

(3) If K is totally complex and $g_2(K) = 1$, then $G_2 = \{\mathbf{1}\}$. □

Lemma 2.19. *For $X \in \mathfrak{M}$, we have*

$$X^2 = 2X = 2\langle discX, -1\rangle = \langle discX, -1\rangle^2.$$

Proof. First note $X^2 = 2X \ \Leftrightarrow \ X^2 - 2X = 0 \ \Leftrightarrow \ X(X - 2\langle 1\rangle) = 0$. We want to show more generally that $X(X - 2\langle 1\rangle) = 0$ for $X \in I \subset W(K)$. Let $X = \langle a_1, \ldots a_{2t}\rangle \in I$. Then

$$\begin{aligned} X(X - 2\langle 1\rangle) &= \sum_{i=1}^{2t} \langle a_i^2\rangle + \sum_{i\neq j} \langle a_i a_j, a_i a_j\rangle + \sum_{i=1}^{2t} \langle -a_i, -a_i\rangle \\ &= 2t\langle 1\rangle + t(2t-1)\langle 1,1\rangle + 2t\langle 1,1\rangle \\ &= 2(t^2+t)\langle 1,1\rangle \\ &= (t^2+t)\langle 1,1\rangle + (t^2+t)\langle -1,-1\rangle = (t^2+t)\mathbb{H} \end{aligned}$$

which is 0 in $W(K)$. □

Recall the subgroup $\Delta = \{d \in E \mid [d, d_1] = \mathbf{1} \in G_2, \ \forall\, d_1 \in E\} \subset E$. Now we define $J \subset W(\mathcal{O}_K)$ to be the set of all $X \in W(\mathcal{O}_K)$ with

$$rk_2(X) = 0 \quad \text{and} \quad discX \in \Delta \subset E\ .$$

The ideal J can be identified with an intersection of ideals of $W(\mathcal{O}_K)$.

Lemma 2.20. *If K be totally complex, then*

$$J = \bigcap_{X \in \mathfrak{M}} \mathrm{Ann}(X).$$

Proof. Consider the annihilator for $X \in W(\mathcal{O}_K)$.

$$\mathrm{Ann}(X) = \{Y \in W(\mathcal{O}_K) \mid XY = 0\}$$

If $rk_2(X) = 1$, then X is a unit in $W(\mathcal{O}_K)$, and hence $\mathrm{Ann}(X) = \{0\}$. But, if $0 \neq X \in \mathfrak{M}$, then $\mathrm{Ann}(X) \subset \mathfrak{M}$, and, for $Y \in \mathfrak{M}$, we have

$$XY = 0 \;\Leftrightarrow\; \mathrm{c}(XY) = [discX, discY] = \mathbf{1} \in G. \quad \square$$

Remark 2.21.

(1) J is an ideal in $W(\mathcal{O}_K)$ with

$$\mathfrak{M}^2 \subset I^2 \cap W(\mathcal{O}_K) \subset J \subset \mathfrak{M} \subset W(\mathcal{O}_K)$$

(2) For $X \in J$, we have $2X = X^2 = 0$, and $XY = 0$ for all $Y \in \mathfrak{M}$.
So, products of elements in J are all trivial.

(3) Thus J corresponds to $\{0\} \times \Delta \times G_2 \subset \mathrm{Symb}(\mathcal{O}_K)$, and $(J, +)$ is elementary abelian with 2-rank

$$_2\text{-}rk(J, +) = {}_2\text{-}rk\,\Delta + g_2(K) - 1.$$

Now, we restrict the discriminant to $\mathfrak{M}$:

$$disc\colon (\mathfrak{M}, +) \to (E, \cdot)$$

$$X \mapsto discX.$$

Noticing $\mathrm{Ker}(disc) = \{X \in \mathfrak{M} \mid discX = 1\} = I^2 \cap W(\mathcal{O}_K)$, the discriminant induces an isomorphism

$$(\mathfrak{M}/I^2 \cap W(\mathcal{O}_K), +) \cong (E, \cdot).$$

Combined with the quotient homomorphism $\nu\colon E \to E/\Delta$, the discriminant also induces

$$(\mathfrak{M}/J, +) \cong (E/\Delta, \cdot)$$

via the composition

$$(\mathfrak{M}, +) \overset{disc}{\to} (E, \cdot) \overset{\nu}{\to} (E/\Delta, \cdot)$$

$$X \mapsto discX \mapsto discX\Delta$$

$$\text{with} \quad \mathrm{Ker}(\nu \circ disc) = \{X \in \mathfrak{M} \mid discX \in \Delta\} = J.$$

Thus we have a short exact sequence

$$0 \to J \to \mathfrak{M} \to E/\Delta \to 1.$$

Note that, for $X,\ Y \in \mathfrak{M}$, we actually have $XY \in I^2 \cap W(\mathcal{O}_K) \subset J$. To use this exact sequence let us define the following function first.

Definition 2.22. Define

$$\phi\colon E/\Delta \times E/\Delta \to J$$

by

$$\phi(\alpha, \beta) = \langle a, -1\rangle\langle b, -1\rangle \in \mathfrak{M}^2 \subset J$$

where $a,\ b \in E$ are chosen so that $\nu(a) = \alpha,\ \ \nu(b) = \beta$.

To check if ϕ is well-defined we need to show that

$$\langle a, -1\rangle\langle b, -1\rangle = \langle a_1, -1\rangle\langle b_1, -1\rangle$$

for the chosen $a,\ a_1\ , b,\ b_1 \in E$ so that

$$\nu(a) = \alpha = \nu(a_1),\ \ \nu(b) = \beta = \nu(b_1)$$

with $\alpha,\ \beta \in E/\Delta$. Let $X = \langle a, -1\rangle\langle b, -1\rangle$ and $Y = \langle a_1, -1\rangle\langle b_1, -1\rangle$. It is clear that X and Y have the same rank modulo 2 and discriminant. So we only need to

show that $c_D(X) = c_D(Y)$ for a dyadic prime ideal D. Since aa_1^{-1} and $bb_1^{-1} \in \Delta$, we have

$$[aa_1^{-1}, d] = \mathbf{1} \text{ and } [bb_1^{-1}, d] = \mathbf{1} \ \forall\, d \in E,$$

that is, for any dyadic prime ideal $D \in \mathcal{O}_K$, we have

$$(a, d)_D = (a_1, d)_D, \quad (b, d)_D = (b_1, d)_D \ \forall\, d \in E.$$

Now, by adding $2\langle 1, -1\rangle$ to both X and Y, we have

$$\begin{aligned} c_D(X) &= (a, b)_D(a, a)_D(b, b)_D(-1, -1)_D, \\ c_D(Y) &= (a_1, b_1)_D(a_1, a_1)_D(b_1, b_1)_D(-1, -1)_D. \end{aligned}$$

And $(a_1, b_1)_D = (a_1, b)_D = (a, b)_D$. Similarly, we have $(a, a)_D = (a_1, a_1)_D$, $(b, b)_D = (b_1, b_1)_D$. Thus ϕ is well-defined.

Remark 2.23. Let $\alpha,\ \beta \in E/\Delta$ with $\nu(a) = \alpha,\ \nu(b) = \beta$. Then

(1) $[\alpha, \beta] = [a, b] \in G_2$ also well-defined with

$$c(\phi(\alpha, \beta)) = [a, b] = [\alpha, \beta] \in G_2.$$

(2) $\phi(\alpha, \beta) = \phi(\beta, \alpha)$ and $\phi(\alpha\alpha_1, \beta) = \phi(\alpha, \beta) + \phi(\alpha_1, \beta)$.

(3) If $\alpha \in E/\Delta$ is fixed, then

$$\phi(\alpha, \beta) = 0 \ \text{(i.e., } [\alpha, \beta] = \mathbf{1} \in G_2) \ \ \forall\, \beta \in E/\Delta \iff \alpha = e \in E/\Delta\ .$$

We define addition and multiplication on $E/\Delta \times J$ by

- Addition: $(\alpha, X) \dotplus (\beta, Y) = (\alpha\beta,\ \phi(\alpha, \beta) + X + Y)$
- Multiplication: $(\alpha, X) \divideontimes (\beta, Y) = (e,\ \phi(\alpha, \beta))$

so that we can identify it with $(\mathfrak{M}, +, \cdot)$.

Lemma 2.24. *Let K be a totally complex number field.*

(1) To each homomorphism $\chi\colon E/\Delta \to E$ with $\nu\chi(\alpha) \equiv \alpha$ $(\alpha \in E/\Delta)$, there is an associated isomorphism

$$\tau\colon (E/\Delta \times J, \dotplus, \divideontimes) \cong (\mathfrak{M}, +, \cdot)\ .$$

(2) If $-1 \in \Delta$, then $2\langle 1_K\rangle \in J$ and $(e, 2\langle 1_K\rangle)$ corresponds to $2\langle 1_K\rangle \in \mathfrak{M}$.

(3) If $-1 \notin \Delta$ and $\chi(\gamma) = -1 \in E$, then $4\langle 1_K\rangle \in J$ and $(\gamma, 4\langle 1_K\rangle)$ corresponds to $2\langle 1_K\rangle \in \mathfrak{M}$.

Proof. (1) Since E and E/Δ are elementary abelian 2-groups, we may choose a homomorphism

$$\chi\colon E/\Delta \to E$$

so that

$$\nu\chi(\alpha) = \alpha \quad \forall\ \alpha \in E/\Delta\ .$$

Then we define $\tau\colon (E/\Delta \times J, \dotplus, \divideontimes) \to (\mathfrak{M}, +, \cdot)$ by

$$(\alpha, X) \mapsto \langle \chi(\alpha), -1\rangle + X \in \mathfrak{M}.$$

We claim that τ is a ring monomorphism.

(i) τ preserves addition and multiplication:

Let $(\alpha, X),\ (\beta, Y) \in E/\Delta \times J$. Note that we have

$$\phi(\alpha, \beta) = \langle \chi(\alpha), -1\rangle\langle \chi(\beta), -1\rangle$$

since $\chi(\alpha)$ and $\chi(\beta)$ can be representatives of α and β, respectively. Then, for addition, we have

$$\begin{aligned} \tau(\alpha, X) + \tau(\beta, Y) &= \langle \chi(\alpha), -1\rangle + X + \langle \chi(\beta), -1\rangle + Y \\ &= \langle \chi(\alpha), -1\rangle + \langle \chi(\beta), -1\rangle + X + Y \end{aligned}$$

while

$$\begin{aligned}\tau(\alpha\beta,\ \phi(\alpha,\beta)+X+Y) &= \langle\chi(\alpha\beta),-1\rangle+\phi(\alpha,\beta)+X+Y\\ &= \langle\chi(\alpha)\chi(\beta),-1\rangle+\langle\chi(\alpha),-1\rangle\langle\chi(\beta),-1\rangle+X+Y\\ &= \langle\chi(\alpha)\chi(\beta),\chi(\alpha)\chi(\beta),-\chi(\alpha),-\chi(\beta),1,-1\rangle+X+Y\\ &= \langle 1,1,-\chi(\alpha),-\chi(\beta)\rangle+X+Y\\ &= \langle-\chi(\alpha),1\rangle+\langle-\chi(\beta),1\rangle+X+Y.\end{aligned}$$

For multiplication, we have

$$\begin{aligned}\tau(\alpha,X)\tau(\beta,Y) &= (\langle\chi(\alpha),-1\rangle+X)(\langle\chi(\beta),-1\rangle+Y)\\ &= \langle\chi(\alpha)\chi(\beta),-\chi(\alpha),-\chi(\beta),1\rangle\\ &\quad +\langle\chi(\alpha),-1\rangle Y+\langle\chi(\beta),-1\rangle X+XY\\ &= \langle\chi(\alpha)\chi(\beta),-\chi(\alpha),-\chi(\beta),1\rangle\end{aligned}$$

while

$$\begin{aligned}\tau(e,\ \phi(\alpha,\beta)) &= \langle\chi(e),-1\rangle+\phi(\alpha,\beta)\\ &= \langle 1,-1\rangle+\langle\chi(\alpha),-1\rangle\langle\chi(\beta),-1\rangle\\ &= \langle\chi(\alpha)\chi(\beta),-\chi(\alpha),-\chi(\beta),1\rangle.\end{aligned}$$

Thus τ preserves addition and multiplication.

(ii) τ is injective:

If $\langle\chi(\alpha),-1\rangle+X=0\in\mathfrak{M}$, then, since $X\in J$, we see $\langle\chi(\alpha),-1\rangle)\in J$. But $disc\langle\chi(\alpha),-1\rangle=\chi(\alpha)\in\Delta$. Thus $\alpha=\nu\chi(\alpha)=e\in E/\Delta$. Clearly $\chi(e)=1\in E$, so $\langle\chi(\alpha),-1\rangle=\langle\chi(e),-1\rangle=0$. Thus $X=0$, too.

Since $\#(E/\Delta\times J)=\#\mathfrak{M}$, we conclude

$$(E/\Delta\times J,\dashv,\ltimes)\cong(\mathfrak{M},+,\cdot)\ .$$

To show (2) and (3) we recall $\gamma = \nu(-1) \in E/\Delta$.

(2) If $\gamma = e \in E/\Delta$, then $-1 \in \Delta$ and $2\langle 1_K\rangle \in J$ since $disc 2\langle 1_K\rangle = -1$. Thus, for any $\chi\colon E/\Delta \to E$, we have $\chi(\gamma) = \chi(e) = 1 \in E$, and hence

$$\tau(e, 2\langle 1_K\rangle) = \langle \chi(e), -1\rangle + 2\langle 1_K\rangle = \langle 1, -1\rangle + 2\langle 1_K\rangle = 2\langle 1_K\rangle \in \mathfrak{M}.$$

(3) If $\gamma \neq e$, we can choose the $\chi\colon E/\Delta \to E$ so that $\chi(\gamma) = -1 \in E$. Surely, $4\langle 1_K\rangle \in J$. Then we have

$$\tau(\gamma, 4\langle 1_K\rangle) = \langle \chi(\gamma), -1\rangle + 4\langle 1_K\rangle = \langle -1, -1\rangle + 4\langle 1_K\rangle = 2\langle 1_K\rangle \in \mathfrak{M}. \quad \square$$

We should point out that the additive subgroup generated by $\phi(\alpha, \beta)$ with $\alpha,\ \beta \in E/\Delta$ is the ideal $\mathfrak{M}^2$.

3. The Main Results

Definition 3.1. Two number fields K and L are *exotically integrally Witt equivalent* if there is a ring isomorphism between the integral Witt rings $W(\mathcal{O}_K)$ and $W(\mathcal{O}_L)$ of K and L, respectively.

Theorem 3.2. *Let K, L be totally complex number fields for which there is a ring isomorphism $h\colon W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$. Then*

(1) $levelK = levelL$

(2) $c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L$

(3) $h(\mathfrak{M}_K) = \mathfrak{M}_L$

(4) $h(J_K) = J_L$

(5) h induces an isomorphism

$$H_1\colon (E_K/\Delta_K, \cdot) \cong (E_L/\Delta_L, \cdot)$$

for which $H_1(\gamma_K) = \gamma_L \in E_L/\Delta_L$.

Proof. (1) is clear since the additive order of $\langle 1_K \rangle \in (W(\mathcal{O}_K), +)$ is $2levelK$ (see [Lam, Corollary 2.3, p.303]).

(2) is clear because $\#W(\mathcal{O}_K) = 2^{c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K}$.

(3) is also clear by noticing that $W(\mathcal{O}_K)$ is a local ring with the unique maximal ideal $\mathfrak{M}_K$.

(4) If, for a fixed $X \in \mathfrak{M}_K$, we have $XY = 0$ for all $Y \in \mathfrak{M}_K$, then we have $0 = h(XY) = h(X)h(Y)$ for all $h(Y) \in h(\mathfrak{M}_K) = \mathfrak{M}_L$. Since $h(\mathfrak{M}_K) = \mathfrak{M}_L$ and $J = \bigcap_{X \in \mathfrak{M}} \mathrm{Ann}(X)$, we have $h(J_K) = J_L$.

(5) From the results (3) and (4) above, h induces a group isomorphism

$$(\mathfrak{M}_K/J_K, +) \cong (\mathfrak{M}_L/J_L, +).$$

Combining this with the isomorphism $(\mathfrak{M}/J, +) \cong (E/\Delta, \cdot)$ induced by $\nu \circ disc$ will induce the isomorphism H_1:

$$\begin{array}{ccc} (\mathfrak{M}_K/J_K, +) & \xrightarrow{h} & (\mathfrak{M}_L/J_L, +) \\ \cong\downarrow & (\star) & \downarrow\cong \\ (E_K/\Delta_K, \cdot) & \xrightarrow[H_1]{} & (E_L/\Delta_L, \cdot) \end{array}$$

Clearly, $h\langle 1_K\rangle = \langle 1_L\rangle$. Thus $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle$. Now, since $2\langle 1_K\rangle \in \mathfrak{M}_K$ with discriminant -1, $2\langle 1_K\rangle$ maps to $\gamma_K = \nu_K(-1) \in E_K/\Delta_K$. Thus the induced $H_1 \colon E_K/\Delta_K \cong E_L/\Delta_L$ must take γ_K to γ_L . □

Observe that 2-$rk(W(\mathcal{O}_K), +)$ and 4-$rk(W(\mathcal{O}_K), +)$ are preserved (see Proposition 2.14).

Lemma 3.3. *Let K, L be totally complex number fields. Then there is a ring isomorphism*

$$h \colon W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$$

iff there is an isomorphism

$$h \colon (\mathfrak{M}_K, +, \cdot) \cong (\mathfrak{M}_L, +, \cdot)$$

for which $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle \in \mathfrak{M}_L$.

Proof. ($\Rightarrow$) This follows from Theorem 3.2.

($\Leftarrow$) Suppose that we have an isomorphism $h \colon (\mathfrak{M}_K, +, \cdot) \cong (\mathfrak{M}_L, +, \cdot)$ for which $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle \in \mathfrak{M}_L$. Let $X \in W(\mathcal{O}_K)$, then we can write $X = \langle 1_K\rangle + X_1$

with $X_1 \in \mathfrak{M}_K$. Define $\bar{h}\colon W(\mathcal{O}_K) \to W(\mathcal{O}_L)$ by

$$\bar{h}(X) = \begin{cases} h(X) & \text{if } X \in \mathfrak{M}_K \\ h(X + \langle 1_K \rangle) - \langle 1_L \rangle & \text{if } X \notin \mathfrak{M}_K. \end{cases}$$

Clearly, $\bar{h}$ is a ring homomorphism on $\mathfrak{M}_K$. Now, let $X,\ Y \in W(\mathcal{O}_K) \setminus \mathfrak{M}_K$, then $XY \notin \mathfrak{M}_K$ and $X + Y \in \mathfrak{M}_K$.

$$\begin{aligned} \bar{h}(X) + \bar{h}(Y) &= h(X + \langle 1_K \rangle) + h(Y + \langle 1_K \rangle) - 2\langle 1_L \rangle \\ &= h(X + \langle 1_K \rangle + Y + \langle 1_K \rangle) - 2\langle 1_L \rangle \\ &= h(X + Y) + h(2\langle 1_K \rangle) - 2\langle 1_L \rangle = h(X + Y) = \bar{h}(X + Y) \end{aligned}$$

and

$$\begin{aligned} \bar{h}(X)\bar{h}(Y) &= [h(X + \langle 1_K \rangle) - \langle 1_L \rangle][h(Y + \langle 1_K \rangle) - \langle 1_L \rangle] \\ &= h[(X + \langle 1_K \rangle)(Y + \langle 1_K \rangle)] \\ &\quad -\langle 1_L \rangle h(X + \langle 1_K \rangle) - \langle 1_L \rangle h(Y + \langle 1_K \rangle) + \langle 1_L \rangle \\ &= h(XY + X + Y + \langle 1_K \rangle) - h(X + \langle 1_K \rangle) - h(Y + \langle 1_K \rangle) + \langle 1_L \rangle \\ &= h(XY + \langle 1_K \rangle) + h(X + Y) - h(X + Y + 2\langle 1_K \rangle) + \langle 1_L \rangle \\ &= h(XY + \langle 1_K \rangle) + h(X + Y) - h(X + Y) - h(2\langle 1_K \rangle) + \langle 1_L \rangle \\ &= h(XY + \langle 1_K \rangle) - 2\langle 1_L \rangle + \langle 1_L \rangle \\ &= h(XY + \langle 1_K \rangle) - \langle 1_L \rangle = \bar{h}(XY) \end{aligned}$$

which implies $\bar{h}$ is a ring homomorphism.

To show that $\bar{h}$ is surjective let $Y \in W(\mathcal{O}_L) \setminus \mathfrak{M}_K$. Then $Y_1 = Y + \langle 1_L \rangle \in \mathfrak{M}_L$. Since $\mathfrak{M}_K \cong \mathfrak{M}_L$, there is an $X_1 \in \mathfrak{M}_K$ such that $h(X_1) = Y_1$. Take $X \in W(\mathcal{O}_K)$ so that $X + \langle 1_K \rangle = X_1$. Then

$$\bar{h}(X) = h(X + \langle 1_K \rangle) - \langle 1_L \rangle = h(X_1) - \langle 1_L \rangle = Y_1 - \langle 1_L \rangle = Y.$$

Finally, we claim that $\bar{h}$ is injective. Suppose that $\bar{h}(X) = 0 \in W(\mathcal{O}_L)$ for $X \in W(\mathcal{O}_K)$. If $X \notin \mathfrak{M}_K$, then $\bar{h}(X) = h(X + \langle 1_K \rangle) - \langle 1_L \rangle = 0$. Thus we have $h(X + \langle 1_K \rangle) = \langle 1_L \rangle$. But since $\mathfrak{M}_K \cong \mathfrak{M}_L$, we have $\langle 1_L \rangle \in \mathfrak{M}_L$ which is a contradiction. So, X must be in $\mathfrak{M}_K$, and hence $\bar{h}(X) = h(X) = 0$. Thus X must be 0 in $W(\mathcal{O}_K)$. □

We now use the characteristic ideal J.

Proposition 3.4. *Let K, L be totally complex number fields. Then there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ iff there is a pair of isomorphisms*

$$H_1 \colon (E_K/\Delta_K, \cdot) \cong (E_L/\Delta_L, \cdot) \quad \textit{and} \quad H_2 \colon (J_K, +) \cong (J_L, +)$$

satisfying the following:

(1) $H_1(\gamma_K) = \gamma_L \in E_L/\Delta_L$

(2) $H_2(\phi_K(\alpha, \beta)) = \phi_L(H_1(\alpha), H_1(\beta)) \quad \forall\ \alpha,\ \beta \in E_K/\Delta_K$

where $\phi \colon E/\Delta \times E/\Delta \to J$ is defined in Definition 2.22

(3) If $\gamma_K = e$, and hence $\gamma_L = e$, then $H_2(2\langle 1_K \rangle) = 2\langle 1_L \rangle \in J_L \subset \mathfrak{M}_L$.

Proof. ($\Rightarrow$) From Theorem 3.2-(4),(5), we have H_1 and $H_2 = h|_{J_K}$ with

$$H_1(\gamma_K) = \gamma_L \in E_L/\Delta_L$$

which gives the condition (1).

To show the condition (2) recall that, for $\alpha,\ \beta \in E_K/\Delta_K$, we defined

$$\phi_K(\alpha, \beta) = \langle a, -1 \rangle \langle b, -1 \rangle \in J_K$$

for some $a,\ b \in E_K$ with $\nu_K(a) = \alpha$ and $\nu_K(b) = \beta$. Then we have

$$H_2(\phi_K(\alpha, \beta)) = h(\phi_K(\alpha, \beta)) = h(\langle a, -1 \rangle \langle b, -1 \rangle)$$

while

$$\phi_L(H_1(\alpha), H_1(\beta)) = \langle a', -1\rangle\langle b', -1\rangle \in J_L$$

for some $a',\ b' \in E_L$ with $\nu_L(a') = H_1(\alpha)$ and $\nu_L(b') = H_1(\beta)$. Then it is enough to show

$$h(\langle a, -1\rangle\langle b, -1\rangle) = \langle a', -1\rangle\langle b', -1\rangle.$$

For $\nu_K(a) = \alpha$, we can take $\langle a, -1\rangle \in \mathfrak{M}_K/J_K$ via $E_K/\Delta_K \cong \mathfrak{M}_K/J_K$. Note that we have $h\colon \mathfrak{M}_K/J_K \cong \mathfrak{M}_L/J_L$. Set $a' = disc(h\langle a, -1\rangle) \in E_L$. Then since the diagram $(\star)$ in the proof of Theorem 3.2-(5) commutes, we have $a'\Delta_L = H(\alpha)$. Then we have $\langle a', -1\rangle = h\langle a, -1\rangle$ because $disc\langle a', -1\rangle = a' = disc(h\langle a, -1\rangle)$. Picking b' similarly, we have

$$h(\langle a, -1\rangle\langle b, -1\rangle) = h\langle a, -1\rangle h\langle b, -1\rangle = \langle a', -1\rangle\langle b', -1\rangle$$

since $h\colon W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ is a ring homomorphism.

The condition (3) follows from Lemma 2.24-(2) on page 33 and the diagram $(\star)$ in the proof of Theorem 3.2-(5).

($\Leftarrow$) By Lemma 3.3, it is enough to show that there is a ring isomorphism

$$h\colon (\mathfrak{M}_K, +, \cdot) \cong (\mathfrak{M}_L, +, \cdot)$$

for which $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle \in \mathfrak{M}_L$.

Recall from Lemma 2.24 that we have

$$\tau_K\colon (E_K/\Delta_K \times J_K, \dotplus, \divideontimes) \cong (\mathfrak{M}_K, +, \cdot)$$

and

$$\tau_L\colon (E_L/\Delta_L \times J_L, \dotplus, \divideontimes) \cong (\mathfrak{M}_L, +, \cdot)$$

where, in general, $\tau\colon (E/\Delta \times J, \dotplus, \divideontimes) \cong (\mathfrak{M}, +, \cdot)$ is defined by

$$(\alpha, Y) \mapsto \langle \chi(\alpha), -1\rangle + Y$$

with a homomorphism $\chi\colon E/\Delta \to E$ satisfying $\nu\chi = (\alpha) \equiv \alpha$. Now define

$$\rho\colon E_K/\Delta_K \times J_K \to E_L/\Delta_L \times J_L$$

by

$$\rho(\alpha, Y) = (H_1(\alpha), H_2(Y)).$$

Then ρ is well-defined and bijective because both coordinate maps are well-defined and bijective. So, it remains to show that

(i) ρ is a ring homomorphism

(ii) $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle$.

(i) Let $(\alpha, Y),\ (\beta, Y_1) \in E_K/\Delta_K \times J_K$. Then

$$\begin{aligned}
\rho((\alpha, Y)\dotplus(\beta, Y_1)) &= \rho(\alpha\beta, \phi_K(\alpha, \beta) + Y + Y_1) \\
&= (H_1(\alpha\beta), H_2(\phi_K(\alpha, \beta) + Y + Y_1)) \\
&= (H_1(\alpha)H_1(\beta), H_2(\phi_K(\alpha, \beta)) + H_2(Y) + H_2(Y_1) \\
&= (H_1(\alpha)H_1(\beta), \phi_L(H_1(\alpha), H_1(\beta)) + H_2(Y) + H_2(Y_1) \\
&= ((H_1(\alpha), H_2(Y))\dotplus(H_1(\beta), H_2(Y_1)) = \rho(\alpha, Y)\dotplus\rho(\beta, Y_1)
\end{aligned}$$

and

$$\begin{aligned}
\rho((\alpha, Y)\divideontimes(\beta, Y_1)) &= \rho(e_K, \phi_K(\alpha, \beta)) \\
&= (H_1(e_K), H_2(\phi_K(\alpha, \beta))) \\
&= (e_L, \phi_L(H_1(\alpha), H_1(\beta))) \\
&= ((H_1(\alpha), H_2(Y))\divideontimes(H_1(\beta), H_2(Y_1)) = \rho(\alpha, Y)\divideontimes\rho(\beta, Y_1).
\end{aligned}$$

Hence we have a sequence of ring isomorphisms:

$$h\colon \mathfrak{M}_K \overset{\tau_K}{\cong} E_K/\Delta_K \times J_K \overset{\rho}{\cong} E_L/\Delta_L \times J_L \overset{\tau_L}{\cong} \mathfrak{M}_L$$

(ii) To show $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle$ we will use the fact from Lemma 2.24-(2),(3) that $2\langle 1\rangle \in \mathfrak{M}$ corresponds to either $(e, 2\langle 1\rangle)$ or $(\gamma, 4\langle 1\rangle)$ in $E/\Delta \times J$.

Case 1. Suppose that $2\langle 1\rangle \in \mathfrak{M}$ corresponds to $(e, 2\langle 1\rangle)$. Then we have

$$2\langle 1_K\rangle \;\mapsto\; (e_K, 2\langle 1_K\rangle) \;\mapsto\; (H_1(e_K), H_2(2\langle 1_K\rangle))$$

under $\mathfrak{M}_K \cong E_K/\Delta_K \times J_K \cong E_L/\Delta_L \times J_L$, and

$$2\langle 1_L\rangle \;\mapsto\; (e_L, 2\langle 1_L\rangle)$$

under $\mathfrak{M}_L \cong E_L/\Delta_L \times J_L$. Then, since $H_1(e_K) = e_L$ and $H_2(2\langle 1_K\rangle) = 2\langle 1_L\rangle$ by the hypothesis (3), we have $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle$.

Case 2. Suppose that $2\langle 1\rangle \in \mathfrak{M}$ corresponds to $(\gamma, 4\langle 1\rangle)$. Then we have

$$2\langle 1_K\rangle \;\mapsto\; (\gamma_K, 4\langle 1_K\rangle) \;\mapsto\; (H_1(\gamma_K), H_2(4\langle 1_K\rangle))$$

under $\mathfrak{M}_K \cong E_K/\Delta_K \times J_K \cong E_L/\Delta_L \times J_L$, and

$$2\langle 1_L\rangle \;\mapsto\; (\gamma_L, 4\langle 1_L\rangle)$$

under $\mathfrak{M}_L \cong E_L/\Delta_L \times J_L$. By the hypothesis (1), we have $H_1(\gamma_K) = \gamma_L$. And

$$\begin{aligned} H_2(4\langle 1_K\rangle) &= H_2(\langle -1,-1\rangle\langle -1,-1\rangle) \\ &= H_2(\phi_K(\gamma_K, \gamma_K)) \\ &= \phi_L(H_1(\gamma_K), H_1(\gamma_K)) \quad \text{by the hypothesis (2)} \\ &= \phi_L(\gamma_L, \gamma_L) = \langle -1,-1\rangle\langle -1,-1\rangle = 4\langle 1_L\rangle \end{aligned}$$

Thus we have $h(2\langle 1_K\rangle) = 2\langle 1_L\rangle$. □

4. The Class $\mathcal{K}_0$

Let $\mathcal{K}_0$ be the class of all totally complex number fields with $\Delta = E$. From Lemma 2.18, if a totally complex number field K has only one dyadic prime, that is, $g_2(K) = 1$, then $\Delta_K = E_K$. Note that, since $K = \mathbb{Q}(\sqrt{-1})$ has only one dyadic prime, $\mathbb{Q}(\sqrt{-1})$ is in the class $\mathcal{K}_0$. Therefore, $\mathcal{K}_0$ is not empty. We want to find necessary and sufficient conditions for two fields in the class $\mathcal{K}_0$ to be exotically integrally Witt equivalent.

4.1 Exotic Integral Witt Equivalence in $\mathcal{K}_0$

Remark 4.1. Assume $K \in \mathcal{K}_0$. Then

(1) $level K = 1$ or 2.

(2) $2\langle 1_K \rangle \in J$ and $\mathfrak{M} = J$.

(3) $$\begin{aligned} 2\text{-}rk(J,+) &= 2\text{-}rk\,\Delta + g_2(K) - 1 = 2\text{-}rk\,E + g_2(K) - 1 \\ &= c_K + 2\text{-}rk\,\mathcal{C}_K + g_2(K) - 1. \end{aligned}$$

(4) If L is any number field with a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$, then, by Theorem 3.2, we have $E_K/\Delta_K \cong E_L/\Delta_L$ and hence $L \in \mathcal{K}_0$.

Theorem 4.2. *For $K,\ L \in \mathcal{K}_0$, there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ iff we have*

(1) $level K = level L$,

(2) $c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L$.

Proof. ($\Rightarrow$) It follows from Theorem 3.2.

($\Leftarrow$) Assume that we have $level K = level L$ and $\#W(\mathcal{O}_K) = \#W(\mathcal{O}_L)$. Then, by

Remark 4.1, $(J_K, +)$ and $(J_L, +)$ are elementary abelian 2-groups with the same 2-rank. Since $levelK = levelL$, either $2\langle 1_K \rangle$ and $2\langle 1_L \rangle$ are both 0, or neither is 0. Thus we can choose an isomorphism

$$H_2 \colon (J_K, +) \cong (J_L, +) \quad \text{with } H_2(2\langle 1_K \rangle) = 2\langle 1_L \rangle.$$

Obviously, $H_1 \colon E_K/\Delta_K \cong E_L/\Delta_L$ is a trivial map. By Proposition 3.4, there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$. □

Therefore, for $K \in \mathcal{K}_0$, the isomorphism type of $W(\mathcal{O}_K)$ is determined only by $levelK$ and $\#W(\mathcal{O}_K) = 2^{c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K}$.

4.2 An Exotic Example

In this section we give an example of two exotically integrally Witt equivalent totally complex number fields of different degrees over $\mathbb{Q}$. Since a totally complex number field with one dyadic prime ideal is in the class $\mathcal{K}_0$, we will restrict our interests to the totally complex number field K with $g_2(K) = 1$.

Example. Let $K = \mathbb{Q}(\alpha)$ with the minimal polynomial $f_\alpha(x) = x^4 + x^3 + 2x^2 - 4x + 3$. The polynomial f_α is found by using PARI-GP. Note that K is a subfield of the 13th cyclotomic field $\mathbb{Q}(\zeta_{13})$ which is normal over $\mathbb{Q}$. Since $|\mathrm{Aut}_K\mathbb{Q}(\zeta_{13})| = [\mathbb{Q}(\zeta_{13}) \colon K] = 3$ and $[K \colon \mathbb{Q}] = r_K + 2c_K = 4$, K must be totally complex, and hence $c_K = 2$. Since f_α is irreducible over $\mathbb{Z}/2\mathbb{Z}$, 2 is inert in K. Thus K has only one dyadic prime with the ramification index $e = 1$ and the inertial degree $f = 4$. So, the level of K is either 1 or 2. We can determine the level of K by checking if the polynomial $x^2 + 1$ is factorable over K. With the aid of the computer program PARI-GP (ver.2.1.0), we find $2\text{-}rk\mathcal{C}_K = 0$ and $levelK = 2$. Therefore, for the number field $K = \mathbb{Q}(\alpha)$, we have

$$[K \colon \mathbb{Q}] = 4, \;\; c_K = 2, \;\; g_2(K) = 1, \;\; 2\text{-}rk\mathcal{C}_K = 0, \;\; \text{and} \;\; levelK = 2.$$

For the number field $L = \mathbb{Q}(\sqrt{-5})$, we can find, without using PARI-GP,

$$[L\colon \mathbb{Q}] = 2, \;\; c_L = 1, \;\; g_2(L) = 1, \;\; 2\text{-}rk\mathcal{C}_L = 1, \;\; \text{and} \;\; levelL = 2.$$

Thus both K and L are in the class $\mathcal{K}_0$. Then since we have

$$\begin{aligned} levelK = \;\; & 2 \;\; = levelL \\ c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K = \;\; & 3 \;\; = c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L \end{aligned}$$

we have $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ by Theorem 4.2. But since $[K\colon \mathbb{Q}] = 4$ and $[L\colon \mathbb{Q}] = 2$, K and L are not Witt equivalent, that is, $W(K) \ncong W(L)$.

The following is the procedure of computing the values above by using PARI-GP. First, two functions `subcyclo()` and `efprintt()` are defined and written in a file `tmp.gp` as follows:

```
subcyclo(n,d=-1)=
{
  local(Z,G,S);
  if(d<0, d=n);
  Z=znstar(n); G=matdiagonal(Z[2]); S=[\hskip2mm];
  forsubgroup(H=G,d,
     S=concat(S,galoissubcyclo(n,mathnf(concat(G,H)),Z));
  );
  S
}

efprint(dec)
=for(k=1,length(dec),print("e=",dec[k].e," f=",dec[k].f))
```

Note that the function `subcyclo(n,d)` will compute all subfields of the `n`-th cyclotomic field, of order less than or equal to `d`, if `d` is set, and that the function `efprint(dec)` will print the ramification indices e and the inertial degrees f of the pre-calculated prime ideal decomposition `dec` of a prime number over the given number field. To use these functions this file should be read into PARI-GP as follows (**Important:** the file `tmp.gp` should be in the same directory that PARI-GP would be run):

```
? \rtmp.gp        [means to read the file tmp.gp]
```

Note that the line starting with `?` is the command line to be typed in, and that the line with `%number` or nothing is the output line.

We first try to find every subfield of the 13th cyclotomic field $\mathbb{Q}(\zeta_{13})$, of degree 4. Note that the value of `%1` below lists the minimal polynomial of each u where $\mathbb{Q}(u)$ is a subfield of $\mathbb{Q}(\zeta_{13})$.

```
? subcyclo(13,4)
%1 = [x^4 + x^3 + 2*x^2 - 4*x + 3, x^2 + x - 3, x^3 + x^2 - 4*x
+ 1, x + 1]
```

Now, we take the minimal polynomial of degree 4: `pol1 = x^4 + x^3 + 2*x^2 - 4*x + 3`. And we generate `nf1`, the number field $K = \mathbb{Q}(\alpha)$ with the minimal polynomial `pol1` of α by using the built-in function `nfinit()`.

```
? pol1=%1[1]        [%n[e] means the e-th entry of the output line n]
%2 = x^4 + x^3 + 2*x^2 - 4*x + 3        [output: the value of pol1]
? nf1=nfinit(pol1);
```

Then put the prime ideal decomposition of $(2) = 2\mathcal{O}_K$ into the variable `pdec` to get all dyadic prime ideals. Writing the ramification indices e and the inertial degrees f will let us find $g_2(K)$, the number of dyadic prime ideals of $\mathcal{O}_K$. Or $g_2(K)$ can be found easily by using the command `length()`. In this case we have only one dyadic prime ideal, that is, we have $g_2(K) = 1$, and hence $E_K = \Delta_K$.

```
? pdec=idealprimedec(nf1,2);        [pdec: decomposition of (2) over nf1]
? efprint(pdec)        [writes e and f]
e = 1 f = 4
? g2=length(pdec)        [another way to get g2(K)]
%3 = 1
? print(``r(K)='',nf1.sign[1],'',c(K)='',nf1.sign[2],''g2(K)='',g2)
r(K)=0,c(K)=2,g2(K)=1        [print result]
```

where `r(K)` is the number of real embeddings, `c(K)` the number of pairs of complex conjugate embeddings, and `g2(K)` the number of dyadic prime ideals. Note that the built-in function `nf1.sign` will give a 2-ary vector `[r(K), c(K)]`. We can see that these three computed values agree with those we found earlier.

Now we can find the class number and the structure of the ideal class group as a products of cyclic groups by using the built-in function `bnfclassunit()` as follows.

```
? classno=bnfclassunit(pol1).clgp.no        [the class number]
%4 = 1
? classgrp=bnfclassunit(pol1).clgp.cyc        [the group structure]
%5 = [ ]
```

In this case the class number is 1 and the class group $\mathcal{C}_K$ is trivial. So, the 2-rank $_2\text{-}rk\mathcal{C}_K$ of the class group is 0. Note that, if the class number is bigger than 1, then we can determine the 2-rank of the class group by its group structure.

Finally, we will determine the level of the field K. It can be done by checking if the polynomial x^2+1 is factorable over K since we know that the level of K must be either 1 or 2 in this case.

```
? factornf(x^2+1,subst(pol1,x,y))
  %6 = [Mod(1,y^4 + y^3 + 2*y^2 - 4*x + 3)*x^2 + Mod(1,y^4 + y^3
+ 2*y^2 - 4*x + 3) 1]
```

where `subst(pol1,x,y) = y^4 + y^3 + 2*y^2 - 4*x + 3`, the polynomial `pol1` in the variable `y`. Note that the function `subst(pol1,x,y)` will substitute the variables of the polynomial `pol1`. In this case x^2+1 is not factorable over K, and hence we must have $levelK = 2$.

5. The Class $\mathcal{K}_1$

In this chapter we consider totally complex number fields K for which

$$2\text{-}rk(\mathfrak{M}^2, +) = 1, \quad \text{i.e., } (\mathfrak{M}^2, +) \text{ is cyclic order 2.}$$

Then we must have E/Δ non-trivial since $\mathfrak{M}^2 = \{0\}$ *iff* $E = \Delta$.

Let us consider the function defined in Definition 2.22

$$\phi\colon E/\Delta \times E/\Delta \to \mathfrak{M}^2 = \mathbb{F}_2 = \{0, 1\}.$$

Then, for any $\alpha,\ \beta \in E/\Delta$, either $\phi(\alpha, \beta) = 0$, or $\phi(\alpha, \beta)$ generates $(\mathfrak{M}^2, +)$. Recall that $\phi(\alpha, \beta) = \phi(\beta, \alpha)$, $\phi(\alpha\alpha_1, \beta) = \phi(\alpha, \beta) + \phi(\alpha_1, \beta)$, and that ϕ is non-degenerate. So, we may regard $(E/\Delta, \phi)$ as an inner product space structure on $(E/\Delta, \cdot)$ with values in $\mathbb{F}_2$.

Lemma 5.1. *$\nu(-1) = \gamma \in E/\Delta$ is the unique "characteristic" element, i.e.,*

$$\phi(\alpha, \alpha) = \phi(\alpha, \gamma) \in \mathbb{F}_2 \quad \forall\ \alpha \in E/\Delta.$$

Proof. For any $\alpha,\ \beta \in E/\Delta$, we have $\mathrm{c}(\phi(\alpha, \beta)) = [\alpha, \beta] \in G_2$ and if $\mathrm{c}(\phi(\alpha, \beta)) = \mathrm{c}(\phi(\alpha', \beta'))$, then $\phi(\alpha, \beta) = \phi(\alpha', \beta')$ in $\mathfrak{M}^2$. Also, note that we have $[d, d] = [d, -1] \in G_2$ for any $d \in E$. □

Lemma 5.2. *$(E/\Delta, \phi)$ is Type II iff $-1 \in \Delta$.*

Proof. $(E/\Delta, \phi)$ is Type II *iff* $\phi(\alpha, \gamma) = \phi(\alpha, \alpha) = 0\ \ \forall\ \alpha \in E/\Delta$
iff $\gamma = e \in E/\Delta$ *iff* $-1 \in \Delta$. □

Lemma 5.3.

$$level K = 4 \ \Leftrightarrow\ \phi(\gamma, \gamma) \neq 0 \in \mathbb{F}_2 \ \Leftrightarrow\ 2\text{-}rk(E/\Delta) \equiv 1 \pmod 2.$$

Proof. Note that

$$\begin{aligned}
[-1,-1] = \mathbf{1} \in G_2 &\Leftrightarrow -1 \text{ is a norm from } K(\sqrt{-1}) \text{ over } K \\
&\Leftrightarrow -1 = (x+y\sqrt{-1})(x-y\sqrt{-1}) = x^2+y^2 \text{ over } K \\
&\Leftrightarrow level K = 1,\ 2.
\end{aligned}$$

So, we have $[-1,-1] \neq \mathbf{1} \in G_2 \Leftrightarrow level K = 4$. Then, since

$$\phi(\alpha,\beta) = 0 \Leftrightarrow [\alpha,\beta] = \mathbf{1} \in G_2$$

for $\alpha,\ \beta \in E/\Delta$, we have

$$level K = 4 \Leftrightarrow [-1,-1] \neq \mathbf{1} \in G_2 \Leftrightarrow \phi(\gamma,\gamma) \neq 0.$$

For the second equivalence, we claim more generally that, for a characteristic element u of an inner product space $(V, <:>)$ over $\mathbb{F}_2$, we have

$$< u : u > \equiv \dim_{\mathbb{F}_2} V \pmod 2$$

so that we can have $\phi(\gamma,\gamma) \equiv 2\text{-}rk(E/\Delta) \pmod 2$ since $\dim_{\mathbb{F}_2}(E/\Delta) = 2\text{-}rk(E/\Delta)$.

We first note that both the inner product $<:>$ and the dimension are additive. By Kaplansky's lemma (see [Kap, Theorem 19, 20]), we know that any n-dimensional $\mathbb{F}_2$-inner product space V is isometric to ${\mathbb{F}_2}^n$ whose matrix of inner products is

$$\text{either } \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}.$$

So, it is enough to show our claim for $n = 1$ or 2. If $n = 1$, then $V \sim \mathbb{F}_2$ with the 1×1 identity matrix and $u = 1$. If $n = 2$, then $V \sim \mathbb{F}_2^2$ with the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $u = \vec{0}$. And it is easy to see that both cases satisfy our claim. □

Remark 5.4.

(1) If $-1 \notin \Delta$, then we have the following equivalence:

$level K = 2$ *iff* $(E/\Delta, \phi)$ is Type I and $2\text{-}rk(E/\Delta) \equiv 0 \pmod 2$.

(2) If $-1 \in \Delta$, then we see $0 \neq 2\langle 1_K \rangle \in J$ is not in $\mathfrak{M}^2$ unless we have $level K = 1$ in which case $2\langle 1_K \rangle = 0$.

Now, let $\mathcal{K}_1$ be the class of all totally complex number fields K with $(\mathfrak{M}^2, +)$ cyclic order 2. Note that, if L is a number field for which there is a ring isomorphism $h\colon W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$, then $h(\mathfrak{M}_K^2) = \mathfrak{M}_L^2$. Thus we only consider pairs K, L in $\mathcal{K}_1$.

Theorem 5.5. *For K, $L \in \mathcal{K}_1$, there is a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ iff we have*

(1) $level K = level L$,

(2) $c_K + g_2(K) + 2\text{-}rk\, \mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\, \mathcal{C}_L$,

(3) Either -1 lies in both Δ_K and Δ_L, or it lies in neither one,

(4) $2\text{-}rk(E_K/\Delta_K) = 2\text{-}rk(E_L/\Delta_L)$.

Proof. ($\Rightarrow$) If we have a ring isomorphism $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$, then, by Theorem 3.2, it's easy to see that these 4 conditions hold.

($\Leftarrow$) To prove the converse we will use Proposition 3.4. Suppose that the 4 conditions above are true. Consider $(E_K/\Delta_K, \phi_K)$ and $(E_L/\Delta_L, \phi_L)$. Since they have

the same 2-rank and the same type, there is an isometry

$$(E_K/\Delta_K, \phi_K) \cong (E_L/\Delta_L, \phi_L),$$

and hence we have an isomorphism $H_1 \colon (E_K/\Delta_K, \cdot) \cong (E_L/\Delta_L, \cdot)$.

To find an isomorphism $H_2 \colon (J_K, +) \cong (J_L, +)$ we only need to show $2\text{-}rk(J_K, +) = 2\text{-}rk(J_L, +)$ because $(J, +)$ is always an elementary abelian 2-group. If $2\text{-}rk(E_K/\Delta_K) = 2\text{-}rk(E_L/\Delta_L)$, then we have

$$2\text{-}rk(J_K, +) = 2\text{-}rk(J_L, +) \;\Leftrightarrow\; \#W(\mathcal{O}_K) = \#W(\mathcal{O}_L)$$

since we have $\#W(\mathcal{O}_K) = 2^{2-rk(E_K)+g_2(K)}$ and $2\text{-}rk(J_K) = 2\text{-}rk(\Delta_K) + g_2(K) - 1$. Thus we can find an isomorphism $H_2 \colon (J_K, +) \cong (J_L, +)$ such that

$$H_2(\mu_K) = \mu_L$$

where μ_K and μ_L are any generators of $\mathfrak{M}_K^2$ and $\mathfrak{M}_L^2$, respectively.

Now, consider the map $\phi_K \colon E_K/\Delta_K \times E_K/\Delta_K \to \mathfrak{M}_K^2 = \mathbb{F}_2$. Since we can think of ϕ as an inner product, we can write

$$\phi_K(\alpha, \beta) = \phi_K(\alpha, \beta)\mu_K.$$

Thus, if we have the isometry $H_1 \colon (E_K/\Delta_K, \phi_K) \cong (E_L/\Delta_L, \phi_L)$, then we have

$$\begin{aligned} H_2(\phi_K(\alpha, \beta)) &= H_2(\phi_K(\alpha, \beta)\mu_K) \\ &= \phi_K(\alpha, \beta)H_2(\mu_K) \\ &= \phi_K(\alpha, \beta)\mu_L \\ &= \phi_L(H_1(\alpha), H_1(\beta))\mu_L \\ &= \phi_L(H_1(\alpha), H_1(\beta)) \in \mathfrak{M}_L^2 \subset J_L \end{aligned}$$

for every $\alpha,\ \beta \in E_K/\Delta_K$. Furthermore, we have $H_1(\gamma_K) = \gamma_L$ since $\gamma \in E/\Delta$ is the unique characteristic element and

$$\phi_L(H_1(\alpha), H_1(\alpha)) = H_2(\phi_K(\alpha, \alpha)) = H_2(\phi_K(\alpha, \gamma_K)) = \phi_L(H_1(\alpha), H_1(\gamma_K))$$

for any $\alpha \in E_K/\Delta_K$, and hence for any $H_1(\alpha) \in E_L/\Delta_L$. Thus, either -1 lies in neither of Δ_K and Δ_L, or -1 lies in both Δ_K and Δ_L.

Now, we only need to show that the last condition in Proposition 3.4. If -1 lies in neither of Δ_K and Δ_L, then we are done. On the other hand, if -1 lies in both Δ_K and Δ_L, then γ_K and γ_L are both trivial. In this case, $levelK = levelL = 1$ or 2 by Lemma 2.9.

Case 1. If $levelK = levelL = 1$, then $2\langle 1_K\rangle = 2\langle 1_L\rangle = 0$. Hence

$$H_2(2\langle 1_K\rangle) = H_2(0) = 0 = 2\langle 1_L\rangle.$$

Case 2. If $levelK = levelL = 2$, then neither of $2\langle 1_K\rangle$ and $2\langle 1_L\rangle$ is zero. Thus $2\langle 1_K\rangle \in J_K$ but $2\langle 1_K\rangle \notin \mathfrak{M}_K^2$, and $2\langle 1_L\rangle \in J_L$ but $2\langle 1_L\rangle \notin \mathfrak{M}_L^2$. So, we simply choose $H_2 \colon (J_K, +) \cong (J_L, +)$ so that

$$H_2(\mu_K) = \mu_L \quad \text{and} \quad H_2(2\langle 1_K\rangle) = 2\langle 1_L\rangle. \quad \square$$

We may ask if there are totally complex number fields K in $\mathcal{K}_1$. In fact, if K is a complex number field with $g_2(K) = 2$, then we have

$$K \in \mathcal{K}_1 \;\Leftrightarrow\; E \neq \Delta\,.$$

We simply note that if $g_2(K) = 2$, then G_2 is cyclic order 2. Thus $\mathfrak{M}_K^2$ is trivial or cyclic of order 2. But we know $\mathfrak{M}^2 = \{0\} \;\Leftrightarrow\; \Delta = E$. Here's an example of a number field in the class $\mathcal{K}_1$.

Example 5.6. Let $\sigma > 0$ be a square free rational integer with $\sigma \equiv 7 \pmod 8$. Then $K = \mathbb{Q}(\sqrt{-\sigma})$ is totally complex, $c_K = 1$, $g_2(K) = 2$, and $levelK = 4$. Thus $4\langle 1_K\rangle \in \mathfrak{M}_K^2$ but $4\langle 1_K\rangle \neq 0$ which implies that $\mathfrak{M}_K^2$ is cyclic of order 2. Hence $K \in \mathcal{K}_1$. Moreover, $2\text{-}rk\mathcal{C}_K$ is one less than the number of distinct rational primes dividing σ.

Proof. First, we want to show that $g_2(K) = 2$ and $levelK = 4$.

(1) Since $-\sigma \equiv 1 \pmod 8$, we have the prime ideal decomposition

$$2\mathcal{O}_K = \left(2, \frac{1+\sqrt{-\sigma}}{2}\right)\left(2, \frac{1-\sqrt{-\sigma}}{2}\right).$$

Thus we have $g_2(K) = 2$. So, $(G_2, \cdot)$ is cyclic of order 2.

(2) Since $\sigma \equiv 7 \pmod 8$, σ can't be written as a sum of 3 squares in $\mathbb{Z}$, and hence in $\mathbb{Q}$. Thus $levelK \nleqslant 2$. Hence $levelK = 4$.

Since the additive order of $\langle 1_K \rangle$ is $2levelK = 8$, we have $4\langle 1_K \rangle \neq 0$. Note that $4\langle 1_K \rangle$ is always in $\mathfrak{M}_K^2$. Thus $\mathfrak{M}_K^2$ is not trivial. Since $\mathfrak{M}_K^2$ is isomorphic to a subgroup of $(G_2, \cdot)$, $\mathfrak{M}_K^2$ must be cyclic of order 2. The last statement about the 2-rank of $\mathcal{C}_K$ follows from the Theorem of Gauss (see [B-S, Theorem 8, p.247]). $\square$

6. CM Extensions in $\mathcal{K}_0$ or $\mathcal{K}_1$

A *CM-extension* K of F is a quadratic extension $K = F(\sqrt{-\sigma})$ of a totally real number field F where σ is totally positive (see [C-H, p.66]). In this chapter, we are concerned with CM-extensions K of totally real number fields F containing units with independent signs to obtain totally complex number fields in $\mathcal{K}_0$ or $\mathcal{K}_1$.

Definition 6.1. A number field F (or its number ring $\mathcal{O}_F$) has *units with independent signs* if for each (real) embedding $\varepsilon\colon F \to \mathbb{R}$ there is a unit in $\mathcal{O}_F^*$ whose image under the embedding ε is negative but whose image under every other real embedding of F is positive.

Lemma 6.2. *Let F be a totally real number field. Then the following are equivalent:*

(1) $\mathcal{O}_F^*$ has units with independent signs

(2) A unit in $\mathcal{O}_F^*$ is a square iff it is totally positive

(3) $\mathcal{C}_F^+ \cong \mathcal{C}_F$, where $\mathcal{C}_F^+$ is the narrow ideal class group of F.

Proof. It is shown on page 55 with Definition 12.1 and Lemma 12.2 in [C-H]. □

Let $\mathfrak{p}_\infty$ be a real infinite prime in F. Then the real embedding ε of F corresponding to $\mathfrak{p}_\infty$ can be extended to

(1) either a real embedding of K,

(2) or a pair of complex conjugate embeddings of K

which means that

(1) either $\mathfrak{p}_\infty$ is inert in K,

(2) or $\mathfrak{p}_\infty$ ramifies in K.

Since, for a CM-extension $K = F(\sqrt{-\sigma})$ of a totally real number field F, $-\sigma$ is negative with respect to every real embedding of F, every real infinite prime of F ramifies in the CM-extension K. Hence CM-extensions are totally complex.

Lemma 6.3. *If F is totally real and contains units with independent signs, then for $1 \neq u \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}$, at least one dyadic prime ideal in $\mathcal{O}_F$ ramifies in $F(\sqrt{u})$.*

Proof. Let $K = F(\sqrt{u})$. First, we want to show that at least one infinite prime of F ramifies in K. Since u is not a square in $\mathcal{O}_F^*$, u is not totally positive. So there is a real embedding ε of F such that $\varepsilon(u)$ is negative. Then ε is extended to a pair of complex conjugate embeddings of K. Therefore, the infinite prime corresponding to ε ramifies in K.

Now, suppose that no finite prime of F ramifies in K. Since the ray class field $\mathcal{H}_F^+$ of F is the maximal abelian extension of F in which no finite prime ramifies, K must be a subfield of $\mathcal{H}_F^+$. Note that $\mathrm{Gal}\,(\mathcal{H}_F^+/\mathcal{H}_F) \cong \mathrm{Ker}(\mathcal{C}_F^+ \to \mathcal{C}_F)$ and $\mathcal{C}_F^+ \cong \mathcal{C}_F$ where $\mathcal{H}_F$ is the Hilbert class field of F. It follows that $\mathcal{H}_F^+ \cong \mathcal{H}_F$. Since $\mathcal{H}_F$ is the maximal unramified extension of F, K must be an unramified extension of F, which is a contradiction.

Finally, we want to show that if a finite prime of F ramifies in K, then the prime is in fact dyadic. Note that a finite prime $\mathfrak{p}$ of F ramifies in K *iff* $\mathfrak{p}$ divides the principal ideal $(disc(K/F))$ in $\mathcal{O}_F$, generated by the discriminant $disc(K/F)$ of K over F. It is easy to calculate that the discriminant $disc(f)$ of the minimal polynomial f of $\sqrt{u}$ is $4u$. And we know that $disc(K/F)$ divides $disc(f)$. So, if $\mathfrak{p}$ ramifies in K, then $\mathfrak{p}$ should divide (4) which follows that $\mathfrak{p}$ should be dyadic. □

Lemma 6.4. *Let F be a totally real field with $h^+(F) \equiv 1 \pmod 2$ where $h^+(F)$ is the narrow class number of F. If $1 \neq \sigma \in F^*/F^{*2}$ is totally positive and exactly one*

prime ideal in $\mathcal{O}_F$ ramifies in $F(\sqrt{\sigma})$, then $h^+(F(\sqrt{\sigma})) \equiv 1 \pmod 2$ and $F(\sqrt{\sigma})$ is totally real with $r_{F(\sqrt{\sigma})} = 2r_F$.

Proof. See Corollary 12.5, p.59, [C-H]. □

First, we want to use CM-extensions to produce totally complex number fields $K \in \mathcal{K}_0$.

Lemma 6.5. *Let F be a totally real field containing units with independent signs, and let $\sigma \in F^*/F^{*2}$ is totally positive. If no dyadic prime ideal in $\mathcal{O}_F$ ramifies in the CM-extension $K = F(\sqrt{-\sigma})$, then K is totally complex, $c_K = r_F$, and $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap R = \{1\}$.*

Proof. First, we note that $2\text{-}rk(\mathcal{O}_K^*/\mathcal{O}_K^{*2}) = c_K = r_F = 2\text{-}rk(\mathcal{O}_F^*/\mathcal{O}_F^{*2})$ (from Dirichlet's unit theorem). Since no dyadic prime ideal ramifies in K, we see by Lemma 6.3 that $-\sigma \notin \mathcal{O}_F^*/\mathcal{O}_F^{*2}$. Thus, $\mathcal{O}_F^* \subset \mathcal{O}_K^*$ induces

$$\mathcal{O}_F^*/\mathcal{O}_F^{*2} = \mathcal{O}_K^*/\mathcal{O}_K^{*2}$$

(Up to square class, every unit in $\mathcal{O}_K^*$ can be regarded as a unit in $\mathcal{O}_F^*$.)

Now, for $1 \neq u \in \mathcal{O}_F^*/\mathcal{O}_F^{*2} = \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, we want to see $K(\sqrt{u})$ is ramified over K. First, by considering the discriminant of K over F again, the only possible ramified finite primes are dyadic. If no dyadic prime ideal in $\mathcal{O}_K$ ramifies in $K(\sqrt{u})$, then, since no dyadic prime ideal in $\mathcal{O}_F$ ramifies in $K =$, it follows that no dyadic prime ideal in $\mathcal{O}_F$ can ramify in $K(\sqrt{u})$. But $K(\sqrt{u}) = F(\sqrt{u}, \sqrt{-\sigma})$, thus no dyadic prime ideal in $\mathcal{O}_F$ ramifies in $F(\sqrt{u})$, contradicting Lemma 6.3. □

Corollary 6.6. *Under the hypothesis above, every element in $E \subset K^*/K^{*2}$ can be uniquely written as*

$$ud \quad \textit{with } u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2} \textit{ and } d \in R\ .$$

Proof. It follows from Lemma 2.5, 2.7 and $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap R = \{1\}$. □

Bender's Identity *Let K be an extension of a local field k. Suppose $\lambda \in K$ and $b \in k$. Then*

$$(\lambda, b)_K = (\mathcal{N}_{K/k}(\lambda), b)_k$$

where $(,)_K$ and $(,)_k$ are the Hilbert symbols over K and k, respectively, and $\mathcal{N}_{K/k}$ is the local norm [Bender].

We obtain totally complex K in the class $\mathcal{K}_0$ as follows.

Proposition 6.7. *Let F be a totally real field containing units with independent signs. If $\sigma \in F^*/F^{*2}$ is totally positive and all dyadic prime ideals in $\mathcal{O}_F$ are inert (remain primes) in the CM-extension $K = F(\sqrt{-\sigma})$, then*

$$c_K = r_F, \quad g_2(K) = g_2(F), \quad \textit{and} \quad K \in \mathcal{K}_0 \, .$$

Proof. By Corollary 6.6, every element in $E \subset K^*/K^{*2}$ can be uniquely written as

$$ud \quad \text{with } u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2} \text{ and } d \in R \, .$$

We already know $R \subset \Delta$. Thus to get $E = \Delta$ we only have to show that, for $u,\ v \in \mathcal{O}_F^*/\mathcal{O}_F^{*2} = \mathcal{O}_K^*/\mathcal{O}_K^{*2}$,

$$(u, v)_{\mathfrak{D}} = +1 \quad \text{at all dyadic prime ideals } \mathfrak{D} \subset \mathcal{O}_K.$$

If $\mathfrak{D} \subset \mathcal{O}_K$ is a dyadic prime ideal, then

$$\mathfrak{D} = D\mathcal{O}_K \quad \text{for a unique dyadic prime ideal } D \subset \mathcal{O}_F.$$

Since $u,\ v \in \mathcal{O}_F^*$, we see, by Bender's identity for the Hilbert symbol,

$$(u, v)_{\mathfrak{D}} = (u, \mathcal{N}_{\mathfrak{D}}(v))_D = (u, v^2)_D = +1$$

where $\mathcal{N}_{\mathfrak{D}} \colon K_{\mathfrak{D}}^* \to F_D^*$ is the local norm. □

Corollary 6.8. *If $K \in \mathcal{K}_0$ and $level K = 2$, then*

there is a totally complex quadratic extension $L \in \mathcal{K}_0$ of K with

$$c_L = 1, \quad g_2(L) = 1, \quad \textit{and} \quad W(\mathcal{O}_K) \cong W(\mathcal{O}_L)\ .$$

Proof. For $K \in \mathcal{K}_0$ we have $\#W(\mathcal{O}_K) = 2^N$ with

$$N = c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K \geqslant 2.$$

Choose a positive square free rational integer $\sigma \equiv 3 \pmod 8$ divisible by exactly $N-1$ distinct rational primes, and set $L = \mathbb{Q}(\sqrt{-\sigma})$. Since $-\sigma \equiv 3 \pmod 8$, the only dyadic prime (2) of $\mathbb{Q}$ is inert in L, and $level L \leqslant 2$. But since $\sqrt{-1}$ can not be in $L = \mathbb{Q}(\sqrt{-\sigma})$, we must have $level L = 2$. Then, by Proposition 6.7, we have $L \in \mathcal{K}_0$ with

$$c_L = r_{\mathbb{Q}} = 1 \ \text{ and } \ g_2(L) = g_2(\mathbb{Q}) = 1.$$

By the Theorem of Gauss (see [B-S, Theorem 8, p.247]), we have $2\text{-}rk\,\mathcal{C}_L = N-2$. So, we have $K,\ L \in \mathcal{K}_0$, $level K = level L = 2$, and $c_K + g_2(K) + 2\text{-}rk\,\mathcal{C}_K = c_L + g_2(L) + 2\text{-}rk\,\mathcal{C}_L = N$. Therefore, by Theorem 4.2, we have $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$. □

Now, we want to use CM-extensions to produce totally complex number fields $K \in \mathcal{K}_1$. Assume that F is totally real and contains units with independent signs. If $1 \neq u \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}$, by Lemma 6.2 there is at least one real infinite prime $\mathfrak{p}_\infty$ at which u is negative. Then there is a unit $v \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}$ which is negative only at $\mathfrak{p}_\infty$ and positive at all other real infinite primes. So, $(u,v)_{\mathfrak{p}_\infty} = -1$ and $(u,v)_{Q_\infty} = 1$ for any other infinite primes Q_∞. Thus, by the Hilbert reciprocity law, there must be at least one dyadic prime ideal $D \subset \mathcal{O}_F$ for which

$$(u,v)_D = -1.$$

Definition 6.9. Let F be a totally real field containing units with independent signs. A dyadic prime ideal $D \subset \mathcal{O}_F$ is *effective* if

$$(u, v)_{\mathfrak{D}} = -1 \quad \text{for some pair } u,\ v \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}.$$

Lemma 6.10. *Let F be a totally real field containing units with independent signs and select an effective dyadic prime ideal $D_0 \subset \mathcal{O}_F$. Let $K = F(\sqrt{-\sigma})$ with totally positive $\sigma \in F^*/F^{*2}$ and assume*

1. *no dyadic prime ideal of $\mathcal{O}_F$ ramifies in K;*
2. *the effective dyadic prime ideal D_0 splits ;*
3. *all other effective dyadic prime ideals in $\mathcal{O}_F$, if any, are inert.*

Then $K \in \mathcal{K}_1$.

Proof. Let us write $D_0\mathcal{O}_K = \mathfrak{D}_1\mathfrak{D}_2$ for a conjugate pair of dyadic prime ideals in $\mathcal{O}_K$. From Corollary 6.6 we know elements in $E \subset K^*/K^{*2}$ can be written as ud with $u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$ and $d \in R \subset \Delta$. For any $u,\ v \in \mathcal{O}_F^*/\mathcal{O}_F^{*2} = \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ we can say $(u, v)_{\mathfrak{D}} = +1$ for all dyadic prime ideals $\mathfrak{D} \subset \mathcal{O}_K$, $\mathfrak{D} \neq \mathfrak{D}_1$ nor $\mathfrak{D}_2$. However, by Bender's identity, we have $(u, v)_{\mathfrak{D}_1} = (u, v)_{\mathfrak{D}_2} = (u, v)_{D_0}$. Thus we may regard $[u, v] \in G_2$ simply as $(u, v)_{\mathfrak{D}_1} = \pm 1$. But D_0 was effective, so it's possible to have $(u, v)_{\mathfrak{D}_1} = (u, v)_{\mathfrak{D}_2} = (u, v)_{D_0} = -1$. Since $\mathfrak{M}^2$ is a subgroup of G_2 and is nontrivial, we can see $\mathfrak{M}^2$ is cyclic of order 2. Hence $K \in \mathcal{K}_1$. □

So far we only know $0 < 2\text{-}rk(E/\Delta) \leq c_K = r_F$ in general. Here's an example with $2\text{-}rk(E/\Delta) = c_K = r_F$.

Proposition 6.11. *Assume F is a totally real field containing units with independent signs for which $g_2(F) = 1$. Let $\sigma \in F^*/F^{*2}$ be a totally positive element for*

which the unique dyadic prime ideal D_0 in $\mathcal{O}_F$ splits in $K = F(\sqrt{-\sigma})$. Then we have the following

(1) $K \in \mathcal{K}_1$ *with* $2\text{-}rk(E/\Delta) = c_K = r_F$.

(2) $levelK = 2 \Leftrightarrow [F\colon \mathbb{Q}] = r_F \equiv 0 \pmod 2$.

(3) $levelK = 4 \Leftrightarrow [F\colon \mathbb{Q}] = r_F \equiv 1 \pmod 2$.

Proof. We know that there must be at least one effective dyadic prime ideal in $\mathcal{O}_F$. So the unique dyadic ideal D_0 must be effective. Then, By Lemma 6.10, we have $K \in \mathcal{K}_1$.

To show $2\text{-}rk(E/\Delta) = c_K$ we claim first that $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap \Delta = \{1\}$. Let's write $D_0\mathcal{O}_K = \mathfrak{D}_1\mathfrak{D}_2$ with distinct dyadic primes $\mathfrak{D}_1,\ \mathfrak{D}_2$ in $\mathcal{O}_K$. Then we have $(u,v)_{\mathfrak{D}_1} = (u,v)_{\mathfrak{D}_2} = (u,v)_{D_0}$ for any $u,\ v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$. Since D_0 is the 'unique' dyadic prime ideal and is effective, for any $1 \neq u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$, there's a $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$ such that $(u,v)_{D_0} = -1$. Thus any $1 \neq u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ cannot be in Δ. From Corollary 6.6 we can write $E = R \times \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. Note that we always have $R \subset \Delta$. Thus we have $R \subset \Delta \subset E = R \times \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ and $\Delta \cap \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \{1\}$. Hence we have

$$2\text{-}rk(E/\Delta) = 2\text{-}rk(\mathcal{O}_K^*/\mathcal{O}_K^{*2}) = c_K = 2\text{-}rk(\mathcal{O}_F^*/\mathcal{O}_F^{*2}) = r_F.$$

The second and the third assertions follow from Lemma 5.3 on page 49. □

There may also be noted in Proposition 6.11 that $R = \Delta$. In fact, we can see more generally that $R = \Delta$ if all effective dyadic prime ideals in $\mathcal{O}_F$ split in $K = F(\sqrt{-\sigma})$ and no dyadic prime ideal in $\mathcal{O}_F$ ramifies.

Corollary 6.12. *Let F be a totally real field containing units with independent signs for which $g_2(F) \geqslant 1$. and let $K = F(\sqrt{-\sigma})$ for a totally positive element $\sigma \in F^*/F^{*2}$. Assume that*

1. *no dyadic prime ideal of $\mathcal{O}_F$ ramifies in K;*

2. *all effective dyadic prime ideals in $\mathcal{O}_F$ split in K.*

Then we have $R = \Delta$.

Proof. It's enough to show $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap \Delta = \{1\}$. First note that, for any effective dyadic prime ideal D in $\mathcal{O}_F$ which can be written as $D\mathcal{O}_K = \mathfrak{D}_1\mathfrak{D}_2$ with distinct dyadic primes $\mathfrak{D}_1,\ \mathfrak{D}_2$ in $\mathcal{O}_K$, we have $(u,v)_{\mathfrak{D}_1} = (u,v)_{\mathfrak{D}_2} = (u,v)_D$ for any $u,\ v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$. If there is $1 \neq u_0 \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap \Delta$, then $[u_0, v] = \mathbf{1} \in G_2$ for all $v \in E$, and hence for all $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} \subset E$. Thus, $(u_0,v)_{\mathfrak{D}} = 1$ for all dyadic prime ideals $\mathfrak{D}$ in $\mathcal{O}_K$ and for all $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. Specially, $(u_0,v)_D = (u_0,v)_{\mathfrak{D}_1} = (u_0,v)_{\mathfrak{D}_2} = 1$ for all $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2} = \mathcal{O}_F^*/\mathcal{O}_F^{*2}$. which contradicts that, for any element $1 \neq u \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}$, we can always find an element $v \in \mathcal{O}_F^*/\mathcal{O}_F^{*2}$ and a dyadic prime ideal D in $\mathcal{O}_F$ such that $(u,v)_D = -1$. □

7. Conclusions

For a totally complex number field K, we have three numerical invariants of the isomorphism class of $W(\mathcal{O}_K)$:

- $level K = 1,\ 2,$ or 4
- $c_K + g_2(K) + 2\text{-}rk\, \mathcal{C}_K$
- $0 \leq 2\text{-}rk(E/\Delta) \leq c_K$.

Then we have

- the subgroup $\Delta \subset E$ (and $R \subset \Delta \subset E$) ,
- the essential $\gamma = \nu(-1) \in E/\Delta$,
- the characteristic ideal J with $\mathfrak{M}^2 \subset I^2 \cap W(\mathcal{O}_K) \subset J \subset \mathfrak{M} \subset W(\mathcal{O}_K)$
- $\phi(\alpha, \beta)\colon E/\Delta \times E/\Delta \to \mathfrak{M}^2 \subset J$.

We know that $W(\mathcal{O}_K)$ is, at least, a finite local ring with the unique max ideal $\mathfrak{M}$. For the class $\mathcal{K}_0$, that is, $\Delta = E$, we can settle the isomorphism question using only $level K$ and $\#W(\mathcal{O}_K)$. For $K \in \mathcal{K}_1$, that is, $2\text{-}rk(\mathfrak{M}^2, +) = 1$, we have a reasonable reduction to the classification of the inner product space over $\mathbb{F}_2$ given by $(E/\Delta, \phi)$ and $\gamma = \nu(-1) \in E/\Delta$.

We point out that we can surely have $W(\mathcal{O}_K) \cong W(\mathcal{O}_L)$ even when $W(K) \ncong W(L)$. In fact, $W(\mathcal{O}_K) \cong (\mathcal{O}_L)$ need not preserve degrees over $\mathbb{Q}$ nor the number of dyadic primes.

References

[Bender] E. A. Bender, *A Lifting Formula for the Hilbert Symbol*, Proceeding of the AMS **40**, No.1, Sep. 1973. 58

[B-S] Z. I. Borevich and I. R.Shafarevich, *Number Theory*, Academic Press, New York and London, 1966. 54, 59

[Co] P. E. Conner, *Notes on the Witt Classification of Hermitian Innerproduct Spaces over a Ring of Algebraic Integers*, University of Texas Press, Austin and London, 1979. 13, 14

[C-H] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Series in Pure Math, vol. 8, World Scientific, 1988. 13, 19, 55, 57

[C-P] P. E. Conner and R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, Series in Pure Math, vol. 2, World Scientific, 1984. 7, 23

[Cz] A. Czogała, *On integral Witt equivalence of algebraic number fields*, Actra Math. **4** (1996), 7-20. 1

[Kap] I. Kaplansky, *Linear Algebra and Geometry*, Chelsea Publishing Company, New York, 1974. 50

[Lam] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973. 5, 36

[Lang] S. Lang, *Algebraic Number Theory*, 2nd Edition, GTM **110**, Springer-Verlag, New York, 1994.

[M-H] J. W. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, Berlin, 1973. 1, 6, 8, 9, 11, 16, 17

[P-S-C-L] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witt With Global Fields*, Contemp.Math. **155** (1994), 365-287. 1

[Sh] P. Shastri, *Witt groups of algebraic integers*, J. of Number Theory **30** (1988), 243-266. 1

Vita

Changheon Kang was born on March 25, 1968, in Cheju City, Korea. He finished his undergraduate studies in mathematics at Korea University in Feburary 1990. He earned a Master of Science degree in mathematics from Korea University in Feburary 1994. In August 1995, he came to Louisiana State University to pursue graduate studies in mathematics. He earned a Master of Science degree in mathematics from Louisiana State University in May 1997. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2002.