Doctoral Thesis

Characteristic polynomials of isometries of even unimodular lattices and dynamical degrees of automorphisms of K3 surfaces

（偶ユニモジュラー格子の等長変換の固有多項式と
K3 曲面の自己同型の力学的次数）

Yuta TAKADA

Department of Mathematics,
Graduate School of Science, Hokkaido University

March, 2024

Contents

0 Introduction

This thesis is concerned with characteristic polynomials of isometries of even unimodular lattices and dynamical degrees of automorphisms of K3 surfaces. In recent years, significant progress has been made in these areas by works of E. Bayer-Fluckiger and L. Taelman [3], and of Bayer-Fluckiger [5, 6, 7]. This thesis consists of a detailed and refined version of the author's article [45] and a description of subsequent developments thereafter, which were inspired by their works. In order to make the main theory self-contained, it also includes a survey of prior research as well as preliminaries from algebraic number theory.

In 1999, S. Cantat [12] showed that if a compact complex surface Σ admits an automorphism with positive entropy then Σ is a torus, a K3 surface, an Enriques surface, or a rational surface. Since around that time, the question of which number can be realized as the entropy of an automorphism of a compact complex surface has been considered. This thesis deals with the case of K3 surfaces.

A *K3 surface* is a compact complex surface Σ such that its canonical bundle is trivial and $\dim_{\mathbb{C}}(H^{0,1}(\Sigma)) = 0$. For any K3 surface Σ, the second cohomology group $H^2(\Sigma, \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank 22, and the intersection form makes $H^2(\Sigma, \mathbb{Z})$ an even unimodular lattice of signature $(3, 19)$. We refer to an even unimodular lattice of signature $(3, 19)$ as a *K3 lattice*. It is known that such a lattice is unique up to isomorphism. Let ϕ be an automorphism of a K3 surface Σ. Then, the induced homomorphism $\phi^* : H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma, \mathbb{Z})$ is an isometry of the lattice $H^2(\Sigma, \mathbb{Z})$. Let $d(\phi)$ denote the spectral radius of $\phi^* : H^2(\Sigma, \mathbb{C}) \to H^2(\Sigma, \mathbb{C})$:

$$d(\phi) := \max\{|\mu| \mid \mu \in \mathbb{C} \text{ is an eigenvalue of } \phi^* : H^2(X, \mathbb{C}) \to H^2(X, \mathbb{C})\}.$$

We refer to this value $d(\phi)$ as the *dynamical degree* of ϕ. It is known that the entropy of ϕ is given by $\log d(\phi)$. In this thesis, we handle dynamical degrees rather than entropy, although they are essentially the same thing (in our situation). It is also known that the dynamical degree of a K3 surface automorphism is 1 or a *Salem number*, that is, a real algebraic number $\beta > 1$ such that it is conjugate to β^{-1} and all of its conjugates other than β and β^{-1} have absolute value 1. Our concern is to know which Salem number can be realized as the dynamical degree of an automorphism of a K3 surface.

In connection with the study of automorphisms of K3 surfaces, B.H. Gross and C.T. McMullen [18] raised the following purely lattice-theoretic question.

Question 0.1. *Which polynomial can be realized as the characteristic polynomial of an isometry of an even unimodular lattice with a prescribed signature?*

We deal with the case where the isometry in Question 0.1 is imposed to be semisimple (as a linear transformation). There are two main reasons to do so. One is to avoid complexity of the description. The other concerns its application: the induced homomorphism $\phi^* : H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma, \mathbb{Z})$ of any automorphism ϕ of a K3 surface Σ is semisimple if $d(\phi) > 1$.

Let r and s be non-negative integers. It is known that $r \equiv s \bmod 8$ if (r, s) is the signature of an even unimodular lattice. Let $F(X) \in \mathbb{Z}[X]$ be a monic polynomial with $F(0) \neq 0$. We define a monic polynomial $F^*(X) \in \mathbb{Q}[X]$ by $F^*(X) := F(0)^{-1} X^{\deg F} F(X^{-1})$, and say that F is $*$-*symmetric* if $F^* = F$. In this case, the constant term $F(0)$ is 1 or -1, so we say that F is $+1$-*symmetric* or -1-*symmetric* according to the value $F(0)$. Suppose that F is the characteristic polynomial of a semisimple isometry of an even unimodular lattice of signature (r, s). Then F is a $*$-symmetric polynomial of even degree. Moreover

$$r, s \geq m(F) \text{ and if } F(1)F(-1) \neq 0 \text{ then } r \equiv s \equiv m(F) \bmod 2, \tag{Sign}$$

where $m(F)$ is the number of roots of F whose absolute values are greater than 1 counted with multiplicity; and

$$|F(1)|, |F(-1)| \text{ and } (-1)^{(\deg F)/2}F(1)F(-1) \text{ are all squares.} \qquad \text{(Square)}$$

Gross and McMullen speculated that these necessary conditions for F to be realized as a characteristic polynomial are also sufficient when F is irreducible, and they showed that if F is irreducible and the assumption (Square) is replaced by the more stronger assumption $(-1)^{(\deg F)/2}F(1)F(-1) = 1$, then these are sufficient. Afterwards, Bayer-Fluckiger and Taelman [3] proved that the speculation is correct by using a local-global theory.

Bayer-Fluckiger [5, 6, 7] proceeded to the case where the polynomial F is reducible and $+1$-symmetric. In this case, the conditions (Sign) and (Square) are not sufficient as pointed out in [18]. She showed that the condition (Square) is necessary and sufficient for the existence of an even unimodular lattice over $\mathbb{Z}_p$ having a semisimple isometry with characteristic polynomial F for every prime p, where $\mathbb{Z}_p$ is the ring of p-adic integers. On the other hand, the condition (Sign) is obtained by considering over $\mathbb{R}$. Hence, we can say that these two conditions are local. For a $+1$-symmetric polynomial F with (Sign) and (Square), Bayer-Fluckiger gave a necessary and sufficient condition for F to be realized as the characteristic polynomial of a semisimple isometry of an even unimodular lattice over $\mathbb{Z}$ of signature (r, s), by describing the local-global obstruction. These results are reformulated and extended to the case where F is $*$-symmetric, which covers the -1-symmetric case, in the author's article [45]. We explain the local-global obstruction in the following.

We begin by defining an invariant of an isometry of an inner product space over $\mathbb{R}$, called the *index*. Let t be an isometry of an inner product space V over $\mathbb{R}$ of signature (r, s), and let $F \in \mathbb{R}[X]$ be its characteristic polynomial. Then V decomposes as $V = \sum_f V(f; t)$, where $V(f; t) := \{v \in V \mid f(t)^N.v = 0 \text{ for some } N \in \mathbb{Z}_{\geq 0}\}$ and f ranges over the irreducible factors of F in $\mathbb{R}[X]$. Let $I(F; \mathbb{R})$ denote the set of $*$-symmetric irreducible factors of F. The *index* idx_t of t is the map from $I(F; \mathbb{R})$ to $\mathbb{Z}$ defined by $\mathrm{idx}_t(f) = r_f - s_f$, where (r_f, s_f) is the signature of $V(f; t)$.

For a $*$-symmetric polynomial F and non-negative integers r, s with $r+s = \deg(F)$, we write $\mathrm{Idx}(r, s; F)$ for the set of maps $I(F; \mathbb{R}) \to \mathbb{Z}$ expressed as idx_t for some semisimple isometry t of an inner product space V of signature (r, s), with characteristic polynomial F. Each map in $\mathrm{Idx}(r, s; F)$ is referred to as an *index map* (see Definition 7.27 and Theorem 7.28). Furthermore, we refer to an isometry with characteristic polynomial F and with index $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ as an $(F, \mathfrak{i})$-*isometry* for short. As a detailed version of Question 0.1, we will investigate when the following condition holds for a given index map $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$.

> There exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry. (♠)

Let Γ be an infinite cyclic group, and let $\mathbb{Q}[\Gamma]$ denote the group algebra of Γ over $\mathbb{Q}$. We next define a $\mathbb{Q}[\Gamma]$-module for a polynomial. Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial. For a factor f of F, we write m_f for the multiplicity of f in F. Let $I(F; \mathbb{Q})$ denote the set of $*$-symmetric irreducible factors of F, and $I_2(F; \mathbb{Q})$ the set of non-$*$-symmetric irreducible factors of F in $\mathbb{Q}[X]$. Furthermore, we put $I_1(F; \mathbb{Q}) = I(F; \mathbb{Q}) \setminus \{X - 1, X + 1\}$ (see Definitions 7.6 and 7.8 for the meaning of subscripts). Then F can be expressed as

$$F(X) = \prod_{f \in I(F;\mathbb{Q})} f(X)^{m_f} \times \prod_{\{g, g^*\} \subset I_2(F;\mathbb{Q})} (g(X)g^*(X))^{m_g}$$

or

$$F(X) = (X-1)^{m_+}(X+1)^{m_-} \times \prod_{f \in I_1(F;\mathbb{Q})} f(X)^{m_f} \times \prod_{\{g, g^*\} \subset I_2(F;\mathbb{Q})} (g(X)g^*(X))^{m_g},$$

where $m_\pm := m_{X\mp 1}$. For a factor f which is in $I(F;\mathbb{Q})$ or of the form gg^* for some $g \in I_2(F;\mathbb{Q})$, we define $M^f := (\mathbb{Q}[X]/(f))^{m_f}$, and

$$M := M^+ \times M^- \times \prod_{f \in I_1(F;\mathbb{Q})} M^f \times \prod_{\{g,g^*\} \subset I_2(F;\mathbb{Q})} M^{gg^*},$$

where $M^\pm := M^{X\mp 1}$. Let $\alpha : M \to M$ be the linear transformation defined by the multiplication by X. Then, it is a semisimple transformation with characteristic polynomial F. Furthermore the $\mathbb{Q}$-algebra M can be seen as a $\mathbb{Q}[\Gamma]$-module by the action determined by $\tau \mapsto \alpha$, where τ is a generator of Γ. In this case, we refer to M as the *associated* $\mathbb{Q}[\Gamma]$*-module of* F with transformation α.

A key idea in tackling Question 0.1 is to consider when there exists an inner product $b : M \times M \to \mathbb{Q}$ on the $\mathbb{Q}$-vector space M such that α becomes an isometry having a prescribed index $\mathfrak{i}$ and the inner product space (M, b) contains an α-stable even unimodular lattice. By reinterpreting Question 0.1 as an existence problem for inner products in this way, a local-global argument works well.

Let $\mathcal{V}$ denote the set of all places of $\mathbb{Q}$. In the following, we fix the following data: non-negative integers r and s with $r \equiv s \bmod 8$; a $*$-symmetric polynomial $F \in \mathbb{Z}[X]$ with the conditions (Sign) and (Square); and an index map $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$. We write $I = I(F;\mathbb{Q})$, $I_1 = I_1(F;\mathbb{Q})$, and $I_2 = I_2(F;\mathbb{Q})$ for short. Let M be the associated $\mathbb{Q}[\Gamma]$-module with transformation α. For each place $v \in \mathcal{V}$, we define $M_v := M \otimes \mathbb{Q}_v$. Similarly $M_v^f := M^f \otimes \mathbb{Q}_v$ for f which is in I or of the form gg^* for some $g \in I_2$. Then

$$M_v = M_v^+ \oplus M_v^- \oplus \bigoplus_{f \in I_1} M_v^f \oplus \bigoplus_{\{g,g^*\} \subset I_2} M_v^{gg^*}$$

as $\mathbb{Q}_v[\Gamma]$-modules, where $\alpha : M \to M$ is extended to a $\mathbb{Q}_v$-linear transformation on M_v in a unique way. For each $v \in \mathcal{V}$, we consider the following three properties (P1)–(P3) of an inner product $b_v : M_v \times M_v \to \mathbb{Q}_v$ on M_v. The first property is that

$$\alpha : M_v \to M_v \text{ is an isometry with respect to } b_v. \tag{P1}$$

Assume that b_v has the property (P1). The second property is that

$$\begin{aligned} &\text{if } v \neq \infty \text{ then there exists an } \alpha\text{-stable even unimodular lattice over } \mathbb{Z}_v \text{ on } (M_v, b_v), \text{ and} \\ &\text{if } v = \infty \text{ then the isometry } \alpha \text{ of } (M_\infty, b_\infty) \text{ has index } \mathfrak{i}. \end{aligned} \tag{P2}$$

Let $b_v|_{M_v^\pm}$ denote the inner product on $M_v^\pm$ obtained by restricting b_v to $M_v^\pm \times M_v^\pm \subset M_v \times M_v$. The last property is that

$$\det(b_v|_{M_v^\pm}) = \begin{cases} (-1)^{(m_\pm - \mathrm{i}(X\mp 1))/2} \, |F_1(\pm 1) F_2(\pm 1)| & \text{if } m_+ \text{ is even} \\ (-1)^{(m_\pm - \mathrm{i}(X\mp 1))/2} \, 2|F_1(\pm 1) F_2(\pm 1)| & \text{if } m_+ \text{ is odd} \end{cases} \quad \text{in } \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}, \tag{P3}$$

where det is the determinant (that is, the square class of the determinant of a Gram matrix, see Definition 4.5), and $F_i(X) = \prod_{f \in I_i} f(X)^{m_f}$ for $i = 1, 2$. We write $\mathcal{B}_\mathfrak{i}$ for the set of families $\{b_v\}_{v \in \mathcal{V}}$ of inner products on M_v such that each b_v has the properties (P1)–(P3) and $\#\{v \in \mathcal{V} \mid \mathrm{hw}_v(b_v|_{M_v^f}) \neq 0\}$ is finite for all $f \in I$, where hw_v is the Hasse-Witt invariant (taking values in $\mathbb{Z}/2\mathbb{Z}$), see Definitions 4.30 and 4.58. The conditions (Sign) and (Square) guarantee that $\mathcal{B}_\mathfrak{i}$ is not empty.

If b is an inner product on M such that $\alpha : M \to M$ becomes an isometry having index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice over $\mathbb{Z}$, then the family $\{b \otimes \mathbb{Q}_v\}_{v \in \mathcal{V}}$ of

inner products $b \otimes \mathbb{Q}_v : M_v \times M_v \to \mathbb{Q}_v$ obtained by localizations belongs to $\mathcal{B}_{\mathfrak{i}}$. The local-global principle for the existence of such an inner product on M is described as the equivalence of the following two conditions (Theorem 9.7):

There exists an inner product b on M such that $\alpha : M \to M$ becomes an isometry having index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice over $\mathbb{Z}$. (♣)

There exists a family $\{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}}$ such that $\sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) = 0$ for any $f \in I$. (♢)

We remark that the former condition (♣) is equivalent to (♠). Let us rephrase the latter condition (♢) further. Let $C(I)$ denote the $\mathbb{Z}/2\mathbb{Z}$-module consisting of all maps from I to $\mathbb{Z}/2\mathbb{Z}$, that is, $C(I) := \{\gamma : I \to \mathbb{Z}/2\mathbb{Z}\} = (\mathbb{Z}/2\mathbb{Z})^{\oplus I}$. Moreover, we define a map $\eta : \mathcal{B}_{\mathfrak{i}} \to C(I)$ by

$$\eta(\{b_v\}_v)(f) = \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) \in \mathbb{Z}/2\mathbb{Z} \quad (\{b_v\}_v \in \mathcal{B}_{\mathfrak{i}},\ f \in I).$$

Under this notation, the condition (♢) can be rephrased as the one that there exists a family $\{b_v\}_v \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\{b_v\}_v) = \mathbf{0}$, where $\mathbf{0} \in C(I)$ is the zero map. For a prime p and a monic polynomial $f \in \mathbb{Z}[X]$, we define

$$\overline{I(f; \mathbb{Q}_p)} := \left\{ \bar{h} \in \mathbb{F}_p[X] \;\middle|\; \begin{array}{l} \bar{h} \text{ is irreducible, and there exists a } *\text{-symmetric} \\ \text{irreducible factor of } f \text{ in } \mathbb{Z}_p[X] \text{ whose reduction} \\ \text{modulo } p \text{ is divisible by } \bar{h} \text{ in } \mathbb{F}_p[X] \end{array} \right\}.$$

Moreover, for two monic polynomials f and $g \in \mathbb{Z}[X]$, we define a set $\Pi(f, g)$ of primes by

$$\Pi(f, g) := \{p : \text{prime} \mid \overline{I(f; \mathbb{Q}_p)} \cap \overline{I(g; \mathbb{Q}_p)} \neq \emptyset\}.$$

For simplicity of explanation, we assume that each of the multiplicities m_+ and m_- of $X-1$ and $X+1$ is 0 or at least 3. Let $\sim$ be the equivalence relation on I generated by the binary relation $\{(f, g) \in I \times I \mid \Pi(f, g) \neq \emptyset\}$, and let Ω be the submodule $\{c \in C(I) \mid\ c(f) = c(g) \text{ if } f \sim g\ \}$ of $C(I)$. It will be shown that the homomorphism

$$\Omega \to \mathbb{Z}/2\mathbb{Z},\ c \mapsto \textstyle\sum_{f \in I} \eta(\{b_v\}_v)(f) \cdot c(f)$$

is defined independently of the choice of the family $\{b_v\}_v \in \mathcal{B}_{\mathfrak{i}}$. This homomorphism is called the *obstruction map* for $(F, \mathfrak{i})$ and denoted by $\mathrm{ob}_{\mathfrak{i}} : \Omega \to \mathbb{Z}/2\mathbb{Z}$. The submodule $\Omega \subset C(I)$ is called the *obstruction group* for $(F, \mathfrak{i})$ (it does not depend on $\mathfrak{i}$ under the current assumption on m_+ and m_-). It is obvious that if there exists a family $\{b_v\}_v \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\{b_v\}_v) = \mathbf{0}$ then

$$\text{the obstruction map } \mathrm{ob}_{\mathfrak{i}} : \Omega \to \mathbb{Z}/2\mathbb{Z} \text{ is the zero map.} \quad (♡)$$

Our first main theorem is as follows.

Theorem A. *Let r, s be non-negative integers with $r \equiv s \bmod 8$, $F \in \mathbb{Z}[X]$ a $*$-symmetric polynomial of degree $r+s$ with the conditions* (Sign) *and* (Square)*, and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ an index map. Assume that each of m_+ and m_- is* 0 *or at least* 3*. The conditions* (♠)*,* (♣)*,* (♢)*, and* (♡) *are all equivalent.*

We prove this theorem without the assumption on m_+ and m_-, see Theorem 9.25. In this case, the definition of the set $\Pi(f, g)$ (and hence that of the equivalence relation $\sim$ on I) needs to be modified. The equivalence (♠) $\Leftrightarrow$ (♡) was first proved by Bayer-Fluckiger in [6], under the assumption that F is $+1$-symmetric. However, the first proof did not take account of subtle conditions for obstruction. On the framework established by her, the author [45] modified

the definition of obstruction, and moreover, extended the theorem to the case where F is $*$-symmetric, which covers the -1-symmetric case, mainly by careful analysis at the prime 2, see also Remark 9.26. This thesis also gives a systematic way to compute obstruction.

Let us revisit the problem of dynamical degrees of K3 surface automorphisms. As mentioned earlier, for an automorphism ϕ of a K3 surface Σ, the induced homomorphism ϕ^* is an isometry of the K3 lattice $H^2(\Sigma, \mathbb{Z})$. Conversely, as a consequence of two fundamental theorems for K3 surfaces, the Torelli theorem and surjectivity of the period mapping, an isometry of a K3 lattice with some additional conditions is realized as the induced homomorphism of an automorphism of a K3 surface. We recall that if an automorphism ϕ of a K3 surface Σ has dynamical degree greater than 1 then it is a Salem number. More strongly, in this case, the induced homomorphism $\phi^* : H^2(\Sigma, \mathbb{C}) \to H^2(\Sigma, \mathbb{C})$ is semisimple, and its characteristic polynomial is of the form $F = SC$, where S is the minimal polynomial of a Salem number and C is a product of cyclotomic polynomials. So, we approach the problem of dynamical degrees by describing when a K3 lattice admits a semisimple isometry having such a polynomial as the characteristic polynomial through Theorem A and computations of obstruction.

We say that a Salem number β is *projectively* (resp. *nonprojectively*) *realizable* if there exists an automorphism of a projective (resp. nonprojective) K3 surface with dynamical degree β. Note that the degree of any Salem number (that is, the degree of its minimal polynomial over $\mathbb{Q}$) is even. If a Salem number β is projectively realizable then $2 \leq \deg(\beta) \leq 20$; and if β is nonprojectively realizable then $4 \leq \deg(\beta) \leq 22$. The nonprojective case is more tractable than the projective case (see Proposition 13.16), and our second main theorem is as follows.

Theorem B (Theorem 13.14)**.** *Let β be a Salem number of degree d with $4 \leq d \leq 22$, and S its minimal polynomial. Let $\mathcal{C}_{10}$ and $\mathcal{C}_{18}$ be the sets consisting of integers defined by*

$$\mathcal{C}_{10} := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 21, 22, 24, 28, 30, 36, 42\},$$
$$\mathcal{C}_{18} := \{1, 2, 3, 4, 6, 12\}.$$

(i) *Suppose that $d = 22$. Then β is nonprojectively realizable if and only if $|S(1)|$ and $|S(-1)|$ are squares.*

(ii) *Suppose that $d = 4, 6, 8, 12, 14, 16$, or 20. Then β is nonprojectively realizable.*

(iii) *Suppose that $d = 10$ or 18. Then β is nonprojectively realizable if and only if there exists $l \in \mathcal{C}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$. Here Φ_l is the l-th cyclotomic polynomial.*

The proof of (i) was given by Bayer-Fluckiger and Taelman in [3] for the first time. The assertion (ii) was proved by Bayer-Fluckiger [6, 7] for $d = 4, 6, 8, 12, 14, 16$, and by the author [45] for $d = 20$, see also Remark 13.15. Although a close result can be found in [7], the assertion (iii) appears for the first time in this thesis. This thesis gives the proofs of all assertions (i)–(iii), in a consistent manner. We also give a brief survey of the problem of which number can be realized as the dynamical degree of an automorphism of a compact complex surface, not only of a K3 surface, in §13.4.

The organization of this thesis is as follows. We review basic facts on algebraic number theory in Chapter I. Chapter II summarizes the classical theory of inner products. Inner products over a field are treated in §4, and over a Dedekind domain in §5. Chapters I and II are prepared so that the main theory in Chapter III is self-contained. These two chapters would be helpful for some experts in dynamical systems who are not familiar with algebraic number theory.

Chapter III is the main part of this thesis. In §6, we introduce equivariant Witt groups for inner product spaces. By using that terminology, we can describe when an inner product space over a discrete valuation field contains a unimodular lattice, in a manner compatible with a group

action. In §7, we study isometries of inner product spaces over an arbitrary field, and over $\mathbb{R}$. We deal with the localized version of Question 0.1 in §8, and give the proof of a general version of Theorem A in §9. Sections 10 and 11 present a systematic way to compute obstruction.

Chapter IV discusses the application of results established in Chapter III to dynamical degrees of K3 surface automorphisms. After making a minimal explanation of K3 surfaces in §12, we prove Theorem B in §13.

Acknowledgments I would like to express my gratitude to my supervisor, Professor Katsunori Iwasaki, for his unfailing guidance over the past five years. I have learned not only mathematics but also many other things, such as the attitude as a researcher and the way to write documents. Thanks to his invitation to join his work on dynamics on K3 surfaces, I was able to take the first step as a researcher. During the joint work, he showed me the tenacity for problems and calculations, which I lacked. The theme of this thesis was encountered in the joint work.

I am also grateful to Professor Eva Bayer-Fluckiger for her kind replies to my questions and for invaluable comments. This work is inspired by her work. It is honor to have a direct discussion with the person who established the foundation of the theory in this thesis.

I would like to thank all staffs of Department of Mathematics, Hokkaido University. They helped me whenever I asked. I would also like to thank my colleagues, especially those in the same graduate student room. I received a lot of information from them, and their diligent attitude toward their research encouraged me.

This work is supported by JSPS KAKENHI Grant Number JP22KJ0009.

Conventions on terminology The symbol $\mathbb{Z}$ denotes the ring of integers. We write $\mathbb{Z}_{\geq 0} = \{n \in \mathbb{Z} \mid n \geq 0\}$ and $\mathbb{Z}_{>0} = \{n \in \mathbb{Z} \mid n > 0\}$. The symbols $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ denote the field of rational numbers, real numbers, and complex numbers respectively. The characteristic of a field K is denoted by $\operatorname{char} K$. The term *almost all* means 'all but a finite number of'. Let R be a ring. The multiplicative group consisting of all invertible elements of R is denoted by $R^\times$. We write $R^{\times 2} = \{r^2 \mid r \in R^\times\} \subset R^\times$. For R-algebras A and A', the set of all homomorphisms $A \to A'$ of R-algebras is denoted by $\operatorname{Hom}_R^{\mathrm{al}}(A, A')$. For R-modules M and M', the set of all homomorphisms $M \to M'$ of R-modules is denoted by $\operatorname{Hom}_R(M, M')$.

Chapter I
Preliminaries from algebraic number theory

1 Dedekind domains and valuations of fields

This section gives a quick review of Dedekind domains and valuations of fields, which are fundamental concepts of number theory. We refer to [16], [41], and [32] for field theory, Dedekind domains, and valuations respectively.

1.1 Field extension

The (extension) *degree* of a field extension L/K, denoted $[L : K]$, is the dimension of L over K as a vector space. A *finite extension* means a field extension of finite degree. A field extension L/K is said to be an *algebraic extension* if any element x of L is *algebraic* over K, that is, x is a root of a nonzero polynomial with coefficients in K. A field K is *algebraically closed* if any non-constant polynomial with coefficients in K has a root in K. A field L is an *algebraically closure* of a field K if L/K is an algebraic extension and L is algebraically closed.

Theorem 1.1. *Let K be a field.*

(i) *There exists an algebraic closure of K.*

(ii) *Let $\tau : K \to K'$ be an isomorphism of fields, and let Ω and Ω' be algebraic closures of K and K' respectively. Then τ extends to an isomorphism from Ω to Ω'.*

(iii) *An algebraic closure of K is unique up to isomorphism.*

Proof. See [16, Theorems 2.18, 2.19 and 2.20]. Note that the assertion (iii) is a consequence of (ii). □

As for homomorphisms between fields, the following result is useful.

Theorem 1.2 (Dedekind)**.** *Let K and K' be fields, and let $\sigma_1, \dots, \sigma_m$ be m distinct homomorphisms from K to K'. Suppose that m elements $\beta_1, \dots, \beta_m$ of K' satisfy the equation*

$$\beta_1\sigma_1(\alpha) + \cdots + \beta_m\sigma_m(\alpha) = 0$$

for all $\alpha \in K$. Then $\beta_1, \dots, \beta_m$ are all 0. In other words $\sigma_1, \dots, \sigma_m$ are linearly independent in the K'-vector space consisting of all homomorphisms $K \to K'$.

Proof. See [16, Corollary of Theorem 2.39]. □

Corollary 1.3. *Let L/K be a field extension of finite degree n, and $\overline{K}$ an algebraic closure of K. The number of homomorphisms $L \to \overline{K}$ of K-algebras is at most n, i.e., $\#\operatorname{Hom}_K^{\mathrm{al}}(L, \overline{K}) \leq n$.*

Proof. Suppose to the contrary that $m := \#\operatorname{Hom}_K^{\mathrm{al}}(L, \overline{K}) > n$, and $\sigma_1, \ldots, \sigma_m \in \operatorname{Hom}_K^{\mathrm{al}}(L, \overline{K})$ are distinct homomorphisms. Let $y_1, \ldots, y_n \in L$ be a basis of L over K. Then the equation system

$$\begin{pmatrix} \sigma_1(y_1) & \cdots & \sigma_m(y_1) \\ \vdots & & \vdots \\ \sigma_1(y_n) & \cdots & \sigma_m(y_n) \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} = \mathbf{0}$$

has a nontrivial solution $(\beta_1, \ldots, \beta_m) \in \overline{K}^m$ since $m > n$. However, this would imply that $\beta_1\sigma_1(\alpha) + \cdots + \beta_m\sigma_m(\alpha) = 0$ for all $\alpha \in L$, which contradicts Theorem 1.2. Therefore m must be at most n. □

Let L/K be an algebraic extension. For any $\alpha \in L$, there exists a unique monic polynomial $m(X) \in K[X]$ of lowest degree with coefficients in K such that $m(\alpha) = 0$, where a *monic* polynomial means a nonzero polynomial with the leading coefficient equal to 1. Such a unique polynomial is called the *minimal polynomial* of α over K. We say that L/K is *separable* if the minimal polynomial of every element of L is *separable* over K, that is, it has no multiple root in an algebraic closure of K. It is known that any field of characteristic 0 or of finite cardinality is *perfect*, that is, every algebraic extension of it is separable ([16, Theorems 2.44 and 2.45]). If L is generated by finitely many elements whose minimal polynomials are separable over K then L is separable ([16, Theorem 2.46]). For example, if $f(X) \in K[X]$ is an irreducible separable polynomial over K then the field $K[X]/(f)$ is separable. Moreover, every finite separable extension is a *simple* extension. Namely, if L/K is a finite separable extension then there exists $\alpha \in L$ such that $L = K(\alpha)$ ([16, Corollary 1 of Theorem 2.57]). We say that L/K is *normal* if the minimal polynomial of every element of L over K decomposes over L into a product of linear factors.

Example 1.4. Every quadratic extension is normal. Moreover if $\operatorname{char} K \neq 2$ then it is separable. To show this, let L be a quadratic extension of K and take $\alpha \in L$ arbitrarily. If $\alpha \in K$ then its minimal polynomial over K is the linear polynomial $X - \alpha$, which is separable clearly. If $\alpha \in L \setminus K$ then its minimal polynomial is a quadratic polynomial, say $X^2 - aX + b \in K[X]$. This polynomial decomposes as $X^2 - aX + b = (X - \alpha)(X - (a - \alpha))$ over L. Hence L/K is normal. Moreover if $\operatorname{char} K \neq 2$ then $X^2 - aX + b$ is separable because otherwise we would have $\alpha = a/2$, which contradicts $\alpha \in L \setminus K$. Therefore L/K is separable.

A *Galois extension* is an algebraic extension which is separable and normal. For a Galois extension L/K, the automorphism group $\operatorname{Aut}_K(L)$ is called the *Galois group* of L/K and denoted by $\operatorname{Gal}(L/K)$. A Galois extension is said to be a *cyclic extension* if its Galois group is a cyclic group. Let L/K be a finite extension. We have $\#(\operatorname{Aut}_K(L)) \leq [L : K]$ by Corollary 1.3, and L/K is a Galois extension if and only if the equality $\#(\operatorname{Aut}_K(L)) = [L : K]$ holds ([16, Theorem 3.3]). Suppose that L/K is a finite separable extension, and let $\overline{K}$ be an algebraic closure containing L. Then there exists a unique finite Galois extension E/K such that $L \subset E \subset \overline{K}$ and $E \subset N$ for any Galois extension N/K with $L \subset N \subset \overline{K}$. This field E is called the *Galois closure* of L/K. By writing L as $L = K(\alpha)$ for some $\alpha \in L$, the Galois closure is given by $K(\alpha_1, \ldots, \alpha_d)$ where $\alpha_1, \ldots, \alpha_d \in \overline{K}$ are all conjugates of α over K, that is, all roots of the minimal polynomial of α over K.

Let L/K be a Galois extension. For an intermediate field M of L/K, that is, a field between K and L, the extension L/M is a Galois extension. Its Galois group $\operatorname{Gal}(L/M)$ is naturally a subgroup of $\operatorname{Gal}(L/K)$ by regarding each automorphism $L \to L$ over M as one over K. Conversely, for a subgroup H of $\operatorname{Gal}(L/K)$, the *fixed subfield* $L^H := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ is an intermediate field of L/K.

Theorem 1.5 (Fundamental theorem of Galois theory)**.** *Let L/K be a finite Galois extension. The mapping from the set of all intermediate fields of L/K to the set of all subgroups of $\mathrm{Gal}(L/K)$ sending an intermediate field M to its Galois group $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ is a bijection. Its inverse is given by $H \mapsto L^H$.*

Proof. See [16, Theorem 3.12]. □

Let K be a field, and E a commutative K-algebra whose K-dimension is finite. The *trace* $\mathrm{Tr}_{E/K}(\alpha)$ and *norm* $\mathrm{N}_{E/K}(\alpha)$ of an element $\alpha \in E$ are respectively the trace and determinant of the K-linear transformation $E \to E$, $x \mapsto \alpha x$. Then the *trace map* $\mathrm{Tr}_{E/K} : E \to K$ is a K-linear map, and the *norm map* $\mathrm{N}_{E/K} : E^\times \to K^\times$ is a group homomorphism, where $E^\times$ and $K^\times$ are the multiplicative groups of E and K respectively. For commutative K-algebras $E_1, \dots, E_m$ whose K-dimensions are finite, we have

$$\mathrm{Tr}_{(\prod_{i=1}^m E_i)/K}(\alpha_1, \dots, \alpha_m) = \sum_{i=1}^m \mathrm{Tr}_{E_i/K}(\alpha_i), \quad \mathrm{N}_{(\prod_{i=1}^m E_i)/K}(\alpha_1, \dots, \alpha_m) = \prod_{i=1}^m \mathrm{N}_{E_i/K}(\alpha_i)$$

for any $(\alpha_1, \dots, \alpha_m) \in \prod_{i=1}^m E_i$. If L is an extension field of K contained in E, then E can be seen as an L-algebra. In this case, we have

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{E/L}(\alpha)), \quad \mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{L/K}(\mathrm{N}_{E/L}(\alpha))$$

for any $\alpha \in E$. This property is referred to as the transitivity.

Theorem 1.6. *Let L be a finite separable extension. For any $\alpha \in L$ we have*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})} \sigma(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})} \sigma(\alpha).$$

Proof. See [16, Theorem 2.64]. □

Corollary 1.7. *Let L/K be a finite separable extension. The trace map $\mathrm{Tr}_{L/K} : L \to K$ is surjective.*

Proof. There exists $\beta \in L$ such that its trace $\mathrm{Tr}_{L/K}(\beta)$, which is equal to $\sum_{\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})} \sigma(\beta)$ by Theorem 1.6, is not zero, because otherwise it would contradict Theorem 1.2. Then, for any $\alpha \in K$ we have $\mathrm{Tr}_{L/K}(\mathrm{Tr}_{L/K}(\beta)^{-1}\alpha\beta) = \mathrm{Tr}_{L/K}(\beta)^{-1}\alpha \,\mathrm{Tr}_{L/K}(\beta) = \alpha$. This means that the trace map is surjective. □

As for the norm, the group $K^\times / \mathrm{N}_{E/K}(E^\times)$ of norm classes is nontrivial in general, and it requires some effort to figure out. In this thesis, the group of norm classes for quadratic extension is of particular importance.

Definition 1.8. Let E be a commutative K-algebra. A K-algebra automorphism $\sigma : E \to E$ is said to be an (K-*algebra*) *involution* if $\sigma^2 = \mathrm{id}_E$. If E is equipped with a K-algebra involution then E is referred to as a (commutative) K-*algebra with involution*. In this case, we write E^σ for the fixed subalgebra $\{x \in E \mid \sigma(x) = x\}$. Two K-algebras $(E, \sigma), (E', \sigma')$ with involution are *isomorphic* if there exists an isomorphism $\phi : E \to E'$ of K-algebras such that $\phi(\sigma(x)) = \sigma'(\phi(x))$ for all $x \in E$.

There are two types of K-algebras with involution treated mainly in this thesis: E is a field; or E is of type (sp) defined below.

Definition 1.9. Let E_0 be a field, and put $E = E_0 \times E_0$. We define an involution σ of E to be the transposition of the first and second components:

$$\sigma((x, y)) = (y, x) \quad (x, y \in E_0).$$

A K-algebra with involution isomorphic to (E, σ) is said to be *of type* (sp). In this case, the fixed subalgebra E^σ is the diagonal, which is a field isomorphic to E_0.

Definition 1.10. Let E be a commutative algebra over a field K, and let $\sigma : E \to E$ be a non-trivial E-algebra involution. Suppose that E^σ is a field. Then, the quotient group

$$\mathrm{Tw}(E, \sigma) := (E^\sigma)^\times / \{x\sigma(x) \mid x \in E^\times\}$$

is referred to as the *twisting group*.

If E/E^σ is a separable extension of fields then $\mathrm{Tw}(E, \sigma) = (E^\sigma)^\times / N_{E/E^\sigma}(E^\times)$ by Theorem 1.6. This is also true clearly in the case where E is of type (sp).

Proposition 1.11. *Let E is a K-algebra with involution σ of type* (sp)*. Then* $\mathrm{Tw}(E, \sigma) = \{1\}$.

Proof. We may assume that $E = E_0 \times E_0$, where E_0 is a field isomorphic to E^σ. For any $z \in E_0^\times$, we have $(1, z)\sigma((1, z)) = (z, z)$. This means that $\{(x, y)\sigma((x, y)) \mid (x, y) \in E\} = (E^\sigma)^\times$, and we are done. □

1.2 Discrete valuation rings and Dedekind domains

This subsection gives a brief review of discrete valuation rings and Dedekind domains. We refer to [41, Chapter I] for more detail.

Integral elements Let R be a ring, and A a subring of R. An element b of R is *integral* over A if b is a root of a monic polynomial with coefficients in A. Integrality can be rephrased as follows.

Proposition 1.12. *Finitely many elements $b_1, \ldots, b_n \in R$ are all integral over A if and only if $A[b_1, \ldots, b_n] \subset R$ is finitely generated as an A-module.*

Proof. See [32, Chapter I, Proposition 2.2]. □

This proposition implies that if $b_1, b_2 \in R$ are two elements integral over A then $b_1 + b_2$ and $b_1 b_2$ are also integral over A because $A[b_1, b_2, b_1 + b_2, b_1 b_2] = A[b_1, b_2]$. Hence, the subset of R consisting of all elements integral over A forms a ring. This subring of R is called the *integral closure* of A in R. If the integral closure of A in R is A itself, then A is said to be *integrally closed in R*. We say that an integral domain is *integrally closed* if it is integrally closed in its field of fractions.

Let A be an integrally closed domain, and K its field of fractions. Let L/K be a finite separable extension. In this case, the trace map and the norm map send any integral element into A. More precisely, for any element $b \in L$ integral over A, we have

$$\mathrm{Tr}_{L/K}(b) \in A \quad \textit{and} \quad \mathrm{N}_{L/K}(b) \in A. \tag{1}$$

Indeed, if b is integral over A then so are its conjugates, and thus Theorem 1.6 implies that $\mathrm{Tr}_{L/K}(b)$ and $\mathrm{N}_{L/K}(b)$ are also integral over A. Hence, we get (1) since A is integrally closed. The following proposition is also an important property of an integrally closed domain.

Proposition 1.13. *Let A be an integrally closed domain, and K its field of fractions. For monic polynomials $f(X), g(X) \in K[X]$, if $f(X)g(X) \in A[X]$ then $f(X) \in A[X]$ and $g(X) \in A[X]$.*

Proof. Let $f, g \in K[X]$ be monic polynomials with $f(X)g(X) \in A[X]$, and let $\overline{K}$ be an algebraic closure of K. Then f and g factor into linear polynomials over $\overline{K}$, say

$$f(X) = \prod_{i=1}^{m}(X - \alpha_i),\ g(X) = \prod_{j=1}^{n}(X - \beta_j) \quad (\alpha_i, \beta_j \in \overline{K}).$$

Since α_i and β_j $(i = 1, \ldots, m, j = 1, \ldots, n)$ are roots of the monic polynomial fg with coefficients in A, they are integral over A. Hence, the coefficients of f and g are also integral over A. On the other hand, any element of K integral over A belongs to A since A is integrally closed. Therefore, the coefficients of f and g belong to A. □

Discrete valuation rings A *discrete valuation ring* is a principal ideal domain with exactly one nonzero prime ideal. Let A be a discrete valuation ring, and let $\mathfrak{p}$ denote the nonzero prime ideal of A. Because $\mathfrak{p}$ is a maximal ideal, the quotient $A/\mathfrak{p}$ is a field. This field is called the *residue field* of A. There exists an element $\pi \in A$ which generates the ideal $\mathfrak{p}$ since A is a principal ideal domain. Such an element is called a *uniformizer* of A. If we fix a uniformizer π of A then any nonzero element $x \in A$ can be uniquely written as $x = u\pi^n$ where u is a unit of A and n is a non-negative integer.

Let K be the field of fractions of A. Any nonzero element $x \in K$ can be uniquely written as $x = u\pi^n$ where u is a unit of A and n is an integer (n can be negative). In this case, the integer n is called the *valuation of* x. The valuation of $0 \in K$ is defined to be ∞. If we write $v(x)$ for the valuation of x, it is clear that

(i) the map $v : K^\times \to \mathbb{Z}$ is a surjective homomorphism;

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$ for $x, y \in K$.

The ring A and the prime ideal $\mathfrak{p}$ can be expressed in K as $A = \{x \in K \mid v(x) \geq 0\}$ and $\mathfrak{p} = \{x \in K \mid v(x) > 0\}$ respectively.

In general, for an arbitrary field K, a function $v : K \to \mathbb{Z} \cup \{\infty\}$ with $v(0) = \infty$ and with the properties (i) and (ii) is called a (normalized) *discrete valuation*. General theory of valuations will be discussed in §1.4.

Proposition 1.14. *Let K be a field with a discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$. Then $A := \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring having v as its associated valuation.*

Proof. See [41, Chapter I, Proposition 1]. □

It is known that a Noetherian domain is a discrete valuation ring if and only if it is integrally closed and has a unique nonzero prime ideal, see [41, Chapter I, Proposition 3].

Dedekind domains Let A be a Noetherian domain, and K its field of fractions. A *fractional ideal* of A is a finitely generated A-submodule of K. Of course, any ideal of A is a fractional ideal. An ideal of A is called an *integral ideal* if we emphasize that it is contained in A. For two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$, the product

$$\mathfrak{ab} := \left\{ \sum_i a_i b_i \in K \text{ (finite sum)} \;\middle|\; a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}$$

is also a fractional ideal. With this product, the set of all nonzero fractional ideals of A forms a commutative monoid with the identity element A. Moreover, for any nonzero fractional ideal $\mathfrak{a}$, it can be checked that

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subset A\}$$

is also a nonzero fractional ideal. For a positive integer $n \in \mathbb{Z}_{>0}$, we write $\mathfrak{a}^{-n} = (\mathfrak{a}^{-1})^n$.

Let $\mathfrak{p}$ be a prime ideal of A. Then the set $S := A \setminus \mathfrak{p}$ is a multiplicative set. The ring $S^{-1}A$ is called the *localization* of A at $\mathfrak{p}$ and denoted by $A_\mathfrak{p}$. Similarly, for a fractional ideal $\mathfrak{a}$ of A, the localization $\mathfrak{a}_\mathfrak{p}$ of $\mathfrak{a}$ at $\mathfrak{p}$ is defined by $\mathfrak{a}_\mathfrak{p} := S^{-1}\mathfrak{a} = \mathfrak{a}A_\mathfrak{p}$. This is a fractional ideal of $A_\mathfrak{p}$.

Proposition 1.15. *Let A be a Noetherian domain. The following are equivalent.*

(i) *For every nonzero prime ideal $\mathfrak{p}$, the localization $A_\mathfrak{p}$ is a discrete valuation ring.*

(ii) *A is integrally closed and any nonzero prime ideal is a maximal ideal.*

Proof. See [41, Chapter I, Proposition 4]. □

Definition 1.16. A *Dedekind domain* is a Noetherian domain which has the two equivalent properties of Proposition 1.15.

For example, every principal ideal domain (in particular, every discrete valuation ring) is a Dedekind domain. Another example is the ring of integers of an algebraic number field, see Example 1.20.

Let A be a Dedekind domain and K its field of fractions. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then K is also the field of fractions of the localization $A_\mathfrak{p}$. Hence, the discrete valuation ring $A_\mathfrak{p}$ defines a discrete valuation on K. This discrete valuation is referred to as the *valuation associated with* $\mathfrak{p}$ and denoted by $v_\mathfrak{p}$. If $\mathfrak{a}$ is a nonzero fractional ideal of A then there exists a unique integer $v_\mathfrak{p}(\mathfrak{a})$ such that $\mathfrak{a}_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})}$ since $\mathfrak{a}_\mathfrak{p}$ is a fractional ideal of $A_\mathfrak{p}$. This integer is called the *valuation of* $\mathfrak{a}$ with respect to $\mathfrak{p}$. Because we have $v_\mathfrak{p}(xA) = v_\mathfrak{p}(x)$ for any $x \in K$, the valuation of a fractional ideal can be seen as a generalization of that of an element.

The following theorems are crucial properties of a Dedekind domain, see [41, Chapter I, Propositions 5 and 7] for their proofs.

Theorem 1.17 (Unique prime factorization)**.** *Let A be a Dedekind domain, and $\mathfrak{a}$ a nonzero fractional ideal of A. Then $v_\mathfrak{p}(\mathfrak{a}) = 0$ for almost all nonzero prime ideals $\mathfrak{p}$, and $\mathfrak{a}$ can be written as a product of finitely many prime ideals in a unique way: $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$.* □

Theorem 1.18. *Let A be a Dedekind domain. For any nonzero fractional ideal $\mathfrak{a}$ of A, we have $\mathfrak{a}\mathfrak{a}^{-1} = A$.* □

As a consequence of Theorem 1.18, for a Dedekind domain, the monoid consisting of all nonzero fractional ideals is a group.

1.3 Extension of Dedekind domains

Let A be a Noetherian domain, and K its field of fractions. Let L/K be a finite extension, and B the integral closure of A in L. In this situation, the field of fractions of B is L. We consider the following condition:

$$B \text{ is finitely generated over } A \text{ as an } A\text{-module.} \tag{F}$$

For example, if L/K is separable then the condition (F) holds, see [41, Chapter I, Proposition 8].

Proposition 1.19. *Under the assumption* (F)*, if A is a Dedekind domain then so is B.*

Proof. See [41, Chapter I, Proposition 9]. □

Example 1.20. A finite extension field of $\mathbb{Q}$ is called an *algebraic number field*. For an algebraic number field L, the integral closure of $\mathbb{Z}$ in L is called *the ring of integers* of L. Since $\mathbb{Q}$ is perfect and $\mathbb{Z}$ is a Dedekind domain, Proposition 1.19 implies that the ring of integers of any algebraic number field is a Dedekind domain.

In the following, we assume that (F) holds and A is a Dedekind domain. Let $\mathfrak{p}$ be a nonzero prime ideal of A and $\mathfrak{P}$ a nonzero prime ideal of B. We say that $\mathfrak{P}$ *divides* $\mathfrak{p}$ or is *above* $\mathfrak{p}$ if $\mathfrak{p} = \mathfrak{P} \cap A$, and write $\mathfrak{P} \mid \mathfrak{p}$. The prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$ if and only if $\mathfrak{P}$ contains the ideal $\mathfrak{p}B$ generated by $\mathfrak{p}$. Hence $\mathfrak{p}B$ factors as $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{p}B)}$. Note that the residue field $B/\mathfrak{P}$ is naturally an extension field of $A/\mathfrak{p}$, and the degree of this extension is finite by the assumption (F).

Definition 1.21. Suppose that $\mathfrak{P}$ divides $\mathfrak{p}$. The valuation $v_{\mathfrak{P}}(\mathfrak{p}B)$ is called the *ramification index* of $\mathfrak{P}$ over $\mathfrak{p}$ and denoted by $e(\mathfrak{P}/\mathfrak{p})$. The degree of the field extension $(B/\mathfrak{P})/(A/\mathfrak{p})$ is called the *inertia degree* or *residue degree* of $\mathfrak{P}$ over $\mathfrak{p}$ and denoted by $f(\mathfrak{P}/\mathfrak{p})$.

Proposition 1.22 (Fundamental identity)**.** *Let $\mathfrak{p}$ be a nonzero prime ideal of A, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ be all distinct prime ideals above $\mathfrak{p}$. Then we have*

$$[L : K] = \sum_{j=1}^{l} e(\mathfrak{P}_j/\mathfrak{p}) f(\mathfrak{P}_j/\mathfrak{p}).$$

Proof. The Chinese remainder theorem gives the isomorphism $B/\mathfrak{p}B \cong \prod_{j=1}^{l} B/\mathfrak{P}^{e(\mathfrak{P}_j/\mathfrak{p})}$. We can get the desired identity by comparing the dimensions of both sides over $A/\mathfrak{p}$. See [32, Chapter I, Proposition 8.2] for detail. □

Definition 1.23. Let $\mathfrak{p}$ be a nonzero prime ideal of A. The prime ideal $\mathfrak{p}$ is said to be (*totally*) *split in L* if the number of distinct prime ideals of B above $\mathfrak{p}$ is $[L : K]$, that is, $l = [L : K]$ in the setting of Proposition 1.22. A prime ideal $\mathfrak{P}$ of B above $\mathfrak{p}$ is *unramified over K* if the extension $(B/\mathfrak{P})/(A/\mathfrak{p})$ is separable and $e(\mathfrak{P}/\mathfrak{p}) = 1$. If not, $\mathfrak{P}$ is said to be *ramified over K*. The prime ideal $\mathfrak{p}$ is *unramified in L* if all prime ideals of B above $\mathfrak{p}$ are unramified over K, and otherwise *ramified in L*.

1.4 Valuations

We review valuations of fields in this and the next subsection. We refer to [32, §§3 and 4 of Chapter II]. Let K be a field.

Definition 1.24. A (*multiplicative*) *valuation* of K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ having the following conditions: For $x, y \in K$,

(i) $|x| = 0$ if and only if $x = 0$;

(ii) $|xy| = |x||y|$;

(iii) $|x + y| \leq |x| + |y|$.

We exclude the *trivial valuation*, that is, $|x| = 1$ for all $x \neq 0$. Any valuation $|\cdot|$ of K defines naturally the distance function

$$K \times K \to \mathbb{R}_{\geq 0},\ (x, y) \mapsto |x - y|.$$

Two valuations $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if distance functions defined by them induce the same topology on K.

For example, the usual absolute value of $\mathbb{Q}$ is a valuation. There is a useful criterion for the equivalence of valuations.

Proposition 1.25. *Two valuations $|\cdot|_1$ and $|\cdot|_2$ of K are equivalent if and only if there exists a real positive number s such that $|x|_1 = |x|_2^s$ for all $x \in K$.*

Proof. See [32, Chapter II, Proposition 3.3]. □

Valuations of a field play the role of prime ideals of a (commutative) ring in some sense. The following theorem can be seen as an analog of the Chinese remainder theorem.

Theorem 1.26 (Approximation theorem)**.** *Let $|\cdot|_1, \ldots, |\cdot|_m$ be inequivalent valuations of K, and let $x_1, \ldots, x_m$ be elements of K. For any $\varepsilon > 0$ there exists an element $x \in K$ such that $|x - x_i|_i < \varepsilon$ for each $i = 1, \ldots, m$.*

Proof. See [32, Chapter II, Theorem 3.4]. □

Definition 1.27. A valuation $|\cdot|$ of K is said to be *non-archimedean* if it satisfies the *strong triangle inequality*:

$$|x + y| \leq \max\{|x|, |y|\} \quad \text{for any } x, y \in K.$$

Otherwise it is said to be *archimedean*.

For any non-archimedean valuation $|\cdot|$ and elements $x, y \in K$, if $|x| \neq |y|$ then $|x + y| = \max\{|x|, |y|\}$. We will see that non-archimedean valuations correspond to exponential valuations, which are defined as follows.

Definition 1.28. A (*exponential*) *valuation* of K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ having the following conditions: For $x, y \in K$,

(i) $v(x) = \infty$ if and only if $x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

We exclude the *trivial valuation*, that is, $v(x) = 0$ for all $x \neq 0$. Two exponential valuations v_1 and v_2 are *equivalent* if there exists a real positive number s such that $v_1 = sv_2$.

Any exponential valuation v defines a multiplicative valuation $|\cdot|_v$ by

$$|x|_v = q^{-v(x)} \quad (x \in K)$$

where $q > 1$ is a fixed real number. It is obvious that this multiplicative valuation is non-archimedean. By Proposition 1.25, the topology defined by $|\cdot|_v$ does not depend on the choice of q. Moreover, two exponential valuations v_1 and v_2 are equivalent if and only if their associated multiplicative valuations $|\cdot|_{v_1}$ and $|\cdot|_{v_2}$ define the same topology.

Proposition 1.29. *Sending an exponential valuation v of K to the associated valuation $|\cdot|_v$ gives rise to one-to-one corresponding between the equivalent classes of exponential valuations of K and the equivalent classes of non-archimedean valuations of K.*

Proof. Straightforward. □

Definition 1.30. An exponential valuation v of K is called a *discrete valuation* if $v(K^\times) = s\mathbb{Z}$ for some positive real number s. A discrete valuation is *normalized* if $v(K^\times) = \mathbb{Z}$. Note that for every discrete valuation there exists a unique normalized one equivalent to it.

Let v be an exponential valuation of K. The subset

$$\mathcal{O} := \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x|_v \leq 1\}$$

is referred to as the *valuation ring of* K with respect to v. This is a local ring with maximal ideal $\mathfrak{p} := \{x \in K \mid v(x) > 0\}$, and its unit group is given by $\mathcal{O}^\times = \{x \in K \mid v(x) = 0\}$. The maximal ideal and residue field of $\mathcal{O}$ will be referred to as the maximal ideal and residue field of K with respect to v respectively. When there is no danger of confusion, the clause 'with respect to v' is omitted. If v is a discrete valuation then $\mathcal{O}$ is a discrete valuation ring as mentioned in Proposition 1.14.

1.5 Complete fields

A *complete field* is a field equipped with a valuation that is complete with respect to the distance induced by the valuation. When considering valuations of a field in parallel with prime ideals of a ring, the counterpart to the localization at a prime ideal is the completion with respect to a valuation. So, it is important to study complete fields.

We remark that for any field K and its valuation $|\cdot|$, there exists a *completion* of K with respect to $|\cdot|$, that is a complete field $\widehat{K}$ with valuation $|\cdot|_{\widehat{K}}$ such that it contains K as a subfield, the valuation $|\cdot|_{\widehat{K}}$ coincides with $|\cdot|$ on K, and K is dense in $\widehat{K}$. Furthermore, a completion of K is unique in the following sense: if $\widehat{K}'$ is another completion of K with valuation $|\cdot|_{\widehat{K}'}$ then the mapping from $\widehat{K}$ to $\widehat{K}'$ defined by

$$|\cdot|_{\widehat{K}}\text{-}\lim_{n\to\infty} a_n \mapsto |\cdot|_{\widehat{K}'}\text{-}\lim_{n\to\infty} a_n \quad ((a_n)_n \text{ is a Cauchy sequence in } K)$$

is an isomorphism of K-algebras preserving valuations, see [32, Chapter II-§4]. The valuation of the completion will often be denoted by the same symbol as that of the original field.

Let K be a field and v an exponential valuation of K. We write $\mathcal{O}$ and $\mathfrak{p}$ for the valuation ring and maximal ideal of K. Furthermore $\widehat{K}$ denotes the completion of K with respect to v, and let $\widehat{\mathcal{O}}$ and $\widehat{\mathfrak{p}}$ be the valuation ring and maximal ideal of $\widehat{K}$. Then, the inclusion $\mathcal{O} \to \widehat{\mathcal{O}}$ gives rise to an isomorphism $\mathcal{O}/\mathfrak{p} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ between residue fields. Moreover, if v is a discrete valuation then it also induces an isomorphism $\mathcal{O}/\mathfrak{p}^n \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n$ for any $n \in \mathbb{Z}_{>0}$, see [32, Chapter II, Proposition 4.3].

A complete field is referred to as a *complete archimedean* (resp. *non-archimedean*) *field* if the equipped valuation is archimedean (resp. non-archimedean). The fields $\mathbb{R}$ and $\mathbb{C}$ are complete archimedean fields (with respect to the usual absolute value). It is known that there is no complete archimedean field other than $\mathbb{R}$ and $\mathbb{C}$. More precisely, the following theorem holds.

Theorem 1.31 (Ostrowski)**.** *Let K be a complete archimedean field with valuation $|\cdot|$. There exists an isomorphism σ from K to $\mathbb{R}$ or $\mathbb{C}$ such that $|\sigma(\cdot)|$ is equivalent to the usual absolute value of $\mathbb{R}$ or $\mathbb{C}$.*

Proof. See [32, Chapter II, Proposition 4.2]. □

We proceed to the non-archimedean case. For a complete non-archimedean field, Hensel's lemma is fundamental. Let K be a complete non-archimedean field with valuation $|\cdot|$, and let $\mathcal{O}_K, \mathfrak{p}$, and κ denote its valuation ring, maximal ideal, and residue field respectively.

Definition 1.32. Let $f(X) = a_d X^d + \cdots a_1 X + a_0 \in K[X]$ be a polynomial. We define $|f| := \max\{|a_0|, |a_1|, \ldots, |a_d|\}$. Suppose that all coefficients $a_0, a_1, \ldots, a_d$ are in $\mathcal{O}_K$. The *reduction modulo* $\mathfrak{p}$, denoted $f \bmod \mathfrak{p}$, is the polynomial $\overline{a_d} X^d + \cdots \overline{a_1} X + \overline{a_0}$ in $\kappa[X]$, where $\overline{a} = a + \mathfrak{p} \in \kappa$ for $a \in A$. We say that f is *primitive* if its reduction $f(X) \bmod \mathfrak{p} \in \kappa[X]$ is not zero, or equivalently, $|f| = 1$.

Theorem 1.33 (Hensel's lemma)**.** *Let $f \in \mathcal{O}_K[X]$ be a primitive polynomial. Suppose that f admits modulo $\mathfrak{p}$ a factorization*

$$f(X) \equiv \bar{g}(X)\bar{h}(X) \bmod \mathfrak{p}$$

into coprime polynomials $\bar{g}, \bar{h} \in \kappa[X]$. Then f admits a factorization

$$f(X) \equiv g(X)h(X)$$

into polynomials $f, g \in \mathcal{O}_K[X]$ such that $\deg(g) = \deg(\bar{g})$, $g \bmod \mathfrak{p} = \bar{g}$ and $h \bmod \mathfrak{p} = \bar{h}$.

Proof. See [32, Chapter II, Theorem 4.6]. □

Corollary 1.34. *Let $f(X) = a_d X^d + \cdots + a_1 X + a_0 \in K[X]$ be a polynomial with $a_d \neq 0$. If $|a_d| < |f|$ and $|f| = |a_r|$ for some $r > 0$ then f is reducible. Hence, if f is irreducible then $|f| = \max\{|a_0|, |a_d|\}$. In particular, an element α of a finite extension field L of K is integral if and only if $|\mathrm{N}_{L/K}(\alpha)| \leq 1$.*

Proof. Suppose that $|a_d| < |f|$ and $|f| = |a_r|$ for some $r > 0$. Let $r > 0$ be the smallest index satisfying $|f| = |a_r|$, and put

$$g(X) = a_r^{-1} f(X) = b_0 + b_1 X + \cdots + b_d X^d \quad (b_i := a_i/a_r).$$

Then $|g| = 1$ and

$$g(X) \equiv X^r(1 + \overline{b_{r+1}} X + \cdots + \overline{b_d} X^{d-r}) \bmod \mathfrak{p}.$$

Thus g has a factor of degree $r > 0$ corresponding to X^r by Hensel's lemma (Theorem 1.33). Note that $r < d$ since $|a_d| < |f|$. Hence g is reducible over K, and so is f. Therefore, if f is irreducible then $|f| = \max\{|a_0|, |a_d|\}$. The last assertion is obtained by applying it to the minimal polynomial of an element α. □

For any algebraic extension L/K, the valuation of K extends uniquely to a valuation on L. More precisely, the following theorem holds.

Theorem 1.35 (Unique extension of valuation)**.** *Let K be a complete valuation field with valuation $|\cdot|_K$ (it can be archimedean), and let L/K be an algebraic extension. Then the valuation $|\cdot|_K$ is extended in a unique way to a valuation of L, and it is archimedean (resp. non-archimedean) if $|\cdot|_K$ is archimedean (resp. non-archimedean). If L/K is a finite extension then the unique extension $|\cdot|_L$ is given by*

$$|x|_L = \sqrt[[L:K]]{|\mathrm{N}_{L/K}(x)|_K} \quad (x \in L),$$

and L is complete with respect to this valuation. Moreover, if L/K is a finite extension and $|\cdot|_K$ is non-archimedean then the valuation ring of L coincides with the integral closure of that of K in L, and the maximal ideal of L is an only prime ideal above that of K.

Proof. See [32, Chapter II, Theorem 4.8]. □

Corollary 1.36. *Let K be a complete valuation field with normalized discrete valuation v_K, and let L/K be a finite extension of degree n. Then v_K is extended in a unique way to a discrete valuation $\tilde{v}_L$ of L. Moreover, the normalized discrete valuation v_L equivalent to $\tilde{v}_L$ is given by*

$$v_L(x) = \frac{e(\mathfrak{P}/\mathfrak{p})}{n} v_K(\mathrm{N}_{L/K}(x)) \quad (x \in L),$$

where $\mathfrak{p}$ and $\mathfrak{P}$ are the maximal ideals with respect to v_K and $\tilde{v}_L$ respectively. In particular, we have $v_L(x) = e(\mathfrak{P}/\mathfrak{p}) v_K(x)$ for $x \in K$.

Proof. By Theorem 1.35, the valuation v_K is extended in a unique way to an exponential valuation $\tilde{v}_L$ of L, and it is given by

$$\tilde{v}_L(x) = \frac{1}{n} v_K(\mathrm{N}_{L/K}(x)) \quad \text{for } x \in L.$$

This equation shows that $\tilde{v}_L$ is a discrete valuation since so is v_K. Let s be a positive real number such that $v_L = s\tilde{v}_L$. Note that v_L is the valuation associated with $\mathfrak{P}$ by its uniqueness. Then we have $v_K(\mathfrak{p}) = 1$ and $v_L(\mathfrak{P}) = 1$. On the other hand, we have

$$v_K(\mathfrak{p}) = \tilde{v}_L(\mathfrak{p}) = \tilde{v}_L(\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}) = e(\mathfrak{P}/\mathfrak{p}) \tilde{v}_L(\mathfrak{P}) = \frac{e(\mathfrak{P}/\mathfrak{p})}{s} v_L(\mathfrak{P}).$$

Thus $s = e(\mathfrak{P}/\mathfrak{p})$, which completes the proof. □

We will need a variant of Hensel's lemma which is specialized for quadratic forms. Let K be a complete non-archimedean field with valuation $|\cdot|$, and let $\mathcal{O}_K, \mathfrak{p}$, and κ denote its valuation ring, maximal ideal, and residue field respectively. We say a point $(x_1, \dots, x_d) \in (\mathcal{O}_K)^d$ is *primitive* if $(\overline{x_1}, \dots, \overline{x_d}) \neq \mathbf{0}$ in κ^d, or equivalently, $|x_i| = 1$ for some i.

Proposition 1.37. *Assume that* $\operatorname{char} \kappa \neq 2$. *Let $(a_{ij})_{ij}$ is a symmetric matrix of size d with entries in $\mathcal{O}_K$ such that $|\det((a_{ij}))| = 1$. We define a quadratic form q by $q(X_1, \dots, X_d) := \sum_{i,j} a_{ij} X_i X_j$. Let $a \in \mathcal{O}_K$ be any element, and let $(y_1, \dots, y_d) \in (\mathcal{O}_K)^d$ be a primitive point with $q(y_1, \dots, y_d) \equiv a \bmod \mathfrak{p}$. Then, there exists $(x_1, \dots, x_d) \in (\mathcal{O}_K)^d$ such that $q(x_1, \dots, x_d) = a$ and $x_i \equiv y_i \bmod \mathfrak{p}$ for all $i = 1, \dots, d$.*

Proof. For $k = 1, \dots, d$, we define a quadratic polynomial $f_k \in \mathcal{O}_K[X]$ by

$$\begin{aligned} f_k(X) &:= q(y_1, \dots, y_{k-1}, X, y_{k+1} \dots, y_d) - a \\ &= a_{kk} X_k^2 + 2 \left(\sum_{i \neq k} a_{ki} y_i \right) X_k + \sum_{i,j \neq k} a_{ij} y_i y_j - a, \end{aligned}$$

and write $D_k \in \mathcal{O}_K$ for the discriminant of f_k. Then

$$\begin{aligned} D_k/4 &= \left(\sum_{i \neq k} a_{ki} y_i \right)^2 - a_{kk} \left(\sum_{i,j \neq k} a_{ij} y_i y_j - a \right) \\ &\equiv \left(\sum_{i \neq k} a_{ki} y_i \right)^2 + a_{kk} \left(a_{kk} y_k^2 + 2 \left(\sum_{i \neq k} a_{ki} y_i \right) y_k \right) \\ &= \left(\sum_{i=1}^{d} a_{ki} y_i \right)^2 \mod \mathfrak{p}, \end{aligned}$$

where the congruence is by $f_k(y_k) \equiv 0 \bmod \mathfrak{p}$. This implies that $D_k \equiv 0 \bmod \mathfrak{p}$ if and only if $\sum_{i=1}^d a_{ki} y_i \equiv 0 \bmod \mathfrak{p}$, or equivalently $\sum_{i=1}^d \overline{a_{ki}}\,\overline{y_i} = 0$ in κ. Hence, there exists k_0 such that $D_{k_0} \not\equiv 0 \bmod \mathfrak{p}$ since $(\overline{y_1}, \dots, \overline{y_d}) \neq \mathbf{0}$ and $(\overline{a_{ij}})_{ij}$ is invertible over κ. This means that the reduction $f_{k_0} \bmod \mathfrak{p}$ factors as $f_{k_0}(X) \equiv (X - \overline{y_{k_0}})(X - \overline{y_{k_0}}')$ mod $\mathfrak{p}$ for some $\overline{y_{k_0}}' \in \kappa \setminus \{\overline{y_{k_0}}\}$, since $\operatorname{char}\kappa \neq 2$. Thus, by Hensel's lemma (Theorem 1.33), there exists $x_{k_0} \in \mathcal{O}_K$ such that $(X - x_{k_0}) \mid f_{k_0}(X)$ and $\overline{x_{k_0}} = \overline{y_{k_0}}$. Then

$$q(y_1, \dots, y_{k_0-1}, x_{k_0}, y_{k_0+1}, \dots, y_d) - a = f_{k_0}(x_{k_0}) = 0,$$

and $(y_1, \dots, y_{k_0-1}, x_{k_0}, y_{k_0+1}, \dots, y_d)$ is the desired point. □

1.6 Different

Let A be a Dedekind domain, and K its field of fractions. Let L/K be a finite separable extension, and B the integral closure of A in L. As mentioned in §1.3, the integral closure B is also a Dedekind domain. We will define the *different ideal* $\mathfrak{D}_{B/A}$ for the extension B/A of Dedekind domains, and explain that it has information on ramification of prime ideals.

The field L admits the nondegenerate symmetric K-bilinear form $T : L \times L \to K$ defined by

$$T(x, y) = \operatorname{Tr}_{L/K}(xy) \quad (x, y \in L).$$

This form is called the *trace form*. The B-module $B^\vee := \{y \in L \mid T(y, x) \in B \text{ for all } x \in B\}$ is called the *codifferent ideal* of B/A. It follows from lattice theory that the codifferent ideal $B^\vee$ is finitely generated over A (see Theorem 5.2 and Lemma 5.10), and in particular it is a fractional ideal of B.

Definition 1.38. The inverse $(B^\vee)^{-1}$ of the fractional ideal $B^\vee$ is called the *different ideal* of B/A, and denoted by $\mathfrak{D}_{B/A}$. We sometimes write $\mathfrak{D}_{L/K}$ for $\mathfrak{D}_{B/A}$ when the ring A is obvious, for example, when K is an algebraic number field or when a valuation of K is fixed.

We have $B \subset B^\vee$ since $\operatorname{Tr}_{L/K}(B) \subset A$, see §1.2. This shows that $\mathfrak{D}_{B/A} = (B^\vee)^{-1} \subset B^{-1} = B$, and hence the different ideal $\mathfrak{D}_{B/A}$ is an integral ideal.

Proposition 1.39. *Different ideals have the following properties.*

(i) *If E/L is a finite separable extension and C denotes the integral closure of B in E, we have $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$.*

(ii) *If S is a multiplicative set in A then $S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A}$.*

(iii) *Let $\mathfrak{p}$ be a nonzero prime ideal of A and $\mathfrak{P}$ a prime ideal of B above $\mathfrak{p}$. If $\widehat{A}_\mathfrak{p}$ and $\widehat{B}_\mathfrak{P}$ denote the completions of A and B at $\mathfrak{p}$ and $\mathfrak{P}$ respectively, then $\mathfrak{D}_{B/A}\widehat{B}_\mathfrak{P} = \mathfrak{D}_{\widehat{B}_\mathfrak{P}/\widehat{A}_\mathfrak{p}}$.*

Proof. See [32, Chapter III, Proposition 2.2] or [41, Chapter III-§4]. □

A nonzero prime ideal $\mathfrak{P}$ of B, above a nonzero prime ideal $\mathfrak{p}$ of A, is said to be *tamely ramified over K* if the extension $(B/\mathfrak{P})/(A/\mathfrak{p})$ of residue fields is separable and the ramification index $e(\mathfrak{P}/\mathfrak{p})$ and $\operatorname{char}(A/\mathfrak{p})$ are coprime. By definition, if $\mathfrak{P}$ is unramified over K then it is tamely ramified over K.

Theorem 1.40. *Let $\mathfrak{P}$ be a nonzero prime ideal of B. Then $\mathfrak{P}$ is ramified over K if and only if $\mathfrak{P}$ divides $\mathfrak{D}_{B/A}$. More precisely, putting $\mathfrak{p} = \mathfrak{P} \cap A$, we have $v_\mathfrak{P}(\mathfrak{D}_{B/A}) \geq e(\mathfrak{P}/\mathfrak{p}) - 1$, and the equality holds if and only if $\mathfrak{P}$ is tamely ramified over K.*

Proof. See [32, Chapter III, Theorem 2.6] or [41, Chapter III, Theorem 1 and Proposition 13]. An important step of the proof is to reduce to the case where A and B are complete discrete valuation rings by using Proposition 1.39. □

Corollary 1.41. *There are only finitely many prime ideals of A which are ramified in L.*

Proof. Let $\mathfrak{P}_1, \dots, \mathfrak{P}_l$ be all prime ideals of B which appear in the prime factorization of $\mathfrak{D}_{B/A}$. Theorem 1.40 implies that there is no prime ideal of A which is ramified in L other than $\mathfrak{P}_1 \cap A, \dots, \mathfrak{P}_l \cap A$. This completes the proof. See [32, Chapter I, Proposition 8.4] for another proof. □

1.7 Extension and valuations

Let K be a field, and let v be a valuation of K. In this subsection, v can be an archimedean valuation although we have used the letter v for an exponential valuation so far. Let K_v denote the completion with respect to v of K, and $\overline{K_v}$ the algebraic closure of K_v. Then, there exists a unique extension $\bar{v}$ of v to $\overline{K_v}$ by Theorem 1.35.

Let L/K be an algebraic extension. Each embedding $\tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$ defines a valuation w of L extending v by the composition $w := \bar{v} \circ \tau$. In this case, the topological closure of $\tau(L)$ in $\overline{K_v}$ is a completion of L with respect to w. We say that two embeddings τ and $\tau' \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$ are *conjugate* if there exists an automorphism $\sigma \in \mathrm{Aut}_{K_v}(\overline{K_v})$ such that $\tau' = \sigma \circ \tau$. Conjugate embeddings τ and τ' define the same valuation of L because $\bar{v} = \bar{v} \circ \sigma$ by Theorem 1.35. The following theorem states that all valuations of L extending v are obtained in the manner described above, and they correspond to the conjugate classes of embeddings.

Theorem 1.42. *Let L/K be an algebraic extension.*

(i) *For any valuation w of L extending v, there exists an embedding $\tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$ such that $w = \bar{v} \circ \tau$.*

(ii) *Two extensions $\bar{v} \circ \tau$ and $\bar{v} \circ \tau'$, where $\tau, \tau' \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$, coincide if and only if τ and τ' are conjugate.*

Proof. See [32, Chapter II, Theorem 8.1]. □

Let $\mathcal{E}_L$ be the set of all conjugate classes of embeddings $\tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$. For a valuation w of L, we write $w \mid v$ if w is an extension of v. Let us check that there exists an isomorphism $L \otimes K_v \cong \prod_{w|v} L_w$ if L/K is a finite separable extension, where L_w is the completion of L with respect to w.

Lemma 1.43. *Let $f(X) \in K[X]$ be an irreducible polynomial. We define a field L to be $K[X]/(f)$, and an element $\alpha \in L$ to be $X + (f) \in L$. We write the decomposition of f over K_v into irreducible factors as*

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r} \quad (f_i(X) \in K_v[X], m_i \in \mathbb{Z}_{>0}).$$

Sending an embedding $\tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$ to the factor f_i such that $f_i(\tau(\alpha)) = 0$ gives rise to a bijection from $\mathcal{E}_L$ to $\{f_1, \dots, f_r\}$.

Proof. See [32, Chapter II, Proposition 8.2]. □

In the situation of Lemma 1.43, there is also a canonical bijection between $\mathcal{E}_L$ and the set of all valuations of L extending v by Theorem 1.42. Hence, there is a canonical one-to-one corresponding between the irreducible factors $f_1, \dots, f_r \in K_v[X]$ and the valuations of L extending v. The irreducible factor of f over K_v corresponding to a valuation $w \mid v$ of L will be denoted by f_w.

Theorem 1.44. *Let K be a field, v a valuation of K, and L/K a finite separable extension. For each valuation w of L extending v, take an embedding $\tau_w \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K_v})$ such that $w = \bar{v} \circ \tau_w$. Then, the map*

$$L \otimes_K K_v \to \prod_{w|v} L_w, \quad x \otimes y \mapsto (\tau_w(x)y)_w \tag{2}$$

is an isomorphism of K_v-algebras, where L_w is identified with the topological closure of $\tau_w(L)$ in $\overline{K_v}$.

Proof. Let $\alpha \in L$ be an element such that $L = K(\alpha)$, and let $f \in K[X]$ be the minimal polynomial of α over K. For a valuation w of L extending v, we write $f_w \in K_v[X]$ for the irreducible factor of f over K_v corresponding to w. Since L/K is separable, the multiplicity of every f_w is one. Thus f factors as $f = \prod_{w|v} f_w$ over K_v.

Let w be a valuation of L extending v. We now claim that the topological closure $\tau_w(L)^{\mathrm{cl}}$ of $\tau_w(L)$ coincides with $K_v(\tau_w(\alpha))$ in $\overline{K_v}$. It is clear that $K_v(\tau_w(\alpha)) \subset \tau_w(L)^{\mathrm{cl}}$ since $\tau_w(L)$ contains K and $\tau_w(\alpha)$. On the other hand, the subfield $K_v(\tau_w(\alpha))$ is complete by Theorem 1.35 since the extension degree of $K_v(\tau_w(\alpha))/K_v$, which is equal to $\deg f_w$, is finite. Furthermore $K_v(\tau_w(\alpha))$ contains $\tau(L) = \tau(K(\alpha))$, which leads to $\tau(K(\alpha))^{\mathrm{cl}} \subset K_v(\tau_w(\alpha))^{\mathrm{cl}} = K_v(\tau_w(\alpha))$. Hence we obtain $K_v(\tau_w(\alpha)) = \tau_w(L)^{\mathrm{cl}}$.

Let us consider the following three natural isomorphisms:

$$\begin{aligned}
&K_v[X]/(\textstyle\prod_{w|v} f_w) \cong (K[X]/(f)) \otimes_K K_v \to L \otimes_K K_v && \text{induced by } X \mapsto \alpha \otimes 1,\\
&K_v[X]/(\textstyle\prod_{w|v} f_w) \to \prod_{w|v} (K_v[X]/(f_w)) && \text{induced by } X \mapsto (X + (f_w))_w,\\
&K_v[X]/(f_w) \to K_w(\tau_w(\alpha)) = \tau_w(L)^{\mathrm{cl}} && \text{induced by } X \mapsto \tau_w(\alpha).
\end{aligned}$$

These isomorphisms make the diagram

$$\begin{array}{ccc}
L \otimes_K K_v & \xrightarrow{(2)} & \prod_{w|v} \tau_w(L)^{\mathrm{cl}} \\
\uparrow & & \uparrow \\
K_v(X)/(\prod_{w|v} f_w) & \longrightarrow & \prod_{w|v} (K_v[X]/(f_w))
\end{array}$$

commutative. Therefore, the map (2) is an isomorphism. □

2 Fields of number theory

This section gives an explanation of finite fields, local fields, and algebraic number fields. The relationship among these fields is as follows: a local field is obtained by the completion of an algebraic number field with respect to a valuation; and a finite field appears as the residue field of a (non-archimedean) local field. We refer to [40, Chapter I] for finite fields; [32, Chapter II], [35, §63], [41, Chapter III-§5] for local fields; and [32, Chapter III-§1] for algebraic number fields.

2.1 Finite fields

A *finite field* is a field whose cardinality is finite. Let p be a prime. The quotient ring $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is an example of a finite field of characteristic p. Any finite field of characteristic p is of order p^d for some $d \in \mathbb{Z}_{>0}$, because it has an $\mathbb{F}_p$-vector space structure. Let Ω_p be an algebraically closed field of characteristic p. Then the map $\tau_0 : \Omega_p \to \Omega_p,\ x \mapsto x^p$ is an automorphism. Let

d be a positive integer and put $q = p^d$. We remark that the polynomial $X^q - X$ has q distinct roots in Ω_p since it is coprime to its derivative -1. Hence, the subfield

$$\Omega_p^{\tau_0^d} = \{x \in \Omega_p \mid \tau_0^d(x) = x\} = \{x \in \Omega_p \mid x^q = x\}$$

fixed by the d-th iterate τ_0^d of τ_0 is a finite field of order q. This shows that there exists a finite field of order p^d for every $d \in \mathbb{Z}_{>0}$. Moreover, it can be seen that any finite field of order p^d is isomorphic to $\Omega_p^{\tau_0^d}$ (see [40, Chapter I, Theorem 1]).

Let κ be a finite field of order $q = p^d$ where $d \in \mathbb{Z}_{>0}$. The symbol $\kappa^\times$ denotes the multiplicative group κ, and $\kappa^{\times 2}$ denotes the subgroup consisting of all nonzero squares: $\kappa^\times = \kappa \backslash \{0\}, \kappa^{\times 2} = \{x^2 \mid x \in \kappa^\times\}$. We will use the following facts, see [40, Chapter I, Theorems 2 and 4] for their proofs.

Proposition 2.1. *The multiplicative group $\kappa^\times$ is a cyclic group of order $q - 1$.* □

Proposition 2.2. *The following assertions hold.*

(i) *If* $\operatorname{char} \kappa = 2$ *then any element of κ is a square.*

(ii) *If* $\operatorname{char} \kappa \neq 2$ *then the homomorphism $\kappa \to \{1, -1\} \subset \kappa$ defined by $x \mapsto x^{(q-1)/2}$ gives rise to the following exact sequence:*

$$1 \to \kappa^{\times 2} \to \kappa^\times \to \{1, -1\} \to 1$$

where $\kappa^{\times 2} \to \kappa^\times$ is the inclusion. In particular, the quotient $\kappa^\times/\kappa^{\times 2}$ is of order 2. □

Corollary 2.3. *Suppose that* $\operatorname{char} \kappa \neq 2$. *Then -1 is a square if $q \equiv 1 \bmod 4$ and not a square if $q \equiv 3 \bmod 4$.*

Proof. This follows from Proposition 2.2 (ii) because $(-1)^{(q-1)/2} = 1$ if $q \equiv 1 \bmod 4$ and $(-1)^{(q-1)/2} = -1$ if $q \equiv 3 \bmod 4$. □

We now show that any finite extension of a finite field is a cyclic extension.

Proposition 2.4. *Let λ be a finite extension field of κ. Then λ/κ is a cyclic extension, and the Galois group* $\operatorname{Gal}(\lambda/\kappa)$ *is generated by the automorphism $\tau : x \mapsto x^q$.*

Proof. Put $m = [\lambda : \kappa]$. If $m = 1$ then the assertion is obvious. Suppose that $m > 1$. We claim that τ has order m in the automorphism group $\operatorname{Aut}_\kappa(\lambda)$. Since $\tau^m(x) = x^{q^m} = x$ for any $x \in \lambda$, the order of τ is at most m. Let $x \in \lambda^\times$ be an element of (multiplicative) order $q^m - 1$. Such an element exists by Proposition 2.1. Then

$$\tau^j(x) = x^{q^j} \neq x \quad \text{for any } 1 \leq j \leq m - 1,$$

which implies that the order of τ is at least m. Therefore τ has order m.

Let $G \subset \operatorname{Aut}_\kappa(\lambda)$ denote the subgroup generated by τ. Then

$$m = |G| \leq |\operatorname{Aut}_\kappa(\lambda)| \leq [\lambda : \kappa] = m,$$

which shows that $|\operatorname{Aut}_\kappa(\lambda)| = [\lambda : \kappa]$ and $G = \operatorname{Aut}_\kappa(\lambda)$. Hence λ/κ is a Galois extension and $\operatorname{Gal}(\lambda/\kappa) = G$. This completes the proof. □

Corollary 2.5. *Let λ be an extension field of κ. Then the norm map $N_{\lambda/\kappa} : \lambda^\times \to \kappa^\times$ is surjective.*

Proof. Since $\kappa^\times$ is a cyclic group of order $q-1$ (Proposition 2.1), it suffices to show that there exists an element $x \in \lambda^\times$ such that the order of its norm $\mathrm{N}_{\lambda/\kappa}(x) \in \kappa^\times$ is equal to $q-1$. Note that $\mathrm{Gal}(\lambda/\kappa) = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{m-1}\}$ by Proposition 2.4, where $m := [\lambda : \kappa]$ and τ is as in Proposition 2.4. Let $x \in \lambda^\times$ be an element of order $q^m - 1$. Then

$$N_{\lambda/\kappa}(x) = \prod_{\sigma \in \mathrm{Gal}(\lambda/\kappa)} \sigma(x) = \prod_{i=0}^{m-1} x^{q^i} = x^{\frac{q^m-1}{q-1}}.$$

Thus, for any $1 \leq j \leq q-2$, we get

$$(N_{\lambda/\kappa}(x))^j = (x^{\frac{q^m-1}{q-1}})^j = x^{(q^m-1)\cdot\frac{j}{q-1}} \neq x$$

since the order of x is $q^m - 1$. This shows that $N_{\lambda/\kappa}(x)$ is of order $q-1$ as required. The proof is complete. □

2.2 Local fields

Definition 2.6. An *archimedean local field* is the field $\mathbb{R}$ or $\mathbb{C}$. A *non-archimedean local field* is a complete field with discrete valuation such that its residue field is a finite field. A non-archimedean local field is said to be *dyadic* if the characteristic of its residue field equals 2, and *non-dyadic* otherwise.

Definition 2.7. Let $p \in \mathbb{Z}$ be a prime number. We write v_p for the valuation of $\mathbb{Q}$ associated with the prime ideal $p\mathbb{Z}$. The completion of $\mathbb{Q}$ with respect to v_p is called *the field of p-adic numbers* and denoted by $\mathbb{Q}_p$. The valuation ring of $\mathbb{Q}_p$ is called *the ring of p-adic integers* and denoted by $\mathbb{Z}_p$.

The field $\mathbb{Q}_p$ is an example of a non-archimedean local field because the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is naturally isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Another example is $\mathbb{F}_p((t))$, the field of formal Laurent series over $\mathbb{F}_p$. It is known that any non-archimedean local field is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, see [32, Chapter II, Proposition 5.2].

In the following, we study square numbers of a non-archimedean local field. First, let K be an arbitrary field with exponential valuation v. Let $\mathcal{O}, \mathfrak{p}$, and κ be the valuation ring, maximal ideal, and residue field with respect to v. Then

$$1 + \mathfrak{p} = \{1 + z \in \mathcal{O}^\times \mid z \in \mathfrak{p}\} = \{x \in \mathcal{O}^\times \mid v(x-1) > 0\} \subset \mathcal{O}^\times$$

is a subgroup of $\mathcal{O}^\times$. Indeed, for $x_1, x_2 \in 1 + \mathfrak{p}$ we have

$$v(x_1 x_2^{-1} - 1) = v(x_1 - x_2) = v((x_1 - 1) - (x_2 - 1)) \geq \min\{v(x_1 - 1), v(x_2 - 1)\} > 0.$$

In the case where v is a discrete valuation, assuming v to be normalized, for any $i \in \mathbb{Z}_{>0}$ the subset

$$1 + \mathfrak{p}^i = \{1 + z \in \mathcal{O}^\times \mid z \in \mathfrak{p}^i\} = \{x \in \mathcal{O}^\times \mid v(x-1) \geq i\}$$

is a subgroup of $\mathcal{O}^\times$. If we fix a uniformizer π of $\mathcal{O}$, any element of $1 + \mathfrak{p}^i$ can be uniquely written as $1 + x\pi^i$, where $x \in \mathcal{O}$.

Now, we assume that K is a non-archimedean local field. Namely, v is a discrete valuation, K is complete with respect to the topology defined by v, and κ is a finite field. We also assume that v is normalized. Let π be a uniformizer of $\mathcal{O}$, and let q denote the cardinality of κ.

Lemma 2.8. *Let $i, j \in \mathbb{Z}$ be integers with $1 \leq i \leq j$. The order of the quotient group $(1 + \mathfrak{p}^i)/(1 + \mathfrak{p}^j)$ is q^{j-i}.*

Proof. Let r be an positive integer. Then, the kernel of the surjection

$$1+\mathfrak{p}^r \to \kappa,\ 1+x\pi^r \mapsto x+\mathfrak{p} \quad (x \in \mathcal{O})$$

is $1+\mathfrak{p}^{r+1}$. Thus, it induces an isomorphism $(1+\mathfrak{p}^r)/(1+\mathfrak{p}^{r+1}) \to \kappa$, and $\#((1+\mathfrak{p}^r)/(1+\mathfrak{p}^{r+1})) = q$. Now, let $i, j \in \mathbb{Z}$ be integers with $1 \leq i \leq j$. From the chain

$$1+\mathfrak{p}^j \subset 1+\mathfrak{p}^{j-1} \subset \cdots \subset 1+\mathfrak{p}^{i+1} \subset 1+\mathfrak{p}^i,$$

we obtain

$$\#((1+\mathfrak{p}^i)/(1+\mathfrak{p}^j)) = \#((1+\mathfrak{p}^i)/(1+\mathfrak{p}^{i+1})) \cdots \#((1+\mathfrak{p}^{j-1})/(1+\mathfrak{p}^j)) = q^{j-i}$$

as required. □

Lemma 2.9. *Suppose that the characteristic of K is not 2. For any positive integer $r \in \mathbb{Z}$, we have $(1+2\mathfrak{p}^r)^2 = 1+4\mathfrak{p}^r$. In particular, if K is non-dyadic then $(1+\mathfrak{p})^2 = 1+\mathfrak{p}$.*

Proof. Let r be a positive integer. We have $(1+2\mathfrak{p}^r)^2 \subset 1+4\mathfrak{p}^r+4\mathfrak{p}^{2r} \subset 1+4\mathfrak{p}^r$. We show the reverse inclusion. Take an element $1+4\pi^r\alpha$ of $1+4\mathfrak{p}^r$ where $\alpha \in \mathcal{O}$, and consider the quadratic polynomial $f(X) := X^2+\pi^{-r}X-\pi^{-r}\alpha \in K[X]$. This polynomial is reducible by Corollary 1.34. Let $\beta, \beta' \in K$ be the roots of f. Since $\beta+\beta' = -\pi^{-r}$ we have $-r = v(\beta+\beta') \geq \min\{v(\beta), v(\beta')\}$, and thus $v(\beta) \leq -r$ or $v(\beta') \leq -r$. We assume that $v(\beta') \leq -r$ without loss of generality. Furthermore, since $\beta\beta' = -\pi^r\alpha$ we get $-r+v(\alpha) = v(\beta)+v(\beta') \leq v(\beta)-r$, and hence $v(\beta) \geq v(\alpha) \geq 0$. This means that $\beta \in \mathcal{O}$. Since β is a root of f, we have $1+4\pi^r\alpha = (1+2\pi^r\beta)^2$. This completes the proof. □

Let r be a positive integer, and let $\varsigma : \mathcal{O}^\times \to \mathcal{O}^\times$ denote the homomorphism $x \mapsto x^2$. We consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1+2\mathfrak{p}^r & \longrightarrow & \mathcal{O}^\times & \longrightarrow & (\mathcal{O}/2\mathfrak{p}^r)^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varsigma|_{1+2\mathfrak{p}^r}} & & \downarrow{\scriptstyle \varsigma} & & \downarrow{\scriptstyle \bar{\varsigma}} & & \\ 1 & \longrightarrow & 1+2\mathfrak{p}^r & \longrightarrow & \mathcal{O}^\times & \longrightarrow & (\mathcal{O}/2\mathfrak{p}^r)^\times & \longrightarrow & 1 \end{array} \tag{3}$$

where $\bar{\varsigma}$ is the homomorphism induced by ς, and horizontal arrows are natural homomorphisms. Two horizontal sequences are exact.

Theorem 2.10. *Let K be a non-archimedean local field of characteristic not 2, and let $v, \mathcal{O}, q$ be as above.*

(i) *If K is non-dyadic then the natural surjection $\mathcal{O}^\times \to \kappa^\times$ gives rise to an isomorphism $\mathcal{O}^\times/\mathcal{O}^{\times 2} \to \kappa^\times/\kappa^{\times 2}$. Furthermore, we have $\#(K^\times/K^{\times 2}) = 4$.*

(ii) *If K is dyadic then $\#(K^\times/K^{\times 2}) = 4q^{v(2)}$.*

Proof. We first remark that $K^\times = \mathcal{O}^\times \times \{\pi^n \mid n \in \mathbb{Z}\}$ since any nonzero element of K can be uniquely written as $u\pi^n$, where u is a unit of $\mathcal{O}$ and n is an integer. This leads to $K^\times/K^{\times 2} = \mathcal{O}^\times/\mathcal{O}^{\times 2} \times \{1, \pi\}$.

(i). Suppose that K is non-dyadic. Substituting $r = 1$ in the diagram (3), we have

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1+\mathfrak{p} & \longrightarrow & \mathcal{O}^\times & \longrightarrow & \kappa^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varsigma|_{1+\mathfrak{p}}} & & \downarrow{\scriptstyle \varsigma} & & \downarrow{\scriptstyle \bar{\varsigma}} & & \\ 1 & \longrightarrow & 1+\mathfrak{p} & \longrightarrow & \mathcal{O}^\times & \longrightarrow & \kappa^\times & \longrightarrow & 1, \end{array}$$

which induces the exact sequence

$$(1+\mathfrak{p})/(1+\mathfrak{p})^2 \to \mathcal{O}^\times/\mathcal{O}^{\times 2} \to \kappa^\times/\kappa^{\times 2} \to 1.$$

On the other hand, Lemma 2.9 shows that $(1+\mathfrak{p})/(1+\mathfrak{p})^2 = 1$. Hence, the natural homomorphism $\mathcal{O}^\times/\mathcal{O}^{\times 2} \to \kappa^\times/\kappa^{\times 2}$ is an isomorphism. Furthermore, since $\kappa^\times/\kappa^{\times 2}$ has order 2 by Proposition 2.2 (ii), we obtain

$$\#(K^\times/K^{\times 2}) = \#(\mathcal{O}^\times/\mathcal{O}^{\times 2}) \cdot \#\{1,\pi\} = \#(\kappa^\times/\kappa^{\times 2}) \cdot 2 = 4.$$

(ii). Suppose that K is dyadic, and let r be a positive integer. In the diagram (3), we have $\ker(\varsigma|_{1+2\mathfrak{p}^r}) = \{1\}$ because $-1 \in (1+2\mathcal{O}) \setminus (1+2\mathfrak{p})$. We also have $\#\ker(\bar{\varsigma}) = \#\operatorname{coker}(\bar{\varsigma}) < \infty$ since $(\mathcal{O}/2\mathfrak{p}^r)^\times$ is of finite order. Moreover, the image of $\varsigma|_{1+2\mathfrak{p}^r}$ is $1+4\mathfrak{p}^r$ by Lemma 2.9. Now we apply the snake lemma to the diagram (3) and get the exact sequence

$$1 \to \{1,-1\} \to \ker(\bar{\varsigma}) \to (1+2\mathfrak{p}^r)/(1+4\mathfrak{p}^r) \to \mathcal{O}^\times/\mathcal{O}^{\times 2} \to \operatorname{coker}(\bar{\varsigma}) \to 1.$$

Then, the order of $\mathcal{O}^\times/\mathcal{O}^{\times 2}$ is finite since those of the others are finite, and

$$\frac{\#\ker(\bar{\varsigma}) \cdot \#(\mathcal{O}^\times/\mathcal{O}^{\times 2})}{\#\{1,-1\} \cdot \#((1+2\mathfrak{p}^r)/(1+4\mathfrak{p}^r)) \cdot \#\operatorname{coker}(\bar{\varsigma})} = 1.$$

Since $\#((1+2\mathfrak{p}^r)/(1+4\mathfrak{p}^r)) = \#((1+\mathfrak{p}^{v(2)+r})/(1+\mathfrak{p}^{2v(2)+r})) = q^{v(2)}$ by Lemma 2.8, we obtain $\#(\mathcal{O}^\times/\mathcal{O}^{\times 2}) = \#\{1,-1\} \cdot \#((1+2\mathfrak{p}^r)/(1+4\mathfrak{p}^r)) = 2q^{v(2)}$, and $\#(K^\times/K^{\times 2}) = 4q^{v(2)}$. □

Let K be a non-archimedean local field of characteristic not 2. By Theorem 2.10, if K is non-dyadic then there exists a non-square unit $\epsilon \in \mathcal{O}^\times$, and the group $K^\times/K^{\times 2}$ of square classes can be written as $K^\times/K^{\times 2} = \{1,\epsilon,\pi,\epsilon\pi\}$. In the case $K = \mathbb{Q}_2$, we can get a natural isomorphism $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \cong (\mathbb{Z}/8\mathbb{Z})^\times$ as follows.

Example 2.11. We have $(\mathbb{Z}_2/8\mathbb{Z}_2)^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times = \{1,-1,3,-3\}$, and $(\mathbb{Z}_2/8\mathbb{Z}_2)^{\times 2} = \{1\}$. Thus, by applying the snake lemma to the diagram (3) under $r = 2$, we get the exact sequence

$$1 \to \{1,-1\} \to (\mathbb{Z}_2/8\mathbb{Z}_2)^\times \to (1+8\mathbb{Z}_2)/(1+16\mathbb{Z}_2) \xrightarrow{\iota} \mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \to (\mathbb{Z}_2/8\mathbb{Z}_2)^\times \to 1.$$

In this case, ι is the trivial map, i.e., $\operatorname{im}\iota = \{1\}$, since $\#((\mathbb{Z}_2/8\mathbb{Z}_2)^\times) = 4 = \#\{1,-1\} \cdot \#((1+8\mathbb{Z}_2)/(1+16\mathbb{Z}_2))$. Thus, the natural homomorphism $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \to (\mathbb{Z}_2/8\mathbb{Z}_2)^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times$ is an isomorphism. As a result, we can write $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{1,-1,3,-3,2,-2,6,-6\}$.

The following proposition is another consequence of Lemma 2.9.

Proposition 2.12. *Let K be a non-archimedean local field of characteristic not 2. The set $K^{\times 2}$ of nonzero squares is an open subset of K. Furthermore, any subgroup H of $K^\times$ with index 2 is an open subset of K.*

Proof. Let $\beta \in K^{\times 2}$ be a nonzero square, and put and $N = v(\beta) + v(4\pi)$. Let $\alpha \in K$ be any element with $v(\alpha-\beta) > N$. Then $v(\beta) < v(\alpha-\beta)$ and thus $v(\alpha) = \min\{v(\beta), v(\alpha-\beta)\} = v(\beta)$. Hence, we can write $\alpha = \pi^n\alpha'$ and $\beta = \pi^n\beta'$, where $n := v(\beta)$ and $\alpha', \beta' \in \mathcal{O}^\times$ are units. Note that n is even and $\beta' \in \mathcal{O}^{\times 2}$ since β is a nonzero square. We have $\alpha' \equiv \beta' \mod 4\pi$ because

$$v(\alpha'-\beta') = v(\pi^{-n}(\alpha-\beta)) > -n + N = v(4\pi).$$

This implies that

$$\beta'^{-1}\alpha' \in 1+4\mathfrak{p} = (1+2\mathfrak{p})^2 \subset \mathcal{O}^{\times 2},$$

where the equality $1+4\mathfrak{p} = (1+2\mathfrak{p})^2$ is by Lemma 2.9. Thus $\alpha' \in \beta'\mathcal{O}^{\times 2} = \mathcal{O}^{\times 2}$, and the element $\alpha = \pi^n\alpha'$ is also a nonzero square. This shows that $K^{\times 2}$ an open subset of K. As a result, for any subgroup H of $K^\times$ with index 2 is open because $H \supset K^{\times 2}$. The proof is complete. □

Note that two points which are sufficiently close belong to the same square class by this proposition.

Remark 2.13. For a non-archimedean local field K of characteristic 0, one can show that $\{x^n \mid x \in K^\times\}$ is an open set in K for any $n \in \mathbb{Z}_{>0}$, and hence any subgroup of $K^\times$ with finite index is also open, see [32, Chapter II-§4, Exercise 4].

2.3 Unramified extension

Let K be a non-archimedean local field, and let $\mathcal{O}_K, \mathfrak{p}$, and κ denote its valuation ring, maximal ideal, and residue field respectively. For any finite extension L/K, we write $\mathcal{O}_L$ for the valuation ring of L, which is also the integral closure of $\mathcal{O}_K$ in L, see Theorem 1.35.

Definition 2.14. Let L be a finite separable extension field of K. The extension L/K is said to be *unramified* if the maximal ideal of L is unramified over K, or equivalently, $[\lambda : \kappa] = [L : K]$ where λ is the residue field of L.

For any $n \in \mathbb{Z}_{>0}$, there exists an unramified extension L/K of degree n. (see [41, Chapter III-§5, Theorem 2]). Moreover, such an extension is unique. We verify the uniqueness by using the following theorem.

Theorem 2.15. *Let L/K be a finite unramified extension, and L'/K an arbitrary finite extension. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be the maximal ideals, and λ and λ' be the residue fields of L and L' respectively. For a homomorphism $\sigma : L \to L'$ of K-algebras, we write $\bar{\sigma}$ for the homomorphism $\lambda \to \lambda'$ of κ-algebras defined by*

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}' \quad \text{for } x \in \mathcal{O}_L. \tag{4}$$

Then the map $\sigma \mapsto \bar{\sigma}$ gives a bijection between $\mathrm{Hom}_K^{\mathrm{al}}(L, L')$ and $\mathrm{Hom}_\kappa^{\mathrm{al}}(\lambda, \lambda')$.

Proof. See [41, Chapter III-§5, Theorem 3]. □

Corollary 2.16. *Let $\overline{K}$ be an algebraic closure of K. For any positive integer $n \in \mathbb{Z}_{>0}$, there exists one and only one unramified extension field K_n of degree n over K contained in $\overline{K}$.*

Proof. If N/K is an unramified extension of degree n then it is algebraic, and thus, there exists an extension field $K_n \subset \overline{K}$ isomorphic to N. We then show uniqueness. Let $K_n, K_n' \subset \overline{K}$ be unramified extension fields of degree n over K. We write L for the composite field $K_n K_n' \subset \overline{K}$ and λ for its residue field. Then, residue fields of K_n and K_n' have the same cardinality $(\#\kappa)^n$, and they coincide as a subfield of λ, say κ_n. By Theorem 2.15, the trivial commutative diagram

$$\begin{array}{ccc} \kappa_n & \xrightarrow{\mathrm{id}} & \kappa_n \\ & {\scriptstyle \mathrm{incl}} \searrow \quad \swarrow {\scriptstyle \mathrm{incl}} & \\ & \lambda & \end{array}$$

leads to the commutative diagram

$$\begin{array}{ccc} K_n & \xrightarrow{\widehat{\mathrm{id}}} & K_n' \\ & {\scriptstyle \mathrm{incl}} \searrow \quad \swarrow {\scriptstyle \mathrm{incl}} & \\ & L & \end{array}$$

where incl denotes the inclusion and $\widehat{\mathrm{id}} : K_n \to K_n'$ denotes the homomorphism which induces $\mathrm{id} : \kappa_n \to \kappa_n$. This diagram shows that $\widehat{\mathrm{id}}(x) = x$ for any $x \in K_n$, and hence $K_n = K_n'$. This completes the proof. □

Theorem 2.15 also implies that any finite unramified extension is a cyclic extension.

Corollary 2.17. *Let L/K be a finite unramified extension, and λ the residue field of L. Then the map $\mathrm{Aut}_K(L) \to \mathrm{Aut}_\kappa(\lambda)$, $\sigma \mapsto \bar{\sigma}$ is a group automorphism. In particular L/K is a cyclic extension.*

Proof. It is easy to check that the map $\sigma \mapsto \bar{\sigma}$ is a group homomorphism. Thus, it is an automorphism by Theorem 2.15. Moreover, since the group $\mathrm{Aut}_\kappa(\lambda) = \mathrm{Gal}(\lambda/\kappa)$ is a cyclic group of order $[\lambda : \kappa] = [L : K]$ by Proposition 2.4, so is $\mathrm{Aut}_K(L)$. This completes the proof. □

This corollary leads to an important concept, that is, the Frobenius automorphism.

Definition 2.18. Let L/K be a finite unramified extension, and λ the residue field of L. If q denotes the cardinality of κ, the automorphism $\lambda \to \lambda$, $x \mapsto x^q$ generates $\mathrm{Gal}(\lambda/\kappa)$ (see Proposition 2.4). Hence, by Corollary 2.17, the automorphism of L corresponding to this generator of $\mathrm{Gal}(\lambda/\kappa)$ is also a generator of $\mathrm{Gal}(L/K)$. This generator of $\mathrm{Gal}(L/K)$ is called the *Frobenius automorphism* of L/K. If we write $\tau \in \mathrm{Gal}(L/K)$ for the Frobenius automorphism then it is characterized by the property

$$\tau(x) \equiv x^q \bmod \mathfrak{P} \quad \text{for any } x \in \mathcal{O}_L,$$

where $\mathfrak{P}$ is the maximal ideal of L.

Corollary 2.17 also leads to the following proposition.

Proposition 2.19. *Let L/K be a finite unramified extension, and let $\mathfrak{P}$ and λ be the maximal ideal and residue field of L. Then $\mathrm{Tr}_{L/K}(x) + \mathfrak{p} = \mathrm{Tr}_{\lambda/\kappa}(x + \mathfrak{P})$ in κ for any $x \in \mathcal{O}_L$.*

Proof. Let $x \in \mathcal{O}_L$. we have

$$\mathrm{Tr}_{L/K}(x) + \mathfrak{p} = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) + \mathfrak{p} = \sum_{\sigma \in \mathrm{Gal}(L/K)} \bar{\sigma}(x + \mathfrak{P}).$$

Moreover, it follows from Corollary 2.17 that

$$\sum_{\sigma \in \mathrm{Gal}(L/K)} \bar{\sigma}(x + \mathfrak{P}) = \sum_{\tau \in \mathrm{Gal}(\lambda/\kappa)} \tau(x + \mathfrak{P}) = \mathrm{Tr}_{\lambda/\kappa}(x + \mathfrak{P}).$$

Therefore $\mathrm{Tr}_{L/K}(x) + \mathfrak{p} = \mathrm{Tr}_{\lambda/\kappa}(x + \mathfrak{P})$ as required. □

Corollary 2.20. *Let L/K be a finite unramified extension. Then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.*

Proof. The inclusion $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$ holds in general, see §1.2. Let $x \in \mathcal{O}_K$. Since $\mathrm{Tr}_{\lambda/\kappa} : \lambda \to \kappa$ is surjective by Corollary 1.7, there exists $y_0 \in \mathcal{O}_L$ such that $\mathrm{Tr}_{\lambda/\kappa}(y_0 + \mathfrak{P}) = x + \mathfrak{p}$. Then, Proposition 2.19 shows that $x - \mathrm{Tr}_{L/K}(y_0) \in \mathfrak{p}$. Let π be a uniformizer of $\mathcal{O}_K$. Then $\pi^{-1}(x - \mathrm{Tr}_{L/K}(y_0)) \in \mathcal{O}_K$, and as above, we can take $y_1 \in \mathcal{O}_L$ such that $\pi^{-1}(x - \mathrm{Tr}_{L/K}(y_0)) - \mathrm{Tr}_{L/K}(y_1) \in \mathfrak{p}$, or equivalently $x - \mathrm{Tr}_{L/K}(y_0) - \pi \,\mathrm{Tr}_{L/K}(y_1) \in \mathfrak{p}^2$. By repeating this procedure, we get a sequence $(y_n)_{n \geq 0}$ in $\mathcal{O}_L$ such that

$$x - \mathrm{Tr}_{L/K}(y_0) - \pi \,\mathrm{Tr}_{L/K}(y_1) - \cdots - \pi^n \,\mathrm{Tr}_{L/K}(y_n) \in \mathfrak{p}^{n+1}$$

for any n. Let $(z_n)_{\geq 0}$ be the Cauchy sequence in $\mathcal{O}_L$ defined by $z_n = \sum_{j=0}^{n} \pi^j y_j$. Then $x - \mathrm{Tr}_{L/K}(z_n) = x - \sum_{j=0}^{n} \pi^j \,\mathrm{Tr}_{L/K}(y_j) \in \mathfrak{p}^{n+1}$. Noting that $\mathrm{Tr}_{L/K} : L \to K$ is continuous, we obtain $\mathrm{Tr}_{L/K}(\lim_{n \to \infty} z_n) = x$. This shows that $\mathcal{O}_K \subset \mathrm{Tr}_{L/K}(\mathcal{O}_L)$, and the proof is complete. □

Let L/K be a finite unramified extension. We close this subsection by verifying that the group $K^\times/\mathrm{N}_{L/K}(L^\times)$ of norm classes is isomorphic to $\mathbb{Z}/[L:K]\mathbb{Z}$. Let $\mathfrak{P}$ and λ be the maximal ideal and residue field of L. We remark that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ by the fundamental identity (Proposition 1.22). This means that any uniformizer of $\mathcal{O}_K$ is also a uniformizer of $\mathcal{O}_L$.

Lemma 2.21. *We have* $\mathrm{N}_{L/K}(1+\mathfrak{P}) = 1+\mathfrak{p}$.

Proof. See [41, Chapter V, Proposition 3]. □

Theorem 2.22. *Let L/K be an unramified extension of degree n. The kernel of the surjection*

$$\overline{v_K} : K^\times \to \mathbb{Z}/n\mathbb{Z},\ \alpha \mapsto v_K(\alpha) + n\mathbb{Z}$$

is equal to $\mathrm{N}_{L/K}(L^\times)$, where v_K is the normalized valuation of K. In particular, it gives rise to an isomorphism $K^\times/\mathrm{N}_{L/K}(L^\times) \to \mathbb{Z}/n\mathbb{Z}$.

Proof. Let π be a unimodular of $\mathcal{O}_K$. Then π is also a uniformizer of $\mathcal{O}_L$, and any element of L can be expressed as $u\pi^m$, where u is a unit of $\mathcal{O}_L$ and m is an integer. Thus, the inclusion $\mathrm{N}_{L/K}(L^\times) \subset \ker(\overline{v_K})$ follows from $N_{L/K}(\pi) = \pi^n$. We prove the reverse inclusion. Consider the following commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & 1+\mathfrak{P} & \longrightarrow & \mathcal{O}_L^\times & \longrightarrow & \lambda^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{\lambda/\kappa}} & & \\
1 & \longrightarrow & 1+\mathfrak{p} & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \kappa^\times & \longrightarrow & 1
\end{array}$$

where rows are exact with natural homomorphisms. Since $\mathrm{N}_{L/K} : 1+\mathfrak{P} \to 1+\mathfrak{p}$ and $\mathrm{N}_{\lambda/\kappa} : \lambda^\times \to \kappa^\times$ are surjective by Lemma 2.21 and Corollary 2.5, so is $\mathrm{N}_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$. Now, let $\alpha \in K^\times$ belong to $\ker(\overline{v_K})$, i.e., $v_K(\alpha) \equiv 0 \bmod n$. By surjectivity of $\mathrm{N}_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$, there exists $\beta \in \mathcal{O}_L^\times$ such that $\mathrm{N}_{L/K}(\beta) = \pi^{-v_K(\alpha)}\alpha$. Then $\alpha = \pi^{v_K(\alpha)}\,\mathrm{N}_{L/K}(\beta) = \mathrm{N}_{L/K}(\pi^{-v_K(\alpha)/n}\beta)$, which shows that $\ker(\overline{v_K}) \subset \mathrm{N}_{L/K}(L^\times)$. The proof is complete. □

Remark 2.23. It will turn out that there exists an isomorphism $K^\times/\mathrm{N}_{L/K}(L^\times) \cong \mathbb{Z}/n\mathbb{Z}$ for a cyclic extension L/K of degree n even if L/K is not unramified, see Corollary 3.28.

2.4 Algebraic number fields

An *algebraic number field* is a finite extension field of $\mathbb{Q}$. Algebraic number fields have many analogies with function fields of algebraic curves over a finite field, and they are together called *global fields*. However, we treat only algebraic number fields in this thesis.

Let L be an algebraic number field. The integral closure of $\mathbb{Z}$ in L is called *the ring of integers* of L, and denoted by $\mathcal{O}_L$. This is a Dedekind domain as seen in Example 1.20.

Definition 2.24. A *place* of L is an equivalence class of valuations of L. A place is called a *finite place* if it is represented by a non-archimedean valuation, and a *infinite place* otherwise.

When there is no danger of confusion, we will use the same symbol for a place and a valuation representing it. The following proposition means that finite places correspond naturally to nonzero prime ideals of $\mathcal{O}_L$.

Proposition 2.25. *Any non-archimedean valuation of L is equivalent to the valuation associated with a nonzero prime ideal of $\mathcal{O}_L$.*

Proof (Sketch). Let w be a non-archimedean valuation of L. Then $w|_{\mathbb{Q}}$ is a non-archimedean valuation of $\mathbb{Q}$. It is known that a valuation of $\mathbb{Q}$ is equivariant to the one associated with a prime ideal of $\mathbb{Z}$ or the usual absolute value, see [32, Chapter II, Proposition 3.7]. Thus, we may assume that $w|_{\mathbb{Q}} = v_p$ for some prime p, where v_p is the valuation associated with $p\mathbb{Z}$.

Let $B \subset L$ be the valuation ring with respect to w. We have $\mathbb{Z} \subset B$ since $w(\mathbb{Z}) = v_p(\mathbb{Z}) \geq 0$. On the other hand, one can show that any valuation ring of a field with exponential valuation is integrally closed. Thus B contains the integral closure $\mathcal{O}_L$ of $\mathbb{Z}$ in L. Let $\mathfrak{Q}$ be the maximal ideal of B. Then $\mathfrak{P} := \mathfrak{Q} \cap \mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$. Put $S = \mathcal{O}_L \setminus \mathfrak{P}$. We have

$$\mathcal{O}_L \subset S^{-1}\mathcal{O}_L \subset S^{-1}B = B$$

in L. Then $S^{-1}\mathcal{O}_L$ must be equal to B because it can be shown that any discrete valuation ring is a maximal subring of its field of fractions. This implies that w is equivalent to the valuation defined by $\mathfrak{P}$. The proof is complete. □

For any place w of L, the completion of L with respect to w is referred to as the *completion* or *localization of L at w*, and denoted by L_w.

Proposition 2.26. *Let w be a place of L. The completion L_w is a local field.*

Proof. If w is archimedean then $L_w \cong \mathbb{R}$ or $\mathbb{C}$ by Ostrowski's theorem 1.31, and we are done. Suppose that w is non-archimedean. Then, it is represented by the valuation associated with a nonzero prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ by Proposition 2.25. In particular, it is a discrete valuation. Let p be a prime such that $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Then, the residue field of L_w with respect to w is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ since the valuation ring of L_w, which is equal to the integral closure of $\mathbb{Z}_p$ in L_w, is finitely generated as a $\mathbb{Z}_p$-module (see §1.3), Thus, it is a finite field. This completes the proof. □

Definition 2.27. Let L/K be a finite extension of algebraic number fields, and let v be a place of K. A place w of L is *above* v, or v is *below* w, if w is an extension of v as valuations up to equivalence. In this case, we write $w \mid v$. We say that v is (*totally*) *split in L* if the number of places of L above v is $[L : K]$. For finite places, we use the terms *ramified* and *unramified* when the corresponding prime ideals do so.

We will need the following proposition concerning decompositions of prime ideals.

Proposition 2.28. *Let L/K be a finite extension of algebraic number fields with $[L : K] > 1$. There exist infinitely many prime ideals of $\mathcal{O}_K$ that are not totally split in L.*

Proof (Sketch). For any algebraic number field K, it is known that the *Dedekind zeta function*

$$\zeta_K(s) := \sum_{\mathfrak{a}} \mathfrak{N}(\mathfrak{a})^{-s} \quad (s \in \mathbb{C}),$$

where $\mathfrak{a}$ ranges over all nonzero integral ideal of $\mathcal{O}_K$ and $\mathfrak{N}(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$, is a meromorphic function having a simple pole at $s = 1$ (see [32, Chapter VII-§5]). Note that it can be written as

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathcal{V}'} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}}$$

by the uniqueness of prime factorization (Theorem 1.17), where $\mathcal{V}'$ is the set of all nonzero prime ideals of $\mathcal{O}_K$.

Let L/K be a finite extension of algebraic number fields with $[L:K] > 1$, and suppose that there were only finitely many prime ideals of $\mathcal{O}_K$ that are not totally split in L, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Then

$$\begin{aligned}\zeta_L(s) &= \prod_{\mathfrak{p}\in\mathcal{V}'} \prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1-\mathfrak{N}(\mathfrak{P})^{-s}} \\ &= \prod_{\mathfrak{p}\in\mathcal{V}'\setminus\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}} \left(\frac{1}{1-\mathfrak{N}(\mathfrak{p})^{-s}}\right)^{[L:K]} \times \prod_{i=1}^{r} \prod_{\mathfrak{P}|\mathfrak{p}_i} \frac{1}{1-\mathfrak{N}(\mathfrak{P})^{-s}} \\ &= \zeta_K(s)^{[L:K]} \times \prod_{i=1}^{r} \left(\left(\frac{1}{1-\mathfrak{N}(\mathfrak{p}_i)^{-s}}\right)^{-[L:K]} \prod_{\mathfrak{P}|\mathfrak{p}_i} \frac{1}{1-\mathfrak{N}(\mathfrak{P})^{-s}} \right).\end{aligned}$$

By comparing the order at the pole $s = 1$, we would have $[L : K] = 1$. This contradicts the assumption $[L : K] > 1$, and the proof is complete. □

3 Brauer groups

The Brauer group is a group obtained as a quotient of the monoid consisting of isomorphism classes of central simple algebras over a field. Brauer groups are useful to describe relationship between local and global fields, although its definition does not tell it at a glace. We refer to [14] and [39, Chapter 8] for general theory of central simple algebras and Brauer groups. In this section, the letter K stands for a field. For a K-algebra A, we write $[A : K]$ for the dimension of A over K.

3.1 Definitions

For a K-algebra A and its subset S, the subalgebra $Z_S(A) := \{a \in A \mid as = sa \text{ for all } s \in S\}$ is called the *centralizer of* S in A. The *center* of A is the centralizer $Z_A(A)$ of itself.

Definition 3.1. Let A be a K-algebra.

(i) A is *simple* if A contains no two-sided ideal other then 0 and A itself.

(ii) A is *central* (over K) if its center is K.

We write $M_n(A)$ for the algebra of all $n \times n$ matrices with entries in a K-algebra A. If A is a division algebra with center K then the full matrix algebra $M_n(A)$ is simple and central over K (see [39, Chapter 8, Theorem 1.4]). Conversely, Wedderburn's theorem claims that any simple algebra is isomorphic to the full matrix algebra over a division algebra.

Theorem 3.2 (Wedderburn)**.** *Let A be a simple K-algebra whose K-dimension is finite. Then there exists a division K-algebra and a positive integer n such that $A \cong M_n(D)$. Furthermore, D is unique up to isomorphism and n is also unique.*

Proof. See Corollary 1.6 and Theorem 1.9 of [39, Chapter 8]. □

Whenever we say a *central simple K-algebra A*, we assume that A is finite dimensional over K. The *Brauer group* $\mathrm{Br}(K)$ of K is defined as follows. First, let $\mathcal{A}_K$ denote the set of all isomorphism classes of central simple K-algebras. The tensor product of two central simple K-algebras is again a central simple K-algebra (see [39, Chapter 8, Theorem 3.2]). Hence the set $\mathcal{A}_K$ becomes a commutative monoid with the operation $\otimes_K$. Note that the identity element of this monoid is the K-algebra K.

Next, we introduce an equivalence relation on $\mathcal{A}_K$. Let A, A' be central simple K-algebras. Then, by Wedderburn's theorem 3.2, there exist division K-algebras D, D' such that $A \cong M_n(D)$ and $A' \cong M_{n'}(D')$ for some $n, n' \in \mathbb{Z}_{>0}$, and D, D' are uniquely determined by A, A' respectively. We say that A and A' are *Brauer equivalent*, denoted $A \sim A'$, if $D \cong D'$. Then it can be easily seen that the Brauer equivalence defines an equivalence relation on $\mathcal{A}_K$. Each equivalence class is called a *Brauer class*, and we write $[A]_K$ for the Brauer class represented by A. The quotient $\mathcal{A}_K/\sim$ is denoted by $\mathrm{Br}(K)$. Wedderburn's theorem 3.2 shows that each Brauer class is represented by exactly one division K-algebra.

Finally, we check that the set $\mathrm{Br}(K)$ is in fact a group with the operation induced by $\otimes_K$. The following lemma gives a characterization of the Brauer equivalence.

Lemma 3.3. *Let A, A' be central simple K-algebras. Then $A \sim A'$ if and only if there exist integers $r, r' \in \mathbb{Z}_{>0}$ such that $M_r(A) \cong M_{r'}(A')$.*

Proof. Let D and D' denote division K-algebras such that $A \cong M_n(D)$ and $A' \cong M_{n'}(D')$ where $n, n' \in \mathbb{Z}_{>0}$. Suppose that $A \sim A'$. Then $D \cong D'$, and we have $M_{n'}(A) \cong M_{n'}(M_n(D)) \cong M_{nn'}(D)$ and $M_n(A') \cong M_n(M_{n'}(D)) \cong M_{nn'}(D)$. Hence $M_{n'}(A) \cong M_n(A')$. Conversely, suppose that there exist $r, r' \in \mathbb{Z}_{>0}$ such that $M_r(A) \cong M_{r'}(A')$. Since $M_r(A) \cong M_r(M_n(D)) \cong M_{rn}(D)$ and $M_{r'}(A') \cong M_{r'}(M_{n'}(A')) \cong M_{r'n'}(D')$, we obtain $M_{rn}(D) \cong M_{r'n'}(D')$. Thus $D \cong D'$ by the uniqueness part of Wedderburn's theorem 3.2. This means that $A \sim A'$, and the proof is complete. □

Proposition 3.4. *Let A, A', B, B' be central simple K-algebras.*

(i) *If $A \sim A'$ and $B \sim B'$ then $A \otimes_K B \sim A' \otimes_K B'$.*

(ii) *The opposite A^{op} of A is also a central simple K-algebra. Here the* opposite A^{op} *of A is the K-algebra which is the same as A as a K-vector space, with the multiplication performed in the reverse order.*

(iii) $A \otimes_K A^{\mathrm{op}} \cong M_{[A:K]}(K)$.

Proof. Suppose that $A \sim A'$ and $B \sim B'$. By Lemma 3.3, there are integers r, r', s, s' such that $M_r(A) \cong M_{r'}(A')$ and $M_s(B) \cong M_{s'}(B')$. Then

$$\begin{aligned} M_{rs}(A \otimes_K B) &\cong M_{rs}(K) \otimes_K (A \otimes_K B) \cong (M_r(K) \otimes_K A) \otimes_K (M_s(K) \otimes_K B) \\ &\cong M_r(A) \otimes_K M_s(B) \cong M_{r'}(A') \otimes_K M_{s'}(B') \cong M_{r's'}(A' \otimes_K B'). \end{aligned}$$

Again by Lemma 3.3, we obtain $A \otimes_K B \sim A' \otimes_K B'$. This shows the assertion (i). The assertion (ii) is clear because any two-sided ideal of A^{op} is also a two-sided ideal of A. For (iii), see [39, Chapter 8, Theorem 3.4]. □

Proposition 3.4 (i) shows that the tensor product induces an operation on the quotient $\mathrm{Br}(K) = \mathcal{A}_K/\sim$, and it becomes a monoid again. We write $+$ for this induced operation additively:

$$[A]_K + [B]_K := [A \otimes_K B]_K \quad (A, B \in \mathcal{A}_K).$$

Moreover, for any $A \in \mathcal{A}_K$, it follows from Proposition 3.4 (ii) and (iii) that $A^{\mathrm{op}} \in \mathcal{A}_K$ and

$$[A]_K + [A^{\mathrm{op}}]_K = [A \otimes_K A^{\mathrm{op}}]_K = [M_{[A:K]}(K)]_K = [K]_K = 0.$$

This means that the inverse of $[A]_K$ is given by $[A^{\mathrm{op}}]_K$. Therefore, the monoid $\mathrm{Br}(K)$ is in fact a group.

Definition 3.5. The group $\mathrm{Br}(K)$ is called the *Brauer group* of K.

Remark 3.6. The Brauer group can be written in terms of Galois cohomology: if K^{sep} denotes a separable closure of K then there is a natural isomorphism between the second cohomology group $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$ and the Brauer group $\mathrm{Br}(K)$. We refer to [14, §12] and [41, Chapter X-§§4 and 5].

3.2 Restriction and corestriction

Here, we explain two homomorphisms between Brauer groups called the restriction map and corestriction map. Let L be an extension field of K (extension degree can be infinite). For a central simple K-algebra A, the tensor product $A \otimes_K L$ is a central simple L-algebra. In fact, we have:

Proposition 3.7. *Let A be a K-algebra. Then A is a central simple K-algebra if and only if $A \otimes_K L$ is a central simple L-algebra.*

Proof. See [14, §7 Corollary 6]. □

Definition 3.8. The *restriction map* is the natural map defined by

$$\mathrm{res}_{L/K} : \mathrm{Br}(K) \to \mathrm{Br}(L),\ [A]_K \mapsto [A \otimes_K L]_L \quad (A \in \mathcal{A}_K).$$

The restriction map is a group homomorphism because $(A \otimes_K A') \otimes_K L \cong (A \otimes_K L) \otimes_L (A' \otimes_K L)$ for $A, A' \in \mathcal{A}_K$. Furthermore, restriction maps have transitivity: if E/L is a field extension then

$$\mathrm{res}_{E/K} = \mathrm{res}_{E/L} \circ \mathrm{res}_{L/K},$$

because $(A \otimes_K L) \otimes_L E = A \otimes_K E$ for $A \in \mathcal{A}_K$.

Definition 3.9. Let L/K be a field extension. A central simple K-algebra A (or its Brauer class) is *split* by L if $A \otimes_K L \cong M_n(L)$ for some $n \in \mathbb{Z}_{\geq 0}$, i.e., $\mathrm{res}_{L/K}([A]_K) = 0$. We define $\mathrm{Br}(L/K) := \ker(\mathrm{res}_{L/K})$. This is the subgroup of $\mathrm{Br}(K)$ consisting of all Brauer classes split by L.

Transitivity of restriction maps implies that if a central simple K-algebra A is split by an extension field L of K then A is split also by any extension field of L.

The corestriction map is a homomorphism in the reverse direction defined when L/K is a finite separable extension. We give a brief sketch of its definition and properties. We begin by defining a K-algebra called the corestriction for an L-algebra. Let L/K be a finite separable extension, and N the Galois closure of L/K. Put $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(N/L)$. For an N-algebra C and an automorphism $\sigma \in G$, we define ${}^\sigma C$ to be the ring C equipped with the N-algebra structure $i_C \circ \sigma^{-1} : N \to C$, where $i_C : N \to C$ is the N-algebra structure of C.

Let B be a L-algebra, and let $\mathcal{R}$ be a system of representatives for the left cosets of H in G, that is, $G = \bigcup_{\rho \in \mathcal{R}} \rho H$. Then, the N-algebra $B^{(G:H)} := \bigotimes_{\rho \in \mathcal{R}} {}^\rho(B \otimes_L N)$ does not depend on the choice of $\mathcal{R}$ up to isomorphism ([14, §8, Lemma 3]). Moreover, the Galois group G acts on $B^{(G:H)}$ from the left in a little complicated but standard way, and the fixed subalgebra $(B^{(G:H)})^G$ is a K-algebra such that $(B^{(G:H)})^G \otimes_K N \cong B^{(G:H)}$ (Lemma 3 and Corollary 1 of [14, §8]). This K-algebra $(B^{(G:H)})^G$ is called the *corestriction* of B with respect to the extension L/K, and denoted by $\mathrm{cor}_{L/K}(B)$. Corestrictions have following properties.

Proposition 3.10. *Let L/K be a finite separable extension.*

(i) *For a K-algebra A, we have* $\mathrm{cor}_{L/K}(A \otimes_K L) \cong A^{\otimes [L:K]}$.

(ii) *For L-algebras B and B', we have* $\mathrm{cor}_{L/K}(B \otimes_L B') \cong \mathrm{cor}_{L/K}(B) \otimes_K \mathrm{cor}_{L/K}(B')$.

(iii) *Let E/L be a finite separable extension. For an E-algebra C, we have* $\mathrm{cor}_{E/K}(C) \cong \mathrm{cor}_{L/K}(\mathrm{cor}_{E/L}(C))$.

Proof. See [14, §8, Lemmas 9, 10, and 11]. □

Let L/K be a finite separable extension, and $N, G, H, \mathcal{R}$ as above. Let B is a central simple K-algebra. Then $B \otimes_K N$ is a central simple N-algebra by Proposition 3.7. It is clear that ${}^{\sigma}(B \otimes_K N)$ is also a central simple N-algebra for any $\sigma \in G$, and hence so is the tensor product $B^{(G:H)} = \bigotimes_{\rho \in \mathcal{R}} {}^{\rho}(B \otimes_L N)$. By the isomorphism $(B^{(G:H)})^G \otimes_K N \cong B^{(G:H)}$ and Proposition 3.7, it follows that the corestriction $\mathrm{cor}_{L/K}(B) = (B^{(G:H)})^G$ is a central simple K-algebra.

Definition 3.11. Let L/K is a finite separable extension. The *corestriction map* is the map defined by

$$\mathrm{cor}_{L/K} : \mathrm{Br}(L) \to \mathrm{Br}(K),\ [B]_L \mapsto [\mathrm{cor}_{L/K}(B)]_K \quad (B \in \mathcal{A}_L).$$

Proposition 3.10 (ii) and (iii) shows that the corestriction maps are group homomorphisms and have transitivity. Moreover, Proposition 3.10 (i) implies that

$$\mathrm{cor}_{L/K} \circ \mathrm{res}_{L/K}([A]_K) = [L : K] \cdot [A]_K \tag{5}$$

for any $A \in \mathcal{A}_K$.

3.3 General results for central simple algebras

Here we review some general results in the theory of central simple algebras. The Skolem-Noether theorem, described below, is fundamental.

Theorem 3.12 (Skolem-Noether)**.** *Let A, B be simple K-algebras, and suppose that $[A : K] < \infty$ and B is central over K. For any homomorphisms $\phi, \psi : A \to B$ of K-algebras, there exists $y \in B^{\times}$ such that $\psi(x) = y\phi(x)y^{-1}$ for all $x \in A$. In other words, there exists an inner automorphism τ of B such that $\psi = \tau \circ \phi$.*

Proof. See [14, §7, Skolem-Noether Theorem]. □

Its proof is omitted here, but one can obtain the following theorem by using the Skolem-Noether theorem.

Theorem 3.13 (Centralizer theorem)**.** *Let A be a central simple K-algebra and B its subalgebra. Then $Z_A(B) \otimes_K M_{[B:K]}(K) \cong A \otimes_K B^{\mathrm{op}}$.*

Proof. See [14, §7, Centralizer Theorem]. □

By using the centralizer theorem, we show some propositions about a central simple K-algebra and field extension L/K.

Proposition 3.14. *Let A be a central simple K-algebra, and let L be an extension field of K contained in A. If $[A : K] = [L : K]^2$ then $Z_A(L) = L$, and A is split by L.*

Proof. It is obvious that $L \subset Z_A(L)$. So it suffices to show that $[Z_A(L) : K] = [L : K]$ in order to get $Z_A(L) = L$. By the centralizer theorem 3.13, it follows that

$$Z_A(L) \otimes_K M_{[L:K]}(K) \cong A \otimes_K L^{\mathrm{op}} = A \otimes_K L. \tag{6}$$

By considering their dimensions, we get $[Z_A(L) : K][L : K]^2 = [A : K][L : K]$. We now suppose that $[A : K] = [L : K]^2$. Then $[Z_A(L) : K][L : K]^2 = [L : K]^3$, and $[Z_A(L) : K] = [L : K]$ as required. This implies that $Z_A(L) = L$. Therefore, by the isomorphism (6) again, we obtain

$$A \otimes_K L \cong Z_A(L) \otimes_K M_{[L:K]}(K) = L \otimes_K M_{[L:K]}(K) \cong M_{[L:K]}(L).$$

This means that A is split by L. The proof is complete. □

The converse of this proposition holds in the sense of the following proposition.

Proposition 3.15. *Let A be a central simple K-algebra, and let L be an extension field of K with finite degree. If A is split by L then there exists a central simple K-algebra B such that $[B]_K = [A]_K$, $L \subset B$, and $[B : K] = [L : K]^2$.*

Proof. Suppose that A is split by L, and let m denote the integer such that $A \otimes_K L \cong M_m(L)$. We have

$$A^{\mathrm{op}} \otimes_K L = (A \otimes_K L^{\mathrm{op}})^{\mathrm{op}} \cong M_m(L)^{\mathrm{op}} \cong M_m(L), \tag{7}$$

where the last isomorphism is given by the homomorphism sending a matrix to its transpose. On the other hand, the field L can be embedded in the algebra $\mathrm{End}_K(L)$ of endomorphisms by left multiplication. Furthermore $\mathrm{End}_K(L)$ can be embedded in $M_n(K)$, where $n := [L : K]$, by fixing a basis of L over K. Hence, we can consider L to be contained in $M_n(K)$. Combining this with the isomorphism (7), we regard $A^{\mathrm{op}} \otimes_K L$ as a subalgebra of $M_{mn}(K)$:

$$A^{\mathrm{op}} \otimes_K L \xrightarrow{\sim} M_m(L) \hookrightarrow M_m(M_n(K)) = M_{mn}(K).$$

We now define $B := Z_{M_{mn}(K)}(A^{\mathrm{op}}) \subset M_{mn}(K)$. Then it is clear that $L \subset B$, and the centralizer theorem 3.13 implies that

$$B \otimes_K M_{[A^{\mathrm{op}}:K]}(K) \cong M_{mn}(K) \otimes_K (A^{\mathrm{op}})^{\mathrm{op}} = M_{mn}(K) \otimes_K A. \tag{8}$$

Hence $[B]_K = [A]_K$. It remains to prove $[B : K] = n^2$. Note that $[A : K] = m^2$ since $A \otimes_K L \cong M_m(L)$. We have $[B \otimes_K M_{[A^{\mathrm{op}}:K]}(K) : K] = [B : K][A : K]^2 = [B : K]m^4$ and $[M_{mn}(K) \otimes_K A : K] = [M_{mn}(K) : K][A : K] = m^4n^2$. Therefore, by the isomorphism (8) again, we obtain $[B : K]m^4 = m^4n^2$, and $[B : K] = n^2$. This completes the proof. □

Another consequence of the centralizer theorem is:

Proposition 3.16. *Every central simple K-algebra is split by a finite Galois extension of K. Namely $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$, where L ranges over all finite Galois extension of K.*

Proof. Let A be a central simple K-algebra, and D a division K-algebra with $[D]_K = [A]_K$. It is sufficient to show that D is split by a finite separable extension of K, because A is split by the Galois closure of the field in that case. Let L be a maximal commutative subalgebra of D. Of course it is a field. Moreover, Köthe's theorem ([14, p. 64]) states that L can be chosen so that L/K is separable. So we assume that L/K is separable. By maximality of L, we have $Z_D(L) = L$. Then the centralizer theorem 3.13 gives the isomorphism $D \otimes_K L \cong M_{[L:K]}(L)$ as in the proof of Proposition 3.14. This means that D is split by the finite separable extension L. □

3.4 Cyclic algebras

Here, we introduce central simple algebras called cyclic algebras, which will play a crucial role in calculating the Brauer group of a local field. In fact, every Brauer class is represented by a cyclic algebra when the considering field is a local field. Some important results on cyclic algebras will be aggregated into one exact sequence (Theorem 3.20). The letter K continues to be an arbitrary field.

Definition 3.17. Let L/K be a cyclic extension of degree n, and fix a generator $\sigma \in \mathrm{Gal}(L/K)$ of the Galois group. For $\alpha \in K^\times$, the symbol $(\sigma, \alpha)_K$ denotes the n^2-dimensional K-algebra defined by the following data:

- $(\sigma, \alpha)_K$ contains L and has an L-basis of the form $1, \mathbb{e}, \mathbb{e}^2, \dots, \mathbb{e}^{n-1}$:
$$(\sigma, \alpha)_K = L \cdot 1 \oplus L \cdot \mathbb{e} \oplus L \cdot \mathbb{e}^2 \oplus \cdots \oplus L \cdot \mathbb{e}^{n-1}.$$
- The multiplication is determined by
$$\mathbb{e}^n = \alpha \quad \text{and} \quad \mathbb{e} \cdot y = \sigma(y) \cdot \mathbb{e} \text{ for any } y \in L.$$

Such a K-algebra is called a *cyclic algebra* over K. When emphasizing the cyclic extension L/K, we also write $(\sigma, L/K, \alpha)_K$ for $(\sigma, \alpha)_K$.

In the following, we fix a cyclic extension L/K of degree n and a generator $\sigma \in \mathrm{Gal}(L/K)$ of the Galois group. Any cyclic algebra $(\sigma, \alpha)_K$ ($\alpha \in K^\times$) is a central simple K-algebra (see [39, Chapter 8, Theorem 12.1]), and it is split by L by Proposition 3.14. The Brauer class of the cyclic algebra $(\sigma, \alpha)_K$ is denoted by $[\sigma, \alpha]_K$. We consider the map
$$K^\times \to \mathrm{Br}(K),\ \alpha \mapsto [\sigma, \alpha]_K. \tag{9}$$

Lemma 3.18. *For any $\alpha, \beta \in K^\times$, we have $(\sigma, \alpha)_K \otimes_K (\sigma, \beta)_K \cong M_n((\sigma, \alpha\beta)_K)$. As a result, the map (9) is a group homomorphism.*

Proof (Sketch). Put $A = (\sigma, \alpha)_K$, $B = (\sigma, \beta)_K$, $C = (\sigma, \alpha\beta)_K$, and write
$$E = L \cdot 1 \oplus L \cdot \mathbb{e}_E \oplus L \cdot \mathbb{e}_E^2 \oplus \cdots \oplus L \cdot \mathbb{e}_E^{n-1} \quad (E = A, B, \text{ or } C)$$
as in Definition 3.17. Let Id_m denote the identity matrix of size m. A K-algebra homomorphisms $\phi : A \to M_n(C)$ is defined by
$$\phi(\mathbb{e}_A) = \left(\begin{array}{c:c} \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & \mathrm{Id}_{n-1} \\ \hdashline \alpha & \begin{matrix} 0 & \cdots & 0 \end{matrix} \end{array}\right) \in M_n(C),$$
$$\phi(y) = \mathrm{diag}(y, \sigma(y), \dots, \sigma^{n-1}(y)) \in M_n(C) \text{ for any } y \in L.$$
Also, a K-algebra homomorphisms $\psi : B \to M_n(C)$ is defined by
$$\psi(\mathbb{e}_B) = \mathbb{e}_C\, \phi(\mathbb{e}_A)^{-1}, \quad \psi(y) = y\, \mathrm{Id}_n \text{ for any } y \in L.$$
Then, a homomorphism $A \otimes_K B \to M_n(C)$ is induced by
$$A \times B \to M_n(C),\ (a, b) \mapsto \phi(a)\psi(b).$$
The induced homomorphism is injective since $A \otimes_K B$ is simple, and then surjective since $[A \otimes_K B : K] = n^4 = [M_n(C) : K]$. Therefore $A \otimes_K B \cong M_n(C)$. By taking Brauer classes, we obtain $[\sigma, \alpha]_K + [\sigma, \beta]_K = [\sigma, \alpha\beta]_K$. This means that the map (9) is a group homomorphism. See [14, §10, Lemma 4] for more detail. □

Note that this lemma implies that $[\sigma, 1]_K = 0$ in $\mathrm{Br}(K)$ and hence $(\sigma, 1)_K \cong M_n(K)$. The following theorem means that the homomorphism (9) induces an injection $K^\times/N_{L/K}(L^\times) \to \mathrm{Br}(K)$.

Proposition 3.19. *Let $\alpha \in K^\times$. The quaternion algebra $(\sigma, \alpha)_K$ is isomorphic to $(\sigma, 1)_K$ if and only if $\alpha \in N_{L/K}(L^\times)$.*

Proof (Sketch). Put $A = (\sigma, \alpha)_K, B = (\sigma, 1)_K$, and let $\mathbb{e}_A \in A, \mathbb{e}_B \in B$ be as in Definition 3.17. Suppose that $\alpha \in N_{L/K}(L^\times)$, and write $\alpha = N_{L/K}(z)$ where $z \in L^\times$. Then, the K-algebra homomorphism $\phi : A \to B$ defined by

$$\phi(\mathbb{e}_A) = z\mathbb{e}_B, \quad \phi(y) = y \text{ for all } y \in L$$

is an automorphism. Suppose conversely that $A \cong B$. We fix an isomorphism $\phi : A \to B$. By the Skolem-Noether theorem 3.12, there exists an inner automorphism $\tau : B \to B$ such that the diagram

$$\begin{array}{ccccc} L & \xrightarrow{\text{incl}} & A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle \sigma} & & & & \downarrow{\scriptstyle \tau} \\ L & & \xrightarrow{\qquad\text{incl}\qquad} & & B \end{array}$$

is commutative. Put $y = \mathbb{e}_B^{-1}\tau(\phi(\mathbb{e}_A)) \in B$. A computation shows that $y \in Z_B(L) = L$, where the equality $Z_B(L) = L$ follows from Proposition 3.14. Then

$$\alpha = \tau(\phi(\mathbb{e}_A))^n = (\mathbb{e}_B\, y)^n = (\textstyle\prod_{i=1}^n \sigma(y))\, \mathbb{e}_B^n = \mathrm{N}_{L/K}(y),$$

which means that $\alpha \in \mathrm{N}_{L/K}(L^\times)$. This completes the proof. □

As a result, the order of the Brauer class of any cyclic algebra is at most n. Indeed, we have

$$n \cdot [\sigma, \alpha]_K = [\sigma, \alpha^n]_K = [\sigma, \mathrm{N}_{L/K}(\alpha)]_K = 0$$

for any $\alpha \in K^\times$. The main theorem of this subsection is as follows.

Theorem 3.20. *The sequence*

$$1 \to K^\times/N_{L/K}(L^\times) \overset{[\sigma, \cdot]_K}{\longrightarrow} \mathrm{Br}(K) \overset{\mathrm{res}_{L/K}}{\longrightarrow} \mathrm{Br}(L)$$

is exact. In particular $K^\times/N_{L/K}(L^\times) \cong \mathrm{Br}(L/K)$.

Proof. Injectivity of the homomorphism $[\sigma, \cdot]_K : K^\times/N_{L/K}(L^\times) \to \mathrm{Br}(K)$ is by Proposition 3.19. So we prove that $\mathrm{im}([\sigma, \cdot]_K) = \ker(\mathrm{res}_{L/K})$. We already have the inclusion $\mathrm{im}([\sigma, \cdot]_K) \subset \ker(\mathrm{res}_{L/K})$ because Proposition 3.14 shows that the cyclic algebra $(\sigma, \alpha)_K$ is split by L for any $\alpha \in K^\times$. Suppose that a central simple K-algebra A is split by L. Then, by Proposition 3.15, there exists a central simple K-algebra B such that $[B]_K = [A]_K$, $L \subset B$, and $[B : K] = n^2$. Note that $Z_B(L) = L$ by Proposition 3.14. We show that $B \cong (\sigma, \beta)_K$ for some $\beta \in K^\times$. By the Skolem-Noether theorem 3.12, there exists $\mathbb{e}_B \in B^\times$ such that $\sigma(y) = \mathbb{e}_B\, y\, \mathbb{e}_B^{-1}$ for all $y \in L$. Put $\beta = \mathbb{e}_B^n$. Then β is in $Z_B(L) = L$ because for any $y \in L$ we have

$$\beta y \beta^{-1} = \mathbb{e}_B^n\, y\, \mathbb{e}_B^{-n} = \sigma^n(y) = \mathrm{id}_L(y) = y.$$

Moreover, we have $\sigma(\beta) = \mathbb{e}_B\, \mathbb{e}_B^n\, \mathbb{e}_B^{-1} = \beta$, which implies that β belongs to K by the fundamental theorem of Galois theory. Therefore, a K-algebra homomorphism $(\sigma, \beta)_K \to B$ is defined by

$$\sum_{i=0}^{n-1} y_i\, \mathbb{e}^i \mapsto \sum_{i=0}^{n-1} y_i\, \mathbb{e}_B^i \quad (y_0, \ldots, y_{n-1} \in L)$$

where $\mathfrak{e} \in (\sigma, \beta)_K$ is as in Definition 3.17. This is injective since $(\sigma, \beta)_K$ is simple, and then surjective since $[(\sigma, \beta)_K : K] = n^2 = [B : K]$. Hence $B \cong (\sigma, \beta)_K$, and $[A]_K = [B]_K = [\sigma, \beta]_K$. This means that $\ker(\mathrm{res}_{L/K}) \subset \mathrm{im}([\sigma, \cdot]_K)$, and the proof is complete. □

The following proposition is another important result.

Proposition 3.21. *Let M be an intermediate field of L/K, and put $m = [M : K]$.*

(i) *σ^m is a generator of $\mathrm{Gal}(L/M)$, and $(\sigma, L/K, \alpha)_K \otimes_K M \sim (\sigma^m, L/M, \alpha)_M$.*

(ii) *$\sigma|_M$ is a generator of $\mathrm{Gal}(M/K)$, and $(\sigma, L/K, \alpha^{n/m})_K \sim (\sigma|_M, M/K, \alpha)_K$.*

Proof. See [14, §10 Lemmas 6 and 8]. □

3.5 Brauer groups of local fields

Here we compute Brauer groups of local fields.

Archimedean case We recall that an archimedean local field is $\mathbb{R}$ or $\mathbb{C}$.

Theorem 3.22. *The Brauer group $\mathrm{Br}(\mathbb{R})$ is of order 2, and $\mathrm{Br}(\mathbb{C})$ is a trivial group.*

Proof. The finite Galois extensions of $\mathbb{R}$ are $\mathbb{R}$ itself and $\mathbb{C}$. Thus $\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}/\mathbb{R})$ by Proposition 3.16. On the other hand, the extension $\mathbb{C}/\mathbb{R}$ is a cyclic extension having the complex conjugate $\bar{\cdot}$ as a generator of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Hence $\mathrm{Br}(\mathbb{C}/\mathbb{R}) \cong \mathbb{R}^\times/\{z\bar{z} \mid z \in \mathbb{C}\} \cong \{1, -1\}$ by Theorem 3.20. This shows the first assertion. Similarly, we get $\mathrm{Br}(\mathbb{C}) = 0$ since there is no finite Galois extension of $\mathbb{C}$ other than $\mathbb{C}$ itself. □

This theorem means there is a unique non-commutative division algebra over $\mathbb{R}$, that is, *the algebra of Hamilton quaternions*.

Remark 3.23. In a similar way to the proof of Theorem 3.22, one can show that the Brauer group of any finite field is trivial, since the norm map of any finite extension of a finite field is surjective (Corollary 2.5). As a result, every finite division algebra is a field. This fact is known as Wedderburn's little theorem.

Definition 3.24. By Theorem 3.22, there exists a unique nontrivial homomorphism $\mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}$ (assign $1/2 + \mathbb{Z}$ to the nonzero class in $\mathrm{Br}(\mathbb{R})$). This homomorphism is referred to as the *invariant map* and denoted by $\mathrm{inv}_\mathbb{R}$. Similarly, the zero map $\mathrm{Br}(\mathbb{C}) \to \mathbb{Q}/\mathbb{Z}$ is also referred to as the *invariant map* and denoted by $\mathrm{inv}_\mathbb{C}$.

Non-archimedean case Suppose that K is a non-archimedean local field. In this case, there exists a canonical isomorphism $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$. We explain it here by accepting the following fact.

Theorem 3.25. *Any central simple K-algebra is split by a finite unramified extension of K.*

Proof. See [41, Chapter XII, Theorem 1]. □

Let $\overline{K}$ denote the algebraic closure of K, and $K_n \subset \overline{K}$ the unramified extension of degree n over K for each $n \in \mathbb{Z}_{>0}$, see Corollary 2.16. Theorem 3.25 means that for any $[A]_K \in \mathrm{Br}(K)$ there exists positive integer n such that $[A]_K \in \mathrm{Br}(K_n/K)$. In other words, we have

$$\mathrm{Br}(K) = \bigcup_{n \geq 1} \mathrm{Br}(K_n/K).$$

On the other hand, for the group $\mathbb{Q}/\mathbb{Z}$ we have

$$\mathbb{Q}/\mathbb{Z} = \bigcup_{n \geq 1} \left(\frac{1}{n}\mathbb{Z} \right) / \mathbb{Z}.$$

To get an isomorphism $\mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, we first define the isomorphism $\mathrm{inv}_{K_n/K} : \mathrm{Br}(K_n/K) \to \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$ as follows. We recall that the extension K_n/K is a cyclic extension (Corollary 2.17), and there is a generator of $\mathrm{Gal}(K_n/K)$ called the Frobenius automorphism. Let $\sigma_n \in \mathrm{Gal}(K_n/K)$ denote the Frobenius automorphism of K_n/K. Then the homomorphism $[\sigma_n, \cdot\,]_K : K_n^\times \to \mathrm{Br}(K)$ gives rise to an isomorphism $K^\times / \mathrm{N}_{K_n/K}(K_n^\times) \to \mathrm{Br}(K_n/K)$ by Theorem 3.20. This induced isomorphism is denoted by ϕ_n. On the other hand, the map

$$\psi_n : K^\times / \mathrm{N}_{L/K}(K_n^\times) \to \left(\frac{1}{n}\mathbb{Z} \right) / \mathbb{Z},\ \alpha \mapsto \frac{1}{n} v_K(\alpha) \bmod \mathbb{Z}$$

is also an isomorphism by Theorem 2.22. The isomorphism $\mathrm{inv}_{K_n/K} : \mathrm{Br}(K_n/K) \to \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$ is defined to be the composition $\psi_n \circ \phi_n^{-1}$. For positive integers $m, n \in \mathbb{Z}_{>0}$ with $m \mid n$, the diagram

$$\begin{array}{ccccc} \mathrm{Br}(K_m/K) & \xleftarrow{\phi_m} & K^\times / \mathrm{N}_{K_m/K}(K_m^\times) & \xrightarrow{\psi_m} & \left(\frac{1}{m}\mathbb{Z}\right)/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{incl}} & & \downarrow{\scriptstyle \alpha \mapsto \alpha^{n/m}} & & \downarrow{\scriptstyle \mathrm{incl}} \\ \mathrm{Br}(K_n/K) & \xleftarrow{\phi_n} & K^\times / \mathrm{N}_{K_n/K}(K_n^\times) & \xrightarrow{\psi_n} & \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z} \end{array} \tag{10}$$

is commutative. Indeed, commutativity of the right square is clear, and that of the left square follows from Proposition 3.21 (ii).

Definition 3.26. By the commutative diagram (10), the mapping $\mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ sending $[A]_K \in \mathrm{Br}(K)$ to $\mathrm{inv}_{K_n/K}([A]_K)$, where n is an integer such that $[A]_K \in \mathrm{Br}(K_n/K)$, is a well-defined automorphism. This automorphism is called the *invariant map* and denoted by $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.

The invariant map has the following property.

Proposition 3.27. *Let L/K be a finite separable extension. Then $\mathrm{inv}_L \circ \mathrm{res}_{L/K} \circ \mathrm{inv}_K^{-1} : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ is multiplication by $[L : K]$, and $\mathrm{inv}_L \circ \mathrm{cor}_{L/K} \circ \mathrm{inv}_K^{-1} : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ is the identity map. Namely, following diagrams are commutative:*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{res}_{L/K}} & \mathrm{Br}(L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z}, \end{array} \qquad \begin{array}{ccc} \mathrm{Br}(L) & \xrightarrow{\mathrm{cor}_{L/K}} & \mathrm{Br}(K) \\ \downarrow{\scriptstyle \mathrm{inv}_L} & & \downarrow{\scriptstyle \mathrm{inv}_K} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Proof (Sketch). We may assume that $L \subset \overline{K}$, and let f be the inertia degree of L/K. Let $[A]_K \in \mathrm{Br}(K)$, and let $n \in \mathbb{Z}_{>0}$ be an integer with $f \mid n$ such that $[A]_K$ is split by K_n. Then $[A]_K$ can be written as $[A]_K = [\sigma_n, K_n/K, \alpha]_K$ for some $\alpha \in K^\times$. Note that $v_L(\alpha) = \frac{[L:K]}{f} v_K(\alpha)$ by Corollary 1.36 and the fundamental identity (Proposition 1.22). Then

$$[L : K] \cdot \mathrm{inv}_K([A]_K) = [L : K]\frac{1}{n} v_K(\alpha) = [L : K]\frac{1}{n}\frac{f}{[L : K]} v_L(\alpha) = \frac{1}{m} v_L(\alpha), \tag{$*$}$$

where $m := n/f$. On the other hand, we have

$$(\sigma_n, K_n/K, \alpha)_K \otimes_K L = (\sigma_n, K_n/K, \alpha)_K \otimes_K K_f \otimes_{K_f} L \sim (\sigma_n^f, K_n/K_f, \alpha)_{K_f} \otimes_{K_f} L$$

by Proposition 3.21 (i). We also have $L \cap K_n = K_f$, and $L \otimes_{K_f} K_n \cong LK_n = L_m$, where L_m is the unramified extension of degree m over L. Under this isomorphism, the automorphism $\mathrm{id}_L \otimes \sigma_n^f$ of $L \otimes_{K_f} K_n$ corresponds to the Frobenius automorphism τ_m of L_m/L. So one obtain an isomorphism $(\sigma_n^f, K_n/K_f, \alpha)_{K_f} \otimes_{K_f} L \cong (\tau_m, L_m/L, \alpha)_L$. Hence

$$\mathrm{inv}_L \circ \mathrm{res}_{L/K}([A]_K) = \mathrm{inv}_L([\tau_m, L_m/L, \alpha]_L) = \frac{1}{m} v_L(\alpha).$$

This equation with $(*)$ shows commutativity of the diagram for the restriction map. Combining it with (5), we also get commutativity of the diagram for the corestriction map. □

Corollary 3.28. *For any cyclic extension L/K of degree n, we have $K^\times / \mathrm{N}_{L/K}(L^\times) \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let L/K be an cyclic extension L/K of degree n. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K^\times / \mathrm{N}_{L/K}(L^\times) & \xrightarrow{[\sigma,\cdot]_K} & \mathrm{Br}(K) & \xrightarrow{\mathrm{res}_{L/K}} & \mathrm{Br}(L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\times 1/n} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where the first row is exact by Theorem 3.20, and the second rows is also exact clearly. This diagram is commutative by Proposition 3.27. Therefore, the automorphism $K^\times / \mathrm{N}_{L/K}(L^\times) \cong \mathbb{Z}/n\mathbb{Z}$ is induced. □

3.6 The Brauer-Hasse-Noether theorem

The Brauer group of an algebraic number field is described as follows.

Theorem 3.29 (Brauer-Hasse-Noether)**.** *Let K be an algebraic number field, and $\mathcal{V}$ the set of all places of K. For each $\theta \in \mathrm{Br}(K)$, we have $\mathrm{res}_{K_v/K}(\theta) = 0$ for almost all $v \in \mathcal{V}$, where K_v is the completion of K at v. Moreover, the sequence*

$$0 \to \mathrm{Br}(K) \xrightarrow{(\mathrm{res}_{K_v/K})_v} \bigoplus_{v \in \mathcal{V}} \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z} \to 0$$

is exact.

Proof. See [19, Theorem 14.11]. This is true also for a function field over a finite field. □

It will be seen in §4 that this theorem plays a central role when discussing the local-global principle for inner products over an algebraic number field.

We close this section by extracting an exact sequence of twisting groups (see Definition 1.10) from the Brauer-Hasse-Noether theorem. Let E be an algebraic number field with a nontrivial involution σ, and let $\mathcal{W}$ be the set of all places of the fixed subfield E^σ.

Notation 3.30. Let $w \in \mathcal{W}$ be a place of E^σ. The completion $(E^\sigma)_w$ of E^σ at w is abbreviated to E_w^σ. We define $E_w := E \otimes_{E^\sigma} E_w^\sigma$. Note that the involution σ extends to the involution $\sigma \otimes \mathrm{id}_{E_w^\sigma}$ of E_w, and we write σ for it again. Then, the fixed subalgebra $(E_w)^\sigma$ is canonically identified with $E_w^\sigma = (E^\sigma)_w$. Moreover, the embedding $E^\times \to E_w^\times$ induces an homomorphism $\mathrm{Tw}(E, \sigma) \to \mathrm{Tw}(E_w, \sigma)$ between twisting groups. If w is not split in E then there exists a unique place u above w, and E_w is (isomorphic to) the completion E_u. In this case, we write

$$\iota_w : \mathrm{Tw}(E_w, \sigma) = (E_w^\sigma)^\times / \mathrm{N}_{E_w/E_w^\sigma}(E_w^\times) \to \mathbb{Z}/2\mathbb{Z}$$

for the isomorphism mentioned in Corollary 3.28. If w is split in E then there exist exactly two places u_1, u_2 of E above w, and $E_w \cong E_{u_1} \times E_{u_2} = E_w^\sigma \times E_w^\sigma$, by Theorem 1.44. In this case, we have $\mathrm{Tw}(E_w, \sigma) = \{1\}$ by Proposition 1.11, and $\iota_w : \mathrm{Tw}(E_w, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ denotes the trivial homomorphism.

Proposition 3.31. *Let E be an algebraic number field with a nontrivial involution σ, and $\mathcal{W}$ the set of all places of E^σ. For each $\mu \in (E^\sigma)^\times$, we have $\mu = 1$ in $\mathrm{Tw}(E_w, \sigma)$ for almost all $w \in \mathcal{W}$, and the sequence*

$$0 \to \mathrm{Tw}(E, \sigma) \longrightarrow \bigoplus_{w \in \mathcal{W}} \mathrm{Tw}(E_w, \sigma) \xrightarrow{\sum_w \iota_w} \mathbb{Z}/2\mathbb{Z} \to 0$$

is exact. Moreover $\mathrm{Tw}(E, \sigma)$ has infinite order.

Proof. For a place $w \in \mathcal{W}$ split in E, we define $[\sigma, \cdot]_{E_w^\sigma} : \mathrm{Tw}(E_w, \sigma) \to \mathrm{Br}(E_w^\sigma)$ to be the trivial homomorphism. Let $\widehat{\mathcal{W}}$ be the set of places of E, and consider the diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Tw}(E,\sigma) & \longrightarrow & \displaystyle\bigoplus_{w\in\mathcal{W}} \mathrm{Tw}(E_w,\sigma) & \xrightarrow{\sum_w \iota_w} & \mathbb{Z}/2\mathbb{Z} & & \\
 & & \downarrow{\scriptstyle [\sigma,\cdot]_{E^\sigma}} & & \downarrow{\scriptstyle \bigoplus_w [\sigma,\cdot]_{E_w^\sigma}} & & \downarrow{\scriptstyle \times 1/2} & & \\
0 & \longrightarrow & \mathrm{Br}(E^\sigma) & \longrightarrow & \displaystyle\bigoplus_{w\in\mathcal{W}} \mathrm{Br}(E_w^\sigma) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{res}_{E/E^\sigma}} & & \downarrow & & \downarrow{\scriptstyle \times 2} & & \\
0 & \longrightarrow & \mathrm{Br}(E) & \longrightarrow & \displaystyle\bigoplus_{u\in\widehat{\mathcal{W}}} \mathrm{Br}(E_u) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0,
\end{array}$$

where the second and third rows are exact sequences of the Brauer-Hasse-Noether theorem, and $\bigoplus_{w\in\mathcal{W}} E_w^\sigma \to \bigoplus_{u\in\widehat{\mathcal{W}}} \mathrm{Br}(E_u)$ is given by

$$(\theta_w)_w \mapsto ((\mathrm{res}_{E_u/E_w}(\theta_w))_{u|w})_w \quad (\theta_w \in \mathrm{Br}(E_w^\sigma)).$$

Then, the diagram is commutative, and all columns are exact (it is clear for the right one, and follows from Theorem 3.20 for the rest). Hence, we obtain exactness of the sequence

$$0 \to \mathrm{Tw}(E, \sigma) \longrightarrow \bigoplus_{w \in \mathcal{W}} \mathrm{Tw}(E_w, \sigma) \xrightarrow{\sum_w \iota_w} \mathbb{Z}/2\mathbb{Z}. \qquad (*)$$

Furthermore, Proposition 2.28 shows that there exist infinitely many places of E^σ that are non-split in E. Thus $\sum_w \iota_w : \bigoplus_{w\in\mathcal{W}} \mathrm{Tw}(E_w, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ is surjective since ι_w is an isomorphism for a place $w \in \mathcal{W}$ non-split in E. Moreover $\bigoplus_{w\in\mathcal{W}} \mathrm{Tw}(E_w, \sigma)$ has infinite order. Hence $\mathrm{Tw}(E, \sigma)$ also has infinite order by exactness of the sequence $(*)$. The proof is complete. □

Chapter II
Inner products

4 Inner products and hermitian products over fields

We here discuss inner products and hermitian products over fields. In particular, (classical known) classification results over fields of number theory will be given. This section is written with primary reference to books [35], [39], and [40]. However, differently from these books, local-global arguments are made by using the Brauer-Hasse-Noether theorem.

4.1 Inner products over arbitrary fields

Let K be a field.

Definition 4.1. Let V be a finite dimensional K-vector space. For a symmetric bilinear form $b : V \times V \to K$, we write b^* for the linear map $V \to V^* := \mathrm{Hom}(V, K)$ defined by

$$b^*(v) = (u \mapsto b(u, v)) \quad (v, u \in V).$$

A symmetric bilinear form $b : V \times V \to K$ is *nondegenerate* if the linear map b^* is injective. We refer to a nondegenerate symmetric bilinear form as an *inner product*. If b is an inner product on V then the pair (V, b) is called an *inner product space*. An inner product space (V, b) is sometimes denoted only by V or b.

Remark 4.2. Let V be a finite dimensional K-vector space. For any inner product b on V, the injection $b^* : V \to V^*$ is in fact an isomorphism since V and V^* have the same dimension. However, when considering a symmetric bilinear form over a ring, for example $\mathbb{Z}$, there is a gap between b^* being an injection and b^* being an isomorphism.

Definition 4.3. Let V, V' be finite dimensional K-vector spaces, and b, b' symmetric bilinear forms on V, V' respectively. An *isometry* from (V, b) to (V', b') is a K-linear map $t : V \to V'$ satisfying $b'(t(u), t(v)) = b(u, v)$ for any $u, v \in V$. We say that (V, b) and (V', b') are *isomorphic* if there exists an isomorphism $V \to V'$ of K-vector spaces which is also an isometry. Note that if b is nondegenerate then any isometry $(V, b) \to (V', b')$ is injective. In the case where b is nondegenerate, an isometry from (V, b) to (V, b) itself is referred to as a *isometry of* (V, b), and the group of all isometries of (V, b) is denoted by $\mathrm{O}(V, b)$ or just by $\mathrm{O}(V)$.

Let V be a finite dimensional K-vector space, and $b : V \times V \to K$ a symmetric bilinear form. Let U be a subspace of V. The symmetric bilinear form on U obtained by restricting b to $U \times U$ is denoted by $b|_U$. We say that U is nondegenerate if $b|_U$ is nondegenerate. We define $U^\perp := \{v \in V \mid b(u, v) = 0 \text{ for any } u \in U\}$. Two subspaces U and U' of V are *orthogonal* if $U' \subset U^\perp$, or equivalently $(U')^\perp \subset U$. The following proposition is fundamental.

Proposition 4.4. *Suppose that b is nondegenerate (i.e., (V, b) is an inner product space). Let U be a subspace of V. Then the sequence*

$$0 \to U^\perp \to V \xrightarrow{b^*(\cdot)|_U} U^* \to 0 \tag{11}$$

is exact, where $U^\perp \to V$ is the inclusion. Moreover, we have:

(i) $\dim V = \dim U^\perp + \dim U$.

(ii) $(U^\perp)^\perp = U$.

(iii) *If U is nondegenerate then so is $U^\perp$, and $V = U \oplus U^\perp$.*

Proof. It is clear by definition that $\ker(b^*(\cdot)|_U : V \to U^*) = U^\perp$. We prove that $b^*(\cdot)|_U$ is surjective. Let $\xi \in U^*$, and fix a complement U^c of U in V. Then the map $\tilde{\xi} : V \to K$ defined by

$$\tilde{\xi}(u + u') = \xi(u) \quad (u \in U, u' \in U^c)$$

belongs to V^*. Since b is nondegenerate, there exists a vector $v \in V$ such that $b^*(v) = \tilde{\xi}$. Then we have $b^*(v)|_U = \xi$. This shows that $b^*(\cdot)|_U$ is surjective.

(i). It follows from the exact sequence (11) that

$$\dim V = \dim U^\perp + \dim U^* = \dim U^\perp + \dim U.$$

(ii). It is clear that $U \subset (U^\perp)^\perp$. Hence, it suffices to prove that $\dim(U^\perp)^\perp = \dim U$. By applying (i) to $U^\perp$ we get

$$\dim V = \dim(U^\perp)^\perp + \dim(U^\perp)^* = \dim(U^\perp)^\perp + \dim U^\perp.$$

This equation and the assertion (i) imply that $\dim(U^\perp)^\perp = \dim U$, and therefore $(U^\perp)^\perp = U$.

(iii). Suppose that U is nondegenerate. Then $U \cap U^\perp = 0$. Thus the assertion (i) implies that $V = U \oplus U^\perp$. Furthermore $U^\perp$ must be nondegenerate because otherwise $V = U \oplus U^\perp$ would be degenerate. □

The symbols V and b continue to be a finite dimensional K-vector space and a symmetric bilinear form on V respectively. Let $d \in \mathbb{Z}_{\geq 0}$ denote the dimension of V. For a basis $e_1, \ldots, e_d$ of V, the $d \times d$ matrix $(b(e_i, e_j))_{ij}$ is called the *Gram matrix* of (V, b) with respect to the basis $e_1, \ldots, e_d$. If $e'_1, \ldots, e'_d$ is another basis and T is the change-of-basis matrix, then

$$G' = {}^tTGT \tag{12}$$

where G and G' are the Gram matrices with respect to $e_1, \ldots, e_d$ and $e'_1, \ldots, e'_d$ respectively. If we say 'a' Gram matrix then it means the Gram matrix with respect to some basis. Any Gram matrix is clearly a symmetric matrix. The bilinear form b is nondegenerate if and only if a Gram matrix is nondegenerate, that is, its determinant is not zero (this property does not depend on the choice of a Gram matrix by (12)).

Definition 4.5. Let G be a Gram matrix of (V, b). If b is nondegenerate then equation (12) shows that the class of $\det G$ in $K^\times/K^{\times 2}$ is independent of the choice of a basis. This class is referred to as the *determinant* of (V, b), and denoted by $\det(V, b)$ or $\det b$. If b is degenerate then the determinant of (V, b) is defined to be 0.

It is useful to express an inner product by using a matrix.

Notation 4.6. For a $d \times d$ nondegenerate symmetric matrix $G = (g_{ij})_{ij}$, the symbol

$$\langle G \rangle_K \quad \text{or} \quad \left\langle \begin{matrix} g_{11} & \cdots & g_{1d} \\ \vdots & \ddots & \vdots \\ g_{d1} & \cdots & g_{dd} \end{matrix} \right\rangle_K$$

denote the inner product space such that its underlying space is K^d and G is the Gram matrix with respect to the standard basis of K^d. If G is a diagonal matrix, say $\mathrm{diag}(a_1, \ldots, a_d)$, then we write $\langle a_1, \ldots, a_d \rangle_K$ instead of $\langle \mathrm{diag}(a_1, \ldots, a_d) \rangle_K$ for short. An inner product space (V, b) is isomorphic to $\langle G \rangle_K$ if and only if G is the Gram matrix of (V, b) with respect to some basis.

Definition 4.7. Let (V, b) be an inner product space over K.

(i) A basis of V is called an *orthogonal basis* if the corresponding Gram matrix is diagonal.

(ii) A nonzero vector $v \in V$ is *isotropic* if $b(v, v) = 0$, and *anisotropic* otherwise. The space V (or the bilinear form b) is *isotropic* if V has an isotropic vector, and *totally isotropic* if $b(v, v) = 0$ for all $v \in V$.

(iii) We say that b *represents* $\alpha \in K$ if there exists a nonzero vector v such that $b(v, v) = \alpha$.

We now show that any inner product space can be decomposed into a subspace which has an orthogonal basis and a totally isotropic subspace. As a result, it will be seen that there exists an orthogonal basis if $\mathrm{char}\, K \neq 2$.

Lemma 4.8. *Let (V, b) be an inner product space over K.*

(i) *If b represents a nonzero element $\alpha \in K^\times$ then $b \cong \langle \alpha \rangle_K \oplus b'$ for a suitable inner product b'.*

Suppose that $\mathrm{char}\, K \neq 2$.

(ii) *If b is isotropic then b represents any element of K.*

(iii) *For any $\alpha \in K^\times$, the direct sum $\langle \alpha \rangle_K \oplus b$ is isotropic if and only if b represents $-\alpha$.*

Proof. (i). Suppose that b represents $\alpha \in K^\times$, and take $v \in V$ such that $b(v, v) = \alpha$. Put $b' = b|_{(Kv)^\perp}$. Since the one-dimensional subspace $(Kv, b|_{Kv})$ is nondegenerate, Proposition 4.4 shows that b' is nondegenerate and $(V, b) = (Kv, b|_{Kv}) \oplus ((Kv)^\perp, b') \cong \langle \alpha \rangle_K \oplus ((Kv)^\perp, b')$.

(ii). Suppose that $\mathrm{char}\, K \neq 2$ and b is isotropic. Let $\alpha \in K^\times$ be a nonzero element, and take a nonzero vector $v \in V$ such that $b(v, v) = 0$. Since b is nondegenerate, there exists a vector u such that $b(u, v) = 1$. We define $\beta := b(u, u)$ and $u' := u + \frac{\alpha - \beta}{2} v$. Then

$$b(u', u') = b(u, u) + (\alpha - \beta) b(u, v) + \frac{(\alpha - \beta)^2}{4} b(v, v) = \beta + (\alpha - \beta) = \alpha.$$

This means that b represents α, and we are done.

(iii). Let $\alpha \in K^\times$ be a nonzero element, and let (U, b_U) be a one-dimensional inner product space with a basis u such that $b_U(u, u) = \alpha$. Of course $(U, b_U) \cong \langle \alpha \rangle_K$. Suppose that b represents $-\alpha$, and take a vector $v \in V$ satisfying $b(v, v) = -\alpha$. Then $u + v \in U \oplus V$ is an isotropic vector, and the space $U \oplus V \cong \langle \alpha \rangle_K \oplus V$ is isotropic.

Suppose conversely that $(U \oplus V, b_U \oplus b)$ has an isotropic vector, say $\gamma u + v \in U \oplus V$ where $\gamma \in K$ and $v \in V$. Then $\gamma^2 \alpha + b(v, v) = 0$. If $\gamma \neq 0$ then $b(\gamma^{-1} v, \gamma^{-1} v) = -\alpha$, which means that b represents $-\alpha$. If $\gamma = 0$ then b is isotropic, and hence it represents $-\alpha$ by the assertion (ii). This completes the proof. $\square$

Proposition 4.9. *Let (V, b) be an inner product space over K.*

(i) *We have $(V, b) \cong \langle \alpha_1, \ldots, \alpha_m \rangle_K \oplus (N, b_N)$, where $\alpha_1, \ldots, \alpha_m \in K^\times$ are invertible elements and (N, b_N) is a totally isotropic space.*

(ii) *If $\operatorname{char} K \neq 2$ then (V, b) has an orthogonal basis.*

Proof. (i). If V is totally isotropic then there is nothing to prove. Suppose that V contains an anisotropic vector v_1, and put $\alpha_1 = b(v_1, v_1) \in K^\times$. Then $(V, b) \cong \langle \alpha_1 \rangle_K \oplus (V_1, b_1)$ for a suitable inner product space (V_1, b_1) by Lemma 4.8 (i). If V_1 is totally isotropic then we are done. If V_1 contains an anisotropic vector then the same discussion yields $(V_1, b_1) \cong \langle \alpha_2 \rangle_K \oplus (V_2, b_2)$ for some $\alpha_2 \in K^\times$ and some inner product space (V_2, b_2). Hence $V \cong \langle \alpha_1, \alpha_2 \rangle_K \oplus (V_2, b_2)$. By repeating this discussion, we arrive at the assertion.

(ii). Suppose that $\operatorname{char} K \neq 2$. By assertion (i), it suffices to show that there is no nondegenerate totally isotropic space other than the zero-dimensional space. Let (N, b_N) be a nondegenerate totally isotropic space, and suppose that N were not zero. Then N contains an isotropic vector, but this implies that N would have an anisotropic vector by Lemma 4.8 (ii). This contradicts the fact that (N, b_N) is totally isotropic. Therefore N is zero as required. This completes the proof. □

Remark 4.10. Proposition 4.9 (i) still holds even if b is degenerate, see e.g. [MH73, Chapter I, §3].

An example of an inner product space which has no orthogonal basis is given by a metabolic space, defined below.

Definition 4.11. The symbol $\mathbb{H}_K$ denotes the 2-dimensional inner product space

$$\left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle_K.$$

A *hyperbolic plane* is an inner product space isomorphic to $\mathbb{H}_K$. A basis of a hyperbolic plane is called a *hyperbolic basis* if the corresponding Gram matrix equals $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. An inner product space is said to be *metabolic* if it is isomorphic to $\mathbb{H}_K^{\oplus n}$ for some $n \in \mathbb{Z}_{\geq 0}$, or equivalently, isomorphic to

$$\left\langle \begin{matrix} 0 & \mathrm{Id}_n \\ \mathrm{Id}_n & 0 \end{matrix} \right\rangle_K,$$

where Id_n is the identity matrix of size n.

Example 4.12. Let (V, b) be a metabolic space over a field K with $\operatorname{char} K = 2$. Then V is totally isotropic because V has a basis consisting of isotropic vectors. This implies that V has no orthogonal basis.

The idea of representing elements comes from the view of quadratic forms. We close this subsection with a mention of quadratic forms.

Definition 4.13. Let V be a finite dimensional K-vector space. A *quadratic form* on V is a function $q : V \to K$ such that $q(\alpha v) = \alpha^2 v$ for any $\alpha \in K$ and $v \in V$, and such that the map

$$V \times V \to K,\ (u, v) \mapsto q(u + v) - q(u) - q(v) \tag{13}$$

is bilinear over K. A quadratic form q is *nondegenerate* if so is the symmetric bilinear form (13).

For example, if b is a bilinear form on K-vector space V then the map $v \mapsto b(v,v)$ is a quadratic form. This quadratic form is called the *quadratic form associated with* b and denoted by q_b. An isotropic vector of an inner product space (V,b) is nothing but a nontrivial zero of the quadratic form q_b.

Definition 4.14. Let q be a quadratic form on a finite dimensional K-vector space. Suppose that $\operatorname{char} K \neq 2$. The symmetric bilinear form b_q on V defined by

$$b_q(u,v) = \frac{1}{2}(q(u+v) - q(u) - q(v)) \quad (u,v \in V)$$

is called the *the symmetric bilinear form associated with* q. Note that this is $1/2$ times the bilinear form (13).

Under the assumption $\operatorname{char} K \neq 2$, we have $b = b_{q_b}$ for any symmetric bilinear form b, and $q = q_{b_q}$ for any quadratic form q over K. Hence, by correspondences $b \mapsto q_b$ and $q \mapsto b_q$, the theory of symmetric bilinear forms and that of quadratic form are essentially the same in this case.

Let $G = (g_{ij}) \in M_d(K)$ be a symmetric matrix of size d. The homogeneous polynomial

$$q(X_1, \ldots, X_d) = \sum_{i,j} g_{ij} X_i X_j$$

of degree 2 in d variables can be seen as a quadratic form on the K-vector space K^d. Let $e_1, \ldots, e_d$ be the standard basis of K^d. If $\operatorname{char} K \neq 2$ then $b_q(e_i, e_j) = g_{ij}$, that is, $b_q = \langle G \rangle_K$. In particular, the quadratic form $a_1 X_1^2 + \cdots + a_d X_d^2$ corresponds to the inner product $\langle a_1, \ldots, a_d \rangle_K$.

4.2 Witt's theorem

Let K be a field, and we assume that $\operatorname{char} K \neq 2$ in this subsection. We give an important theorem on extension of an isometry, called Witt's theorem. It leads to the cancellation property of the monoid consisting of all isomorphic classes of inner product spaces.

Lemma 4.15. *Let $(V,b), (V',b')$ be two inner product spaces over K. Let U be a degenerate subspace of V, and $s : U \to V'$ an injective isometry. Then, we can extend s to an isometry $\widehat{U} \to V'$ where $\widehat{U}$ is a nondegenerate subspace of V containing U.*

Proof. Let $u \in U$ be a vector such that $b(u, U) = 0$. Since b is nondegenerate, there exists $v \in V$ such that $b(u,v) = 1$. Put $U_1 := U \oplus Kv \subset V$ and $U' = s(U) \subset V'$. Since $b'^*(\cdot)|_{U'} : V' \to U'^*$ is surjective by Proposition 4.4, there exists $v' \in V'$ such that $b'^*(v')|_{U'} = b^*(v)|_U \circ s^{-1}$, or equivalently $b'(x', v') = b(s^{-1}(x'), v)$ for all $x' \in U'$. Moreover, we may assume that $b'(v',v') = b(v,v)$ by replacing v' with $v' + \frac{1}{2}(b(v,v) - b(v',v'))s(u)$. Let $s_1 : U_1 \to V'$ be the map defined by

$$s_1(x + \alpha v) = s(x) + \alpha v' \quad (x \in U, \alpha \in K).$$

A computation shows that s_1 is an injective isometry extending s. If U_1 is nondegenerate then we are done. If not, by repeating the same procedure, we obtain an injective isometry from a nondegenerate subspace such that it is an extension of s. □

Definition 4.16. Let (V,b) be an inner product space over K, and let $z \in V$ be an anisotropic vector. Then the map $\sigma_z : V \to V$ defined by

$$\sigma_z(v) = v - 2\frac{b(v,z)}{b(z,z)} z \quad (v \in V)$$

is an isometry of V. This isometry is called the *reflection* orthogonal to z. It is clear that $\sigma_z(z) = -z$ and $\sigma_z(u) = u$ for any $u \in (Kz)^\perp$.

Lemma 4.17. *Let (V, b) be an inner product space over K, and let $u, v \in V$ be anisotropic vectors with $b(u, u) = b(v, v)$. Then there exists an isometry $t \in \mathrm{O}(V)$ which can be expressed as a product of at most two reflections such that $t(u) = v$.*

Proof. Put $z_+ = u + v$ and $z_- = u - v$. Then z_+ or z_- is not isotropic; since otherwise we would have

$$0 = b(z_+, z_+) + b(z_-, z_-) = 2b(u, u) + 2b(v, v) = 4b(u, u),$$

which contradicts the assumption that u is anisotropic. Note that $b(z_+, z_-) = 0$. If z_- is anisotropic then

$$\sigma_{z_-}(u) = \sigma_{z_-}\left(\frac{1}{2}(z_+ + z_-)\right) = \frac{1}{2}(z_+ - z_-) = v,$$

and hence the $\sigma_{z_-} \in \mathrm{O}(V)$ is the required isometry. Suppose that z_+ is anisotropic. Then

$$\sigma_{z_+} \circ \sigma_u(u) = \sigma_{z_+}(-u) = \sigma_{z_+}\left(\frac{-1}{2}(z_+ + z_-)\right) = \frac{1}{2}(z_+ - z_-) = v,$$

and therefore $\sigma_{z_+} \circ \sigma_u \in \mathrm{O}(V)$ is the required isometry. □

Theorem 4.18 (Witt's theorem)**.** *Let (V, b) and (V', b') be two isomorphic inner product spaces over K, and let U be a subspace of V. Any injective isometry $U \to V'$ extends to an isometry from V to V'.*

Proof. We can assume that U is nondegenerate by Lemma 4.15. Furthermore, we assume that $(V, b) = (V', b')$ by fixing an isomorphism. Let $s : U \to V$ be an isometry. We argue by induction on $\dim U$. If $\dim U = 1$ then $U = Ku$ for some anisotropic vector $u \in V$, and Lemma 4.17 shows that there exists $t \in \mathrm{O}(V)$ such that $t(u) = s(u)$. This isometry t is an extension of s. Suppose that $\dim U \geq 2$. There exists an anisotropic vector $u \in U$ since $\mathrm{char}\, K \neq 2$. Put $U_1 = Ku, U_2 = \{v \in U \mid b(v, u) = 0\}$, and $W = U_1^{\perp} = \{v \in V \mid b(v, u) = 0\}$. By the case $\dim U = 1$, there exists an extension $t \in \mathrm{O}(V)$ of $s|_{U_1}$. We have $(t^{-1} \circ s)(U_2) \subset W$ because $(t^{-1} \circ s)(u) = u$. By induction hypothesis, there there exists $t' \in \mathrm{O}(W)$ extending $t^{-1} \circ s : U_2 \to W$. Then $t \circ (\mathrm{id}|_{U_1} \oplus t') \in \mathrm{O}(V)$ is an extension of $s : U \to V$. The proof is complete. □

Theorem 4.19 (Witt's cancellation)**.** *Let $(V, b), (V', b'), (V_1, b_1), (V_2, b_2)$ be inner product spaces over K. If $(V, b) \cong (V', b')$ and $(V, b) \oplus (V_1, b_1) \cong (V', b') \oplus (V_2, b_2)$ then $(V_1, b_1) \cong (V_2, b_2)$. In other words, the monoid consisting of all isomorphism classes of inner product spaces over K has the cancellation property.*

Proof. Suppose that $(V, b) \cong (V', b')$ and $(V, b) \oplus (V_1, b_1) \cong (V', b') \oplus (V_2, b_2)$. Let t be an isometry from V to V', and let $\iota : V' \to V' \oplus V_2$ denote the inclusion. Then there exists an extension $\widehat{t} : V \oplus V_1 \to V' \oplus V_2$ of $\iota \circ t : V \to V' \oplus V_2$ by Theorem 4.18. Because $\widehat{t}(V_1) \subset (V')^{\perp} = V_2$ in $V' \oplus V_2$, the restriction $\widehat{t}\,|_{V_1}$ gives an isomorphism between (V_1, b_1) and (V_2, b_2). □

We remark that Witt's cancellation does not hold when the characteristic of K is 2, see [30, Chapter I-§4].

4.3 Quaternion algebras

Let K be a field of characteristic not 2 as in the previous subsection. In the next subsection, we will introduce an invariant of an inner product called the Hasse-Witt invariant. It takes values in the Brauer group $\mathrm{Br}(K)$ and defined by using central simple K-algebras called quaternion algebras. To this end, this subsection gives a summary of quaternion algebras.

Definition 4.20. For $\alpha, \beta \in K^\times$, the symbol $(\alpha, \beta)_K$ denotes the 4-dimensional K-algebra with basis $1, \mathbb{i}, \mathbb{j}, \mathbb{ij}$, and with the multiplication determined by

$$\mathbb{i}^2 = \alpha, \quad \mathbb{j}^2 = \beta, \quad \mathbb{ij} = -\mathbb{ji}. \tag{14}$$

Such an algebra is called a *quaternion algebra* over K. A K-basis $1, \mathbb{i}, \mathbb{j}, \mathbb{ij}$ with relation (14) is called a *standard basis* of $(\alpha, \beta)_K$. Note that the relation $\mathbb{ij} = -\mathbb{ji}$ means that a quaternion algebra is not commutative since $\operatorname{char} K \neq 2$.

Let $A = (\alpha, \beta)_K$ be a quaternion algebra where $\alpha, \beta \in K^\times$. For elements $x = \alpha_0 + \alpha_1\mathbb{i} + \alpha_2\mathbb{j} + \alpha_3\mathbb{ij}$ and $y = \beta_0 + \beta_1\mathbb{i} + \beta_2\mathbb{j} + \beta_3\mathbb{ij}$ of A, where $\alpha_i, \beta_j \in K$, a direct calculation gives

$$\begin{aligned} xy =\ & \alpha_0\beta_0 + \alpha\alpha_1\beta_1 + \beta\alpha_2\beta_2 - \alpha\beta\alpha_3\beta_3 \\ & + (\alpha_0\beta_1 + \alpha_1\beta_0 - \beta\alpha_2\beta_3 + \beta\alpha_3\beta_2)\mathbb{i} \\ & + (\alpha_0\beta_2 + \alpha\alpha_1\beta_3 + \alpha_2\beta_0 - \alpha\alpha_3\beta_1)\mathbb{j} \\ & + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)\mathbb{ij}. \end{aligned}$$

In particular, we have

$$x^2 = (\alpha_0^2 + \alpha\alpha_1^2 + \beta\alpha_2^2 - \alpha\beta\alpha_3^2) + 2\alpha_0\alpha_1\mathbb{i} + 2\alpha_0\alpha_2\mathbb{j} + 2\alpha_0\alpha_3\mathbb{ij}.$$

Hence, the 3-dimensional K-subspace $A_0 := K\mathbb{i} + K\mathbb{j} + K\mathbb{ij}$ can be expressed as

$$A_0 = \{x \in A \mid x^2 \in K \text{ and } x \notin K^\times\}.$$

This shows that the subspace A_0 depends only on the K-algebra structure of A and does not depend on the standard basis $1, \mathbb{i}, \mathbb{j}, \mathbb{ij}$. For an element $x = \alpha_0 + \alpha_1\mathbb{i} + \alpha_2\mathbb{j} + \alpha_3\mathbb{ij}$, we define $\bar{x} := \alpha_0 - \alpha_1\mathbb{i} - \alpha_2\mathbb{j} - \alpha_3\mathbb{ij}$. Then, a computation shows that the map $\bar{\cdot} : A \to A, x \mapsto \bar{x}$ is an *anti-involution*, that is, a K-linear involution with $\overline{xy} = \bar{y}\bar{x}$ for any $x, y \in A$. Note that this operator is defined only by the K-algebra structure of A since so is A_0.

Definition 4.21. Let $A = (\alpha, \beta)_K$ be a quaternion algebra where $\alpha, \beta \in K^\times$. For an element $x = \alpha_0 + \alpha_1\mathbb{i} + \alpha_2\mathbb{j} + \alpha_3\mathbb{ij}$, the value

$$\operatorname{Nrd}(x) := x\bar{x} = \alpha_0^2 - \alpha\alpha_1^2 - \beta\alpha_2^2 + \alpha\beta\alpha_3^2 \in K \tag{15}$$

is called the *reduced norm* of x. The function $x \mapsto \operatorname{Nrd}(x)$ can be seen as a quadratic form on A over K. The symmetric bilinear form

$$A \times A \to K,\ (x, y) \mapsto \frac{1}{2}(\operatorname{Nrd}(x + y) - \operatorname{Nrd}(x) - \operatorname{Nrd}(y))$$

associated with the quadratic form $x \mapsto \operatorname{Nrd}(x)$ is referred to as the *characteristic form* of A. We remark that the reduced norm and characteristic form depend only on the K-algebra structure of A since so does the anti-involution $\bar{\cdot}$.

By equation (15), the characteristic form of A is isomorphic to the 4-dimensional inner product $\langle 1, -\alpha, -\beta, \alpha\beta\rangle_K$. Hence, the characteristic form of any quaternion algebra represents 1 and has determinant 1. Conversely, it follows from Lemma 4.8 that any 4-dimensional inner product which represents 1 and has determinant 1 is isomorphic to $\langle 1, -\alpha, -\beta, \alpha\beta\rangle_K$ for some $\alpha, \beta \in K^\times$, and to the characteristic form of the quaternion algebra $(\alpha, \beta)_K$. The following proposition states that a quaternion algebra is characterized by its characteristic form.

Proposition 4.22. *Let $\alpha, \beta, \alpha', \beta' \in K^\times$ be nonzero elements of K. Two quaternion algebras $(\alpha, \beta)_K$ and $(\alpha', \beta')_K$ are isomorphic if and only if their characteristic forms are isomorphic, i.e., $\langle 1, -\alpha, -\beta, \alpha\beta\rangle_K \cong \langle 1, -\alpha', -\beta', \alpha'\beta'\rangle_K$.*

Proof. See [39, Chapter 2, Theorem 11.9]. □

The characteristic form of a quaternion algebra A determines the K-algebra structure of A as follows.

Theorem 4.23. *Let A be a quaternion algebra over K. If the characteristic form is anisotropic then A is a division algebra. If the characteristic form is isotropic then $A \cong M_2(K)$. In particular, in either case, A is a central simple K-algebra.*

Proof. If the characteristic form of A is anisotropic, or equivalently $\mathrm{Nrd}(x) \neq 0$ for any nonzero $x \in A$, then any nonzero element x of A has the inverse $\mathrm{Nrd}(x)^{-1}\bar{x}$. Hence A is a division algebra.

Suppose that the characteristic form is isotropic. Then it is isomorphic to $\langle 1, -1, -\gamma, \gamma\rangle_K$ for some $\gamma \in K^\times$ by Lemma 4.8. Thus, Proposition 4.22 shows that $A \cong (1, \gamma)_K$. On the other hand, the quaternion algebra $(1, \gamma)_K$ is isomorphic to $M_2(K)$ by the homomorphism defined by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbb{i} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \mathbb{j} \mapsto \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix},\ \mathbb{ij} \mapsto \begin{pmatrix} 0 & 1 \\ -\gamma & 0 \end{pmatrix}$$

where $1, \mathbb{i}, \mathbb{j}, \mathbb{ij}$ is a standard basis of $(1, \gamma)_K$. Therefore $A \cong M_2(K)$. □

Corollary 4.24. *Let A be a quaternion algebra over K. The Brauer class $[A]_K$ is trivial if and only if the characteristic form is isotropic.* □

As seen above, any quaternion algebra is central simple algebra. In fact, it can be expressed as a cyclic algebra.

Proposition 4.25. *Let $\alpha, \beta \in K^\times$ be nonzero elements, and suppose that α is not a square. Then $L := K(\sqrt{\alpha})$ is a quadratic cyclic extension field of K with the unique generator σ of $\mathrm{Gal}(L/K)$ determined by $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$. The quaternion algebra $(\alpha, \beta)_K$ is isomorphic to the cyclic algebra $(\sigma, \beta)_K$.*

Proof. Let $1, \mathbb{i}, \mathbb{j}, \mathbb{ij}$ be a standard basis of $(\alpha, \beta)_K$, and $\mathbb{e} \in (\sigma, \beta)_K$ be as in Definition 3.17. The cyclic algebra $(\sigma, \beta)_K$ can be written as $(\sigma, \beta)_K = L \cdot 1 + L \cdot \mathbb{e} = K \cdot 1 + K \cdot \sqrt{\alpha} + K \cdot \mathbb{e} + K \cdot \sqrt{\alpha}\,\mathbb{e}$ as a K-vector space, and $1, \sqrt{\alpha}, \mathbb{e}, \sqrt{\alpha}\,\mathbb{e}$ form a K-basis of $(\sigma, \beta)_K$. Thus the K-linear map $(\alpha, \beta)_K \to (\sigma, \beta)_K$ determined by

$$1 \mapsto 1,\ \mathbb{i} \mapsto \sqrt{\alpha},\ \mathbb{j} \mapsto \mathbb{e},\ \mathbb{ij} \mapsto \sqrt{\alpha}\,\mathbb{e}$$

is isomorphic. It can be easily checked that this K-linear isomorphism is a K-algebra homomorphism. Therefore $(\alpha, \beta)_K \cong (\sigma, \beta)_K$ as K-algebras. □

As a result, the order of the Brauer class of any quaternion algebra is at most 2 (this fact can also be checked by using Theorem 4.26 below). Let $\mathrm{Br}_2(K)$ denote the subgroup of $\mathrm{Br}(K)$ consisting of all Brauer classes of order at most 2. For $\alpha, \beta \in K^\times$, the Brauer class of the quaternion algebra $(\alpha, \beta)_K$ is denoted by $[\alpha, \beta]_K$. Brauer classes of quaternion algebras have the following calculation rules. They will be used perhaps without referring.

Theorem 4.26. *Let $\alpha, \beta, \gamma \in K^\times$ be nonzero elements.*

(i) $[1, \beta]_K = 0$.

(ii) $[\alpha\gamma^2, \beta]_K = [\alpha, \beta]_K$.

(iii) $[\beta, \alpha]_K = [\alpha, \beta]_K$.

(iv) $[\alpha, \beta]_K + [\alpha, \gamma]_K = [\alpha, \beta\gamma]_K$.

These properties can be summarized as follows: the symbol $[\cdot, \cdot]_K$ is a symmetric bilinear form $K^\times/K^{\times 2} \times K^\times/K^{\times 2} \to \mathrm{Br}_2(K)$. In addition, we have

(v) $[\alpha, -\alpha]_K = 0$.

Proof. We have $[1, \beta]_K \cong M_2(K)$ by Theorem 4.23 (or its proof). This leads to the assertion (i). One can construct isomorphisms $(\alpha\gamma^2, \beta)_K \cong (\alpha, \beta)_K$ and $(\beta, \alpha)_K \cong (\alpha, \beta)_K$ in an obvious way, and thus, the assertions (ii) and (iii) hold. Furthermore, the characteristic form of $(\alpha, -\alpha)_K$ is isomorphic to $\langle 1, -\alpha, \alpha, -1\rangle_K$ and hence isotropic. This leads to the assertion (v) by Theorem 4.23.

It remains to prove the assertion (iv). This is clear if α is a square. Suppose that α is not a square, and let $\sigma \in \mathrm{Gal}(K(\sqrt{\alpha})/K)$ denote the generator of $\mathrm{Gal}(K(\sqrt{\alpha})/K)$. Then $[\alpha, \beta]_K = [\sigma, \beta]_K$ and $[\alpha, \gamma]_K = [\sigma, \gamma]_K$ by Proposition 4.25. Hence, by Lemma 3.18, we have

$$[\alpha, \beta]_K + [\alpha, \gamma]_K = [\sigma, \beta]_K + [\sigma, \gamma]_K = [\sigma, \beta\gamma]_K,$$

and the right-hand side equals $[\alpha, \beta\gamma]_K$ by Proposition 4.25 again. This completes the proof. □

When K is an algebraic number field or a local field, the symmetric bilinear form $[\cdot, \cdot]_K : K^\times/K^{\times 2} \times K^\times/K^{\times 2} \to \mathrm{Br}_2(K)$ is nondegenerate in the sense of the following theorem.

Theorem 4.27. *Suppose that K is an algebraic number field or a local field. For a non-square element $\alpha \in K^\times \setminus K^{\times 2}$, there exists $\beta \in K^\times$ such that $[\alpha, \beta]_K \neq 0$.*

Proof. Let $\alpha \in K^\times$ be a non-square element, and put $L = K(\sqrt{\alpha})$. Let $\sigma \in \mathrm{Gal}(L/K)$ denote the generator of $\mathrm{Gal}(L/K)$. We remark that the twisting group $\mathrm{Tw}(L, \sigma) = K^\times/\mathrm{N}_{L/K}(L^\times)$ is not the trivial group, by Corollary 3.28 when K is a local field and by Proposition 3.31 when K is an algebraic number field. Let $\beta \in K^\times$ be an element such that $\beta \neq 1$ in $\mathrm{Tw}(L, \sigma)$. Then, the Brauer class $[\alpha, \beta]_K$, which is equal to $[\sigma, \beta]_K \in \mathrm{Br}(K)$ by Proposition 4.25, is not zero since $\mathrm{Tw}(L, \sigma) \to \mathrm{Br}(K)$, $\gamma \mapsto [\sigma, \gamma]_K$ is injective by Theorem 3.20. This completes the proof. □

4.4 Hasse-Witt invariants

We continue to assume that $\mathrm{char}\, K \neq 2$. We introduce an invariant for an inner product called the *Hasse-Witt invariant*. This invariant is important in particular when K is a local field. For example, the isomorphism class of any inner product over a non-archimedean local field (of characteristic not 2) is uniquely determined by its dimension, determinant, and Hasse-Witt invariant (Theorem 4.45). Moreover, it also has the role of describing the relationship between inner products of local and global fields (see §4.7).

Let (V, b) be a d-dimensional inner product space over K. Since $\mathrm{char}\, K \neq 2$, the space has an orthogonal basis $\mathfrak{B} = \{x_1, \ldots, x_d\}$ (see Proposition 4.9). We write $\alpha_i = b(x_i, x_i) \in K^\times$ and define the Brauer class $\mathrm{HW}_K(b; \mathfrak{B}) \in \mathrm{Br}_2(K)$ by

$$\mathrm{HW}_K(b; \mathfrak{B}) := \sum_{i<j} [\alpha_i, \alpha_j]_K.$$

Here, if $d = 0$ or 1 then $\mathrm{HW}_K(b; \mathfrak{B})$ is defined to be 0. For any permutation σ of $\{1, \ldots, d\}$, we have

$$\sum_{i<j} [\alpha_{\sigma(i)}, \alpha_{\sigma(j)}]_K = \sum_{i<j} [\alpha_i, \alpha_j]_K = \mathrm{HW}_K(b; \mathfrak{B})$$

since $[\alpha,\beta]_K = [\beta,\alpha]_K$ for any $\alpha,\beta \in K^\times$. This means that $\mathrm{HW}_K(b;\mathfrak{B})$ does not depend on the ordering of $\mathfrak{B}$. In fact, the Brauer class $\mathrm{HW}_K(b;\mathfrak{B})$ is independent of the choice of the orthogonal basis $\mathfrak{B}$. To show this, we use the following fact.

Lemma 4.28. *Let $\mathfrak{B}'$ be another orthogonal basis of (V,b). If $d \geq 3$ then there exists a sequence $\mathfrak{B}_0 = \mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_{l-1}, \mathfrak{B}_l = \mathfrak{B}'$ of orthogonal bases such that $\mathfrak{B}_{i-1}$ and $\mathfrak{B}_i$ contain a common vector for each $i = 1,\ldots,l$.*

Proof. See [40, Chapter IV, Theorem 2]. □

Proposition 4.29. *The Brauer class $\mathrm{HW}_K(b;\mathfrak{B}) \in \mathrm{Br}(K)$ is independent of the choice of the orthogonal basis $\mathfrak{B}$.*

Proof. Let $\mathfrak{B}' = \{x'_1 \ldots, x'_d\}$ be another orthogonal basis, and write $\alpha'_i = b(x'_i, x'_i)$ for $i = 1,\ldots,d$. We argue by induction on the dimension d. If $d = 0$ or 1 then the assertion is obvious. If $d = 2$ then

$$\langle 1, -\alpha_1, -\alpha_2, \alpha_1\alpha_2\rangle_K \cong \langle 1, -\alpha'_1, -\alpha'_2, \alpha'_1\alpha'_2\rangle_K$$

because $\langle -\alpha_1, -\alpha_2\rangle_K \cong -b \cong \langle -\alpha'_1, -\alpha'_2\rangle_K$ and $\alpha_1\alpha_2 = \det(b) = \alpha'_1\alpha'_2$ in $K^\times/K^{\times 2}$. Hence $\mathrm{HW}_K(b;\mathfrak{B}) = [\alpha_1,\alpha_2]_K = [\alpha'_1,\alpha'_2]_K = \mathrm{HW}_K(b;\mathfrak{B}')$ by Proposition 4.22. Suppose that $d \geq 3$. By Lemma 4.28, it is sufficient to show the assertion when $\mathfrak{B}$ and $\mathfrak{B}'$ have a common vector. Since $\mathrm{HW}_K(b;\mathfrak{B})$ and $\mathrm{HW}_K(b;\mathfrak{B}')$ do not depend the orderings of $\mathfrak{B}$ and $\mathfrak{B}'$ as seen above, we assume that $x_1 = x'_1$ without loss of generality. Put $b_0 = b|_{(Kx_1)^\perp}$. Note that $\mathfrak{B}\setminus\{x_1\}$ and $\mathfrak{B}'\setminus\{x_1\}$ are orthogonal bases of $(Kx_1)^\perp$. Since $\dim(b_0) < d$ we have $\mathrm{HW}_K(b_0;\mathfrak{B}\setminus\{x_1\}) = \mathrm{HW}_K(b_0;\mathfrak{B}'\setminus\{x_1\})$ by induction hypothesis. Thus

$$\begin{aligned}
\mathrm{HW}_K(b;\mathfrak{B}') &= \sum_{j=2}^{d}[\alpha_1,\alpha'_j]_K + \sum_{2\leq i<j}[\alpha'_i,\alpha'_j]_K \\
&= [\alpha_1, \textstyle\prod_{j=2}^{d}\alpha'_j]_K + \mathrm{HW}_K(b_0;\mathfrak{B}'\setminus\{x_1\}) \\
&= [\alpha_1,\det(b_0)]_K + \mathrm{HW}_K(b_0;\mathfrak{B}\setminus\{x_1\}) \\
&= \mathrm{HW}_K(b;\mathfrak{B}).
\end{aligned}$$

This completes the proof. □

Definition 4.30. Let (V,b) be an inner product space over K, and let $\mathfrak{B}$ be an orthogonal basis of (V,b). We write $\mathrm{HW}_K(b)$ for $\mathrm{HW}_K(b;\mathfrak{B}) \in \mathrm{Br}_2(K)$ since it is independent of the choice of $\mathfrak{B}$ (Proposition 4.29). The Brauer class $\mathrm{HW}_K(b)$ is called the *Hasse-Witt invariant* of b. The Hasse-Witt invariant of any zero or one dimensional inner product is defined to be 0.

Lemma 4.31. *Hasse-Witt invariants have the following properties.*

(i) *Let b be a d-dimensional inner product over K and $\gamma \in K^\times$ a nonzero element. Then*

$$\mathrm{HW}_K(\gamma b) = \frac{d(d-1)}{2}[\gamma,\gamma]_K + [\gamma,\det(b)^{d-1}]_K + \mathrm{HW}_K(b).$$

(ii) *Let b, b' be two inner products over K. Then*

$$\mathrm{HW}_K(b\oplus b') = \mathrm{HW}_K(b) + \mathrm{HW}_K(b') + [\det(b),\det(b')]_K.$$

(iii) *Let b_j and b'_j be inner products over K with $\det(b_j) = \det(b'_j)$ for $j = 1,\ldots,l$. Then*

$$\mathrm{HW}_K\left(\bigoplus_{j=1}^{l} b_j\right) - \sum_{j=1}^{l}\mathrm{HW}_K(b_j) = \mathrm{HW}_K\left(\bigoplus_{j=1}^{l} b'_j\right) - \sum_{j=1}^{l}\mathrm{HW}_K(b'_j).$$

Proof. (i). Write $b \cong \langle \alpha_1, \ldots, \alpha_d \rangle_K$ where $\alpha_1, \ldots, \alpha_d \in K^\times$. Then

$$\begin{aligned}
\mathrm{HW}_K(\gamma b) &= \sum_{i<j} [\gamma\alpha_i, \gamma\alpha_j]_K \\
&= \sum_{i<j} ([\gamma,\gamma]_K + [\gamma,\alpha_j]_K + [\alpha_i,\gamma]_K + [\alpha_i,\alpha_j]_K) \\
&= \sum_{i<j} [\gamma,\gamma]_K + \sum_{i<j} [\gamma, \alpha_i\alpha_j]_K + \sum_{i<j} [\alpha_i,\alpha_j]_K \\
&= \frac{d(d-1)}{2}[\gamma,\gamma]_K + \sum_{i<j} [\gamma,\alpha_i\alpha_j]_K + \mathrm{HW}_K(b).
\end{aligned}$$

Moreover

$$\textstyle\sum_{i<j}[\gamma,\alpha_i\alpha_j]_K = [\gamma, \prod_{i<j}\alpha_i\alpha_j]_K = [\gamma, (\alpha_1\cdots\alpha_d)^{d-1}]_K = [\gamma, \det(b)^{d-1}]_K.$$

Hence we get the desired equality.

(ii). Write $b \cong \langle \alpha_1, \ldots, \alpha_d \rangle_K$ and $b' \cong \langle \alpha'_1, \ldots, \alpha'_{d'} \rangle_K$. Then

$$\begin{aligned}
\mathrm{HW}_K(b \oplus b') &= \mathrm{HW}_K(\langle \alpha_1, \ldots, \alpha_d, \alpha'_1, \ldots, \alpha'_{d'} \rangle_K) \\
&= \mathrm{HW}_K(\langle \alpha_1, \ldots, \alpha_d \rangle_K) + \mathrm{HW}_K(\langle \alpha'_1, \ldots, \alpha'_{d'} \rangle_K) + \textstyle\sum_{i=1}^{d}\sum_{j=1}^{d'} [\alpha_i, \alpha'_j]_K \\
&= \mathrm{HW}_K(b) + \mathrm{HW}_K(b') + [\textstyle\prod_{i=1}^{d}\alpha_i, \prod_{j=1}^{d'}\alpha'_j]_K \\
&= \mathrm{HW}_K(b) + \mathrm{HW}_K(b') + [\det(b), \det(b')]_K
\end{aligned}$$

as required.

(iii). We use induction on l, the case $l = 1$ being obvious. Let $l > 1$. Then

$$\begin{aligned}
&\mathrm{HW}_K\left(\textstyle\bigoplus_{j=1}^{l} b_j\right) - \sum_{j=1}^{l} \mathrm{HW}_K(b_j) \\
&\quad= \mathrm{HW}_K(b_1) + \mathrm{HW}_K\left(\textstyle\bigoplus_{j=2}^{l} b_j\right) + \left[\det(b_1), \det\left(\bigoplus_{j=2}^{l} b_j\right)\right]_K - \sum_{j=1}^{l} \mathrm{HW}_K(b_j) \\
&\quad= \mathrm{HW}_K\left(\textstyle\bigoplus_{j=2}^{l} b_j\right) - \sum_{j=2}^{l} \mathrm{HW}_K(b_j) + \left[\det(b_1), \prod_{j=2}^{l} \det\left(b_j\right)\right]_K \\
&\quad= \mathrm{HW}_K\left(\textstyle\bigoplus_{j=2}^{l} b'_j\right) - \sum_{j=2}^{l} \mathrm{HW}_K(b'_j) + \left[\det(b'_1), \prod_{j=2}^{l} \det\left(b'_j\right)\right]_K \\
&\quad= \mathrm{HW}_K\left(\textstyle\bigoplus_{j=1}^{l} b'_j\right) - \sum_{j=1}^{l} \mathrm{HW}_K(b'_j),
\end{aligned}$$

where the third equality is by induction hypothesis. The proof is complete. □

The following theorem states that the isomorphism class of any inner product of dimension at most 3 is uniquely determined by its dimension, determinant, and Hasse-Witt invariant.

Theorem 4.32. *Let $d \in \mathbb{Z}_{\geq 0}$ be a non-negative integer at most 3. Let b and b' be two inner products over K with $\dim(b) = \dim(b') = d$. If $\det(b) = \det(b')$ and $\mathrm{HW}_K(b) = \mathrm{HW}_K(b')$ then $b \cong b'$.*

Proof. If $d = 0$ or 1 then the assertion is clear. Suppose that $d = 2$, and write $b \cong \langle \alpha_1, \alpha_2 \rangle_K$, $b \cong \langle \alpha'_1, \alpha'_2 \rangle_K$ where $\alpha_1, \alpha_2, \alpha'_1, \alpha'_2 \in K^\times$. Then, the quaternion algebras $(\alpha_1, \alpha_2)_K$ and $(\alpha'_1, \alpha'_2)_K$ are isomorphic since $\mathrm{HW}_K(b) = \mathrm{HW}_K(b')$. Thus, their characteristic forms $\langle 1, -\alpha_1, -\alpha_2, \alpha_1\alpha_2 \rangle_K$ and $\langle 1, -\alpha'_1, -\alpha'_2, \alpha'_1\alpha'_2 \rangle_K$ are also isomorphic (as inner products). Since $\alpha_1\alpha_2 = \det(b) = \det(b') = \alpha'_1\alpha'_2$ in $K^\times/K^{\times 2}$, it follows from Witt's cancellation theorem 4.19 that $\langle -\alpha_1, -\alpha_2 \rangle_K \cong \langle -\alpha'_1, -\alpha'_2 \rangle_K$, and hence $b \cong \langle \alpha_1, \alpha_2 \rangle_K \cong \langle \alpha'_1, \alpha'_2 \rangle_K \cong b'$ as required. Finally, suppose that $d = 3$.

Case I: $\det(b) = \det(b') = -1$. In this case, we can write $b \cong \langle \alpha_1, \alpha_2, -\alpha_1\alpha_2 \rangle_K$ and $b' \cong \langle \alpha_1', \alpha_2', -\alpha_1'\alpha_2' \rangle_K$. Then

$$\begin{aligned} \mathrm{HW}_K(b) &= [\alpha_1, \alpha_2]_K + [\alpha_1, -\alpha_1\alpha_2]_K + [\alpha_2, -\alpha_1\alpha_2]_K \\ &= [\alpha_1, \alpha_2]_K + [\alpha_1, \alpha_2]_K + [\alpha_2, \alpha_1]_K \\ &= [\alpha_1, \alpha_2]_K, \end{aligned}$$

and the same calculation yields $\mathrm{HW}_K(b') = [\alpha_1', \alpha_2']_K$. Since $\mathrm{HW}_K(b) = \mathrm{HW}_K(b')$, the quaternion algebras $(\alpha_1, \alpha_2)_K$ and $(\alpha_1', \alpha_2')_K$ are isomorphic. By cancelling out $\langle 1 \rangle_K$ of their characteristic forms, we get $\langle -\alpha_1, -\alpha_2, \alpha_1\alpha_2 \rangle_K \cong \langle -\alpha_1', -\alpha_2', \alpha_1'\alpha_2' \rangle_K$, and hence $b \cong b'$.

Case II: *General case.* Put $\delta := \det(b) = \det(b')$. Then $\det(-\delta b) = \det(-\delta b') = -1$. Moreover $\mathrm{HW}_K(-\delta b) = \mathrm{HW}_K(-\delta b')$ by Lemma 4.31 (i). Hence $-\delta b \cong -\delta b'$ by Case I, and therefore $b \cong b'$. This completes the proof. □

For 4-dimensional inner products, its isomorphism class is not determined by its determinant and Hasse-witt invariant in general, but isotropy can be described in terms of these invariants. We will formulate it together with lower dimensional cases.

Notation 4.33. Let L/K be an extension of fields, and let (V, b) be an inner product space over K. Then $V \otimes_K L$ is an L-vector space, and b extends to an inner product $(V \otimes_K L) \times (V \otimes_K L) \to L$ in a unique way. This extension of b on $V \otimes_K L$ is denoted by $b \otimes_K L$ or just by $b \otimes L$.

Lemma 4.34. *Let (V, b) be a 4-dimensional inner product space over K of determinant δ, and put $L = K(\sqrt{\delta})$. The inner product b is isotropic if and only if $b \otimes L$ is isotropic.*

Proof. If b is isotropic then so is $b \otimes L$ clearly. We show the converse. If $\delta = 1$ in $K^\times/K^{\times 2}$ then the assertion is clear because $L = K$. Suppose that $\delta \neq 1$ in $K^\times/K^{\times 2}$. Then L is a quadratic extension of K, and any vector of $V \otimes L$ can be written as $x + \sqrt{\delta}y$ for some $x, y \in V$. Let $u \in V \otimes_K L$ be an isotropic vector with respect to $b \otimes L$, and write $u = x + \sqrt{\delta}y$ for some $x, y \in V$. Then

$$\begin{aligned} 0 &= (b \otimes L)(u, u) \\ &= (b \otimes L)(x, x) + 2\sqrt{\delta}(b \otimes L)(x, y) + \delta(b \otimes L)(y, y) \\ &= b(x, x) + \delta b(y, y) + \sqrt{\delta} \cdot 2b(x, y), \end{aligned}$$

which implies that $b(x, x) + \delta b(y, y) = 0$ and $b(x, y) = 0$. If $b(x, x) = 0$ then we are done. Suppose that $b(x, x) \neq 0$. Then $b(y, y) = -\delta^{-1}b(x, x) \neq 0$. Furthermore x and y are linearly independent since $b(x, y) = 0$. Thus

$$b \cong \langle b(x, x), b(y, y), \gamma, \delta b(x, x)b(y, y)\gamma \rangle_K \cong \langle b(x, x), b(y, y), \gamma, -\gamma \rangle_K$$

for some $\gamma \in K^\times$. Hence b is isotropic since so is $\langle \gamma, -\gamma \rangle_K$. This completes the proof. □

Theorem 4.35. *Let b be an inner product over K, and put $\delta = \det(b)$.*

(i) *Suppose that* $\dim(b) = 2$. *Then b is isotropic if and only if* $\det(b) = -1$ *in* $K^\times/K^{\times 2}$.

(ii) *Suppose that* $\dim(b) = 3$. *Then b is isotropic if and only if* $\mathrm{HW}_K(b) + [-1, -\delta]_K = 0$.

(iii) *Suppose that* $\dim(b) = 4$. *Then b is isotropic if and only if* $\mathrm{HW}_L(b \otimes L) + [-1, -\delta]_L = 0$, *where* $L = K(\sqrt{\delta})$.

Proof. (i). If b is isotropic then $b \cong \langle \alpha, -\alpha \rangle_K$ for some $\alpha \in K^\times$ by Lemma 4.8, and thus $\det(b) = -1$. If $\det(b) = -1$ then $b \cong \langle \alpha, -\alpha \rangle_K$ for some $\alpha \in K^\times$, and hence b is isotropic.

(ii). If b is isotropic then $b \cong \langle \alpha, -\alpha, -\delta \rangle_K$ for some $\alpha \in K^\times$ by Lemma 4.8, and we get

$$\mathrm{HW}_K(b) + [-1, -\delta]_K = [\alpha, -\alpha]_K + [\alpha, -\delta]_K + [-\alpha, -\delta]_K + [-1, -\delta]_K = 0.$$

Suppose conversely that $\mathrm{HW}_K(b) + [-1, -\delta]_K = 0$, or equivalently $\mathrm{HW}_K(b) = [-1, -\delta]_K$. Then the 3-dimensional isotropic inner product $\langle 1, -1, -\delta \rangle_K$ is isomorphic to b by Theorem 4.32, because they have the same determinant and same Hasse-Witt invariant. Hence b is also isotropic.

(iii). Note that $\delta = 1$ in $L^\times / L^{\times 2}$. By Lemma 4.34, it is enough to show that

$$b_L \text{ is isotropic } \iff \mathrm{HW}_L(b_L) + [-1, -1]_L = 0,$$

where $b_L := b \otimes L$. Let $\gamma \in L^\times$ be a nonzero element represented by b_L. Note that b_L is isotropic if and only if γb_L is isotropic. Since γb_L represents 1, it can be written as $\gamma b_L \cong \langle 1, -\alpha_1, -\alpha_2, \alpha_1\alpha_2 \rangle_L$ where $\alpha_1, \alpha_2 \in L^\times$. In other words, γb_L is isomorphic to the characteristic form of the quaternion algebra $(\alpha_1, \alpha_2)_L$. Hence, it follows from Corollary 4.24 that

$$b_L \text{ is isotropic } \iff \gamma b_L \text{ is isotropic } \iff [\alpha_1, \alpha_2]_L = 0. \qquad (*)$$

On the other hand, $\mathrm{HW}_L(b_L) = \mathrm{HW}_L(\gamma b_L)$ by Lemma 4.31 (i), and a calculation yields $\mathrm{HW}_L(\gamma b_L) = [-1, -1]_L + [\alpha_1, \alpha_2]_L$. Thus $\mathrm{HW}_L(b_L) + [-1, -1]_L = [\alpha_1, \alpha_2]_L$. This equality with $(*)$ completes the proof. □

4.5 Inner products over finite fields

In this subsection, we give standard forms of inner products over a finite field (results in §§4.2 – 4.4 are not needed here). Let κ be a finite field.

Theorem 4.36. *Suppose that* $\mathrm{char}\, \kappa = 2$*, and let* (V, b) *be an inner product space over* κ*. Then*

$$(V, b) \cong \langle 1 \rangle_\kappa^{\oplus m} \oplus \mathbb{H}_\kappa^{\oplus n}$$

for some $m, n \in \mathbb{Z}_{\geq 0}$ *(* $\mathbb{H}_\kappa$ *is defined in Definition* 4.11*).*

Proof. By Proposition 4.9 (i), there exist vectors $v_1, \ldots, v_m \in V$ and a totally isotropic space (N, b_N) such that $V = \kappa v_1 \oplus \cdots \oplus \kappa v_m \oplus N$ with $b(v_i, v_i) \in \kappa^\times$ for all $i = 1, \ldots, m$. Since any element of κ is a square (see Proposition 2.2 (i)), we may assume that $b(v_i, v_i) = 1$ for all i.

Let $u \in N$. Then there exists $u' \in N$ such that $b_N(u, u') = 1$ since b_N is nondegenerate. Since N is totally isotropic, the subspace $H := \kappa u + \kappa u' \subset N$ is a hyperbolic plane with hyperbolic basis (u, u'). Thus $N = H \oplus H^\perp$ by Proposition 4.4 (iii). Moreover, since $H^\perp \subset N$ is again totally isotropic, it can be seen by induction that $N \cong \mathbb{H}_\kappa^{\oplus n}$ for some $n \in \mathbb{Z}_{\geq 0}$. Therefore we obtain $(V, b) \cong \langle 1 \rangle_\kappa^{\oplus m} \oplus \mathbb{H}_\kappa^{\oplus n}$. □

We proceed to the case $\mathrm{char}\, \kappa \neq 2$. The following lemma is needed.

Lemma 4.37. *Any element of* κ *can be expressed as* $\alpha^2 + \beta^2$ *for some* $\alpha, \beta \in \kappa$*. In other words, the* 2*-dimension inner product* $\langle 1, 1 \rangle_\kappa$ *represents every nonzero element (the characteristic of* κ *can be* 2*).*

Proof. If $\mathrm{char}\, \kappa = 2$ then the assertion is clear since any element of κ is a square. Suppose that $\mathrm{char}\, \kappa \neq 2$, and put $S := \{\alpha^2 \mid \alpha \in \kappa\} = \kappa^{\times 2} \cup \{0\}$. Since the cardinality $\#S = (\#\kappa - 1)/2 + 1 = (\#\kappa + 1)/2$ is not a divisor of $\#\kappa$, the subset S cannot be an additive subgroup of κ. In particular,

there exist elements $\alpha, \beta \in S$ such that $\epsilon' := \alpha^2 + \beta^2 \notin S$. Note that $\kappa^\times/\kappa^{\times 2} = \{1, \epsilon'\}$ since ϵ' is not a square (see Proposition 2.2 (ii)).

Now, let $\epsilon \in \kappa$ be any element. If ϵ is a square then the assertion is obvious. If ϵ is not a square then it can be written as $\epsilon = c^2\epsilon'$ for some $c \in \kappa$ since $\kappa^\times/\kappa^{\times 2} = \{1, \epsilon'\}$. Thus

$$\epsilon = c^2(\alpha^2 + \beta^2) = (c\alpha)^2 + (c\beta)^2,$$

which completes the proof. □

Theorem 4.38. *Suppose that* $\operatorname{char}\kappa \neq 2$*, and fix a non-square element* $\epsilon \in \kappa^\times$*. Let* (V, b) *be an inner product space over* κ *of dimension* d*. Then*

$$(V, b) \cong \begin{cases} \langle 1\rangle_\kappa^{\oplus d} & \text{if } \det b = 1 \\ \langle 1\rangle_\kappa^{\oplus d-1} \oplus \langle \epsilon\rangle_\kappa & \text{if } \det b = \epsilon. \end{cases}$$

In particular, the isomorphism class of (V, b) *is uniquely determined by its dimension and determinant.*

Proof. Since $\kappa^\times/\kappa^{\times 2} = \{1, \epsilon\}$, it follows from Proposition 4.9 (ii) that $b \cong \langle 1\rangle_\kappa^{\oplus m} \oplus \langle \epsilon\rangle_\kappa^{\oplus m'}$ where m and m' are non-negative integers with $m+m' = d$. Hence, it is sufficient to show that $\langle \epsilon, \epsilon\rangle_\kappa \cong \langle 1, 1\rangle_\kappa$. Lemma 4.37 shows that $\langle 1, 1\rangle_\kappa$ represents ϵ. Thus $\langle 1, 1\rangle_\kappa \cong \langle \epsilon, \epsilon \cdot \det(\langle 1, 1\rangle_\kappa)\rangle_\kappa \cong \langle \epsilon, \epsilon\rangle_\kappa$. This completes the proof. □

4.6 Inner products over local fields

This subsection gives classification theorems of inner products over a local field. We begin with the archimedean case, which is easier than the non-archimedean case.

Theorem 4.39. *Any inner product over* $\mathbb{C}$ *of dimension* d *is isomorphic to* $\langle 1\rangle_{\mathbb{C}}^{\oplus d}$*, and in particular, its isomorphism class is uniquely determined by its dimension. For any inner product* b *over* $\mathbb{R}$ *there exist unique non-negative integers* r, s *such that* $b \cong \langle 1\rangle_{\mathbb{R}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{R}}^{\oplus s}$*.*

Proof. If b is a d-dimensional inner product over $\mathbb{C}$ then Proposition 4.9 (ii) implies that $b \cong \langle 1\rangle_{\mathbb{C}}^{\oplus d}$ since any element of $\mathbb{C}$ is a square. Let b be an inner product over $\mathbb{R}$. Since $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{1, -1\}$, it follows from Proposition 4.9 (ii) that there exist non-negative integers r and s such that $b \cong \langle 1\rangle^{\oplus r} \oplus \langle -1\rangle^{\oplus s}$. The uniqueness of r and s follows from Witt's cancellation theorem 4.19. □

The latter part of this theorem leads to the following definition.

Definition 4.40. Let (V, b) be an inner product space over $\mathbb{R}$. The *signature* of b is the pair (r, s) of non-negative integers such that $(V, b) \cong \langle 1\rangle_{\mathbb{R}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{R}}^{\oplus s}$. If $s = 0$ (resp. $r = 0$) then (V, b) is said to be *positive* (resp. *negative*) *definite*. The difference $r - s$ is called the *index* of b and denoted by $\operatorname{idx}(b)$.

We remark that the identities

$$r = (\dim(b) + \operatorname{idx}(b))/2, \quad s = (\dim(b) - \operatorname{idx}(b))/2$$

hold for any inner product b over $\mathbb{R}$ of signature (r, s). Hence, the dimension and index determines the signature, and vice versa.

Remark 4.41. The signature of an inner product space over $\mathbb{R}$ can also be defined as the numbers of positive and negative eigenvalues of a Gram matrix. It is known as *Sylvester's law of inertia* that these numbers are independent of the Gram matrix.

We proceed to the non-archimedean case. Suppose that K is a non-archimedean local field of characteristic not 2. We begin with the following proposition about Brauer classes of order 2.

Proposition 4.42. *Let K be a non-archimedean local field of characteristic not 2.*

(i) *The order of $\mathrm{Br}_2(K)$ is two. In particular, a non-trivial Brauer class in $\mathrm{Br}_2(K)$ is unique.*

(ii) *For any quadratic extension L/K, we have $\mathrm{res}_{L/K}(\mathrm{Br}_2(K)) = 0$.*

Proof. (i). The subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of all elements of order at most 2 is $\left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z}$. Hence, the isomorphism $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ maps $\mathrm{Br}_2(K)$ onto $\left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z}$, and in particular, the order of $\mathrm{Br}_2(K)$ is two.

(ii). Let L/K be a quadratic extension. Then L/K is a cyclic extension (see Example 1.4). Thus, the assertion follows from Proposition 3.27. □

Lemma 4.43. *Let b be a 4-dimensional inner product over K. If $\det(b) \neq 1$ then b is isotropic.*

Proof. Suppose that $\det(b) \neq 1$. Then $L := K(\sqrt{\det(b)})$ is a quadratic extension field of K. Thus $\mathrm{HW}_L(b \otimes L) + [-1, -\det(b)]_L = \mathrm{res}_{L/K}(\mathrm{HW}_K(b) + [-1, -\det(b)]_K) = 0$ by Proposition 4.42 (ii). Hence b is isotropic by Theorem 4.35 (iii). □

The following proposition is crucial to obtain the classification theorem.

Proposition 4.44. *Any 4-dimensional inner product over K represents every nonzero element.*

Proof. Let b be a 4-dimensional inner product over K. If $\det(b) \neq 1$ then b is isotropic by Lemma 4.43, and thus b represents every element by Lemma 4.8 (ii). Suppose that $\det(b) = 1$. By considering a scalar multiplication if necessary, we may assume that b represents 1. Then b is (isomorphic to) the characteristic form of some quaternion algebra A.

We first prove that b represents any nonzero element which does not belong to $-K^{\times 2}$. Let $\epsilon \in K^\times \backslash -K^{\times 2}$. Nondegeneracy of the symbol (Theorem 4.27) and Proposition 4.42 (i) show that there exists ϵ' such that $[-\epsilon, \epsilon']_K = [A]_K$, which means $(-\epsilon, \epsilon')_K \cong A$. Since the characteristic form of $(-\epsilon, \epsilon')_K$, which is isomorphic to $\langle 1, \epsilon, -\epsilon', -\epsilon\epsilon' \rangle_K$, represents ϵ, so does the characteristic form b of A. Hence b represents any nonzero element of $K^\times \setminus -K^{\times 2}$.

We remark that the set

$$Q(b) := \{b(v,v)K^{\times 2} \mid v \in A\} \setminus \{0\} = \{\mathrm{Nrd}(v)K^{\times 2} \mid v \in A\} \setminus \{0\} \subset K^\times/K^{\times 2}$$

is a subgroup of $K^\times/K^{\times 2}$ since $\mathrm{Nrd}(vv') = \mathrm{Nrd}(v)\,\mathrm{Nrd}(v')$ for any $v, v' \in A$. What we proved above means that $Q(b)$ contains all classes other than at most one exception $-K^\times$. On the other hand, we have $\#(K^\times/K^{\times 2}) \geq 4$ by Theorem 2.10. Therefore, the subgroup $Q(b)$ must be equal to $K^\times/K^{\times 2}$ itself. This shows that b represents every nonzero element. □

We now prove the classification theorem of inner products over a non-archimedean local field of characteristic not 2.

Theorem 4.45. *Let K be a non-archimedean local field of characteristic not 2. Two inner products over K are isomorphic if and only if they have the same dimension, same determinant, and same Hasse-Witt invariant.*

Proof. Let b_1, b_2 be inner products over K. If $b_1 \cong b_2$ then it is obvious that the three invariants of them are respectively the same. Conversely, suppose that $\dim(b_1) = \dim(b_2)$, $\det(b_1) = \det(b_2)$ and $\mathrm{HW}_K(b_1) = \mathrm{HW}_K(b_2)$. Put $d = \dim(b_1)$. If $d \leq 3$ then $b_1 \cong b_2$ by Theorem 4.32.

Suppose that $d \geq 4$. Proposition 4.44 shows that any inner product over K of dimension at least 4 represents 1. Thus, by using Lemma 4.8 (i) repeatedly, we have

$$b_1 \cong b_1' \oplus \langle 1 \rangle^{\oplus d-3} \quad \text{and} \quad b_2 \cong b_2' \oplus \langle 1 \rangle^{\oplus d-3}$$

for suitable inner products b_1' and b_2' of dimension 3. Because $\det(b_1') = \det(b_1) = \det(b_2) = \det(b_2')$ and $\mathrm{HW}_K(b_1') = \mathrm{HW}_K(b_1) = \mathrm{HW}_K(b_2) = \mathrm{HW}_K(b_2')$, Theorem 4.32 gives the isomorphism $b_1' \cong b_2'$. Therefore $b_1 \cong b_2$. The proof is complete. □

The existence theorem is as follows.

Theorem 4.46. *Let K be a non-archimedean local field of characteristic not 2. Let $d \in \mathbb{Z}_{>0}$, $\delta \in K^\times/K^{\times 2}$, and $\theta \in \mathrm{Br}_2(K)$. There exists an inner product over K with dimension d, determinant δ, and Hasse-Witt invariant θ if and only if one of the following conditions hold:*

(i) *$d = 1$ and $\theta = 0$.*

(ii) *$d = 2$ and $\delta \neq -1$; or $d = 2$, $\delta = -1$, and $\theta = 0$.*

(iii) *$d \geq 3$.*

Proof. We first show the only if part. Let b be an inner product over K with dimension d, determinant δ, and Hasse-Witt invariant θ. If $d = 1$ then $\theta = 0$ by the definition of Hasse-Witt invariant. Suppose that $d = 2$. Then $b \cong \langle \alpha, \alpha\delta \rangle_K$ for some $\alpha \in K^\times$, and

$$\theta = [\alpha, \alpha\delta]_K = [\alpha, -\alpha]_K + [\alpha, -\delta]_K = [\alpha, -\delta]_K.$$

Thus, if $\delta = -1$ then $\theta = 0$. This completes the proof of the only if part.

We then show the if part. If $d = 1$ and $\theta = 0$ then $\langle \delta \rangle_K$ is the desired inner product. Suppose that $d = 2$. If $\delta \neq -1$ and then Theorem 4.27 shows that there exists $\alpha \in K^\times$ such that $[\alpha, -\delta] = \theta$. Then $\langle \alpha, \alpha\delta \rangle_K$ is the desired inner product. If $\delta = -1$ and $\theta = 0$ then $\langle 1, -1 \rangle_K$ is the desired inner product. Suppose that $d \geq 3$. If $\delta \neq -1$ then $\langle \alpha, \alpha\delta \rangle_K \oplus \langle 1 \rangle^{\oplus d-2}$ is the desired inner product, where $\alpha \in K^\times$ is an element such that $[\alpha, -\delta] = \theta$. If $\delta = -1$ then we take $\alpha, \beta \in K^\times$ so that $[\alpha, \beta] = \theta$. This is possible by Theorem 4.27. Then $\langle \alpha, \beta, -\alpha\beta \rangle_K \oplus \langle 1 \rangle^{\oplus d-3}$ is the desired inner product. This completes the proof. □

4.7 Inner products over algebraic number fields

We proceed to the case of algebraic number fields. Let K be an algebraic number field, and $\mathcal{V}$ the set of all places of K.

Definition 4.47. Let (V, b) be an inner product space over K, and $v \in \mathcal{V}$ a place of K. The extension $(V \otimes_K K_v, b \otimes_K K_v)$ of scalars is referred to as the *localization* of (V, b) at v.

In the situation of this definition, the Hasse-Witt invariant $\mathrm{HW}_{K_v}(b \otimes_K K_v)$ of the localization is sometimes abbreviated to $\mathrm{HW}_{K_v}(b)$. It is clearly equal to $\mathrm{res}_{K_v/K}(\mathrm{HW}_K(b))$.

Lemma 4.48. *Let $\alpha \in K$. If α is a square in K_v for every $v \in \mathcal{V}$ then α is also a square in K.*

Proof. If $\alpha = 0$ then there is nothing to prove. Suppose that $\alpha \neq 0$, and it is a square in K_v for every $v \in \mathcal{V}$. Let $\beta \in K^\times$ be any nonzero element of K. Then $[\alpha, \beta]_{K_v} = 0$ for all $v \in \mathcal{V}$ since $\alpha \in K_v^{\times 2}$. Thus $[\alpha, \beta]_K = 0$ since the map $\mathrm{Br}(K) \to \bigoplus_{v \in \mathcal{V}} \mathrm{Br}(K_v)$ is injective by the Brauer-Hasse-Noether theorem 3.29. As β is taken arbitrarily, Theorem 4.27 shows that $\alpha \in K^{\times 2}$. This completes the proof. □

Remark 4.49. When $K = \mathbb{Q}$, Lemma 4.48 can be easily proved by factorizing α into a product of prime numbers. In general, it is known that $\alpha \in K$ is a square if it is a square in K_v for *almost all* $v \in \mathcal{V}$, see [35, Theorem 65:15].

The Hasse-Minkowski theorem below states that there is no obstruction between local and global with respect to isotropy of inner products.

Theorem 4.50 (Hasse-Minkowski)**.** *Let K be an algebraic number field. An inner product space (V, b) over K is isotropic if and only if its localization $(V \otimes K_v, b \otimes K_v)$ is isotropic for every $v \in \mathcal{V}$.*

Proof. Over any field, there is no isotropic inner product space of dimension 1. Hence, the one dimensional case is clear. Let (V, b) be an inner product space over K, and assume that its dimension d is at least 2. If b is isotropic then it is clear that its localizations are isotropic. Conversely, suppose that $b \otimes K_v$ is isotropic for every $v \in \mathcal{V}$.

Case $d = 2$. For any $v \in \mathcal{V}$, it follows from Theorem 4.35 (i) that $-\det(b)$ is a square in $K_v^\times$ since $b \otimes K_v$ is isotropic. Thus $-\det(b)$ is also a square in $K^\times$ by Lemma 4.48. Hence b is isotropic by Theorem 4.35 (i) again.

Case $d = 3$. For any $v \in \mathcal{V}$, we have $\mathrm{HW}_{K_v}(b \otimes K_v) + [-1, -\det(b)]_{K_v} = 0$ by Theorem 4.35 (ii) since $b \otimes K_v$ is isotropic. This implies that $\mathrm{HW}_K(b) + [-1, -\det(b)]_K = 0$ by injectivity of $\mathrm{Br}(K) \to \bigoplus_{v \in \mathcal{V}} \mathrm{Br}(K_v)$ (this is a part of Brauer-Hasse-Noether theorem 3.29). Thus b is isotropic by Theorem 4.35 (ii) again.

Case $d = 4$. The proof is essentially the same as that of Case $d = 3$. Put $L = K(\sqrt{\det(b)})$ and $\theta = \mathrm{HW}_L(b \otimes_K L) + [-1, -\det(b)]_L \in \mathrm{Br}(L)$. By Theorem 4.35 (iii), it suffices to show that $\theta = 0$. We write $\mathcal{U}$ for the set of all places of L. Let $u \in \mathcal{U}$ be any place of L, and let v be the place of K below u. Then $b \otimes_L L_u$, which is equal to $(b \otimes_K K_v) \otimes_{K_v} L_u$, is isotropic since so is $b \otimes_K K_v$. This means that $\mathrm{res}_{L_u/L}(\theta) = \mathrm{HW}_{L_u}(b \otimes_K L_u) + [-1, -\det(b \otimes_K L_u)]_{L_u} = 0$ in $\mathrm{Br}(L_u)$ by Theorem 4.35 (iii), and hence $\theta = 0$ as required by injectivity of $\mathrm{Br}(L) \to \bigoplus_{u \in \mathcal{U}} \mathrm{Br}(L_u)$.

Case $d \geq 5$. We conclude the proof by induction on d. Write $b \cong \langle \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d \rangle_K$ where $\alpha_i \in K^\times$, and set $b' = \langle \alpha_3, \ldots, \alpha_d \rangle_K$. Furthermore, we define

$$\mathcal{S} := \mathcal{V}_\infty \cup \mathcal{V}_2 \cup \{ v \in \mathcal{V} \mid v \text{ is finite and } v(\alpha_i) \neq 0 \text{ for some } i \in \{1, \ldots, d\} \}$$

where $\mathcal{V}_\infty$ and $\mathcal{V}_2$ denote the sets of all places of $\mathcal{V}$ above ∞ and 2 respectively. Then $\mathcal{S}$ is a finite set. Let $v \in \mathcal{S}$. Since the inner product $b \otimes K_v \cong \langle \alpha_1, \alpha_2 \rangle_{K_v} \oplus (b' \otimes K_v)$ is isotropic, there exists a nonzero element $\gamma_v \in K_v^\times$ such that both $\langle \alpha_1, \alpha_2 \rangle_{K_v}$ and $-b' \otimes K_v$ represent γ_v. Let $x_{v,1}, x_{v,2} \in K_v$ be elements satisfying $\alpha_1 x_{v,1}^2 + \alpha_2 x_{v,2}^2 = \gamma_v$.

By the approximation theorem 1.26, there exist elements x_1 and $x_2 \in K$ which are arbitrarily close to $x_{v,1}$ and $x_{v,2}$ with respect to the distance defined by v for any $v \in \mathcal{S}$, since $\mathcal{S}$ is a finite set. We then define $\gamma := \alpha_1 x_1^2 + \alpha_2 x_2^2 \in K$. Note that $\gamma \neq 0$ because it can be arbitrarily close to a nonzero element γ_v with respect to $v \in \mathcal{S}$. Moreover, it follows from Proposition 2.12 that $\gamma = \gamma_v$ in $K_v^\times / K_v^{\times 2}$ for each $v \in \mathcal{V}$.

Claim: The inner product $(\langle \gamma \rangle_K \oplus b') \otimes K_v = \langle \gamma \rangle_{K_v} \oplus (b' \otimes K_v)$ is isotropic for any $v \in \mathcal{V}$. For $v \in \mathcal{S}$, the localization $b' \otimes K_v$ represents $-\gamma_v$ by the definition of γ_v. Thus $\langle \gamma \rangle_{K_v} \oplus (b' \otimes K_v)$ is isotropic since $\gamma = \gamma_v$ in $K_v^\times / K_v^{\times 2}$. Suppose that $v \notin \mathcal{S}$. It suffices to show that the subspace $b' \otimes K_v \cong \langle \alpha_3, \ldots, \alpha_d \rangle_{K_v}$ is isotropic. Note that v is a finite place and the prime below v is not 2. Let $\mathfrak{p}_v$ and κ_v denote the maximal ideal and residue field of K_v respectively. We consider the quadratic form q_v over K_v defined by $q_v(X_3, \ldots, X_d) = \alpha_3 X_3^2 + \cdots + \alpha_d X_d^2$, and write $\overline{q_v}$ for the reduction modulo $\mathfrak{p}_v$, that is, $\overline{q_v}(X_3, \ldots, X_d) = \overline{\alpha_3} X_3^2 + \cdots + \overline{\alpha_d} X_d^2$ where $\overline{\alpha} := \alpha + \mathfrak{p}_v \in \kappa_v$. Since $d \geq 5$ and $v(\alpha_i) = 0$ for all $i = 3, \ldots, d$, the reduction $\overline{q_v}$ has at least 3 variables. Thus

$\overline{q_v}$ has a nontrivial zero over κ_v by Lemma 4.37 and Theorem 4.38, and hence q_v also has a nontrivial zero over K_v by Proposition 1.37. This shows that b' is isotropic as required.

Since $\dim(\langle\gamma\rangle_K \oplus b') = d-1$, the claim proved now and the induction hypothesis imply that $\langle\gamma\rangle_K \oplus b'$ is isotropic. Therefore, the inner product $b \cong \langle\alpha_1,\alpha_2\rangle_K \oplus b'$, which contains the subspace isomorphic to $\langle\gamma\rangle_K \oplus b'$, is also isotropic. The proof is complete. □

Corollary 4.51. *An inner product b over K represents an element $\alpha \in K$ if and only if its localization $b \otimes K_v$ represents α for every $v \in \mathcal{V}$.*

Proof. Let b be an inner product over K and $\alpha \in K$ an element of K. The case $\alpha = 0$ is nothing but the Hasse-Minkowski theorem 4.50. So we assume that $\alpha \neq 0$. If α is represented by b then it is obvious that its localization also represents α. Suppose that $b \otimes K_v$ represents α for every $v \in \mathcal{V}$. Then the inner product $(b \oplus \langle -\alpha\rangle_K) \otimes K_v = (b \otimes K_v) \oplus \langle -\alpha\rangle_{K_v}$ is isotropic for all $v \in \mathcal{V}$. Thus $b \oplus \langle -\alpha\rangle_K$ is also isotropic by Hasse-Minkowski theorem 4.50, and hence b represents α by Lemma 4.8 (iii). □

Corollary 4.52. *Two inner product spaces (V_1, b_1) and (V_2, b_2) over K are isomorphic if and only if their localizations $(V_1 \otimes K_v, b_1 \otimes K_v)$ and $(V_2 \otimes K_v, b_2 \otimes K_v)$ are isomorphic for any $v \in \mathcal{V}$.*

Proof. Let (V_1, b_1) and (V_2, b_2) be two inner product spaces over K. If $b_1 \cong b_2$ then it is obvious that $b_1 \otimes K_v \cong b_2 \otimes K_v$ for any $v \in \mathcal{V}$. Conversely, suppose that $b_1 \otimes K_v \cong b_2 \otimes K_v$ for any $v \in \mathcal{V}$. We argue by induction on the dimension of b_1. If $\dim(b_1) = 0$ then there is nothing to prove. Suppose that $\dim(b_1) \geq 1$. Let $\alpha \in K^\times$ be a nonzero element represented by b_1. Then α is represented by $b_1 \otimes K_v$, and by $b_2 \otimes K_v$ for every $v \in \mathcal{V}$. This means that b_2 also represents α by Corollary 4.51. Thus we can write

$$b_1 \cong b_1' \oplus \langle\alpha\rangle_K \quad \text{and} \quad b_2 \cong b_2' \oplus \langle\alpha\rangle_K$$

for suitable inner products b_1' and b_2'. Then, we have

$$(b_1' \otimes K_v) \oplus \langle\alpha\rangle_{K_v} = b_1 \otimes K_v \cong b_2 \otimes K_v = (b_2' \otimes K_v) \oplus \langle\alpha\rangle_{K_v}$$

for any $v \in \mathcal{V}$. Thus, it follows from Witt's cancellation theorem 4.19 that $b_1' \otimes K_v \cong b_2' \otimes K_v$ for any $v \in \mathcal{V}$. This implies that $b_1' \cong b_2'$ by induction hypothesis since $\dim(b_1') = \dim(b_1) - 1$. Therefore $b_1 \cong b_2$ as required. □

This corollary is a classification theorem for inner products over an algebraic number field. Our next interest is the existence problem: for a given family $\{b_v\}_{v\in\mathcal{V}}$ of inner products b_v over K_v, does there exist an inner product over K such that $b \otimes K_v \cong b_v$ for all $v \in \mathcal{V}$? It is clear that if b is an inner product over K then $\dim_{K_v}(b \otimes K_v) = \dim_K(b)$ and $\det(b \otimes K_v) = \det(b)$ in $K_v^\times / K_v^{\times 2}$ for all $v \in \mathcal{V}$. Moreover, there is a constraint also for Hasse-Witt invariants.

Proposition 4.53 (Reciprocity)**.** *Let b be an inner product over K. Then $\mathrm{HW}_{K_v}(b \otimes K_v) = 0$ for almost all $v \in \mathcal{V}$ and $\sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v} \circ \mathrm{HW}_{K_v}(b \otimes K_v) = 0$ in $\left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.*

Proof. As a part of the Brauer-Hasse-Noether theorem 3.29, the composition

$$\mathrm{Br}(K) \to \bigoplus_{v\in\mathcal{V}} \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$$

is the zero map. Hence, we obtain the assertion by applying this map to $\mathrm{HW}_K(b) \in \mathrm{Br}(K)$. □

The converse of this proposition will be proved in Theorem 4.57. We start with the definition of an inner product being a direct summand of another inner product, which generalizes the definition of an element being represented by an inner product.

Definition 4.54. Let b and b_0 be inner products over any field. We say that b_0 is a *direct summand* of b if there exists an inner product b' such that $b \cong b' \oplus b_0$.

Lemma 4.8 (i) means that an inner product b represents a nonzero element α if and only if the one-dimensional inner product $\langle \alpha \rangle$ is a direct summand of b. We have an analog of Corollary 4.51:

Lemma 4.55. *Let b and b_0 be inner products over K. The inner product b_0 is a direct summand of b if and only if $b_0 \otimes K_v$ is a direct summand of $b \otimes K_v$ for every $v \in \mathcal{V}$.*

Proof. The only if part is obvious. We prove the if part by induction on $d := \dim(b_0)$. Suppose that $b_0 \otimes K_v$ is a direct summand of $b \otimes K_v$ for every $v \in \mathcal{V}$, and write $b_0 \cong \langle \alpha_1 \dots, \alpha_d \rangle_K$ where $\alpha_1 \dots, \alpha_d \in K^\times$. If $d = 1$ then $b_0 \cong \langle \alpha_1 \rangle_K$ is a direct summand of b by Corollary 4.51. Suppose that $d > 1$. For every $v \in \mathcal{V}$, the localization $b \otimes K_v$ can be written as

$$b \otimes K_v \cong b'_v \oplus \langle \alpha_1 \dots, \alpha_{d-1} \rangle_{K_v} \oplus \langle \alpha_d \rangle_{K_v}$$

where b'_v is an inner product over K_v. Thus $\langle \alpha_d \rangle_K$ is a direct summand of b by the one-dimensional case. So, we can write $b \cong b'' \oplus \langle \alpha_d \rangle_K$ where b'' is an inner product over K. By Witt's cancellation theorem 4.19, it follows that $b'' \otimes K_v \cong b'_v \oplus \langle \alpha_1 \dots, \alpha_{d-1} \rangle_{K_v}$ for all $v \in \mathcal{V}$, which means that $\langle \alpha_1 \dots, \alpha_{d-1} \rangle_K$ is a direct summand of b'' at every place. Hence it also holds over K by induction hypothesis. Namely, there exists an inner product b' over K such that $b'' \cong b' \oplus \langle \alpha_1, \dots, \alpha_{d-1} \rangle_K$. Therefore we obtain

$$b \cong b'' \oplus \langle \alpha_d \rangle_K \cong b' \oplus \langle \alpha_1, \dots, \alpha_{d-1} \rangle_K \oplus \langle \alpha_d \rangle_K \cong b' \oplus b_0.$$

This completes the proof. □

We also need the following lemma.

Lemma 4.56. *Let $\gamma \in K^\times$ be a nonzero element, and let $(\alpha_v)_{v \in \mathcal{V}}$ be a family consisting of $\alpha_v \in K_v^\times$ such that $[\alpha_v, \gamma]_{K_v} = 0$ for almost all $v \in \mathcal{V}$ and $\sum_{v \in \mathcal{V}} \mathrm{inv}_{K_v}([\alpha_v, \gamma]_{K_v}) = 0$. Then there exists $\alpha \in K^\times$ such that $[\alpha, \gamma]_{K_v} = [\alpha_v, \gamma]_{K_v}$ for all $v \in \mathcal{V}$.*

Proof. If $\gamma \in K^{\times 2}$ then $[\alpha_v, \gamma]_{K_v}$ must be 0 for any $v \in \mathcal{V}$, and any $\alpha \in K^\times$ satisfies the equality $[\alpha, \gamma]_{K_v} = 0 = [\alpha_v, \gamma]_{K_v}$ for all $v \in \mathcal{V}$. Suppose that $\gamma \notin K^{\times 2}$, and put $E = K(\sqrt{\gamma})$. Let $\sigma \in \mathrm{Gal}(E/K)$ be the generator of $\mathrm{Gal}(E/K)$. Note that $E^\sigma = K$. Then, we have the commutative diagram

$$\begin{array}{ccccc} \mathrm{Tw}(E,\sigma) & \longrightarrow & \bigoplus_{v \in \mathcal{V}} \mathrm{Tw}(E_v,\sigma) & \xrightarrow{\sum_v \iota_v} & \mathbb{Z}/2\mathbb{Z} \\ \downarrow{\scriptstyle [\sigma,\cdot]_K} & & \downarrow{\scriptstyle \bigoplus_v [\sigma,\cdot]_{K_v}} & & \downarrow{\scriptstyle \times 1/2} \\ \mathrm{Br}(K) & \longrightarrow & \bigoplus_{v \in \mathcal{V}} \mathrm{Br}(K_v) & \xrightarrow{\sum_{v \in V} \mathrm{inv}_{K_v}} & \mathbb{Q}/\mathbb{Z} \end{array} \qquad (*)$$

as in the proof of Proposition 3.31, where rows are exact. On the other hand, we have $[\sigma, \beta_v]_{K_v} = [\beta_v, \gamma]_{K_v}$ for any v and any $\beta_v \in K_v^\times$. Indeed, both sides are zero if v is split in E, and otherwise this follows from Proposition 4.25. Thus

$$\textstyle\sum_{v \in \mathcal{V}} \mathrm{inv}_{K_v}([\sigma, \alpha_v]_{K_v}) = \sum_{v \in \mathcal{V}} \mathrm{inv}_{K_v}([\alpha_v, \gamma]_{K_v}) = 0.$$

Hence, it follows from the commutative diagram $(*)$ that $\sum_{v \in \mathcal{V}} \iota_v(\alpha_v) = 0$ and there exists $\alpha \in K^\times$ such that $\alpha = \alpha_v$ in $\mathrm{Tw}(E_v, \sigma)$ for all $v \in \mathcal{V}$. Then

$$([\alpha, \gamma]_{K_v})_{v \in \mathcal{V}} = ([\sigma, \alpha]_{K_v})_{v \in \mathcal{V}} = ([\sigma, \alpha_v]_{K_v})_{v \in \mathcal{V}} = ([\alpha_v, \gamma]_{K_v})_{v \in \mathcal{V}},$$

and this completes the proof. □

Theorem 4.57. *Let $d \in \mathbb{Z}_{>0}$ be a positive integer and $\delta \in K^\times$ a nonzero element. Let $\{b_v\}_{v\in\mathcal{V}}$ is a family consisting of inner products b_v over K_v with $\dim b_v = d$ and $\det b = \delta$. Suppose that $\mathrm{HW}_{K_v}(b_v) = 0$ for almost all $v \in \mathcal{V}$ and $\sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v} \circ \mathrm{HW}_{K_v}(b_v) = 0$. Then there exists an inner product b over K such that $b \otimes K_v \cong b_v$ for all $v \in \mathcal{V}$.*

Proof. If $d = 1$ then $b_v \cong \langle\delta\rangle_{K_v}$ for all $v \in \mathcal{V}$, so $b := \langle\delta\rangle_K$ is the desired inner product. Suppose that $d = 2$. In this case, we can write $b_v \cong \langle\alpha_v, \alpha_v\delta\rangle_{K_v}$ for each $v \in \mathcal{V}$ where $\alpha_v \in K_v^\times$. Then $\mathrm{HW}_{K_v}(b_v) = [\alpha_v, \alpha_v\delta]_{K_v} = [\alpha_v, -\delta]_{K_v}$. Thus, it follows from that the assumption and Lemma 4.56 that there exists $\alpha \in K^\times$ such that $[\alpha, -\delta]_{K_v} = [\alpha_v, -\delta]_{K_v}$ for all $v \in \mathcal{V}$. We now define $b := \langle\alpha, \alpha\delta\rangle_K$. Then, for any $v \in \mathcal{V}$, we have $\det(b \otimes K_v) = \delta = \det(b_v)$ and

$$\mathrm{HW}_{K_v}(b \otimes K_v) = [\alpha, \alpha\delta]_{K_v} = [\alpha, -\delta]_{K_v} = [\alpha_v, -\delta]_{K_v} = \mathrm{HW}_{K_v}(b_v),$$

which means $b \otimes K_v \cong b_v$ by Theorem 4.32. Hence b is the desired inner product.

Suppose that $d \geq 3$ and write $b_v \cong \langle\alpha_{v,1}, \ldots, \alpha_{v,d-1}, \alpha_{v,1}\cdots\alpha_{v,d-1}\delta\rangle_{K_v}$ for each $v \in \mathcal{V}$ where $\alpha_{v,i} \in K_v^\times$. Put $\mathcal{S} = \{v \in \mathcal{V} \mid v \text{ is an infinite place or } \mathrm{HW}_{K_v}(b_v) \neq 0\}$. Then $\mathcal{S}$ is a finite set. Thus, for each $i = 1, \ldots, d-1$, there exists $\alpha_i \in K^\times$ such that $\alpha_i = \alpha_{v,i}$ in $K_v^\times/K_v^{\times 2}$ for all $v \in \mathcal{S}$ by the approximation theorem 1.26 and Proposition 2.12. We define $\widetilde{b} := \langle\alpha_1, \ldots, \alpha_{d-1}, \alpha_1\cdots\alpha_{d-1}\delta\rangle_K$ and put $\mathcal{T} = \{v \in \mathcal{V} \mid \widetilde{b} \otimes K_v \ncong b_v\}$.

Claim 1*: $\mathcal{T}$ is a finite set consisting of finite places, and $\#\mathcal{T}$ is even.* By the definitions of $\widetilde{b}$ and $\alpha_1, \ldots, \alpha_{d-1}$, we have $\widetilde{b} \otimes_K K_v \cong b_v$ for all $v \in \mathcal{S}$. In particular $\mathcal{T}$ has no infinite place. Furthermore $\mathcal{T}$ can be written as

$$\mathcal{T} = \{v \in \mathcal{V} \mid \ v \text{ is finite and } \mathrm{HW}_{K_v}(\widetilde{b} \otimes K_v) \neq \mathrm{HW}_{K_v}(b_v)\}$$

by Theorem 4.45. On the other hand, it follows from Proposition 4.53 and the assumption on $\{b_v\}_v$ that $\mathrm{HW}_{K_v}(\widetilde{b})$ and $\mathrm{HW}_{K_v}(b_v)$ are zero for almost all v. Hence $\mathcal{T}$ is a finite set. Moreover it also follows that $\#\mathcal{T}$ is even because

$$\begin{aligned}&\textstyle\sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}(\mathrm{HW}_{K_v}(\widetilde{b}) - \mathrm{HW}_{K_v}(b_v))\\ &\quad = \textstyle\sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}(\mathrm{HW}_{K_v}(\widetilde{b})) - \sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}(\mathrm{HW}_{K_v}(b_v)) = 0 - 0 = 0.\end{aligned}$$

Claim 2*: There exist two 2-dimensional inner products b_0 and $\widetilde{b}_0$ over K with same determinant such that $\mathrm{HW}_{K_v}(b_0) = \mathrm{HW}_{K_v}(\widetilde{b}_0)$ for all $v \notin \mathcal{T}$ and $\mathrm{HW}_{K_v}(b_0) \neq \mathrm{HW}_{K_v}(\widetilde{b}_0)$ for all $v \in \mathcal{T}$.* Let $\gamma \in K^\times$ be a nonzero element which is not a square in $K_v^\times$ for any $v \in \mathcal{T}$. Such an element exists: for example, we can take $\gamma \in K^\times$ arbitrarily close to a non-square element of K_v for any $v \in \mathcal{T}$ by approximation theorem 1.26, and then γ is not a square in $K_v^\times$ by Proposition 2.12. Now, by Theorem 4.27, we can take a family $(\alpha_v)_{v\in\mathcal{V}}$ ($\alpha_v \in K_v^\times$) so that $[\alpha_v, \gamma]_{K_v} \neq 0$ for $v \in \mathcal{T}$ and $[\alpha_v, \gamma]_{K_v} = 0$ for $v \notin \mathcal{T}$. Note that $\sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}([\alpha_v, \gamma]_{K_v}) = 0$ since $\#\mathcal{T}$ is even. Thus, there exists $\alpha \in K^\times$ such that $[\alpha, \gamma]_{K_v} = [\alpha_v, \gamma]_{K_v}$ for all $v \in \mathcal{V}$ by Lemma 4.56. We define

$$b_0 := \langle 1, \alpha\gamma\rangle_K \quad \text{and} \quad \widetilde{b}_0 := \langle\alpha, \gamma\rangle_K.$$

Then they have the same determinant $\alpha\gamma$. Moreover $\mathrm{HW}_{K_v}(b_0) = 0 = \mathrm{HW}_{K_v}(\widetilde{b}_0)$ for $v \notin \mathcal{T}$ and $\mathrm{HW}_{K_v}(b_0) = 0 \neq \mathrm{HW}_{K_v}(\widetilde{b}_0)$ for $v \in \mathcal{T}$.

Claim 3*: The 2-dimensional inner product $\widetilde{b}_0$ is a direct summand of $\widetilde{b} \oplus b_0$.* By Lemma 4.55, it is sufficient to show that the localization $\widetilde{b}_0 \otimes K_v$ is a direct summand of $(\widetilde{b} \oplus b_0) \otimes K_v = (\widetilde{b} \otimes K_v) \oplus (b_0 \otimes K_v)$ for every $v \in \mathcal{V}$. For $v \notin \mathcal{T}$ we have $\widetilde{b}_0 \otimes K_v \cong b_0 \otimes K_v$ by Theorem 4.32, and the assertion is clear. Let $v \in \mathcal{T}$. Then v is a finite place. Note that any inner product over K_v of dimension at least 4 represents every nonzero element (Proposition 4.44). Thus, any 2-dimensional inner product is a direct summand of any inner product over K_v of dimension at

least 5. In particular $\widetilde{b}_0 \otimes K_v$ is a direct summand of $(\widetilde{b} \otimes K_v) \oplus (b_0 \otimes K_v)$. This completes the proof of Claim 3.

By Claim 3, there exists an inner product b over K such that $\widetilde{b} \oplus b_0 \cong b \oplus \widetilde{b}_0$. For any infinite place v we have $\widetilde{b}_0 \otimes K_v \cong b_0 \otimes K_v$, and hence $b \otimes K_v \cong \widetilde{b} \otimes K_v \cong b_v$ by Witt's calculation theorem 4.19. Let $v \in \mathcal{V}$ be a finite place. We have $\det(b) = \det(\widetilde{b}) = \det(b_v)$ where the first equality follows from $\det(b_0) = \det(\widetilde{b}_0)$. Moreover, it follows from Lemma 4.31 (ii) that

$$\begin{aligned} 0 &= \mathrm{HW}_{K_v}(\widetilde{b} \oplus b_0) - \mathrm{HW}_{K_v}(b \oplus \widetilde{b}_0) \\ &= (\mathrm{HW}_{K_v}(\widetilde{b}) + \mathrm{HW}_{K_v}(b_0) + [\delta, \det(b_0)]_{K_v}) - (\mathrm{HW}_{K_v}(b) + \mathrm{HW}_{K_v}(\widetilde{b}_0) + [\delta, (\det \widetilde{b}_0)]_{K_v}) \\ &= \mathrm{HW}_{K_v}(\widetilde{b}) + \mathrm{HW}_{K_v}(b_0) - \mathrm{HW}_{K_v}(b) - \mathrm{HW}_{K_v}(\widetilde{b}_0). \end{aligned}$$

Hence

$$\mathrm{HW}_{K_v}(b) - \mathrm{HW}_{K_v}(b_v) = (\mathrm{HW}_{K_v}(\widetilde{b}) - \mathrm{HW}_{K_v}(b_v)) - (\mathrm{HW}_{K_v}(\widetilde{b}_0) - \mathrm{HW}_{K_v}(b_0)) = 0$$

because both $\mathrm{HW}_{K_v}(\widetilde{b}) - \mathrm{HW}_{K_v}(b_v)$ and $\mathrm{HW}_{K_v}(\widetilde{b}_0) - \mathrm{HW}_{K_v}(b_0)$ are nonzero if $v \in \mathcal{T}$, and both are zero if $v \notin \mathcal{T}$. Therefore $b \otimes K_v \cong b_v$ by Theorem 4.45. The proof is complete. □

4.8 Explicit computation of Hilbert symbols

We have now gone through the general theory of inner products over fields of number theory. Here is an explicit computation of *Hilbert symbols* over local fields obtained by completions of $\mathbb{Q}$. Let v be a place of $\mathbb{Q}$, that is, the infinite place ∞ or a prime number p. Note that

$$\mathrm{Br}_2(\mathbb{Q}_v) \xrightarrow{\mathrm{inv}_{\mathbb{Q}_v}} \left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \tag{16}$$

is a group isomorphism, see Proposition 4.42 (i).

Definition 4.58. Let $\alpha, \beta \in \mathbb{Q}_v^\times$ be nonzero elements. The *Hilbert symbol* of α and β, denoted $(\alpha, \beta)_v$, is the image of the Brauer class $[\alpha, \beta]_{\mathbb{Q}_v}$ under the isomorphism (16). Similarly, for an inner product b_v over $\mathbb{Q}_v$, we write $\mathrm{hw}_v(b_v)$ for the image of the Hasse-Witt invariant $\mathrm{HW}_{\mathbb{Q}_v}(b_v)$ under (16), and call it the Hasse-Witt invariant again.

By Theorem 4.23, the Hilbert symbol can be written as

$$(\alpha, \beta)_v = \begin{cases} 0 & \text{if } \langle 1, -\alpha, -\beta, \alpha\beta \rangle_{\mathbb{Q}_v} \text{ is isotropic} \\ 1 & \text{if } \langle 1, -\alpha, -\beta, \alpha\beta \rangle_{\mathbb{Q}_v} \text{ is anisotropic} \end{cases}$$

for $\alpha, \beta \in K^\times$.

Remark 4.59. The Hilbert symbol is often expressed multiplicatively and considered to take values in the multiplicative group $\{1, -1\}$ of order 2, though we express it additively. One can also define the Hilbert symbol as

$$(\alpha, \beta)_v = \begin{cases} 0 & \text{if } \langle 1, -\alpha, -\beta \rangle_{\mathbb{Q}_v} \text{ is isotropic} \\ 1 & \text{if } \langle 1, -\alpha, -\beta \rangle_{\mathbb{Q}_v} \text{ is anisotropic} \end{cases}$$

for $\alpha, \beta \in K^\times$, see [39, Chapter 2, Corollary 11.10]. This definition may be more familiar.

As seen in Theorem 4.26, the Hilbert symbol $(\cdot,\cdot)_v$ is a symmetric bilinear form on $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$ which takes values in $\{0,1\}$. We have

$$\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} = \begin{cases} \{1,-1\} & \text{if } v=\infty \\ \{1,\epsilon,p,\epsilon p\} & \text{if } v \text{ is an odd prime } p \\ \{1,-1,3,-3,2,-2,6,-6\} & \text{if } v=2, \end{cases}$$

where ϵ is a non-square unit of $\mathbb{Z}_p$ ($p\neq 2$). This is clear if $v=\infty$, and seen in §2.2 if v is a prime number.

Theorem 4.60. *We have $(-1,-1)_\infty = 1$. For an inner product b over $\mathbb{R}$ of signature (r,s), we have*

$$\mathrm{hw}_\infty(b) = \frac{s(s-1)}{2} = \begin{cases} 0 & \text{if } s\equiv 0,1 \bmod 4 \\ 1 & \text{if } s\equiv 2,3 \bmod 4 \end{cases}$$

in $\mathbb{Z}/2\mathbb{Z}$.

Proof. Straightforward. □

At a finite place, Hilbert symbols can be calculated as follows.

Theorem 4.61. *Let p be a prime number.*

(i) *Suppose that p is an odd prime, and let ϵ be a non-square unit of $\mathbb{Z}_p$. Then*

$$(\epsilon,\epsilon)_p = 0,\ (\epsilon,p)_p = 1,\ (p,p)_p = \begin{cases} 0 & \text{if } p\equiv 1 \bmod 4 \\ 1 & \text{if } p\equiv 3 \bmod 4. \end{cases}$$

(ii) *At the prime 2, we have*

$$(-1,-1)_2 = 1,\ (-1,3)_2 = 1,\ (-1,2)_2 = 0,\ (3,3)_2 = 1,\ (3,2)_2 = 1,\ (2,2)_2 = 0.$$

In particular $(u,-3) = 0$ for any unit $u\in\mathbb{Z}_2^\times$.

Proof. We remark that a quadratic form q over $\mathbb{Q}_p$ has a nontrivial zero over $\mathbb{Q}_p$ if and only if q has a primitive zero over $\mathbb{Z}_p$. For $\alpha,\beta\in\mathbb{Z}_p$, we define

$$q_{\alpha,\beta}(X_1,X_2,X_3,X_4) := X_1^2 - \alpha X_2^2 - \beta X_3^2 + \alpha\beta X_4^2.$$

Then $(\alpha,\beta)_p = 1$ if and only if $q_{\alpha,\beta}$ has no primitive zero over $\mathbb{Z}_p$.

(i). Suppose that p is an odd prime. The quadratic form $q_{\epsilon,\epsilon}$ has a nontrivial zero modulo p by Lemma 4.37. Then, the zero lifts the zero over $\mathbb{Z}_p$ by Proposition 1.37. Thus $(\epsilon,\epsilon)_p = 0$. Let $(x_1,x_2,x_3,x_4)\in(\mathbb{Z}_p)^4$ be a zero of $q_{\epsilon,p}$. Then

$$x_1^2 - \epsilon x_2^2 = p(x_3^2 - \epsilon x_4^2). \tag{17}$$

This shows that $x_1^2-\epsilon x_2^2\equiv 0 \bmod p$, and thus $(x_1,x_2)\equiv(0,0) \bmod p$. Then, again by (17), we get $x_1^3 - \epsilon x_4^2 = x_1^2/p - \epsilon x_2^2/p \equiv 0 \bmod p$, and $(x_3,x_4)\equiv(0,0) \bmod p$. This means that $q_{\epsilon,p}$ has no primitive zero. Hence $(\epsilon,p)_p = 1$. It remains to compute $(p,p)_p$. We remark that -1 is a square if and only if $p\equiv 1 \bmod 4$ by Corollary 2.3 and Proposition 1.37. Suppose first that $p\equiv 1 \bmod 4$. Then $\langle 1,-p,-p,p^2\rangle_{\mathbb{Q}_2} \cong \langle 1,-p,-p,-1\rangle_{\mathbb{Q}_2}$ and it is isotropic. Thus $(p,p)_p = 0$. Suppose that $p\equiv 3 \bmod 4$. Then $\epsilon = -1$ mod squares. Thus $(p,\epsilon p)_p = (p,-p)_p = 0$, and $(p,p)_p = (p,\epsilon p)_p + (p,\epsilon)_p = 1$. This completes the proof of the assertion (i).

(ii). Some computations show that each of quadratic forms $q_{-1,-1}, q_{-1,3}, q_{3,3}$, and $q_{-3,2}$ has no primitive zero modulo 8. Hence $(-1,-1)_2, (-1,3)_2, (3,3)_2$, and $(-3,2)_2$ are all 1. On the other hand, we have $q_{-1,2}(1,1,1,0) = 0$ and $q_{2,2}(0,1,1,1) = 0$. This means that $(-1,2)_2 = (2,2)_2 = 0$. It remains to show that $(u,-3)_2 = 0$ for any unit $u \in \mathbb{Z}_2^\times$. $(1,-3)_2 = 0$ and $(3,-3)_2 = 0$ are obvious. Moreover, we have

$$(-1,-3)_2 = (-1,3)_2 + (-1,-1)_2 = 1+1 = 0,$$
$$(-3,-3)_2 = (-1,-1)_2 + (-1,3)_2 + (3,-1)_2 + (3,3)_2 = 1+1+1+1 = 0.$$

This completes the proof. □

Since the Hilbert symbol is symmetric and bilinear, we can calculate the Hilbert symbol of every pair by Theorem 4.61. A direct computation yields the following corollary, cf. Theorem 4.46.

Corollary 4.62. *Let p be an odd prime and ϵ a non-square unit of $\mathbb{Z}_p$. An inner product over $\mathbb{Q}_p$ with a prescribed dimension, determinant, and Hasse-Witt invariant is given as in Tables 4.1 and 4.2.* □

One can get an analog of this corollary for $p = 2$, but it is omitted in this thesis.

Table 4.1: Inner products with prescribed invariants in the case $p \equiv 1 \bmod 4$

		$\dim(b) = 1$	$\dim(b) = 2$	$\dim(b) \geq 3$
$\det(b) = 1$,	$\mathrm{hw}_p(b) = 0$	$\langle 1\rangle_{\mathbb{Q}_p}$	$\langle 1,1\rangle_{\mathbb{Q}_p}$	$\langle 1\rangle_{\mathbb{Q}_p}^{\oplus d}$
$\det(b) = 1$,	$\mathrm{hw}_p(b) = 1$	None	None	$\langle \epsilon, p, \epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-3}$
$\det(b) = \epsilon$,	$\mathrm{hw}_p(b) = 0$	$\langle \epsilon\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon$,	$\mathrm{hw}_p(b) = 1$	None	$\langle p,\epsilon p\rangle_{\mathbb{Q}_p}$	$\langle p,\epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = p$,	$\mathrm{hw}_p(b) = 0$	$\langle p\rangle_{\mathbb{Q}_p}$	$\langle 1,p\rangle_{\mathbb{Q}_p}$	$\langle 1,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = p$,	$\mathrm{hw}_p(b) = 1$	None	$\langle \epsilon,\epsilon p\rangle_{\mathbb{Q}_p}$	$\langle \epsilon,\epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon p$,	$\mathrm{hw}_p(b) = 0$	$\langle \epsilon p\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon p\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon p$,	$\mathrm{hw}_p(b) = 1$	None	$\langle \epsilon,p\rangle_{\mathbb{Q}_p}$	$\langle \epsilon,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$

Table 4.2: Inner products with prescribed invariants in the case $p \equiv 3 \bmod 4$

		$\dim(b) = 1$	$\dim(b) = 2$	$\dim(b) \geq 3$
$\det(b) = 1$,	$\mathrm{hw}_p(b) = 0$	$\langle 1\rangle_{\mathbb{Q}_p}$	$\langle 1,1\rangle_{\mathbb{Q}_p}$	$\langle 1\rangle_{\mathbb{Q}_p}^{\oplus d}$
$\det(b) = 1$,	$\mathrm{hw}_p(b) = 1$	None	$\langle p,p\rangle_{\mathbb{Q}_p}$	$\langle p,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon$,	$\mathrm{hw}_p(b) = 0$	$\langle \epsilon\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon$,	$\mathrm{hw}_p(b) = 1$	None	None	$\langle \epsilon,p,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-3}$
$\det(b) = p$,	$\mathrm{hw}_p(b) = 0$	$\langle p\rangle_{\mathbb{Q}_p}$	$\langle 1,p\rangle_{\mathbb{Q}_p}$	$\langle 1,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = p$,	$\mathrm{hw}_p(b) = 1$	None	$\langle \epsilon,\epsilon p\rangle_{\mathbb{Q}_p}$	$\langle \epsilon,\epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon p$,	$\mathrm{hw}_p(b) = 0$	$\langle \epsilon p\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon p\rangle_{\mathbb{Q}_p}$	$\langle 1,\epsilon p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$
$\det(b) = \epsilon p$,	$\mathrm{hw}_p(b) = 1$	None	$\langle \epsilon,p\rangle_{\mathbb{Q}_p}$	$\langle \epsilon,p\rangle_{\mathbb{Q}_p} \oplus \langle 1\rangle_{\mathbb{Q}_p}^{\oplus d-2}$

4.9 Hermitian products

Let K be a field, and let E be a commutative K-algebra with a nontrivial involution σ. For an E-module M, we write ${}^{\sigma}M^*$ for the E-module that the underlying abelian group is $M^* := \mathrm{Hom}_E(M, E)$ and scalar multiplication is given by

$$(\alpha.\xi)(x) = \sigma(\alpha)\xi(x) \quad (\alpha \in E, \xi \in M^*, x \in M).$$

Definition 4.63. Let M be a finitely generated free E-module. A map $h : M \times M \to E$ is called a *hermitian form* on M if h is E-linear in the first variable and satisfies $h(y, x) = \sigma h(x, y)$ for any $x, y \in M$. We write h^* for the homomorphism $M \to {}^{\sigma}M^*$ defined by

$$h^*(x) = (y \mapsto h(y, x)) \quad (x, y \in M).$$

A hermitian form $h : M \times M \to E$ is *nondegenerate* if the homomorphism h^* is injective. A nondegenerate hermitian form is called a *hermitian product*. If h is a hermitian product on M, then the pair (M, h) is called a *hermitian product space* (although E is not necessarily a field).

Note that $h(x, x)$ belongs to the fixed subalgebra E^{σ} for any hermitian form h on a free E-module M and for any $x \in M$. Similar terminology is used for hermitian forms as for symmetric bilinear forms. Let M, M' be finitely generated free E-modules, and h, h' be hermitian forms on M, M' respectively. We say that (M, h) and (M', h') are *isomorphic* if there exists an isomorphism $t : M \to M'$ of E-modules such that $h'(t(x), t(y)) = h(x, y)$ for all $x, y \in M$. For a submodule U of M, we define $U^{\perp} := \{y \in M \mid h(y, x) = 0 \text{ for any } x \in U\}$. When E is a field, an analog of Proposition 4.4 holds for hermitian product spaces (the statement is omitted).

Definition 4.64. Let M be a finitely generated free E-module, and $h : M \times M \to E$ a hermitian form on M.

(i) For an E-basis $e_1, \ldots, e_m$ of M, the $m \times m$ matrix $(h(e_i, e_j))_{ij}$ is called the *Gram matrix* of (M, h). Its determinant is not zero if and only if h is nondegenerate. When h is nondegenerate, the class of $\det((h(e_i, e_j))_{ij}) \in (E^{\sigma})^{\times}$ in the twisting group $\mathrm{Tw}(E, \sigma)$ does not depend on the chose of the E-basis. This class is referred to as the *determinant* of (M, h) and denoted by $\det(h)$. If h is degenerate then its determinant is defined to be 0.

(ii) An E-basis of M is called an *orthogonal basis* if the corresponding Gram matrix is diagonal.

(iii) Let $G = (g_{ij})_{ij} \in M_m(E)$ be an $m \times m$ nondegenerate hermitian matrix ('hermitian' means $g_{ji} = \sigma(g_{ij})$ for all i, j). The symbol $\langle G \rangle_E$ denotes the hermitian product space that its underlying space is E^m and G is the Gram matrix with respect to the standard basis of E^m. If G is a diagonal matrix, say $\mathrm{diag}(a_1, \ldots, a_d)$, then we write $\langle a_1, \ldots, a_d \rangle_E = \langle \mathrm{diag}(a_1, \ldots, a_d) \rangle_E$ for short.

Any hermitian product treated in this thesis has an orthogonal basis even if $\mathrm{char}\, K = 2$.

Proposition 4.65. *Suppose that E is a field or of type* (sp) *(see Definition* 1.9*). Then, any hermitian product space (M, h) over E has an orthogonal basis.*

Proof. One can prove it as in Proposition 4.9 when E is a field. However, in order to deal also with the case of type (sp), we imitate the *Gram-Schmidt process* for an inner product space and argue by induction on $m := \mathrm{rk}_E M$. The case $m = 1$ is obvious. Suppose that $m \geq 2$, and let $e_1, \ldots, e_m$ be a basis of M.

Case I*: There exists $i \in \{1, \ldots, m\}$ such that $h(e_i, e_i) \neq 0$.* We may assume that $i = 1$. Note that E^{σ} is a field, and $h(e_1, e_1) \in E^{\sigma}$ is invertible. Put $e'_j := e_j - \frac{h(e_j, e_1)}{h(e_1, e_1)} e_1$ for $j = 2, \ldots, m$.

Then $e_1, e'_2, \ldots, e'_m$ is a basis of M, and $h(e'_j, e_1) = 0$ for all $j = 2, \ldots, m$. Thus M decomposes as $M = Ee_1 \oplus M'$, where $M' \subset M$ is the free E-submodule with basis $e'_2, \ldots, e'_m$. Then M' has an orthogonal basis $e''_2, \ldots, e''_m$ by induction hypothesis. Because $e_1, e''_2, \ldots, e''_m$ is an orthogonal basis of M, we are done.

Case II*: $h(e_i, e_i) = 0$ for all $i = 1, \ldots, m$.* Since h is nondegenerate, there exists j such that $h(e_j, e_1) \neq 0$. Put $\beta = h(e_j, e_1) \in E$. Suppose that β is not invertible. In this case, E is of type (sp). We may assume that $E = E_0 \times E_0$ for a field E_0 isomorphic to E^σ. Since β is not zero and not invertible, it can be written as $\beta = (\gamma, 0)$ or $(0, \gamma) \in E_0 \times E_0$ for some $\gamma \in (E_0)^\times$. Then $\beta + \sigma(\beta) = (\gamma, \gamma)$, and it is not zero. Now, we define $e'_j := e_1 + e_j$. Then $e_1, \ldots, e_{j-1}, e'_j, e_{j+1}, \ldots, e_m$ is a basis of M, and $h(e'_j, e'_j) = \beta + \sigma(\beta) \neq 0$. Hence, it is attributed to Case I. Suppose that β is invertible. For any $\alpha \in E$ we have

$$h(e_1 + \alpha\beta^{-1}e_j, e_1 + \alpha\beta^{-1}e_j) = \sigma(\alpha\beta^{-1})h(e_1, e_j) + \alpha\beta^{-1}h(e_j, e_1) = \alpha + \sigma(\alpha). \qquad (*)$$

We show that there exists $\alpha_0 \in E$ such that $h(e_1 + \alpha_0\beta^{-1}e_j, e_1 + \alpha_0\beta^{-1}e_j) \neq 0$. When $\operatorname{char} K \neq 2$, we can take $\alpha_0 = 1$. Suppose that $\operatorname{char} K = 2$. If $h(e_1 + \alpha\beta^{-1}e_j, e_1 + \alpha\beta^{-1}e_j)$ were equal to 0 for all $\alpha \in E$, then $\alpha + \sigma(\alpha) = 0$ for all $\alpha \in E$ by $(*)$. However, this is a contradiction since σ is nontrivial. Therefore, in any case, there exists $\alpha_0 \in E$ such that $h(e_1 + \alpha_0\beta^{-1}e_j, e_1 + \alpha_0\beta^{-1}e_j) \neq 0$. Then $e_1 + \alpha_0\beta^{-1}e_j, e_2, \ldots, e_m$ is a basis of M, and it is attributed to Case I. This completes the proof. □

Corollary 4.66. *Suppose that E is of type* (sp)*, and (M, h) be a hermitian product space over E of rank m. Then $(M, h) \cong \langle 1 \rangle_E^{\oplus m}$.*

Proof. This follows from Propositions 4.65 and 1.11. □

Hermitian forms over E are accompanied by symmetric bilinear forms over E^σ.

Definition 4.67. Suppose that E^σ is a field. Let M be a finitely generated free E-module, and $h : M \times M \to E$ a hermitian form on M. A symmetric bilinear form $b_h : M \times M \to E^\sigma$ on the E^σ-vector space M is defined by

$$b_h(x, y) = h(x, y) + h(y, x) = h(x, y) + \sigma h(x, y) \quad (x, y \in M).$$

We refer to b_h as the symmetric bilinear form *associated with* h. Note that $b(x, x) = 2h(x, x)$ for any $x \in M$.

In the situation of this definition, the symmetric bilinear form b_h can be expressed as

$$b_h(x, y) = \operatorname{Tr}_{E/E^\sigma} \circ h(x, y) \quad (x, y \in M)$$

if E is a field separable over E^σ, or if E is of type (sp). Moreover, if L is a subfield of E^σ such that E^σ/L is separable then a symmetric bilinear form on the L-vector space M is given by $\operatorname{Tr}_{E/L} \circ h$. For such forms, we have the following propositions.

Proposition 4.68. *Suppose that E is a field separable over E^σ or of type* (sp)*. Let M be a finitely generated free E-module, $h : M \times M \to E$ a hermitian form on M, and L a subfield of E^σ such that E^σ/L is separable. Let $b : M \times M \to L$ denote the symmetric bilinear form $\operatorname{Tr}_{E/L} \circ h$. If h is nondegenerate then so is b.*

Proof. Suppose that h is nondegenerate. Let $x \in M$, and suppose that $b(y, x) = 0$ for all $y \in M$. It suffices to prove that $x = 0$. Suppose to the contrary that $x \neq 0$. Then, there exists $z \in M$ such that $h(z, x) \neq 0$ since h is nondegenerate. Put $\beta := h(z, x)$. If β is not invertible then E

is of type (sp) and $\gamma := \beta + \sigma(\beta) \in E^\sigma$ is not zero, as in the proof of Proposition 4.65. On the other hand, since the extension E^σ/L is separable, there exists $\alpha \in E^\sigma$ such that $\mathrm{Tr}_{E^\sigma/L}(\alpha) \neq 0$ by Corollary 1.7. Then, we would have

$$\begin{aligned} 0 = b(\alpha\gamma^{-1}z, x) &= \mathrm{Tr}_{E^\sigma/L}(\mathrm{Tr}_{E/E^\sigma}(h(\alpha\gamma^{-1}z, x))) \\ &= \mathrm{Tr}_{E^\sigma/L}(\alpha\gamma^{-1}\,\mathrm{Tr}_{E/E^\sigma}(\beta)) = \mathrm{Tr}_{E^\sigma/L}(\alpha) \neq 0, \end{aligned}$$

but this is a contradiction. Similarly, in the case where β is invertible, the existence of an element $\alpha \in E$ with $\mathrm{Tr}_{E/L}(\alpha) \neq 0$ yields a contradiction. Therefore $x = 0$, and the proof is complete. □

Proposition 4.69. *Suppose that E is a field separable over K. Let M be a finite dimensional E-vector space, and let h, h' be hermitian products on M.*

(i) $\det(\mathrm{Tr}_{E/K} \circ h) = \det(\mathrm{Tr}_{E/K} \circ h')$ *in* $K^\times/K^{\times 2}$.

(ii) $\mathrm{HW}_K(\mathrm{Tr}_{E/K} \circ h) = \mathrm{HW}_K(\mathrm{Tr}_{E/K} \circ h') + \mathrm{cor}_{E^\sigma/K}([\sigma, \frac{\det h}{\det h'}]_{E^\sigma})$ *in* $\mathrm{Br}_2(K)$.

Proof. By Proposition 4.65, we may assume that $h = \langle \mu_1, \ldots, \mu_m \rangle_E, h' = \langle \mu'_1, \ldots, \mu'_m \rangle_E$ where $\mu_i, \mu'_j \in (E^\sigma)^\times$. For $\mu \in (E^\sigma)^\times$, let b_μ denote the inner product $E \times E \to K$ defined by

$$b_\mu(x, y) = \mathrm{Tr}_{E/K}(\mu x \sigma(y)) \quad (x, y \in E).$$

Then the inner products $\mathrm{Tr}_{E/K} \circ h$ and $\mathrm{Tr}_{E/K} \circ h'$ can be expressed as

$$\mathrm{Tr}_{E/K} \circ h = b_{\mu_1} \oplus \cdots \oplus b_{\mu_m} \quad \text{and} \quad \mathrm{Tr}_{E/K} \circ h' = b_{\mu'_1} \oplus \cdots \oplus b_{\mu'_m} \tag{$*$}$$

respectively.

(i). By $(*)$, it is sufficient to show that $\det(b_\mu) = \det(b_1)$ for any $\mu \in (E^\sigma)^\times$. Let $\mu \in (E^\sigma)^\times$, and let $e_1, \ldots, e_d$ be a basis of E over K. Let G and A be the Gram matrix of the inner product b_1 and representation matrix of the linear transformation $E \to E$, $x \mapsto \mu x$ with respect to the basis $e_1, \ldots, e_d$. Then, the Gram matrix of b_μ is given by ${}^tAG$ because $b_\mu(x, y) = b_1(\mu x, y)$. Thus $\det(b_\mu) = \det({}^tAG) = \det(A)\det(b_1)$. On the other hand, we have $\det(A) = \mathrm{N}_{E/K}(\mu) = \mathrm{N}_{E^\sigma/K}(\mu^2) = \mathrm{N}_{E^\sigma/K}(\mu)^2$. Hence $\det(b_\mu) = \det(A)\det(b_1) = \det(b_1)$ in $K^\times/K^{\times 2}$ as required.

(ii). The case $M = E$ is essential and follows from [11, Theorem 4.3]. Suppose that $m := \dim M \geq 1$. By Equation $(*)$, Lemma 4.31 (iii), and the case $M = E$, we have

$$\begin{aligned} \mathrm{HW}_K(\mathrm{Tr}_{E/K} \circ h) - \mathrm{HW}_K(\mathrm{Tr}_{E/K} \circ h') &= \mathrm{HW}_K(\textstyle\bigoplus_{i=1}^m b_{\mu_i}) - \mathrm{HW}_K(\bigoplus_{i=1}^m b_{\mu'_i}) \\ &= \textstyle\sum_{i=i}^m \left(\mathrm{HW}_K(b_{\mu_i}) - \mathrm{HW}_K(b_{\mu'_i})\right) \\ &= \textstyle\sum_{i=i}^m \left(\mathrm{cor}_{E^\sigma/K}([\sigma, \mu_i/\mu'_i]_{E^\sigma})\right) \\ &= \mathrm{cor}_{E^\sigma/K}([\sigma, \textstyle\prod_{i=i}^m (\mu_i/\mu'_i)]_{E^\sigma}) \\ &= \mathrm{cor}_{E^\sigma/K}([\sigma, \det(h)/\det(h')]_{E^\sigma}), \end{aligned}$$

as required. □

4.10 Hermitian products over local and global fields

This subsection gives an classification of hermitian products over local fields. Moreover, we show an analog of the global existence theorem 4.57. We begin with the case over $\mathbb{C}$. In this case, the complex conjugate $\overline{\cdot}$ is a nontrivial involution. We remark that $\mathrm{Tw}(\mathbb{C}, \overline{\cdot}) = \{1, -1\}$.

Lemma 4.70. *Let r and s be non-negative integers. The inner product associated with $(r+s)$ dimensional hermitian product $\langle 1\rangle_{\mathbb{C}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{C}}^{\oplus s}$ is isomorphic to the $2(r+s)$ dimensional inner product $\langle 1\rangle_{\mathbb{R}}^{\oplus 2r} \oplus \langle -1\rangle_{\mathbb{R}}^{\oplus 2s}$.*

Proof. Let ϵ be 1 or -1. It is enough to show that the inner product b associated with $(\mathbb{C}, h) := \langle \epsilon\rangle_{\mathbb{C}}$ is isomorphic to $\langle \epsilon, \epsilon\rangle_{\mathbb{R}}$. We have $b(1,1) = 2h(1,1) = 2\epsilon$ and $b(\sqrt{-1}, \sqrt{-1}) = 2h(\sqrt{-1}, \sqrt{-1}) = 2\sqrt{-1}\overline{\sqrt{-1}}h(1,1) = 2\epsilon$. Hence, the Gram matrix of b with respect to the basis $1, \sqrt{-1}$ of the $\mathbb{R}$-vector space $\mathbb{C}$ is $\mathrm{diag}(2\epsilon, 2\epsilon)$, which shows that $b \cong \langle 2\epsilon, 2\epsilon\rangle_{\mathbb{R}} \cong \langle \epsilon, \epsilon\rangle_{\mathbb{R}}$. This completes the proof. □

Theorem 4.71. *Let (M, h) be a hermitian product space over $\mathbb{C}$. There exist unique non-negative integers r and s such that $(M, h) \cong \langle 1\rangle_{\mathbb{C}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{C}}^{\oplus s}$.*

Proof. Since $\mathrm{Tw}(\mathbb{C}, \bar{\cdot}) = \{1, -1\}$, Proposition 4.65 implies that $(M, h) \cong \langle 1\rangle_{\mathbb{C}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{C}}^{\oplus s}$ for some $r, s \in \mathbb{Z}_{\geq 0}$. Moreover, the pair $(2r, 2s)$ is uniquely determined by h since Lemma 4.70 means that $(2r, 2s)$ is the signature of the inner product associated with h. Therefore, the pair (r, s) is also unique. □

This theorem leads to the following definition.

Definition 4.72. Let (M, h) be a hermitian product space over $\mathbb{C}$. The *signature* of (M, h) is the unique pair (r, s) of non-negative integers such that $(M, h) \cong \langle 1\rangle_{\mathbb{C}}^{\oplus r} \oplus \langle -1\rangle_{\mathbb{C}}^{\oplus s}$. The difference $r - s$ is called the *index* of (M, h) and denoted by $\mathrm{idx}(h)$. Note that $\mathrm{idx}(b) = 2\,\mathrm{idx}(h)$ by Lemma 4.70, where b is the inner product associated with h.

We proceed to the case of non-archimedean local fields. In this case, the classification theorem is similar to that of inner products over finite fields (Theorem 4.38).

Theorem 4.73. *Let E be a non-archimedean local field of characteristic not 2 with a nontrivial involution σ, and fix $\nu \in (E^\sigma)^\times$ with $\nu \neq 1$ in $\mathrm{Tw}(E, \sigma)$. Let (M, h) be a hermitian product space over E. If we write $d = \dim M$ then*

$$(M, h) \cong \begin{cases} \langle 1\rangle_E^{\oplus d} & \text{if } \det(h) = 1 \\ \langle 1\rangle_E^{\oplus d-1} \oplus \langle \nu\rangle_E & \text{if } \det(h) = \nu. \end{cases}$$

In particular, the isomorphism class of (M, h) is uniquely determined by its dimension and determinant.

Proof. Note that $\mathrm{Tw}(E, \sigma) = \{1, \nu\}$ by Corollary 3.28. Then, Proposition 4.65 implies that $b \cong \langle 1\rangle_E^{\oplus m} \oplus \langle \nu\rangle_E^{\oplus m'}$ where m and m' are non-negative integers with $m + m' = d$. Hence, it is sufficient to show that $\langle \nu, \nu\rangle_E \cong \langle 1, 1\rangle_E$. Let (U, h_U) be a 2-dimensional hermitian product space isomorphic to $\langle \nu, \nu\rangle_E$, and let b denote the inner product associated with h_U. Then b is 4-dimensional over E^σ. Thus, there exists a vector $u \in U$ such that $b(u, u) = 2$ by Proposition 4.44. Since $h_U(u, u) = \frac{1}{2}b(u, u) = 1$, we have $(U, h_U) \cong \langle 1, \det(h_U)\rangle_E = \langle 1, 1\rangle_E$. This completes the proof. □

We proceed to the global existence theorem. Let E be an algebraic number field with a nontrivial involution σ, and let $\mathcal{W}$ be the set of places of the fixed subfield E^σ. Let $w \in \mathcal{W}$ be a place, and we use the same symbols as in Notation 3.30. If (M, h) is a hermitian product space over E then h extends to a hermitian product $(M \otimes_E E_w) \times (M \otimes_E E_w) \to E_w$ in a unique way. This extension of h is denoted by $h \otimes_E E_w$ or just $h \otimes E_w$. Note that w is a place of E^σ and not of E.

Theorem 4.74. *Let E be an algebraic number field with a nontrivial involution σ, and $\mathcal{W}$ the set of places of E^σ. Let M be an m-dimensional E-vector space, and let $\{h_w\}_{w\in\mathcal{W}}$ be a family consisting of hermitian products $h_w : (M \otimes_E E_w) \times (M \otimes_E E_w) \to E_w$ such that $\det(h_w) = 1$ in $\mathrm{Tw}(E_w, \sigma)$ for almost all $w \in \mathcal{W}$ and $\sum_{w\in\mathcal{W}} \iota_w(\det(h_w)) = 0$, where the algebra E_w and homomorphism $\iota_w : \mathrm{Tw}(E_w, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ are defined as in Notation 3.30. Then there exists a hermitian product h on M such that $h \otimes E_w \cong h_w$ for all $w \in \mathcal{W}$.*

Proof. For each $w \in \mathcal{W}$, put $\mu_w = \det(h_w) \in \mathrm{Tw}(E_w, \sigma)$. By Proposition 3.31, there exists $\mu \in \mathrm{Tw}(E, \sigma)$ such that $\mu = \mu_w$ in $\mathrm{Tw}(E_w, \sigma)$ for all $w \in \mathcal{W}$. Let $\mathcal{W}_\infty \subset \mathcal{W}$ be the set of all infinite places of E^σ. For each $w \in \mathcal{W}_\infty$, we can write

$$h_w \cong \langle \alpha_{w,1}, \ldots, \alpha_{w,m-1}, \alpha_{w,1} \cdots \alpha_{w,m-1}\mu \rangle_{E_w}$$

by Proposition 4.65, where $\alpha_{w,i} \in (E_w^\sigma)^\times$. Since $\mathcal{W}_\infty$ is a finite set, the approximation theorem 1.26 shows that for each $i = 1, \ldots, m-1$ there exists $\alpha_i \in E_w^\sigma$ arbitrarily close to $\alpha_{w,i}$ for all $w \in \mathcal{W}_\infty$. Noting that $\mathrm{Tw}(E_w, \sigma)$ has order at most 2, we get $\alpha_i = \alpha_{w,i}$ in $\mathrm{Tw}(E_w, \sigma)$ by Proposition 2.12. Now, we define a hermitian product h on $M = E^m$ by

$$h = \langle \alpha_1, \ldots, \alpha_{m-1}, \alpha_1 \cdots \alpha_{m-1}\mu \rangle_E.$$

Then

$$h \otimes E_w = \langle \alpha_1, \ldots, \alpha_{m-1}, \alpha_1 \cdots \alpha_{m-1}\mu \rangle_{E_w} \cong \langle \alpha_{w,1}, \ldots, \alpha_{w,m-1}, \alpha_{w,1} \cdots \alpha_{w,m-1}\mu \rangle_{E_w} \cong h_w$$

for each $w \in \mathcal{W}_\infty$. Furthermore, for each finite place $w \in \mathcal{W}$, we have $h \otimes E_w \cong h_w$ by Corollary 4.66 if w is split in E, and by Theorem 4.73 if w is not split in E since $\det(h \otimes E_w) = \mu = \mu_w = \det(h_w)$. Therefore h is the desired hermitian product on M. □

5 Lattices

This section gives an explanation of inner products defined over Dedekind domains. We refer to [35], [39], and [40] as in §4.

5.1 Module theory over Dedekind domains

We summarize results of module theory over Dedekind domains here. Let $\mathcal{O}$ be an integral domain, and M an $\mathcal{O}$-module. For $x \in M$, we define $\mathrm{Ann}(x) := \{\alpha \in \mathcal{O} \mid \alpha.x = 0\}$. This is an ideal of $\mathcal{O}$. If $\mathrm{Ann}(x) \neq 0$ then the element x is called a *torsion element*. We say that M is a *torsion module* if every element of M is a torsion element, and M is *torsion-free* if it has no torsion element except for 0. The submodule of M consisting of all torsion elements is called the *torsion submodule of M*. If T is the torsion submodule of M then it is clear that M/T is torsion-free.

If $\mathcal{O}$ is a Dedekind domain then any finitely generated module is the direct sum of a torsion-free module and a torsion module. More precisely, the following theorem is known, which is a generalization of the structure theorem for finitely generated modules over a principal ideal domain.

Theorem 5.1 (Structure theorem)**.** *Let $\mathcal{O}$ be a Dedekind domain, M a finitely generated $\mathcal{O}$-module, and T the torsion submodule of M. Then M is isomorphic to the direct sum of M/T and T. Moreover, the torsion-free module M/T is isomorphic to the direct sum of finitely many ideals of $\mathcal{O}$, and the torsion module T is isomorphic to the direct sum of finitely many modules of the form $\mathcal{O}/\mathfrak{p}^n$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ and $n \in \mathbb{Z}_{>0}$ is a positive integer.*

Proof. See [21]. □

By this structure theorem, a finitely generated module over a Dedekind domain is projective if and only if torsion-free, because any ideal of a Dedekind domain is a projective module.

Projective modules Let $\mathcal{O}$ be a Dedekind domain and K its field of fractions. We will often consider that projective $\mathcal{O}$-modules are contained in K-vector spaces. Indeed, if Λ is a projective $\mathcal{O}$-module, then it is flat, and the canonical homomorphism $\Lambda = \Lambda \otimes_{\mathcal{O}} \mathcal{O} \to \Lambda \otimes_{\mathcal{O}} K$ is injective. So we identify Λ with its image and consider that Λ is contained in the K-vector space $\Lambda \otimes_{\mathcal{O}} K$. In general, we say that a finitely generated $\mathcal{O}$-module in a K-vector space V is *on* V if its K-span coincides with V. A finitely generated projective $\mathcal{O}$-module Λ is on the K-vector space $\Lambda \otimes_{\mathcal{O}} K$.

Theorem 5.2. *Let $\mathcal{O}$ be a Dedekind domain and K its field of fractions. Let V be a finite dimensional K-vector space, and Λ, Λ' finitely generated $\mathcal{O}$-submodules on V. Then there exists a basis $e_1, \dots, e_d$ of V and fractional ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_d, \mathfrak{b}_1, \dots, \mathfrak{b}_d$ of $\mathcal{O}$ such that*

$$\Lambda = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_d e_d \quad \text{and} \quad \Lambda' = \mathfrak{a}_1\mathfrak{b}_1 e_1 + \cdots + \mathfrak{a}_d\mathfrak{b}_d e_d.$$

In particular, the sum $\Lambda + \Lambda'$ and intersection $\Lambda \cap \Lambda'$ are again finitely generated $\mathcal{O}$-modules on V.

Proof. See [35, Theorem 81:11]. Note that a finitely generated $\mathcal{O}$-module in a K-vector space is called a *lattice* in O'Meara's book [35], see §81A and Example 81:6. However, in this thesis, a lattice will mean a finitely generated projective $\mathcal{O}$-module *equipped with an inner product.* □

Torsion modules For torsion modules over a Dedekind domain, *length* plays the role of dimension for finite dimensional vector spaces, and is helpful. Let $\mathcal{O}$ be a Dedekind domain, and M an $\mathcal{O}$-module. For a chain

$$M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{l-1} \subsetneq M_l \tag{18}$$

of $\mathcal{O}$-submodules of M, its length is the integer $l \geq 0$. The *length* of M, denoted $\mathrm{len}(M)$, is the largest length of its chains. The length is defined to be infinite if there exists a chain of infinite length. Any ideal of $\mathcal{O}$ has infinite length as an $\mathcal{O}$-module. Indeed, if $\mathfrak{a}$ is an ideal with $\mathfrak{a} \subsetneq \mathcal{O}$ then the chain $\mathfrak{a} \supsetneq \mathfrak{a}^2 \supsetneq \mathfrak{a}^3 \supsetneq \cdots$ has infinite length. On the other hand, for a prime ideal $\mathfrak{p}$ and a positive integer n, the module $\mathcal{O}/\mathfrak{p}^n$ has finite length. In fact $\mathcal{O}/\mathfrak{p}^n, \mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n, 0$ are all submodules of $\mathcal{O}/\mathfrak{p}^n$. Hence, when M is finitely generated, it follows from the structure theorem 5.1 that the length of M is finite if and only if M is a torsion module. Note that this is not true when M is not finitely generated. For example, the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a torsion module but has infinite length.

The chain (18) is called a *composition series* if $M_0 = 0$, $M_l = M$, and the quotient M_j/M_{j-1} has no nontrivial submodule for all $j = 1, \dots, l$. For composition series, the Jordan-Hölder theorem is fundamental (it holds in the case $\mathcal{O}$ is an arbitrary ring in fact).

Theorem 5.3 (Jordan-Hölder theorem)**.** *Let M be an $\mathcal{O}$-module which has a composition series. For any two composition series $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{l-1} \subsetneq M_l$ and $M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_{l'-1} \subsetneq M'_{l'}$ of M, we have $l = l'$, and there exists a permutation σ of $\{1, \dots, l\}$ such that $M_j/M_{j-1} \cong M'_{\sigma(j)}/M'_{\sigma(j-1)}$ for all $j = 1, \dots, l$.*

Proof. See [48, Theorem 7.42]. □

As a result, the length of M is the length of its composition series (if it is finite). This leads to the following property of lengths.

Corollary 5.4. *Let* $0 \to T \xrightarrow{\phi} T' \to T'' \to 0$ *be an exact sequence of finitely generated torsion* $\mathcal{O}$*-modules. Then we have* $\mathrm{len}(T') = \mathrm{len}(T) + \mathrm{len}(T'')$.

Proof. Let $0 = T_0 \subsetneq T_1 \subsetneq \cdots \subsetneq T_l = \mathrm{im}(\phi)$ be a composition series of $\mathrm{im}(\phi)$, and let $\mathrm{im}(\phi) = T''_0 \subsetneq T''_1 \subsetneq \cdots \subsetneq T''_{l''} = T$ be a chain such that T''_j/T''_{j-1} has no nontrivial submodule for all j. Then, the chain

$$0 = T_0 \subsetneq T_1 \subsetneq \cdots \subsetneq T_l \subsetneq T''_1 \subsetneq \cdots \subsetneq T''_{l''} = T$$

is a composition series of T, and T has length $l + l''$. On the other hand, we have $l = \mathrm{len}(T)$. Moreover $l'' = \mathrm{len}(T'')$ because $T'' \cong T/\mathrm{im}(\phi)$ and the chain $0 = T''_0/\mathrm{im}(\phi) \subsetneq T''_1/\mathrm{im}(\phi) \subsetneq \cdots \subsetneq T''_{l''}/\mathrm{im}(\phi) = T/\mathrm{im}(\phi)$ is a composition series of $T/\mathrm{im}(\phi)$. This completes the proof. □

Another property we will need concerns the dual. Let K be the field of fractions of $\mathcal{O}$. For a torsion $\mathcal{O}$-module T, the dual module $\mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O})$ (in usual sense) is zero, but the module $\mathrm{Hom}_{\mathcal{O}}(T, K/\mathcal{O})$ plays the role of dual.

Proposition 5.5. *A finitely generated torsion* $\mathcal{O}$*-module* T *is isomorphic to* $\mathrm{Hom}_{\mathcal{O}}(T, K/\mathcal{O})$.

Proof (Sketch). By the structure theorem 5.1, it is enough to show the case where $T = \mathcal{O}/\mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ and positive integer n. In this case, it can be checked that

$$\mathrm{Hom}_{\mathcal{O}}(T, K/\mathcal{O}) \to T,\ \xi \mapsto \pi^n \xi(1)$$

is a well-defined isomorphism, where $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. □

On can prove that $\mathrm{Hom}_{\mathcal{O}}(\mathrm{Hom}_{\mathcal{O}}(T, K/\mathcal{O}), K/\mathcal{O})$ is canonically isomorphic to T if T is a finitely generated torsion $\mathcal{O}$-module, although we do not use this fact.

5.2 Torsion product modules

In this subsection, we introduce *torsion product modules*, which arise naturally from lattices. Let $\mathcal{O}$ be a Dedekind domain and K its field of fractions.

Definition 5.6. Let T be a finitely generated torsion $\mathcal{O}$-module. A *torsion form* on T (over $\mathcal{O}$) is a symmetric $\mathcal{O}$-bilinear form $T \times T \to K/\mathcal{O}$. For a torsion form $b : T \times T \to K/\mathcal{O}$ we write b^* for the homomorphism $T \to T^* := \mathrm{Hom}_{\mathcal{O}}(T, K/\mathcal{O})$ defined by

$$b^*(x) = (y \mapsto b(y, x)) \quad (x, y \in T).$$

A torsion form $b : V \times V \to K$ is *nondegenerate* if the homomorphism b^* is injective, and a nondegenerate torsion form is referred to as a *torsion product*. If $b : T \times T \to K/\mathcal{O}$ is a torsion product on T, then the pair (T, b) is called a *torsion product module* over $\mathcal{O}$.

Properties of torsion product modules are similar to those of inner product spaces. As mentioned in §5.1, it follows from the structure theorem 5.1 that the length of a finitely generated torsion $\mathcal{O}$-module is finite. Let $T = (T, b)$ be a torsion product module over $\mathcal{O}$.

Lemma 5.7. *The homomorphism* $b^* : T \to T^*$ *is isomorphic.*

Proof. we have $\mathrm{len}(T^*) = \mathrm{len}(T)$ since $T^* \cong T$ by Proposition 5.5, and b^* is injective by definition. Thus b^* must be surjective by Corollary 5.4. □

For a submodule $U \subset T$, we define $U^\perp := \{x \in T \mid b(u, x) = 0 \text{ for any } u \in U\}$. The following proposition is an analog of Proposition 4.4.

Proposition 5.8. *Let U be a submodule of T. Then the sequence*

$$0 \to U^\perp \to T \xrightarrow{b^*(\cdot)|_U} U^* \to 0$$

is exact, where the second arrow is the inclusion. Moreover, we have:

(i) $\operatorname{len} T = \operatorname{len} U^\perp + \operatorname{len} U$.

(ii) $(U^\perp)^\perp = U$.

(iii) *If U is nondegenerate then so is $U^\perp$, and $T = U \oplus U^\perp$.*

Proof. We prove surjectivity of $b^*(\cdot)|_U : T \to U^*$. Let $\xi : U \to K/\mathcal{O}$ be an element of U^*. It is known that $K/\mathcal{O}$ is an injective $\mathcal{O}$-module (see [48, §6.3 Exercise 9]). Hence, there exists an extension $\tilde{\xi} : T \to K/\mathcal{O}$ of ξ, and we can take $x \in T$ such that $b^*(x) = \tilde{\xi}$ by Lemma 5.7. Then $b^*(x)|_U = \xi$, which shows that $b^*(\cdot)|_U$ is surjective. The remaining assertions follow similarly to Proposition 4.4. □

5.3 Lattices over Dedekind domains

Let $\mathcal{O}$ be a Dedekind domain and K its field of fractions.

Definition 5.9. Let Λ be a finitely generated projective $\mathcal{O}$-module. For a symmetric bilinear form $b : \Lambda \times \Lambda \to K$ (taking values in the field of fractions), we write b^* for the homomorphism $\Lambda \to \operatorname{Hom}_{\mathcal{O}}(\Lambda, K)$ defined by

$$b^*(x) = (y \mapsto b(y, x)) \quad (x, y \in \Lambda).$$

A symmetric bilinear form $b : \Lambda \times \Lambda \to K$ is *nondegenerate* if the homomorphism b^* is injective, and a nondegenerate symmetric bilinear form is referred to as an *inner product* as in §4. If b is an inner product on Λ then the pair (Λ, b) is called a *lattice*. Let $(\Lambda, b), (\Lambda', b')$ be lattices over $\mathcal{O}$. An *isometry* from (Λ, b) to (Λ', b') is a homomorphism $t : \Lambda \to \Lambda'$ of $\mathcal{O}$-modules satisfying $b'(t(x), t(y)) = b(x, y)$ for any $x, y \in \Lambda$. Two lattices (Λ, b) and (Λ', b') are *isomorphic* if there exists an isomorphism $\Lambda \to \Lambda'$ of $\mathcal{O}$-modules which is also an isometry. An isometry from (Λ, b) to (Λ, b) itself is referred to as an *isometry of* (Λ, b), and the group of all isometries of (Λ, b) is denoted by $\mathrm{O}(\Lambda, b)$ or just by $\mathrm{O}(\Lambda)$.

For a lattice (Λ, b) over $\mathcal{O}$, the inner product b is extended linearly on the K-vector space $\Lambda \otimes_{\mathcal{O}} K$, which is denoted by $b \otimes K$ or just by b, and the pair $(\Lambda \otimes_{\mathcal{O}} K, b)$ becomes an inner product space over K. In this case, we consider that Λ is contained in $\Lambda \otimes_{\mathcal{O}} K$ as in §5.1. Conversely, if (V, b) is an inner product space over K and Λ is a finitely generated $\mathcal{O}$-submodule on V, then Λ is regarded as a lattice with the restriction of b. A lattice *on* an inner product space (V, b) is a finitely generated $\mathcal{O}$-module on V equipped with the inner product defined by the restriction of b. When we say that (V, b) contains a lattice Λ, it is often assumed that Λ is on V. It is clear that a lattice (Λ, b) over $\mathcal{O}$ is a lattice on the inner product space $(\Lambda \otimes_{\mathcal{O}} K, b)$.

For a lattice (Λ, b) over $\mathcal{O}$, the $\mathcal{O}$-module

$$\Lambda^\vee := \{y \in \Lambda \otimes_{\mathcal{O}} K \mid b(y, x) \in \mathcal{O} \text{ for all } x \in \Lambda\}$$

(equipped with the inner product b) is called the *dual lattice* of Λ.

Lemma 5.10. *Let (Λ, b) be a lattice over $\mathcal{O}$, and put $V = \Lambda \otimes_{\mathcal{O}} K$. When Λ is written as $\Lambda = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_d e_d$ in V, where $e_1, \ldots, e_d \in V$ is a basis of V and $\mathfrak{a}_1, \ldots, \mathfrak{a}_d$ are fractional ideals of $\mathcal{O}$, the dual lattice $\Lambda^\vee$ is given by $\Lambda^\vee = \mathfrak{a}_1^{-1} e_1^\vee + \cdots + \mathfrak{a}_d^{-1} e_d^\vee$, where $e_1^\vee, \ldots, e_n^\vee \in V$ is the dual basis of $e_1, \ldots, e_d$ with respect to $b \otimes K$. Hence $\Lambda^\vee$ is a lattice on (V, b), and the double dual $\Lambda^{\vee\vee} := (\Lambda^\vee)^\vee$ is equal to Λ itself.*

Proof. Straightforward. □

Definition 5.11. A lattice (Λ, b) over $\mathcal{O}$ is said to be *integral* if $b(x, y) \in \mathcal{O}$ for any $x, y \in \Lambda$, or equivalently $\Lambda \subset \Lambda^\vee$. If $\Lambda = \Lambda^\vee$ then (Λ, b) is said to be *unimodular*. For an integral lattice (Λ, b), the quotient module $\Lambda^\vee/\Lambda$ is called the *discriminant module* of (Λ, b). We write $\bar{x}$ for $x + \Lambda$ in $\Lambda^\vee/\Lambda$ where $x \in \Lambda^\vee$. An integral lattice (Λ, b) is said to be *even* if $b(x, x) \in 2\mathcal{O}$; and *odd* otherwise. Note that every integral lattice is even if 2 is a unit of $\mathcal{O}$.

Proposition 5.12. *Suppose that $\Lambda = (\Lambda, b)$ is an integral lattice.*

(i) *The discriminant module is a finitely generated torsion module.*

(ii) *The discriminant module is naturally a torsion product module with the torsion form $\bar{b} : (\Lambda^\vee/\Lambda) \times (\Lambda^\vee/\Lambda) \to K/\mathcal{O}$ defined by*

$$\bar{b}(\bar{x}, \bar{y}) = b(x, y) + \mathcal{O} \quad (x, y \in \Lambda^\vee).$$

Proof. (i). The lattice Λ and its dual $\Lambda^\vee$ is on $V := \Lambda \otimes_{\mathcal{O}} K$ by Lemma 5.10. Thus, Theorem 5.2 shows that there exists a basis $e_1, \ldots, e_d$ of V and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_d, \mathfrak{b}_1, \ldots, \mathfrak{b}_d$ of $\mathcal{O}$ such that $\Lambda = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_d e_d$ and $\Lambda^\vee = \mathfrak{a}_1\mathfrak{b}_1 e_1 + \cdots + \mathfrak{a}_d\mathfrak{b}_d e_d$. Moreover $\mathfrak{b}_1, \ldots, \mathfrak{b}_d$ must be integral ideals since $\Lambda \subset \Lambda^\vee$. Then, the discriminant module $\Lambda^\vee/\Lambda$ is isomorphic to $\mathcal{O}/\mathfrak{b}_1 \oplus \cdots \oplus \mathcal{O}/\mathfrak{b}_d$, and it is a finitely generated torsion module.

(ii). It is easy to check that $\bar{b}$ is a well-defined torsion form on $\Lambda^\vee/\Lambda$. We show that $\bar{b}$ is nondegenerate. Let $x \in \Lambda^\vee$, and assume that $\bar{b}(\bar{x}, \bar{y}) = 0$ (in $K/\mathcal{O}$) for any $\bar{y} \in \Lambda^\vee/\Lambda$. Then $b(x, y) \in \mathcal{O}$ for any $y \in \Lambda^\vee$, which means that $x \in \Lambda^{\vee\vee} = \Lambda$. Therefore $\bar{x} = 0$, and this shows that $\bar{b}$ is nondegenerate. □

Let (Λ, b) be a lattice, and U a submodule of Λ. If $b|_U$ is nondegenerate (resp. unimodular) then U is said to be *nondegenerate* (resp. *unimodular*). We define $U^\perp := \{y \in \Lambda \mid b(x, y) = 0 \text{ for any } x \in U\}$. For a lattice (Λ, b), a nondegenerate submodule is not a direct summand of Λ in general, unlike in the case over a field. However, a unimodular submodule of a unimodular lattice is a direct summand.

Proposition 5.13. *Let (Λ, b) be a unimodular lattice over $\mathcal{O}$, and U is a unimodular submodule of Λ. Then $\Lambda = U \oplus U^\perp$, and $U^\perp$ is also unimodular.*

Proof. Put $V = \Lambda \otimes_{\mathcal{O}} K$. Since the K-span KU of U is nondegenerate, V decomposes as $V = KU \oplus (KU)^\perp$ by Proposition 5.8 (iii). Let $x \in \Lambda$. It can be uniquely written as $x = x_1 + x_2$ for some $x_1 \in KU$ and $x_2 \in (KU)^\perp$ by the decomposition $V = KU \oplus (KU)^\perp$. For the equality $\Lambda = U \oplus U^\perp$, it suffices to show that $x_1 \in U$ and $x_2 \in U^\perp$. We have $b(x_1, U) = b(x, U) \subset b(x, \Lambda) \subset \mathcal{O}$ since Λ is unimodular. This means that $x_1 \in U^\vee = U$. Furthermore, we have $x_2 = x - x_1 \in \Lambda$. This implies that $x_2 \in (KU)^\perp \cap \Lambda = U^\perp$. Therefore, we obtain $\Lambda = U \oplus U^\perp$. Then $U^\perp$ must be unimodular because $0 = \Lambda^\vee/\Lambda = (U^\vee/U) \oplus ((U^\perp)^\vee/U^\perp)$. □

In this thesis, we will actually treat mainly the case where $\mathcal{O}$ is a principal integral domain. In this case, any projective module is free. In general, for a lattice whose underlying $\mathcal{O}$-module is free, we can define the Gram matrix in the same way for an inner product over a field.

Definition 5.14. Let (Λ, b) be an integral lattice over $\mathcal{O}$ such that the $\mathcal{O}$-module Λ is free. For a basis $e_1, \ldots, e_d$ of Λ, the $d \times d$ matrix $(b(e_i, e_j))_{ij} \in M_d(\mathcal{O})$ is called the *Gram matrix* of (Λ, b). The square class of $\det((b(e_i, e_j))_{ij}) \in \mathcal{O}^\times$ in $\mathcal{O}^\times/\mathcal{O}^{\times 2}$ does not depend on the chose of the basis. This class is referred to as the *determinant* of (Λ, b) and denoted by $\det(b)$.

Let $G = (g_{ij})_{ij} \in M_d(\mathcal{O})$ be a $d \times d$ nondegenerate symmetric matrix. The symbol $\langle G \rangle_{\mathcal{O}}$ denotes the integral lattice that its underlying space is $\mathcal{O}^d$ and G is the Gram matrix with respect to the standard basis of $\mathcal{O}^d$. If G is a diagonal matrix, say $\mathrm{diag}(a_1, \ldots, a_d)$, then we write $\langle a_1, \ldots, a_d \rangle_{\mathcal{O}} = \langle \mathrm{diag}(a_1, \ldots, a_d) \rangle_{\mathcal{O}}$ for short. The symbol $\mathbb{H}_{\mathcal{O}}$ denotes the lattice

$$\left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle_{\mathcal{O}}$$

as in Definition 4.11. A lattice isomorphic to $\mathbb{H}_{\mathcal{O}}$ is referred to as a *hyperbolic lattice*.

The structure of the discriminant module as a torsion $\mathcal{O}$-module is expressed by the invariant factors of a Gram matrix.

Proposition 5.15. *Let (Λ, b) be an integral lattice over $\mathcal{O}$, and suppose that Λ has a basis $e_1, \ldots, e_d$. Let $G \in M_d(\mathcal{O})$ be the Gram matrix of (Λ, b) with respect to $e_1, \ldots, e_d$, and let $a_1, \ldots, a_d \in \mathcal{O}^\times$ be the invariant factors of G. Then $\Lambda^\vee/\Lambda \cong \mathcal{O}/a_1\mathcal{O} \oplus \cdots \oplus \mathcal{O}/a_d\mathcal{O}$ as torsion $\mathcal{O}$-modules.*

Proof. Let $e_1^\vee, \ldots, e_d^\vee \in \Lambda^\vee$ be the dual basis of $e_1, \ldots, e_d$ with respect to b. Then, it can be seen that G is the representation matrix of the inclusion $\Lambda \to \Lambda^\vee$ with respect to bases $e_1, \ldots, e_d$ and $e_1^\vee, \ldots, e_d^\vee$. Hence, the quotient $\Lambda^\vee/\Lambda$ is isomorphic to $\mathcal{O}/a_1\mathcal{O} \oplus \cdots \oplus \mathcal{O}/a_d\mathcal{O}$. □

As a result, an integral lattice over $\mathcal{O}$ whose underlying $\mathcal{O}$-module is free is unimodular if and only if its Gram matrix is invertible over $\mathcal{O}$.

Definition 5.16. Let (Λ, b) be an integral lattice over $\mathcal{O}$. An *overlattice* of Λ is an integral lattice on $(\Lambda \otimes_{\mathcal{O}} K, b)$ containing Λ.

For an overlattice Λ' of an integral lattice Λ, we have $\Lambda' \subset \Lambda^\vee$, and the quotient Λ'/Λ is a submodule of the discriminant module $\Lambda^\vee/\Lambda$. This submodule Λ'/Λ is *totally isotropic*, i.e., $\bar{b}(\bar{x}, \bar{x}) = 0$ for all $\bar{x} \in \Lambda'/\Lambda$, because Λ' is integral by definition.

Proposition 5.17. *Let Λ be an integral lattice over $\mathcal{O}$. Sending an overlattice Λ' of Λ to the submodule Λ'/Λ gives rise to a one-to-one correspondence between the overlattices of Λ and the totally isotropic submodules of $\Lambda^\vee/\Lambda$.*

Proof. For a totally isotropic submodule U of $\Lambda^\vee/\Lambda$, define $\Lambda_U := \{x \in \Lambda^\vee \mid \bar{x} \in U\}$. Then the mapping $U \mapsto \Lambda_U$ is the inverse of $\Lambda' \mapsto \Lambda'/\Lambda$. □

5.4 Unimodular lattices over the valuation ring of a local field

Let $\mathcal{O}$ be the valuation ring of a non-archimedean local field K of characteristic not 2. In this section, we give a classification theorem of unimodular lattices over $\mathcal{O}$. Let v be the normalized valuation of K. We begin with the non-dyadic case.

Theorem 5.18. *Suppose that 2 is a unit of $\mathcal{O}$, and fix a non-square unit $\epsilon \in \mathcal{O}^\times$. Let (Λ, b) be a unimodular lattice over $\mathcal{O}$. Then*

$$(\Lambda, b) \cong \begin{cases} \langle 1 \rangle_{\mathcal{O}}^{\oplus d} & \text{if } \det b = 1 \\ \langle 1 \rangle_{\mathcal{O}}^{\oplus d-1} \oplus \langle \epsilon \rangle_{\mathcal{O}} & \text{if } \det b = \epsilon. \end{cases}$$

Proof. We first show that there exists $x \in \Lambda$ such that $v(b(x, x)) = 0$. Let $e_1, \ldots, e_d \in \Lambda$ be a basis of Λ. If there is i such that $v(b(e_i, e_i)) = 0$ then we are done. Suppose that $v(b(e_i, e_i)) > 0$ for all i. Since b is unimodular, there exist i, j such that $v(b(e_i, e_j)) = 0$. Then

$$v(b(e_i + e_j, e_i + e_j)) = v(b(e_i, e_i) + 2b(e_i, e_j) + b(e_j, e_j)) = 0,$$

and we are done.

Let $x \in \Lambda$ be an element with $v(b(x,x)) = 0$. Then the submodule $\mathcal{O}x \subset \Lambda$ is unimodular. Thus Λ decomposes as $\Lambda = \mathcal{O}x \oplus (\mathcal{O}x)^{\perp}$, and $(\mathcal{O}x)^{\perp}$ is also unimodular by Proposition 5.13. Hence, by induction on rank, we get $(\Lambda, b) \cong \langle \alpha_1, \ldots, \alpha_d \rangle_{\mathcal{O}}$, where $\alpha_1, \ldots, \alpha_d \in \mathcal{O}^{\times}$ are units of $\mathcal{O}$. Moreover, since $\mathcal{O}^{\times}/\mathcal{O}^{\times 2} = \{1, \epsilon\}$ by Theorem 2.10 (i), we have $(\Lambda, b) \cong \langle 1 \rangle_{\mathcal{O}}^{\oplus m} \oplus \langle \epsilon \rangle_{\mathcal{O}}^{\oplus m'}$, where m and m' are non-negative integers with $m + m' = d$. It remains to show that $\langle \epsilon, \epsilon \rangle_{\mathcal{O}} \cong \langle 1, 1 \rangle_{\mathcal{O}}$. By Lemma 4.37, the equation $X_1^2 + X_2^2 = \epsilon$ has a primitive root modulo $\mathfrak{p}$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$. Thus, it has a primitive root over $\mathcal{O}$ by Proposition 1.37. This means that $\langle 1, 1 \rangle_{\mathcal{O}}$ represents ϵ. Hence, we obtain $\langle 1, 1 \rangle_{\mathcal{O}} \cong \langle \epsilon, \epsilon \cdot \det(\langle 1, 1 \rangle_{\mathcal{O}}) \rangle_{\mathcal{O}} \cong \langle \epsilon, \epsilon \rangle_{\mathcal{O}}$. This completes the proof. □

This theorem leads immediately to the following corollary.

Corollary 5.19. *Suppose that K is non-dyadic, and let (V, b) be an inner product space over K. If (V, b) contains a unimodular lattice over $\mathcal{O}$ then its Hasse-Witt invariant is zero.* □

Let us proceed the dyadic case. We assume that K is dyadic, that is, 2 is not a unit of $\mathcal{O}$, and let (Λ, b) be a lattice over $\mathcal{O}$.

Definition 5.20. The *scale* of Λ, denoted $\mathfrak{s}\Lambda$, is a fractional ideal generated by $\{b(x,y) \mid x, y \in \Lambda\}$. The *norm group* of Λ, denoted $\mathfrak{g}\Lambda$, is the additive group $\{b(x,x) \mid x \in \Lambda\} + 2\mathfrak{s}\Lambda$. The *norm* of Λ, denoted $\mathfrak{n}\Lambda$, is a fractional ideal generated by $\mathfrak{g}\Lambda$. The largest fractional ideal contained in $\mathfrak{g}\Lambda$ is denoted by $\mathfrak{m}\Lambda$.

We have

$$2\mathfrak{s}\Lambda \subset \mathfrak{m}\Lambda \subset \mathfrak{g}\Lambda \subset \mathfrak{n}\Lambda \tag{19}$$

by their definitions. It can be checked that

$$v(\mathfrak{m}\Lambda) + v(\mathfrak{n}\Lambda) \equiv 0 \mod 2, \tag{20}$$

see [35, p.253]. Suppose that (Λ, b) is integral. Then $\mathfrak{s}\Lambda$ is an integral ideal. Furthermore $\mathfrak{n}\Lambda$ and $\mathfrak{m}\Lambda$ are also integral ideals since $\mathfrak{g}\Lambda \subset \mathcal{O}$. If (Λ, b) is unimodular then $\mathfrak{s}\Lambda = \mathcal{O}$.

Theorem 5.21. *Let Λ and Λ' be unimodular lattices on an inner product space (V, b) over a dyadic local field K of characteristic not 2. There exists an isometry $\tau \in \mathrm{O}(V, b)$ such that $\tau(\Lambda') = \Lambda$ if and only if $\mathfrak{g}\Lambda = \mathfrak{g}\Lambda'$.*

Proof. See Theorem 93:16 and p.222 of [35]. □

In the following, we restrict ourselves to the case $K = \mathbb{Q}_2$.

Corollary 5.22. *Let Λ and Λ' be unimodular lattices on an inner product space (V, b) over $\mathbb{Q}_2$. Suppose that Λ and Λ' are both even or both odd. Then there exists an isometry $\tau \in \mathrm{O}(V, b)$ such that $\tau(\Lambda') = \Lambda$.*

Proof. Note that $\mathfrak{s}\Lambda = \mathbb{Z}_2$ since Λ is unimodular. Suppose first that Λ and Λ' are both even. Then $\mathfrak{g}\Lambda \subset 2\mathbb{Z}_2$, and thus $\mathfrak{g}\Lambda = 2\mathbb{Z}_2$ by (19). Similarly, we get $\mathfrak{g}\Lambda' = 2\mathbb{Z}_2$. Thus we are done by Theorem 5.21. Suppose then that Λ and Λ' are both odd. Then $2\mathbb{Z}_2 \subsetneq \mathfrak{g}\Lambda \subset \mathbb{Z}_2$, which means that $\mathfrak{n}\Lambda = \mathbb{Z}_2$. On the other hand, we have $\mathfrak{m}\Lambda = \mathbb{Z}_2$ or $2\mathbb{Z}_2$ by (19). Thus $\mathfrak{m}\Lambda = \mathbb{Z}_2$ by (20), and hence $\mathfrak{g}\Lambda = \mathbb{Z}_2$ by (19) again. Similarly, we get $\mathfrak{g}\Lambda' = \mathbb{Z}_2$. Therefore, Theorem 5.21 completes the proof. □

An even unimodular lattice over $\mathbb{Z}_2$ has the following standard form. We refer to [35, Example 93:18] for a more general result.

Theorem 5.23. *Let (Λ, b) be an even unimodular lattice over $\mathbb{Z}_2$. Then, the rank of Λ is even, say $2n$, and $(-1)^n \det(b) = 1$ or -3 in $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$. Moreover, we have*

$$(\Lambda, b) \cong \begin{cases} \mathbb{H}_{\mathbb{Z}_2}^{\oplus n} & \text{if } (-1)^n \det(b) = 1 \\ \mathbb{H}_{\mathbb{Z}_2}^{\oplus n-1} \oplus \left\langle \begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix} \right\rangle_{\mathbb{Z}_2} & \text{if } (-1)^n \det(b) = -3. \end{cases}$$

Proof (Sketch). Since (Λ, b) is unimodular, there exist $x, y \in \Lambda$ such that $b(x, y) = 1$. Since (Λ, b) is even, x and y are linearly independent, and we can write $b(x, x) = 2\alpha$ and $b(y, y) = 2\beta$ for some $\alpha, \beta \in \mathbb{Z}_2$. Then $\mathbb{Z}_2 x \oplus \mathbb{Z}_2 y$ is a unimodular submodule of Λ isomorphic to $\left\langle \begin{matrix} 2\alpha & 1 \\ 1 & 2\beta \end{matrix} \right\rangle_{\mathbb{Z}_2}$. Thus $(\mathbb{Z}_2 x \oplus \mathbb{Z}_2 y)^\perp$ is also unimodular, and (Λ, b) is decomposes as $(\mathbb{Z}_2 x \oplus \mathbb{Z}_2 y) \oplus (\mathbb{Z}_2 x \oplus \mathbb{Z}_2 y)^\perp$ by Proposition 5.13. On the other hand, one can show that

$$\left\langle \begin{matrix} 2\alpha & 1 \\ 1 & 2\beta \end{matrix} \right\rangle_{\mathbb{Z}_2} \cong \begin{cases} \mathbb{H}_{\mathbb{Z}_2} & \text{if } \alpha\beta \in 2\mathbb{Z}_2 \\ \langle A \rangle_{\mathbb{Z}_2} & \text{if } \alpha\beta \notin 2\mathbb{Z}_2, \end{cases}$$

where $A := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Hence, by induction on rank, we obtain $(\Lambda, b) \cong \mathbb{H}_{\mathbb{Z}_2}^{\oplus m} \oplus \langle A \rangle_{\mathbb{Z}_2}^{\oplus m'}$, where m and m' are non-negative integers. In particular, the rank $\mathrm{rk}(\Lambda) = 2m + 2m'$ is even, and putting $n = \mathrm{rk}(\Lambda)/2$, we have $(-1)^n \det(b) = 1$ or -3 in $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$. It remains to show that $\langle A \rangle_{\mathbb{Z}_2}^{\oplus 2} \cong \mathbb{H}_{\mathbb{Z}_2}^{\oplus 2}$. One can show this isomorphism in a direct way or by using Corollary 5.22. □

5.5 Even unimodular lattices over $\mathbb{Z}$

Here we consider even unimodular lattices over $\mathbb{Z}$. The *signature* and *index* of a lattice (Λ, b) over $\mathbb{Z}$ are respectively those of the inner product space $(\Lambda \otimes \mathbb{R}, b \otimes \mathbb{R})$ over $\mathbb{R}$. The hyperbolic lattice $\mathbb{H}_{\mathbb{Z}}$ is an even unimodular lattice of signature $(1, 1)$. Another example of an even unimodular lattice is given by the matrix

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

The lattice which has this matrix as a Gram matrix is denoted by E_8 (this is the *root lattice* of type E_8). The lattice E_8 is an even unimodular lattice of signature $(8, 0)$.

Theorem 5.24. *Let (Λ, b) be an even unimodular lattice over $\mathbb{Z}$ of signature (r, s). Then, the rank $r + s$ is even, $(-1)^{(r+s)/2} \det(b) = 1$, and $r \equiv s \bmod 8$.*

Proof. The rank $r + s$ of Λ is also the rank of the localization $(\Lambda \otimes \mathbb{Z}_2, b \otimes \mathbb{Z}_2)$ at 2. Thus, it is even by Theorem 5.23. Put $n = (r + s)/2$. Theorem 5.23 also shows that $(-1)^n \det(b) = 1$ or -3 in $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$. On the other hand, since (Λ, b) is unimodular, we have $(-1)^n \det(b) = 1$ or -1 in $\mathbb{Z}^\times/\mathbb{Z}^{\times 2}$, and hence in $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$. These show that $(-1)^n \det(b) = 1$ in $\mathbb{Z}^\times/\mathbb{Z}^{\times 2}$. It remains

to show that $r \equiv s \bmod 8$. We have $n \equiv s \bmod 2$ because $(-1)^n = \det(b \otimes \mathbb{R}) = (-1)^s$. A computation shows that

$$\mathrm{hw}_2(b \otimes \mathbb{Q}_2) = \mathrm{hw}_2(\mathbb{H}_{\mathbb{Q}_2}^{\oplus n}) = \frac{n(n-1)}{2} = \begin{cases} 0 & \text{if } n \equiv 0, 1 \bmod 4 \\ 1 & \text{if } n \equiv 2, 3 \bmod 4, \end{cases}$$

and we have

$$\mathrm{hw}_\infty(b \otimes \mathbb{R}) = \frac{s(s-1)}{2} = \begin{cases} 0 & \text{if } s \equiv 0, 1 \bmod 4 \\ 1 & \text{if } s \equiv 2, 3 \bmod 4 \end{cases}$$

by Theorem 4.60. Moreover, it follows from the reciprocity (Proposition 4.53) and Corollary 5.19 that $\mathrm{hw}_\infty(b \otimes \mathbb{R}) + \mathrm{hw}_2(b \otimes \mathbb{Q}_2) = 0$. Hence $n \equiv s \bmod 4$. Therefore

$$r - s = (2n - s) - s = 2(n - s) \equiv 0 \mod 8.$$

This completes the proof. We refer to [40, Chapter V] for another proof. □

Theorem 5.25. *Let $r, s \in \mathbb{Z}_{\geq 0}$ be non-negative integers with $r \equiv s \mod 8$. Then there exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s). Moreover, if r and s are positive then such a lattice is unique up to isomorphism.*

Proof. Let r, s be non-negative integers with $r \equiv s \mod 8$. If $r - s \geq 0$ then $\mathrm{E}_8^{\oplus (r-s)/8} \oplus \mathbb{H}_{\mathbb{Z}}^{\oplus s}$ is an even unimodular lattice of signature (r, s). If $r - s < 0$ then an even unimodular lattice of signature (r, s) is obtained by multiplying the inner product of $\mathrm{E}_8^{\oplus (s-r)/8} \oplus \mathbb{H}_{\mathbb{Z}}^{\oplus r}$ by -1. For the uniqueness, see [40, Chapter V, Theorem 6]. □

It is known that E_8 is a unique even unimodular lattice of signature $(8, 0)$. However, in Theorem 5.25, the assumption that r and s are positive cannot be dropped for the uniqueness. In fact, it is known that there exist two isomorphism classes of even unimodular lattices of signature $(16, 0)$, and 24 isomorphism classes of even unimodular lattices of signature $(24, 0)$. For these facts, we refer to [40, Chapter V, §2.3].

Chapter III
Isometries and their characteristic polynomials

6 Equivariant Witt groups

This section gives a foundation of equivariant Witt groups. This theory is an equivariant version of that of Witt groups for inner product spaces, and was well known to experts, but the paper [3] of E. Bayer-Fluckiger and L. Taelman published in 2020 seems to be the first document that summarizes the theory explicitly, see Introduction of that paper. This section is written with reference to the paper [3].

6.1 General results

Let K be a field, and let A be a K-algebra with a K-linear involution $\sigma : A \to A$.

Definition 6.1. An *A-inner product space* over K is a pair (V, b) consisting of an A-module V whose K-dimension is finite and an inner product $b : V \times V \to K$ over K satisfying

$$b(ax, y) = b(x, \sigma(a)y) \tag{21}$$

for all $a \in A$ and $x, y \in V$. When we need refer to the A-module structure $\rho : A \to \mathrm{End}(V)$ of V, the A-inner product space is denoted by the triple (V, b, ρ). Two A-inner product spaces (V, b) and (V', b') are *isomorphic* if there exists an isomorphism $V \to V'$ of A-modules which is also an isometry of inner product spaces over K.

Example 6.2. Let (V, b) be an inner product space over K, and let G be a group. Suppose that each element of G acts on V as an isometry. Then we have $b(g.x, y) = b(x, g^{-1}.y)$ for any $g \in G$ and $x, y \in V$. This means that the pair (V, b) can be regarded as a $K[G]$-inner product space, where $K[G]$ is the group algebra with the K-linear involution induced by $g \mapsto g^{-1}$ for all $g \in G$.

Definition 6.3. Let $V = (V, b)$ be an A-inner product space. We refer to an A-submodule of V as an *A-stable subspace*. A *lagrangian* of V is an A-stable subspace X satisfying $X = X^{\perp}$. If V has a lagrangian then V is said to be *neutral*.

It is clear that the direct sum of two neutral spaces is again neutral. The following lemma is useful to check whether an A-stable subspace is a lagrangian.

Lemma 6.4. *Let (V, b) be an A-inner product space. An A-stable subspace X of V is a lagrangian if and only if $X \subset X^{\perp}$ and $2 \dim X = \dim V$. In particular, any neutral space is of even dimension (over K).*

Proof. Let X be an A-stable subspace of V. Note that $\dim V = \dim X^{\perp} + \dim X$ by Proposition 4.4 (i). If X is a lagrangian then $\dim V = \dim X^{\perp} + \dim X = 2 \dim X$. Conversely, suppose that $X \subset X^{\perp}$ and $2 \dim X = \dim V$. Then $\dim X^{\perp} + \dim X = \dim V = 2 \dim X$, and we get $\dim X^{\perp} = \dim X$. This means that $X = X^{\perp}$, and X is a lagrangian. □

Two A-inner product spaces V and V' are *Witt equivalent*, written $V \sim V'$, if there exist neutral spaces N and N' such that $V \oplus N \cong V' \oplus N'$. Any neutral space is Witt equivalent to the 0-dimensional space. Let $\mathcal{M}_A$ denote the monoid of all isomorphism classes of A-inner product spaces, where the operation is the direct sum $\oplus$.

Lemma 6.5. *The Witt equivalence $\sim$ is an equivalence relation on $\mathcal{M}_A$.*

Proof. Reflexivity and symmetry are obvious. Let $V, V', V'' \in \mathcal{M}_A$ satisfy $V \sim V'$ and $V' \sim V''$. By definition, there exist neutral spaces N, N', M', M'' such that $V \oplus N \cong V' \oplus N'$ and $V' \oplus M' \cong V'' \oplus M''$. Then

$$V \oplus N \oplus M' \cong V' \oplus N' \oplus M' \cong (V' \oplus M') \oplus N' \cong V'' \oplus M'' \oplus N',$$

which implies that $V \sim V''$ since $N \oplus M'$ and $M'' \oplus N'$ are neutral. This completes the proof. □

Each equivalence class is called an (*A-equivariant*) *Witt class*. The Witt class of (V, b) will be denoted by $[(V, b)]$ or $[V, b]$ simply. We now show that the quotient $\mathcal{M}_A/\sim$ becomes a group.

Lemma 6.6. *Let $(V, b_V), (V', b_{V'}), (W, b_W), (W', b_{W'})$ be A-inner product spaces.*

(i) *$(V, b_V) \oplus (V, -b_V)$ is neutral, and hence, Witt equivalent to 0.*

(ii) *If $(V, b_V) \sim (W, b_W)$ and $(V', b_{V'}) \sim (W', b_{W'})$ then $(V, b) \oplus (V', b_{V'}) \sim (W, b_W) \oplus (W', b_{W'})$.*

Proof. For (i), put $X = \{(x, x) \in (V, b_V) \oplus (V, -b_V) \mid x \in V\}$. Then $X \subset X^\perp$ and

$$2 \dim X = 2 \dim V = \dim((V, b_V) \oplus (V, -b_V)).$$

Thus, Lemma 6.4 shows that X is a lagrangian of $(V, b_V) \oplus (V, -b_V)$, and $(V, b_V) \oplus (V, -b_V)$ is neutral. We then show the assertion (ii). Suppose that $V \sim W$ and $V' \sim W'$. Then there exist neutral spaces N, M, N', M' such that $V \oplus N \cong W \oplus M$ and $V' \oplus N' \cong W' \oplus M'$. Thus

$$\begin{aligned}(V \oplus V') \oplus (N \oplus N') &\cong (V \oplus N) \oplus (V' \oplus N') \\ &\cong (W \oplus M) \oplus (W' \oplus M') \cong (W \oplus W') \oplus (M \oplus M'),\end{aligned}$$

which shows that $V \oplus V' \sim W \oplus W'$. □

Definition 6.7. Lemma 6.6 means that the operation $+$ defined by

$$[V, b] + [V', b'] = [(V, b) \oplus (V', b')]$$

makes $\mathcal{M}_A/\sim$ an additive group. The zero is the class containing the 0-dimensional space, and the inverse of $[V, b]$ is given by $[V, -b]$. This group is called the (*A-equivariant*) *Witt group* of K or the Witt group for A-inner product spaces, and denoted by $W_A(K)$.

The following proposition means that the set of all neutral spaces forms a Witt class, which is the zero of $W_A(K)$.

Proposition 6.8. *An A-inner product space V is neutral if and only if $V \sim 0$.*

Proof. Let V be an A-inner product space. If V is neutral then the equivalence $V \sim 0$ is clear by definition. Suppose that $V \sim 0$. Then there exists a neutral space M such that $V \oplus M$ is neutral. The dimensions of $V \oplus M$ and M are even since they are neutral, and hence that of V

is also even. Say $\dim V = 2n$ and $\dim M = 2m$. Let $X \subset V \oplus M$ and $Y \subset M$ be lagrangians, and put

$$S := X \cap (V \oplus Y) \subset V \oplus M \quad \text{and} \quad Z := \pi_V(S) \subset V,$$

where $\pi_V : V \oplus M \to V$ is the projection. We show that Z is a lagrangian of V. Let b_V, b_M, and $b_{V\oplus M}$ denote the inner products of V, M, and $V \oplus M$ respectively. For $v + y, v' + y' \in S$ ($v', v' \in V$, $y, y' \in Y$) we have

$$0 = b_{V\oplus M}(x + y, x' + y') = b_V(x, x') + b_M(y, y') = b_V(\pi_V(x + y), \pi_V(x' + y')) + 0.$$

This equation means that $Z \subset Z^\perp$ since any element of Z is of the form $\pi_V(x + y)$. We then calculate the dimension of Z. It follows from the rank-nullity formula that

$$\dim Z = \dim S - \dim \ker(\pi_V|S). \tag{22}$$

On the other hand, we have

$$\ker(\pi_V|S) = S \cap (0 \oplus M) = (X \cap (V \oplus Y)) \cap (0 \oplus M) = X \cap (0 \oplus Y)$$

and

$$(X \cap (0 \oplus Y))^\perp_{V\oplus M} = X^\perp_{V\oplus M} + (0 \oplus Y)^\perp_{V\oplus M} = X + (V \oplus Y^\perp_M) = X + (V \oplus Y),$$

where each subscript stands for the space in which we take the orthogonal space. Thus

$$\begin{aligned}
\dim \ker(\pi_V|S) &= \dim(V \oplus M) - \dim(\ker(\pi_V|S)^\perp) \\
&= 2n + 2m - \dim(X + (V \oplus Y)) \\
&= 2n + 2m - (\dim X + \dim(V \oplus Y) - \dim S) \\
&= 2n + 2m - (n + m + 2n + m - \dim S) \\
&= n - \dim S.
\end{aligned}$$

Combining this equation and equation (22) yields

$$\dim Z = \dim S - (n - \dim S) = n,$$

which means that Z is a lagrangian of V by Lemma 6.4. Therefore V is neutral, and the proof is complete. □

Our next purpose is to obtain a direct sum decomposition of $W_A(K)$. The precise statement is in Theorem 6.11.

Lemma 6.9. *Let (V, b) be an A-inner product space, and X an A-stable subspace with $X \subset X^\perp$. The quotient $X^\perp/X$ is an A-inner product space with the symmetric bilinear form*

$$(v + X, v' + X) \mapsto b(v, v') \quad (v, v' \in V^\perp),$$

which is also denoted by b. Moreover, we have $[V, b] = [X^\perp/X, b]$.

Proof. It is easy to check that the bilinear form b on $X^\perp/X$ is well defined and has the property (21). To show nondegeneracy of b, let $v \in X^\perp$, and assume that $b(v + X, X^\perp/X) = 0$. Then $b(v, X^\perp) = 0$, which means that $v \in X^{\perp\perp} = X$. Thus $v = 0$ in $X^\perp/X$, and b is nondegenerate.

We then prove that $[V, b] = [X^\perp/X, b]$. We claim that the direct sum $(V, -b) \oplus (X^\perp/X, b)$ is neutral. Put $Y = \{(v, v + X) \in V \oplus (X^\perp/X) \mid v \in X^\perp\}$. Then Y is an A-stable subspace with $\dim(Y) = \dim(X^\perp)$ and $Y \subset Y^\perp$. Moreover

$$\dim(V \oplus (X^\perp/X)) = \dim(V) + \dim(X^\perp) - \dim(X) = 2\dim(X^\perp) = 2\dim(Y),$$

where the second equality follows from Proposition 4.4 (i). Hence Y is a lagrangian by Lemma 6.4, and $(V,-b)\oplus(X^\perp/X,b)$ is neutral. Therefore

$$0=[(V,-b)\oplus(X^\perp/X,b)]=-[V,b]+[X^\perp/X,b],$$

and $[V,b]=[X^\perp/X,b]$ as required. □

An A-inner product space (V,b) is *simple* if V is simple as an A-module. If an A-inner product space is expressed as a direct sum of simple spaces, then the A-inner product space is said to be *semisimple*. It is stronger than the underlying A-module being semisimple because it requires that each simple component of the underlying A-module is nondegenerate.

Proposition 6.10. *Any class in $W_A(K)$ is represented by a semisimple A-inner product space.*

Proof. Set

$$\mathcal{M}'_A:=\{(V,b)\in\mathcal{M}_A\mid [V,b]\text{ can be represented by a semisimple space}\}\subset\mathcal{M}_A.$$

It suffices to show that $\mathcal{M}'_A=\mathcal{M}_A$. Suppose to the contrary that $\mathcal{M}'_A\subsetneq\mathcal{M}_A$ and take $V\in\mathcal{M}_A\setminus\mathcal{M}'_A$ so that its K-dimension is minimal. The space V is not simple and thus contains a nontrivial A-stable subspace W. Put $X=W\cap W^\perp$.

If $X=0$, then W and $W^\perp$ are nondegenerate and $V=W\oplus W^\perp$. Hence, we have $[W]\notin\mathcal{M}'_A$ or $[W^\perp]\notin\mathcal{M}'_A$, since otherwise the class $[V]=[W]+[W^\perp]$ would be represented by a semisimple space. However, in either case, this contradicts the minimality of the dimension of V since $\dim(W)$ and $\dim(W^\perp)$ are less than $\dim(V)$.

Suppose that $X\neq 0$. Then $X\subset X^\perp$. Lemma 6.9 shows that $[V]=[X^\perp/X]$. However, we would have

$$\dim(X^\perp/X)=\dim(X^\perp)-\dim(X)\le\dim_K(V)-\dim(X)<\dim(V),$$

which contradicts the minimality of the dimension of V. Therefore $\mathcal{M}'_A=\mathcal{M}_A$, and the proof is complete. □

Let P be a simple A-module. The symbol $W_A(K;P)$ denotes the subgroup of $W_A(K)$ generated by the classes of the form $[P,b]$ where b is an inner product on P over K which makes (P,b) an A-inner product space. Any class in $W_A(K;P)$ is represented by an A-inner product space whose underlying A-module is a direct sum of copies of P. We remark that the subgroup $W_A(K;P)$ is determined only by the isomorphism class of P.

Theorem 6.11. *The Witt group $W_A(K)$ decomposes as*

$$W_A(K)=\bigoplus_P W_A(K;P)$$

where P ranges over the isomorphism classes of simple A-modules.

Proof. Proposition 6.10 implies that $W_A(K)=\sum_P W_A(K;P)$. Hence, it suffices to show that the sum $\sum_P W_A(K;P)$ is a direct sum. Let $\sum_P[V_P]$ be an element of $\sum_P W_A(K;P)$ where each V_P is a direct sum of copies of P, and assume that $\sum_P[V_P]=0$. Since $[\bigoplus_P V_P]=\sum_P[V_P]=0$, Proposition 6.8 implies that the space $V:=\bigoplus_P V_P$ is neutral. Let X be a lagrangian of V, and set $X_P:=X\cap V_P$ for each simple module P. We remark that[†]

$$X=\bigoplus_P X_P. \tag{23}$$

[†]Equation (23) is a not so trivial property of semisimple modules, but its proof is omitted here to avoid getting off the main line. We refer to [48, §7.2].

We claim that X_P is a lagrangian of V_P for each P. The inclusion $X_P \subset (X_P)^\perp$ in V_P is obvious. Moreover, it follows from Lemma 6.4 and equation (23) that

$$\dim(V) = 2\dim(X) = 2\sum_P \dim(X_P) \leq \sum_P \dim(V_P) = \dim(V).$$

Thus $2\dim(X_P)$ must be equal to $\dim(V_P)$ for each P, and this implies that X_P is a lagrangian of V_P. Therefore, V_P is neutral, or equivalently, $[V_P] = 0$. This implies that the sum $\sum_P W_A(K; P)$ is a direct sum. The proof is complete. □

Let Γ be an infinite cyclic group with generator τ. We will use Theorem 6.11 in the case $A = K[\Gamma]$. This is a special case of Example 6.2. For any (non-constant) irreducible polynomial $f \in K[X]$ except for X, the quotient $K[X]/(f)$ is a simple $K[\Gamma]$-module via the action determined by

$$\tau.v = Xv \quad (v \in K[X]/(f))$$

(note that multiplication by X is invertible in $K[X]/(f)$). Conversely, every simple $K[\Gamma]$-module whose K-dimension is finite is isomorphic to $K[X]/(f)$ for some irreducible polynomial $f \in K[X]$. This gives rise to a bijection between the set of irreducible monic polynomials in $K[X]$ except for X and the set of isomorphism classes of simple $K[\Gamma]$-modules. For an irreducible polynomial $f(X) \neq X$, we write $W_{K[\Gamma]}(K; f) = W_{K[\Gamma]}(K; K[X]/(f))$. In this case, Theorem 6.11 is as follows.

Corollary 6.12. *We have*

$$W_{K[\Gamma]}(K) = \bigoplus_f W_{K[\Gamma]}(K; f)$$

where f ranges over all irreducible monic polynomials in $K[X]$ expect for X. □

6.2 Witt groups for torsion product modules

In this subsection, we assume that K is the field of fractions of a Dedekind domain $\mathcal{O}$, and let A be an $\mathcal{O}$-algebra with a linear involution σ. We define the A-equivariant Witt group for torsion product modules similarly to that for inner product spaces.

Definition 6.13. An *A-torsion product module* over $\mathcal{O}$ is a pair (T, b) consisting of an A-module T finitely generated over $\mathcal{O}$ and a torsion product $b : T \times T \to K/\mathcal{O}$ over $\mathcal{O}$ satisfying

$$b(ax, y) = b(x, \sigma(a)y) \tag{24}$$

for all $a \in A$ and $x, y \in T$. Two A-torsion product modules (T, b) and (T', b') are *isomorphic* if there exists an isomorphism $T \to T'$ of A-modules which is also an isometry of torsion product modules over $\mathcal{O}$.

Definition 6.14. A *lagrangian* of an A-torsion product module $T = (T, b)$ is an A-submodule X satisfying $X = X^\perp$. If T has a lagrangian then T is said to be *neutral*. Two A-torsion product modules T and T' are *Witt equivalent*, written $T \sim T'$, if there exist neutral modules N and N' such that $T \oplus N \cong T' \oplus N'$.

Properties of A-torsion product modules can be proved similarly to those of A-inner product spaces by using lengths instead of dimensions.

Lemma 6.15. *Let $T = (T, b)$ be an A-torsion product module. An A-submodule X of T is a lagrangian if and only if $T \subset T^\perp$ and $2\operatorname{len} X = \operatorname{len} T$. In particular, any neutral module is of even length.*

Proof. The same proof as that of Lemma 6.4 is valid by replacing dimensions with lengths, and by using Proposition 5.8 instead of Proposition 4.4. □

Let $\mathcal{MT}_A$ denote the monoid of all isomorphism classes of A-torsion product modules. The Witt equivalence is an equivalence relation of $\mathcal{MT}_A$ as in Lemma 6.5. Each equivalence class is called an (*A-equivalent*) *Witt class*, and the Witt class of (T, b) is denoted by $[(T, b)]$ or $[T, b]$. Moreover, Lemma 6.6 holds mutatis mutandis, and thus, the quotient $\mathcal{MT}_A/\sim$ becomes a group with the operation $+$ defined by

$$[T, b] + [T', b'] = [(T, b) \oplus (T', b')].$$

Here the zero is the class containing the zero module, and the inverse of $[T, b]$ is given by $[T, -b]$.

Definition 6.16. The group $\mathcal{MT}_A/\sim$ is called the (*A-equivariant*) *Witt group* for A-torsion product modules, and denoted by $WT_A(\mathcal{O})$.

We also have analogs of Proposition 6.8 and Lemma 6.9:

Proposition 6.17. *Let T be an A-torsion product module.*

(i) *T is neutral if and only if $T \sim 0$.*

(ii) *If X is an A-submodule of T satisfying $X \subset X^\perp$ then $X^\perp/X$ is an A-torsion product module in a natural way, and $T \sim X^\perp/X$.*

Proof. These can be proved by imitating the proofs of Proposition 6.8 and Lemma 6.9. □

In the rest of this subsection, we assume that $\mathcal{O}$ is a discrete valuation ring. Let κ denote its residue field, and fix a uniformizer π of $\mathcal{O}$. We write A_κ for the κ-algebra $A \otimes_{\mathcal{O}} \kappa$. Our aim is to give an isomorphism between two Witt groups $WT_A(\mathcal{O})$ and $W_{A_\kappa}(\kappa)$ (Theorem 6.21).

Definition 6.18. Let T be a finitely generated torsion module over $\mathcal{O}$. By the structure theorem 5.1, the set $\{n \in \mathbb{Z}_{\geq 0} \mid \pi^n T = 0\}$ is bounded. The minimum of this set is called the *exponent* of T. The exponent is independent of the choice of π.

Lemma 6.19. *Let $T = (T, b)$ be an A-torsion product module of exponent n.*

(i) *If $n \geq 2$ then $U := \pi^{n-1}T$ is a nonzero totally isotropic A-submodule.*

(ii) *T is Witt equivalent to an A-torsion product module of exponent at most 1.*

In particular, any Witt class of $WT_A(\mathcal{O})$ is represented by an A-torsion product module of exponent at most 1.

Proof. (i). Let $n \geq 2$. It is clear that $U = \pi^{n-1}T$ is a nonzero A-submodule. Moreover

$$b(U, U) = b(\pi^{n-1}T, \pi^{n-1}T) = b(\pi^n T, \pi^{n-2}T) = b(0, \pi^{n-2}T) = 0.$$

Thus U is totally isotropic.

(ii). If $n \leq 1$ then there is nothing to prove. Let $n \geq 2$. Then $U = \pi^{n-1}T$ is a totally isotropic A-submodule by (i). Proposition 6.17 (ii) shows that $T \sim U^\perp/U$. Since the exponent of $U^\perp/U$ is at most $n-1$ by the definition of U, it follows inductively that T is equivalent to a module whose exponent is at most 1. □

Let (T, b) be an A-torsion product module of exponent at most 1. The underlying A-module T can be seen as an A_κ-module by the ring homomorphism $A_\kappa = A \otimes_{\mathcal{O}} \kappa \to \mathrm{End}(T)$ determined by

$$a \otimes (\gamma + \pi\mathcal{O}) \mapsto (x \mapsto (a\gamma).x) \quad (a \in A, \gamma \in \mathcal{O}, x \in T).$$

Furthermore b takes values in $(\pi^{-1}\mathcal{O})/\mathcal{O} \subset K/\mathcal{O}$. Indeed, we have

$$\pi b(x, y) = b(\pi x, y) = b(0, y) = 0 \quad \text{in } K/\mathcal{O}$$

for any $x, y \in T$. Hence, we obtain the inner product

$$\pi b : T \times T \xrightarrow{b} (\pi^{-1}\mathcal{O})/\mathcal{O} \xrightarrow{\times\pi} \mathcal{O}/(\pi\mathcal{O}) = \kappa,$$

and the pair $(T, \pi b)$ is an A_κ-inner product space over κ.

Lemma 6.20. *Let $T = (T, b)$ be an A-torsion product module of exponent at most 1. The A-torsion product module (T, b) is neutral if and only if the A_κ-inner product space $(T, \pi b)$ is neutral. In other words, $[T, b] = 0$ in $WT_A(\mathcal{O})$ if and only if $[T, \pi b] = 0$ in $W_{A_\kappa}(\kappa)$.*

Proof. If X is a lagrangian of (T, b) (resp. $(T, \pi b)$) then X is also a lagrangian of $(T, \pi b)$ (resp. (T, b)). Hence (T, b) is neutral if and only if $(T, \pi b)$ is neutral. By Proposition 6.8 and Proposition 6.17 (i), we can also say that $[T, b] = 0$ in $WT_A(\mathcal{O})$ if and only if $[T, \pi b] = 0$ in $W_{A_\kappa}(\kappa)$. □

Theorem 6.21. *Sending $\omega \in WT_A(\mathcal{O})$ to $[T, \pi b] \in W_{A_\kappa}(\kappa)$, where (T, b) is a representative of ω whose exponent at most 1, gives rise to a well-defined isomorphism from $WT_A(\mathcal{O})$ to $W_{A_\kappa}(\kappa)$.*

Proof. Let $\omega \in WT_A(\mathcal{O})$. Then there exists a representative (T, b) of ω whose exponent is at most 1 by Lemma 6.19. We firstly show that the Witt class of $(T, \pi b) \in W_{A_\kappa}(\kappa)$ is independent of the choice of (T, b). Let (T', b') be another representative of ω. Then

$$0 = -[T, b] + [T', b'] = [T, -b] + [T', b'] = [T \oplus T', (-b) \oplus b'] \quad \text{in } WT_A(\mathcal{O}),$$

and thus $0 = [T \oplus T', \pi((-b) \oplus b')]$ in $W_{A_\kappa(\kappa)}$ by Lemma 6.20. Moreover, we have

$$[T \oplus T', \pi((-b) \oplus b')] = [T, -\pi b] + [T', \pi b'] = -[T, \pi b] + [T', \pi b'],$$

and hence $[T, \pi b] = [T', \pi b']$ in $W_{A_\kappa}(\kappa)$. This means that the Witt class of $(T, \pi b)$ is independent of the choice of (T, b).

It is easy to check the mapping $WT_A(\mathcal{O}) \to W_{A_\kappa}(\kappa)$, $\omega \mapsto [T, \pi b]$ is a group homomorphism. We then show that this homomorphism is an isomorphism. Lemma 6.20 implies that the homomorphism is injective. Let (V, b) be an A_κ-inner product space over κ. Then the underlying space V can be naturally seen as an $\mathcal{O}$-torsion module of exponent at most 1. By defining the torsion form $\pi^{-1}b : V \times V \to K/\mathcal{O}$ as

$$\pi^{-1}b : V \times V \xrightarrow{b} \kappa = \mathcal{O}/(\pi\mathcal{O}) \xrightarrow{\times\pi^{-1}} (\pi^{-1}\mathcal{O})/\mathcal{O} \subset K/\mathcal{O},$$

the pair $(V, \pi^{-1}b)$ becomes an A-torsion product module whose exponent is at most 1. Since the image of $[V, \pi^{-1}b] \in WT_A(\mathcal{O})$ is equal to $[V, b] \in W_{A_\kappa}(\kappa)$, the homomorphism $WT_A(\mathcal{O}) \to W_{A_\kappa}(\kappa)$ is surjective. This completes the proof. □

6.3 Stable lattices over discrete valuation rings

In this subsection, we assume that K is a discrete valuation field, and let v, $\mathcal{O}$, and κ denote its normalized valuation, valuation ring, and residue field respectively. Furthermore, we fix a uniformizer π of $\mathcal{O}$. Let A be an $\mathcal{O}$-algebra with a linear involution σ. The K-algebra $A \otimes_{\mathcal{O}} K$ is denoted by A_K. We will give a necessary and sufficient condition for an A_K-inner product space to contain an A-stable unimodular lattice in terms of Witt groups.

Definition 6.22. Let (V, b) be an A_K-inner product space. A lattice Λ on V is *A-stable* if $A\Lambda = \Lambda$. If V contains an A-stable lattice, then V is said to be *bounded*. The subgroup of $W_{A_K}(K)$ generated by the classes which can be represented by a bounded A_K-inner product space is denoted by $W^{\mathrm{b}}_{A_K}(K)$.

Proposition 6.23. *Let $V = (V, b)$ be an A_K-inner product space.*

(i) *For any lattice Λ on V, the set $\{v(b(x, y)) \in \mathbb{Z} \mid x, y \in \Lambda\}$ is bounded below.*

(ii) *If V is bounded then V contains an A-stable integral lattice.*

Proof. (i). Let $e_1, \ldots, e_d$ be a basis of Λ, and let $x, y \in \Lambda$. We can write

$$x = \textstyle\sum_{i=1}^{d} \alpha_i e_i,\ y = \sum_{j=1}^{d} \beta_j e_j \quad \text{where } \alpha_i, \beta_j \in \mathcal{O}.$$

Then

$$\begin{aligned} v(b(x, y)) &= v\left(\textstyle\sum_{i,j} \alpha_i \beta_j b(e_i, e_j)\right) \\ &\geq \min\{v(\alpha_i \beta_j b(e_i, e_j)) \mid 1 \leq i, j \leq d\} \\ &= \min\{v(\alpha_i) + v(\beta_j) + v(b(e_i, e_j)) \mid 1 \leq i, j \leq d\} \\ &\geq \min\{v(b(e_i, e_j)) \mid 1 \leq i, j \leq d\}. \end{aligned}$$

Thus, the set $\{v(b(x, y)) \in \mathbb{Z} \mid x, y \in \Lambda\}$ is bounded below.

(ii). Suppose that V contains an A-stable lattice Λ, and put $m = \min\{v(b(x, y)) \in \mathbb{Z} \mid x, y \in \Lambda\}$. If $m \geq 0$ then Λ is integral, and we are done. Let $m < 0$. It is clear that $\pi^{-m}\Lambda$ is A-stable. Moreover, we have

$$\begin{aligned} \min\{v(b(\pi^{-m}x, \pi^{-m}y)) \in \mathbb{Z} \mid x, y \in \Lambda\} &= \min\{2v(\pi^{-m}) + v(b(x, y)) \in \mathbb{Z} \mid x, y \in \Lambda\} \\ &= -2m + \min\{v(b(x, y)) \in \mathbb{Z} \mid x, y \in \Lambda\} \\ &= -m \\ &> 0, \end{aligned}$$

which implies that $\pi^{-m}\Lambda$ is integral. This completes the proof. □

A usual inner product space V over K can be regarded as a K-inner product space (in the sense of Definition 6.1). In this case, the space V is always bounded (letting $A = \mathcal{O}$) because the $\mathcal{O}$-span of a K-basis of V is an $\mathcal{O}$-stable lattice. There is a non-bounded example.

Example 6.24. Let Γ be an infinite cyclic group with generator τ, and let A be the group algebra $\mathcal{O}[\Gamma]$. Then $A_K = \mathcal{O}[\Gamma] \otimes_{\mathcal{O}} K = K[\Gamma]$. Let (V, b) be a hyperbolic plane over K with hyperbolic basis (e_1, e_2) (see Definition 4.11). Suppose that $K[\Gamma]$ acts on V by $\tau.e_1 = \pi e_1$ and $\tau.e_2 = \pi^{-1}e_2$. Then

$$\begin{aligned} b(\tau.e_1, \tau.e_1) &= b(\pi e_1, \pi e_1) = \pi^2 b(e_1, e_1) = 0, \\ b(\tau.e_2, \tau.e_2) &= b(\pi^{-1}e_2, \pi^{-1}e_2) = \pi^{-2} b(e_2, e_2) = 0, \\ b(\tau.e_1, \tau.e_2) &= b(\pi e_1, \pi^{-1}e_2) = b(e_1, e_2) = 1. \end{aligned}$$

These equations mean that τ acts as an isometry, and hence V is a $K[\Gamma]$-inner product space. Suppose that $\operatorname{char} K \neq 2$, and let Λ be a lattice on V. Then Λ contains an anisotropic vector since so does V, say $z = \alpha_1 e_1 + \alpha_2 e_2 \in \Lambda$ ($\alpha_1, \alpha_2 \in K$). Note that $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$ since z is anisotropic. For any $n \in \mathbb{Z}_{>0}$ we have

$$b(\tau^n.z, z) = b(\alpha_1\pi^n e_1 + \alpha_2\pi^{-n}e_2, \alpha_1 e_1 + \alpha_2 e_2) = \alpha_1\alpha_2(\pi^n - \pi^{-n}),$$

and thus

$$v(b(\tau^n.z, z)) = v(\alpha_1) + v(\alpha_2) + v(\pi^n - \pi^{-n}) = v(\alpha_1) + v(\alpha_2) - n.$$

This means that the set $\{v(b(x,y)) \in \mathbb{Z} \mid x, y \in A\Lambda\}$ is not bounded below. Therefore $A\Lambda$ is not a lattice by Proposition 6.23 (i), and in particular $A\Lambda \neq \Lambda$. This implies that V is not bounded.

We now introduce a homomorphism $W^{\mathrm{b}}_{A_K}(K) \to WT_A(\mathcal{O})$. Let $V = (V, b)$ be a bounded A_K-inner product space, and Λ be an A-stable integral lattice on V. Then, the dual lattice $\Lambda^\vee$ is also A-stable, and the discriminant module $(\Lambda^\vee/\Lambda, \bar{b})$ becomes an A-torsion product module naturally.

Proposition 6.25. *For two A-stable integral lattices Λ_1, Λ_2 on V, we have $[\Lambda_1^\vee/\Lambda_1] = [\Lambda_2^\vee/\Lambda_2]$ in $WT_A(\mathcal{O})$.*

Proof. Set $\Lambda_0 = \Lambda_1 \cap \Lambda_2$. Then Λ_0 is an A-stable integral lattice on V by Theorem 5.2. We show that $[\Lambda_0^\vee/\Lambda_0] = [\Lambda_1^\vee/\Lambda_1]$. Put $U = \Lambda_1/\Lambda_0 \subset \Lambda_0^\vee/\Lambda_0$. Then

$$U^\perp = \{\bar{y} \in \Lambda_0^\vee/\Lambda_0 \mid \bar{b}(\bar{y}, \Lambda_1/\Lambda_0) = 0\} = \overline{\{y \in \Lambda_0^\vee \mid b(y, \Lambda_1) \subset \mathcal{O}\}} = \Lambda_1^\vee/\Lambda_0.$$

Thus

$$[\Lambda_0^\vee/\Lambda_0] = [U^\perp/U] = [(\Lambda_1^\vee/\Lambda_0)/(\Lambda_1/\Lambda_0)] = [\Lambda_1^\vee/\Lambda_1],$$

where the first equality follows from Proposition 6.17 (ii). Similarly, we have $[\Lambda_0^\vee/\Lambda_0] = [\Lambda_2^\vee/\Lambda_2]$. Therefore $[\Lambda_1^\vee/\Lambda_1] = [\Lambda_2^\vee/\Lambda_2]$ in $WT_A(\mathcal{O})$. □

This proposition means that the Witt class of the A-torsion product module $\Lambda^\vee/\Lambda$ does not depend on the choice of Λ. Thus, sending V to $[\Lambda^\vee/\Lambda] \in WT_A(\mathcal{O})$ gives rise to a monoid homomorphism $\mathcal{M}^{\mathrm{b}}_{A_K} \to WT_A(\mathcal{O})$, where $\mathcal{M}^{\mathrm{b}}_{A_K}$ is the submonoid of $\mathcal{M}_{A_K}$ consisting of isomorphism classes represented by bounded spaces. We show that this monoid homomorphism factors through $W^{\mathrm{b}}_{A_K}(K) \subset W_{A_K}(K)$.

Lemma 6.26. *Let (V, b) be an inner product space over K. For any $\mathcal{O}$-submodule M in V, we define $M^\vee := \{y \in V \mid b(y, x) \in \mathcal{O} \text{ for all } x \in M\}$. Let M, M' be $\mathcal{O}$-submodules in V, and assume that they are expressed as $M = W \oplus \Lambda$, $M' = W' \oplus \Lambda'$, where W, W' are K-subspaces and Λ, Λ' are finitely generated $\mathcal{O}$-submodules in V.*[†]

(i) *If M is a K-subspace of V then $M^\vee = M^\perp$.*

(ii) $M^{\vee\vee} = M$.

(iii) $(M + M')^\vee = M^\vee \cap (M')^\vee$.

(iv) $(M \cap M')^\vee = M^\vee + (M')^\vee$.

[†]One can show that any $\mathcal{O}$-submodule in V can be expressed this way.

Proof. (i). It is clear that $M^\perp \subset M^\vee$. Suppose that M is a K-subspace of V, and let $y \in M^\vee$. Then, for any $\alpha \in K$ we have

$$\alpha b(y, M) = b(y, \alpha M) = b(y, M) \subset \mathcal{O}.$$

This implies that $b(y, M) = 0$, and we get $M^\vee \subset M^\perp$.

(ii). Let $e_1, \dots, e_k$ be a K-basis of W, and $e_{k+1}, \dots, e_l$ an $\mathcal{O}$-basis of Λ. Then $e_1, \dots, e_l$ are linearly independent over K, and there exist vectors $e_{l+1}, \dots, e_d$ such that $e_1, \dots, e_d$ is a K-basis of V. Let $e_1^\vee, \dots, e_d^\vee$ denote the dual basis of $e_1, \dots, e_d$ with respect to b. Then, we have

$$M^\vee = \mathcal{O}e_{k+1} + \cdots + \mathcal{O}e_l + Ke_{l+1} + \cdots + Ke_d,$$

and similarly

$$M^{\vee\vee} = Ke_1 + \cdots + Ke_k + \mathcal{O}e_{k+1} + \cdots + \mathcal{O}e_l = M.$$

This shows the assertion (ii).

(iii). Note that the operation $\bullet^\vee$ reverses inclusion. Then, we get $(M + M')^\vee \subset M^\vee, (M')^\vee$, and hence $(M + M')^\vee \subset M^\vee \cap (M')^\vee$. Let $y \in M^\vee \cap (M')^\vee$. For any $x \in M$ and $x' \in M'$ we have $b(y, x + x') = b(y, x) + b(y, x') \in \mathcal{O}$. Hence $M^\vee \cap (M')^\vee \subset (M + M')^\vee$.

(iv). By the assertions (ii) and (iii), we have

$$M^\vee + (M')^\vee = (M^\vee + (M')^\vee)^{\vee\vee} = (M^{\vee\vee} \cap (M')^{\vee\vee})^\vee = (M \cap M')^\vee$$

as required. □

Proposition 6.27. *If (V, b) is neutral, then so is $(\Lambda^\vee/\Lambda, \bar{b})$.*

Proof. Let $X \subset V$ be a lagrangian. Set $U := X \cap \Lambda^\vee$ and write $\overline{U}$ for its image under the natural surjection $\Lambda^\vee \to \Lambda^\vee/\Lambda$. We show that $\overline{U}$ is a lagrangian, that is, $\overline{U}^\perp = \overline{U}$ in $\Lambda^\vee/\Lambda$. The inclusion $\overline{U} \subset \overline{U}^\perp$ follows from $X \subset X^\perp$. Take an element $\bar{z}$ of $\overline{U}^\perp$ where $z \in \Lambda^\vee$. Then $b(z, U) \subset \mathcal{O}$, or equivalently, z is in $U^\vee$. On the other hand, we have

$$U^\vee = (X \cap \Lambda^\vee)^\vee = X^\vee + \Lambda^{\vee\vee} = X^\perp + \Lambda = X + \Lambda$$

by Lemma 6.26. Thus z can be expressed as $z = x + y$ for some $x \in X$ and $y \in \Lambda$. Then $x = z - y \in \Lambda^\vee$, and $\bar{z} = \bar{x} \in \overline{X \cap \Lambda^\vee} = \overline{U}$. This shows that $\overline{U}^\perp \subset \overline{U}$, and the proof is complete. □

This proposition shows that the monoid homomorphism $\mathcal{M}^{\mathrm{b}}_{A_K} \to WT_A(\mathcal{O})$, $V \mapsto [\Lambda^\vee/\Lambda]$ factors through $W^{\mathrm{b}}_{A_K}(K)$. The induced group homomorphism $[V] \mapsto [\Lambda^\vee/\Lambda]$ is denoted by $\widetilde{\partial} : W^{\mathrm{b}}_{A_K}(K) \to WT_A(\mathcal{O})$. We show that V contains an A-stable unimodular lattice if and only if $\widetilde{\partial}[V, b] = 0$. As in Proposition 5.17, we have:

Lemma 6.28. *Let (V, b) be a bounded A_K-inner product space, and Λ an A-stable integral lattice on V. Sending an A-stable overlattice Λ' of Λ to the A_κ-submodule $\Lambda'/\Lambda \subset \Lambda^\vee/\Lambda$ gives rise to a one-to-one correspondence between the A-stable overlattices of Λ and the totally isotropic A_κ-submodules of $(\Lambda^\vee/\Lambda, \bar{b})$.* □

Theorem 6.29. *A bounded A_K-inner product space (V, b) contains an A-stable unimodular lattice if and only if $\widetilde{\partial}[V, b] = 0$.*

Proof. If V contains an A-stable unimodular lattice Λ then $\widetilde{\partial}[V,b] = [\Lambda^\vee/\Lambda, \bar{b}] = 0$. Suppose that $\widetilde{\partial}[V,b] = 0$, and take a maximal A-stable integral lattice Λ on V. Note that $(\Lambda^\vee/\Lambda, \bar{b})$ is neutral since $[\Lambda^\vee/\Lambda, \bar{b}] = \widetilde{\partial}[V,b] = 0$. We show that Λ is unimodular. Suppose to the contrary that Λ were not unimodular. Then $(\Lambda^\vee/\Lambda, \bar{b})$ would have a non-trivial lagrangian U since it is neutral. Because the lagrangian U is totally isotropic, there exists an A-stable overlattice of Λ by Lemma 6.28. However, this contradicts the maximality of Λ. Therefore Λ is unimodular. This completes the proof. □

Definition 6.30. Let $\theta : WT_A(\mathcal{O}) \to W_{A_\kappa}(\kappa)$ denote the isomorphism in Theorem 6.21. The composition $\theta \circ \widetilde{\partial} : W_{A_K}(K) \to W_{A_\kappa}(\kappa)$ is called the *residue homomorphism* and denoted by ∂.

We remark that the residue homomorphism depends on the choice of π since so does $\theta : WT_A(\mathcal{O}) \to W_{A_\kappa}(\kappa)$, but it is independent whether $\partial[V,b]$ is zero or not.

Lemma 6.31. *Any bounded A_K-inner product space contains an A-stable almost unimodular lattice.*

Proof. Let V be a bounded A_K-inner product space, and let Λ be a maximal A-stable integral lattice on V. We show that Λ is almost unimodular. It is sufficient to prove that the exponent of the discriminant module $\Lambda^\vee/\Lambda$ is at most 1, that is, $\pi(\Lambda^\vee/\Lambda) = 0$; because it means that $\pi\Lambda^\vee \subset \Lambda$. Suppose that the exponent n of $\Lambda^\vee/\Lambda$ were greater than 1. Then $U := \pi^{n-1}(\Lambda^\vee/\Lambda)$ is a nonzero totally isotropic A-submodule by Lemma 6.19 (i), and there would exist the A-stable overlattice corresponding U by Lemma 6.28. This contradicts the maximality of Λ. Hence the exponent of $\Lambda^\vee/\Lambda$ is at most 1, and the proof is complete. □

We conclude this subsection with the following theorem, which summarizes the discussion so far.

Theorem 6.32. *Let (V,b) be a bounded A_K-inner product over K. Then V contains an A-stable almost unimodular lattice Λ, and the image of $[V,b]$ under the residue homomorphism $\partial : W^{\mathrm{b}}_{A_K}(K) \to W_{A_\kappa}(\kappa)$ is given by $[\Lambda^\vee/\Lambda, \pi\bar{b}]$. The space (V,b) contains an A-stable unimodular lattice if and only if $\partial[V,b] = 0$ in $W_{A_\kappa}(\kappa)$.*

Proof. By Lemma 6.31, there exists an A-stable almost unimodular lattice Λ on (V,b). The discriminant module $(\Lambda^\vee/\Lambda, \bar{b})$ has exponent at most 1, and $\partial[V,b] = \theta[\Lambda^\vee/\Lambda, \bar{b}] = [\Lambda^\vee/\Lambda, \pi\bar{b}]$. Since $\theta : WT_A(\mathcal{O}) \to W_{A_\kappa}(\kappa)$ is an isomorphism, $\partial[V,b] = 0$ if and only if $\widetilde{\partial}[V,b] = 0$. So, the last assertion follows from Theorem 6.29. □

6.4 Dimensions and discriminants

Let K be an arbitrary field, and A a K-algebra with K-linear involution as in §6.1. Let $\omega \in W_A(K)$ be a Witt class, and (V,b) an A-inner product space representing ω. Then, the dimension $\dim(V)$ modulo 2 is independent of the choice of the representative (V,b) since every neutral space has even dimension. We refer to the value $\dim(V) + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$ as the *dimension* of ω (modulo 2), and write $\dim(\omega)$. We also want to define the determinant of ω, but $\det(b)$ depends on the choose of the representative (V,b). For example, let us consider the case where $A = K$ and -1 is not a square of K. In this case, the hyperbolic plane $\mathbb{H}_K$ is neutral, and thus $(V,b) \oplus \mathbb{H}_K \sim (V,b)$. However $\det((V,b) \oplus \mathbb{H}_K) = \det(b)\det(\mathbb{H}_K) = -\det(b) \neq \det(b)$. To avoid this problem, we introduce the discriminant for an inner product space.

Definition 6.33. Let (V,b) be an inner product space over K of dimension d. The *discriminant* of b, denoted $\mathrm{disc}(b)$, is defined to be $(-1)^{d(d-1)/2}\det(b) \in K^\times/K^{\times 2}$. If the dimension d is even, say $2n$, then $\mathrm{disc}(b) = (-1)^n \det(b)$.

We remark that the equality $\mathrm{disc}(b \oplus b') = \mathrm{disc}(b) \cdot \mathrm{disc}(b')$ does not hold for inner products b, b' in general. However, a short calculation shows that this equality holds if $\dim(b)$ or $\dim(b')$ is even. Moreover, if an inner product space (V, b) over K contains a subspace X with $X = X^\perp$ (i.e., if V is neutral as a K-inner product space), then $\mathrm{disc}(b) = 1$. Indeed, letting $e_1, \ldots, e_{2n}$ be a basis of V such that $e_1, \ldots, e_n$ is a basis of X, then the Gram matrix with respect to this basis is of the form

$$G = \begin{pmatrix} O & A \\ {}^tA & B \end{pmatrix},$$

where $A, B \in M_n(K)$ and A is nondegenerate. Hence

$$\mathrm{disc}(b) = (-1)^n \det(G) = (-1)^n \cdot (-1)^n \det(A) \det({}^tA) = 1$$

in $K^\times / K^{\times 2}$.

Definition 6.34. Let A be a K-algebra with K-linear involution, and $\omega \in W_A(K)$ a Witt class. The *discriminant* of ω, denoted $\mathrm{disc}(\omega)$, is the discriminant of its representative. This is independent of the choice of the representative.

We conclude this subsection with a relation between these invariants and the residue homomorphism defined in Definition 6.30.

Proposition 6.35. *As in* §6.3, *suppose that K is a discrete valuation field, with discrete valuation v, valuation ring $\mathcal{O}$, and residue field κ. Let A be an $\mathcal{O}$-algebra with $\mathcal{O}$-linear involution, and (V, b) a bounded A_K-inner product space. Then* $\dim_\kappa \partial[V, b] \equiv v(\mathrm{disc}(b)) \bmod 2$.

Proof. By Lemma 6.31, there exists an A-stable almost unimodular lattice Λ on V. Let G be a Gram matrix of Λ, and let $\pi^{i_1}, \ldots, \pi^{i_d}$ be the invariant factors of G. Then $\Lambda^\vee/\Lambda \cong \mathcal{O}/\pi^{i_1}\mathcal{O} \oplus \cdots \oplus \mathcal{O}/\pi^{i_d}\mathcal{O}$ by Proposition 5.15. Furthermore $\Lambda^\vee/\Lambda$ has exponent at most 1 since Λ is almost unimodular. Thus $i_1, \ldots, i_d$ must be 0 or 1. Let r be the number of 1's in $i_1, \ldots, i_d$. Then $\Lambda^\vee/\Lambda \cong (\mathcal{O}/\pi\mathcal{O})^{\oplus r}$, and $\dim_\kappa \partial[V, b] \equiv \dim_\kappa(\Lambda^\vee/\Lambda) \equiv r \bmod 2$. On the other hand, we have

$$v(\mathrm{disc}(b)) \equiv v(\det(G)) = v(\pi^{i_1} \cdots \pi^{i_d}) = v(\pi^r) = r \mod 2.$$

This completes the proof. □

6.5 Usual Witt groups of finite fields

This subsection gives the structures of usual Witt groups of finite fields. Here, the *usual* Witt group of a field K means the Witt group for K-inner product spaces. It is denoted by $W(K)$ instead of $W_K(K)$.

Lemma 6.36. *Let κ be a finite field of characteristic not* 2.

(i) *Let (V, b) be an inner product space over κ. If* $\dim V \geq 3$ *then (V, b) is isotropic.*

(ii) *Any Witt class $\omega \in W(\kappa)$ can be represented by an inner product space of dimension at most* 2.

Proof. (i). It suffices to show that every 3-dimensional inner product space is isotropic. Let (V, b) be a 3-dimensional inner product space, and let $\epsilon \in \kappa^\times$ be a non-square element. Then $(V, b) \cong \langle 1 \rangle_\kappa^{\oplus 3}$ or $\langle 1 \rangle_\kappa^{\oplus 2} \oplus \langle \epsilon \rangle_\kappa$ by Theorem 4.38. On the other hand, the 2-dimensional inner product space $\langle 1 \rangle_\kappa^{\oplus 2}$ represents -1 and $-\epsilon$ by Lemma 4.37. Therefore (V, b) is isotropic.

(ii). Let $\omega \in W(\kappa)$ be a Witt class, and V its representative. If $\dim V \leq 2$ then nothing to prove. Suppose that $\dim V \geq 3$. Then there exists a nonzero isotropic vector u by the assertion

(i). Let U denote the one-dimensional subspace $\kappa u \subset V$. Then $U \subset U^\perp$, and $[V] = [U^\perp/U]$ by Lemma 6.9. Since the dimension of $U^\perp/U$ is less than that of V, an induction on dimension shows that V is Witt equivalent to an inner product space of dimension at most 2. The proof is complete. □

Remark 6.37. Lemma 6.36 is also true when $\operatorname{char}\kappa = 2$, although we do not need the case.

Theorem 6.38. *Let κ be a finite field.*

(i) *If $\operatorname{char}\kappa = 2$ then sending $\omega \in W(\kappa)$ to $\dim\omega \bmod 2 \in \mathbb{Z}/2\mathbb{Z}$ gives an isomorphism $W(\kappa) \to \mathbb{Z}/2\mathbb{Z}$.*

(ii) *Suppose that $\operatorname{char}\kappa \neq 2$. Then any class of $W(\kappa)$ is uniquely determined by its dimension (mod 2) and discriminant. In particular, a class $\omega \in W(\kappa)$ is the trivial class if and only if $\dim\omega \equiv 0 \bmod 2$ and $\operatorname{disc}\omega = 1$ in $\kappa^\times/\kappa^{\times 2}$. Moreover, we have*

$$W(\kappa) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } \#\kappa \equiv 1 \bmod 4 \\ \mathbb{Z}/4\mathbb{Z} & \text{if } \#\kappa \equiv 3 \bmod 4. \end{cases}$$

Proof. (i). Let (V, b) be an inner product space over κ. By Theorem 4.36, there exist non-negative integers m and n such that $(V, b) \cong \langle 1\rangle_\kappa^{\oplus m} \oplus \mathbb{H}_\kappa^{\oplus n}$. Since the hyperbolic plane $\mathbb{H}_\kappa$ is neutral, we have $[V] = \langle 1\rangle_\kappa^{\oplus m}$. Moreover $\langle 1\rangle_\kappa^{\oplus 2}$ is neutral. Indeed, if e_1, e_2 is an orthogonal basis of $\langle 1\rangle_\kappa^{\oplus 2}$ with self-inner products are both 1, then the one-dimensional subspace $\kappa(e_1 + e_2)$ is a lagrangian. Hence, we obtain

$$[V, b] = \begin{cases} 0 & \text{if } m \text{ is even} \\ [\langle 1\rangle_\kappa] & \text{if } m \text{ is odd.} \end{cases}$$

Since $\dim V \equiv m \bmod 2$, we arrive at the assertion.

(ii). Any Witt class can be represented by an inner product space of dimension at most 2 by Lemma 6.36 (ii). Hence, by Theorem 4.38, the Witt group $W(\kappa)$ consists of the following at most 5 elements:

$$0,\ [\langle 1\rangle_\kappa],\ [\langle \epsilon\rangle_\kappa],\ [\langle 1, 1\rangle_\kappa],\ [\langle 1, \epsilon\rangle_\kappa],$$

where $\epsilon \in \kappa^\times$ is a non-square element. Furthermore, it can be seen that there are at least 4 distinct elements by considering their dimensions and discriminants.

Suppose that $\#\kappa \equiv 1 \bmod 4$. Then -1 is a square in κ (see Corollary 2.3). Thus $[\langle 1, 1\rangle_\kappa] = [\langle 1, -1\rangle_\kappa] = 0$, which means that

$$W(\kappa) = \{0,\ [\langle 1\rangle_\kappa],\ [\langle \epsilon\rangle_\kappa],\ [\langle 1, \epsilon\rangle_\kappa]\}.$$

This shows that any class is uniquely determined by its dimension and discriminant. Moreover $W(\kappa) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ because any class has order at most 2.

Suppose that $\#\kappa \equiv 3 \bmod 4$. Then -1 is not a square in κ. Thus $[\langle 1, \epsilon\rangle_\kappa] = [\langle 1, -1\rangle_\kappa] = 0$, which means that

$$W(\kappa) = \{0,\ [\langle 1\rangle_\kappa],\ [\langle \epsilon\rangle_\kappa],\ [\langle 1, 1\rangle_\kappa]\}.$$

This shows that any class is uniquely determined by its dimension and discriminant. Moreover $W(\kappa) \cong \mathbb{Z}/4\mathbb{Z}$ because $[\langle 1\rangle_\kappa]$ has order 4. This completes the proof. □

7 Isometries of inner product spaces

We here study isometries of inner product spaces, in particular their characteristic polynomials. We refer to [4] and [29]. The letter K stands for a field throughout this section.

7.1 Symmetric polynomials

Definition 7.1. Let $F(X) \in K[X]$ be a polynomial. We define $F^\vee(X) \in K[X]$ by

$$F^\vee(X) := X^{\deg F} F(X^{-1}).$$

If $F(X) = \sum_{i=0}^n a_i X^i$ $(a_n \neq 0)$ then $F^\vee(X) = \sum_{i=0}^n a_i X^{n-i} = \sum_{i=0}^n a_{n-i} X^i$. For $\epsilon \in \{1, -1\}$, we say that F is *ϵ-symmetric* if $F^\vee(X) = \epsilon F(X)$.

Most of polynomials treated in this thesis are monic and have nonzero constant terms. We may sometimes assume that a factor of a monic polynomial is monic without mentioning.

Definition 7.2. Let $F(X) \in K[X]$ be a monic polynomial with $F(0) \neq 0$. We define a monic polynomial $F^*(X) \in K[X]$ by

$$F^*(X) := F(0)^{-1} F^\vee(X) = F(0)^{-1} X^{\deg F} F(X^{-1}).$$

If $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ $(a_0 \neq 0)$ then

$$F^*(X) = a_0^{-1}(a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n).$$

We say that F is *$*$-symmetric* if $F^* = F$.

It will be turn out in the next subsection that the characteristic polynomial of any isometry of an inner product space is $*$-symmetric. The following are basic properties of $*$.

Lemma 7.3. *Let $F, G \in K[X]$ be monic polynomials with $F(0) \neq 0$ and $G(0) \neq 0$.*

(i) $(F^*)^* = F$.

(ii) $(FG)^* = F^* G^*$.

(iii) *F is irreducible if and only if F^* is irreducible.*

(iv) *If two of three polynomials F, G, FG are $*$-symmetric, then so is the rest one.*

Proof. Let us write $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. Then

$$\begin{aligned}(F^*(X))^* &= \left(X^n + \frac{a_1}{a_0}X^{n-1} + \cdots + \frac{a_{n-1}}{a_0}X + \frac{1}{a_0}\right)^* \\ &= a_0\left(\frac{1}{a_0}X^n + \frac{a_{n-1}}{a_0}X^{n-1} + \cdots + \frac{a_1}{a_0}X + 1\right) \\ &= F(X),\end{aligned}$$

which shows the assertion (i). Furthermore, we have

$$(FG)^* = (F(0)G(0))^{-1} F^\vee G^\vee = F(0)^{-1} F^\vee \cdot G(0)^{-1} G^\vee = F^* G^*,$$

which is the assertion (ii). The assertions (iii) and (iv) follow from (i) and (ii). □

Lemma 7.4. *A monic polynomial F with $F(0) \neq 0$ is $*$-symmetric if and only if F is $+1$-symmetric or -1-symmetric.*

Proof. Let $F \in K[X]$ be a monic polynomial with $F(0) \neq 0$. We remark that $F^\vee(0) = 1$ since F is monic. If F is ϵ-symmetric ($\epsilon \in \{1, -1\}$) then $F(0) = \epsilon F^\vee(0) = \epsilon$. Therefore

$$F^*(X) = F(0)^{-1}F^\vee(X) = \epsilon^{-1}\epsilon F(X) = F(X),$$

which means that F is $*$-symmetric. Conversely, if F is $*$-symmetric then

$$F(0) = F^*(0) = F(0)^{-1}F^\vee(0) = F(0)^{-1},$$

which means that $F(0) = 1$ or -1. Since $F^\vee(X) = F(0)F^*(X) = F(0)F(X)$, the polynomial F is $F(0)$-symmetric. This completes the proof. □

Note that there is no difference between $+1$-symmetric and -1-symmetric when the characteristic of K is 2.

Lemma 7.5. *Let $F \in K[X]$ be a polynomial.*

(i) *If F is $+1$-symmetric and has odd degree then $(X + 1) \mid F$.*

(ii) *If $\mathrm{char}(K) \neq 2$ and F is -1-symmetric then $(X - 1) \mid F$.*

Proof. (i). Suppose that F is $+1$-symmetric and has odd degree. Then F can be written as

$$F(X) = a_0 + a_1X + \cdots + a_lX^l + a_lX^{l+1} + \cdots + a_1X^{2l} + a_0X^{2l+1}$$

where $a_0, \ldots, a_l \in K$. Thus $F(-1) = 0$, which means that $(X + 1) \mid F$.

(ii). Suppose that $\mathrm{char}(K) \neq 2$ and F is -1-symmetric. Then $F(1) = -F^\vee(1) = -F(1)$, which implies that $F(1) = 0$ since $\mathrm{char}(K) \neq 2$. Thus we get $(X - 1) \mid F$. □

This lemma implies that every $*$-symmetric irreducible polynomial other than $X - 1$ and $X + 1$ is $+1$-symmetric and has even degree.

Definition 7.6. We say that a $*$-symmetric polynomial $f \in K[X]$ is of

- *type* 0 if f is a product of powers of $(X - 1)$ and of $(X + 1)$;
- *type* 1 if f is a product of $+1$-symmetric irreducible monic polynomials of even degrees;
- *type* 2 if f is a product of polynomials of the form gg^*, where g is monic, irreducible and $g^* \neq g$.

Note that if f is of type 2 then f is $+1$-symmetric and of even degree as well as the type 1 case. For a monic polynomial $F \in K[X]$, we write $I_i(F; K)$ for the set of its irreducible factors of type i over K ($i = 0, 1$), and define $I(F; K) := I_0(F; K) \cup I_1(F; K)$. The symbol $I_2(F; K)$ denotes the set of non-$*$-symmetric irreducible factors of F in $K[X]$.

Proposition 7.7. *Let $F \in K[X]$ be a $*$-symmetric polynomial. For any irreducible monic polynomial $g \in K[X]$, the multiplicity of g^* in F is equal to that of g. As a result, F can be expressed as*

$$F = \prod_{f \in I_0(F;K)} f^{m_f} \times \prod_{f \in I_1(F;K)} f^{m_f} \times \prod_{\{g, g^*\} \subset I_2(F;K)} (gg^*)^{m_g},$$

where m_f is the multiplicity of $f \in K[X]$ in F.

Proof. Let g be an irreducible monic polynomial. If $g = g^*$ then the assertion is clear. Suppose that $g \neq g^*$, and let m_g, m_{g^*} be the multiplicities of g, g^* respectively. We may assume that $m_{g^*} \geq m_g$ since $g^{**} = g$. Because g and g^* have no common factor, we can write

$$F = g^{m_g}(g^*)^{m_{g^*}}H = (gg^*)^{m_g}(g^*)^{m_{g^*}-m_g}H$$

for some monic polynomial $H \in K[X]$. Since F and $(gg^*)^{m_g}$ are $*$-symmetric, it follows from Lemma 7.3 (iv) that $(g^*)^{m_{g^*}-m_g}H$ is also $*$-symmetric, i.e., $g^{m_{g^*}-m_g}H^* = (g^*)^{m_{g^*}-m_g}H$. In particular $g^{m_{g^*}-m_g} \mid (g^*)^{m_{g^*}-m_g}H$. However, both g^* and H are coprime to g. Hence $m_{g^*} - m_g = 0$. This completes the proof. □

Definition 7.8. Let $F \in K[X]$ be a $*$-symmetric polynomial. For each $i = 0, 1, 2$, the factor $F_i := \prod_{f \in I_i(F;K)} f^{m_f}$ of F is referred to as the *type i component* of F in $K[X]$.

Let $F \in K[X]$ be a $*$-symmetric polynomial. It is clear that F_0 and F_1 are $*$-symmetric polynomials of type 0 and of type 1 respectively. Furthermore, we have $F_2 = \prod_{\{g,g^*\} \subset I_2(F;K)} (gg^*)^{m_g}$ by Proposition 7.7, and it is actually a $*$-symmetric polynomial of type 2. The factorization $F = F_0F_1F_2$ depends on the field being considered. For example, the polynomial $X^2 + 1$ is irreducible and of type 1 in $\mathbb{Q}[X]$, but it is factorized as $X^2 + 1 = (X - \sqrt{-1})(X + \sqrt{-1})$ and of type 2 in $\mathbb{Q}(\sqrt{-1})[X]$. On the other hand, $X - 1$ and $X + 1$ are of type 0 over any field. It can be seen that if a $*$-symmetric polynomial $F \in K[X]$ is of type 2 over K then it is also type 2 over any extension field of K.

We can characterize $*$-symmetric polynomials in terms of their roots.

Proposition 7.9. *Let $F \in K[X]$ be a monic polynomial with $F(0) \neq 0$, and let $\overline{K}$ be the algebraic closure of K. Then F is $*$-symmetric if and only if α and α^{-1} have the same multiplicity as roots of F for all $\alpha \in \overline{K}$.*

Proof. We remark that $(X - \alpha)^* = (X - \alpha^{-1})$ for any $\alpha \in \overline{K}$. Then, the assertion follows from Proposition 7.7. □

A $+1$-symmetric polynomial of even degree can be expressed by using a polynomial of half degree.

Proposition 7.10. *Let $F \in K[X]$ be a $+1$-symmetric polynomial of even degree $2n$. There exists a unique polynomial H of degree n such that $F(X) = X^nH(X + X^{-1})$. Moreover, if F is monic then so does H, and if the coefficients of F are in a subring R of K then those of H are also in R.*

Proof. Let $H_w(Y) = w_n + w_{n-1}Y + \cdots + w_0Y^n \in K[Y]$ be a polynomial of degree n, where we consider the coefficients $w = (w_0, \ldots, w_n)$ to be variables. Then $F'(X) := X^nH_w(X + X^{-1})$ is a $+1$-symmetric polynomial of degree $2n$, and we can write $F'(X) = a'_0 + a'_1X + \cdots + a'_{n-1}X^{n-1} + a'_nX^n + a'_{n-1}X^{n+1} + \cdots + a'_0X^{2n}$. Moreover, we have

$$\begin{aligned} F'(X) &= X^n \left(\sum_{l=0}^{n} w_l \, (X + X^{-1})^{n-l} \right) \\ &= \sum_{l=0}^{n} \left(w_l \, X^n \sum_{j=0}^{n-l} \left(\binom{n-l}{j} X^j X^{-(n-l-j)} \right) \right) \\ &= \sum_{l=0}^{n} \left(w_l \sum_{j=0}^{n-l} \binom{n-l}{j} X^{l+2j} \right). \end{aligned}$$

Thus ${}^t(a'_0,\dots,a'_n) = C\,{}^t(w_0,\dots,w_n)$, where C is an upper triangular matrix such that its entries are in the image of $\mathbb{Z}\to K$ and the diagonal entries are all 1. Note that $\det(C)=1$.

Now we write $F(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n + a_{n-1}X^{n+1} + \cdots + a_0X^{2n}$, and define $b = (b_0,\dots,b_n) \in K^{n+1}$ to be a unique solution of ${}^t(a_0,\dots,a_n) = C\,{}^t(w_0,\dots,w_n)$. Then $H := H_b$ is a polynomial of degree n such that $F(X) = X^nH(X+X^{-1})$, and such a polynomial H is unique by the uniqueness of b.

Moreover, by the form of the matrix C, if $a_0 = 1$ then $b_0 = 1$. In other words, if F is monic then so does H. Let R be a subring of K, and suppose that $a_0,\dots,a_n \in R$. Since $\det(C)=1$ and the entries of C belong to the image of $\mathbb{Z}\to K$ and in particular to R, the equation system ${}^t(a_0,\dots,a_n) = C\,{}^t(w_0,\dots,w_n)$ can be solved over R. Hence, the coefficients of H are in R if those of F are in R. This completes the proof. □

Definition 7.11. In the situation of Proposition 7.10, the polynomial H is call the *trace polynomial* of F.

7.2 $K[\Gamma]$-inner product spaces

Let (V,b) be an inner product space over K, t an isometry of V, and $F\in K[X]$ the characteristic polynomial of t. For a polynomial $f\in K[X]$, we define

$$V(f;t) := \{v\in V \mid f(t)^N.v = 0 \quad \text{for some } N\in\mathbb{Z}_{\geq 0}\}.$$

Note that each $V(f;t)$ is t-stable, i.e., $t.V(f;t)\subset V(f;t)$. For each factor f of F, the symbol m_f denotes the multiplicity of f in F. Linear algebra shows the following lemma, which is independently of the inner product b. The proof is omitted.

Lemma 7.12. *If $f_1,\dots,f_l\in K[X]$ are pairwise coprime monic polynomials such that $F = f_1\cdots f_l$, then V admits the direct sum decomposition $V=\bigoplus_{i=1}^l V(f_i;t)$ as a K-vector space. For an irreducible factor f of F we have $V(f;t) = \{v\in V\mid f(t)^{m_f}.v=0\}$ and $\dim V(f;t) = m_f\deg f$.* □

In taking account of the inner product, the following lemma holds.

Lemma 7.13. *Let f and g be irreducible factors of F. If $f^*\neq g$ then $V(f;t)$ and $V(g;t)$ are orthogonal.*

Proof. Assume that $f^*\neq g$. We claim that the linear map $v\mapsto f(t^{-1}).v$ is an automorphism of $V(g;t)$. To show this, let $v\in V(g;t)$. We have $f(t^{-1}).v\in V(g;t)$ because $g(t)^N.f(t^{-1}).v = f(t^{-1}).g(t)^N.v = 0$ for sufficiently large $N\in\mathbb{Z}_{\geq 0}$. Moreover t and $f^*(t)$ are invertible on $V(g;t)$ since both X and $f^*(X)$ are coprime to $g(X)$. Thus, the operator $f(t^{-1}) = f(0)t^{-\deg f}f^*(t)$ is also invertible on $V(g;t)$. This shows that $v\mapsto f(t^{-1}).v$ is an automorphism of $V(g;t)$.

Let $u\in V(f;t)$ and $v\in V(g;t)$. By the claim proved now, the vector v can be expressed as $v = f(t^{-1})^{m_f}.v'$ for some $v'\in V(g;t)$. Then

$$b(u,v) = b(u, f(t^{-1})^{m_f}.v') = b(f(t)^{m_f}.u, v') = b(0,v') = 0,$$

which means that $V(f;t)$ and $V(g;t)$ are orthogonal. □

The following theorem is fundamental in considering an isometry.

Theorem 7.14. *Let t be an isometry of an inner product space (V,b), and let $F\in K[X]$ denote the characteristic polynomial of t. Then F is $*$-symmetric, and V admits the following orthogonal direct sum decomposition:*

$$V = \bigoplus_{f\in I(F;K)} V(f;t) \oplus \bigoplus_{\{g,g^*\}\subset I_2(F;K)} V(gg^*;t).$$

Proof. In order to show that F is $*$-symmetric, it is sufficient to show that $m_g = m_{g^*}$ for any irreducible factor g of F. This is clear if $g = g^*$. Suppose that $g \neq g^*$, and set $U := V(g;t) \oplus V(g^*;t)$. If we write $F = g^{m_g}(g^*)^{m_{g^*}}h$ then there is the decomposition $V = U \oplus V(h;t)$ by Lemma 7.12, and it is an orthogonal direct sum by Lemma 7.13. Hence $V(h;t)$ and U must be nondegenerate. Moreover $V(g;t) \subset V(g;t)^\perp$ by Lemma 7.13, and $\dim V(g;t) + \dim V(g;t)^\perp = \dim U$ by Proposition 4.4. These mean that $\dim V(g;t) \leq \dim(U)/2$. Similarly we get $\dim V(g^*;t) \leq \dim(U)/2$. Since we also have $\dim U = \dim V(g;t) + \dim V(g^*;t)$, dimensions $\dim V(g;t)$ and $\dim V(g^*;t)$ are both equal to $\dim(U)/2$. Thus, by Lemma 7.12, we have

$$m_g \deg g = \dim V(g;t) = \dim V(g^*;t) = m_{g^*} \deg g^* = m_{g^*} \deg g,$$

which leads to $m_g = m_{g^*}$. Hence F is $*$-symmetric. Furthermore, any irreducible factor g of F is accompanied with g^*. Therefore, we obtain the desired orthogonal direct sum decomposition by Lemmas 7.12 and 7.13. The proof is complete. □

Considering an inner product space together with an isometry is equivalent to considering a $K[\Gamma]$-inner product space:

Notation 7.15. Throughout this thesis, the symbol Γ denotes an infinite cyclic group. Let τ be a generator of Γ. The group algebra $K[\Gamma]$ has the involution determined by $\tau \mapsto \tau^{-1}$. If (V, b) is an inner product space over K and t is an isometry of (V, b), then the triple (V, b, t) denotes the $K[\Gamma]$-inner product space (V, b, ρ), where $\rho : K[G] \to \mathrm{O}(V, b)$ is the action determined by $\rho(\tau) = t$, see Example 6.2.

Proposition 7.16. *Let t be an isometry of an inner product space (V, b) of even dimension $2n$. Suppose that the characteristic polynomial of t can be written as $(gg^*)^m$ for some non-$*$-symmetric irreducible polynomial g and some integer m. Note that $V = V(gg^*;t) = V(g;t) \oplus V(g^*;t)$. Let $T \in M_n(K)$ be a representation matrix of $t|_{V(g;t)} : V(g;t) \to V(g;t)$, and let B denote the inner product on K^{2n} whose Gram matrix with respect to the standard basis is $\begin{pmatrix} O & \mathrm{Id}_n \\ \mathrm{Id}_n & O \end{pmatrix}$. Then (V, b, t) is isomorphic to*

$$\left(K^{2n}, B, \begin{pmatrix} T & O \\ O & {}^tT^{-1} \end{pmatrix}\right)$$

as $K[\Gamma]$-inner product spaces.

Proof. Take a basis $e_1, \ldots, e_n$ of $V(g;t)$ so that T is the representation matrix of $t|_{V(g;t)} : V(g;t) \to V(g;t)$ with respect to this basis. Since $V(g;t)^\perp = V(g;t)$, we have the exact sequence

$$0 \to V(g;t) \to V \overset{b^*(\cdot)|_{V(g;t)}}{\longrightarrow} V(g;t)^* \to 0$$

by Proposition 4.4. From this, it can be seen that

$$b^*(\cdot\,|_{V(g^*;t)})|_{V(g;t)} : V(g^*;t) \to V(g;t)^*,\ v \mapsto b^*(v)|_{V(g;t)} \quad (v \in V(g^*;t))$$

is surjective, and hence isomorphic since $\dim(V(g^*;t)) = n = \dim(V(g^*;t))$. Thus, there exists a basis $e'_1, \ldots, e'_n$ of $V(g^*;t)$ such that $b^*(e'_i) = \xi_i$ for $i = 1, \ldots, n$, where $\xi_1, \ldots, \xi_n \in V(g;t)^*$ is the dual basis of $e_1, \ldots, e_n$. Then, the Gram matrix of b and representation matrix of t with respect to the basis $e_1, \ldots, e_n, e'_1, \ldots, e'_n$ of V are $\begin{pmatrix} O & \mathrm{Id}_n \\ \mathrm{Id}_n & O \end{pmatrix}$ and $\begin{pmatrix} T & O \\ O & {}^tT^{-1} \end{pmatrix}$ respectively. Therefore, the K-linear isomorphism $V \to K^{2n}$ obtained by fixing the basis $e_1, \ldots, e_n, e'_1, \ldots, e'_n$ gives the desired isomorphism of $K[\Gamma]$-inner product spaces. □

7.3 Semisimple modules associated with polynomial

Let Γ be an infinite cyclic group with generator τ as in Notation 7.15. Let $F \in K[X]$ be a monic polynomial with $F(0) \neq 0$. For a factor f of F, we write m_f for the multiplicity of f in F.

Definition 7.17. We define a K-algebra M by

$$M := \prod_f (K[X]/(f))^{\times m_f} \quad \text{where } f \text{ ranges over all irreducible factors of } F.$$

Let $\alpha : M \to M$ denote the K-linear transformation defined by the multiplication by X. It is a semisimple transformation with characteristic polynomial F, and in particular invertible since $F(0) \neq 0$. Thus M has the $K[\Gamma]$-module structure determined by $\tau \mapsto \alpha$. This $K[\Gamma]$-module M is referred to as the *semisimple $K[\Gamma]$-module associated with F* or just the *associated $K[\Gamma]$-module of F* with transformation α.

Lemma 7.18. *Let V be a finite dimensional K-vector space with a semisimple linear transformation t of characteristic polynomial F. Then V is isomorphic to the associated $K[\Gamma]$-module of F when V is regarded as a $K[\Gamma]$-module by $\tau \mapsto t$.*

Proof. By Lemma 7.12, we can write $V = \oplus_f V(f;t)$ where f ranges over all irreducible factors of F. Let f be an irreducible factor of F. Since t is semisimple, the subspace $V(f;t)$ can be seen as a vector field over $K[X]/(f)$. Furthermore $\dim_{K[X]/(f)} V(f;t) = m_f$ by Lemma 7.12. Thus $V(f;t) \cong (K[X]/(f))^{m_f}$ as $K[\Gamma]$-modules. This completes the proof. □

Our purpose is to know which inner product on the associated $K[\Gamma]$-module M of F makes α an isometry. Note that F must be $*$-symmetric by Theorem 7.14 if M admits such an inner product. We use the following notation in considering the associated $K[\Gamma]$-module of a $*$-symmetric polynomial.

Notation 7.19. Let $F \in K[X]$ be a $*$-symmetric polynomial. For a factor f which is in $I(F;K)$ or of the form gg^* for some $g \in I_2(F;K)$, we write E^f for the K-algebra $K[X]/(f)$, and define $M^f := (E^f)^{\times m_f}$. In this case, the associated $K[\Gamma]$-module M of F can be written as

$$M = \prod_{f \in I(F;K)} M^f \times \prod_{\{g,g^*\} \subset I_2(F;K)} M^{gg^*}, \tag{25}$$

or

$$M = M^+ \times M^- \times \prod_{f \in I_1(F;K)} M^f \times \prod_{\{g,g^*\} \subset I_2(F;K)} M^{gg^*},$$

where $M^\pm := M^{X \mp 1}$. Note that M^f is nothing but the associated $K[\Gamma]$-module of f^{m_f}. We write $\alpha^f \in E^f$ for the image of X under the natural surjection $K[X] \to E^f$. The restriction $\alpha|_{M^f} : M^f \to M^f$ (α is as in Definition 7.17) is the same as the multiplication by α^f. Since f is $*$-symmetric, an involution $\sigma : E^f \to E^f$ is defined by $\alpha^f \mapsto (\alpha^f)^{-1}$. Note that this involution is non-trivial if $f(X)$ is neither $X - 1$ nor $X + 1$. If $f = gg^*$ for some $g \in I_2(F;K)$ then E^f is of type (sp) with this involution (type (sp) is defined in Definition 1.9).

Under the setting in Notation 7.19, the submodule M^f can be written as

$$M^f = \{x \in M \mid f(\alpha).x = 0\}$$

for a factor f which is in $I(F;K)$ or of the form gg^* for some $g \in I_2(F;K)$. Hence, Theorem 7.14 means that the decomposition (25) is an orthogonal direct sum decomposition for any inner

product on M making α an isometry. Therefore, the problem of considering inner products on M making α an isometry can be addressed componentwise.

As for the component $M^{\pm}$, any inner product $b^{\pm}$ makes $\alpha|_{M^{\pm}}$ an isometry since $\alpha|_{M^{\pm}} = \pm\mathrm{id}_{M^{\pm}}$. Let f be a factor of F which is in $I_1(F;K)$ or of the form gg^*, and assume that f is separable. Then, for any hermitian product h on M^f over E^f, the symmetric bilinear form

$$M^f \times M^f \to K,\ (x,y) \mapsto \mathrm{Tr}_{E^f/K} \circ h(x,y)$$

is nondegenerate by Proposition 4.68. Furthermore $\alpha|_{M^f}$ is an isometry with respect to this inner product. Indeed, we have

$$\mathrm{Tr}_{E^f/K} \circ h(\alpha^f x, \alpha^f y) = \mathrm{Tr}_{E^f/K} \circ h(x, \alpha^f \sigma(\alpha^f) y) = \mathrm{Tr}_{E^f/K} \circ h(x,y)$$

for any $x, y \in M^f$. Note that separability of f guarantees that the trace map $\mathrm{Tr}_{E^f/K}$ is surjective (see Corollary 1.7).

Proposition 7.20. *Let F be a $*$-symmetric polynomial and M the associated $K[\Gamma]$-module of F with transformation α. Let f be a factor of F which is in $I_1(F;K)$ or of the form gg^* for some $g \in I_2(F;K)$, and suppose that f is separable. If b^f is an inner product on the K-vector space M^f making α an isometry, then there exists one and only one hermitian form h^f on M^f over E^f such that $b^f = \mathrm{Tr}_{E^f/K} \circ h^f$.*

Proof. Let b (instead of b^f) be an inner product on M^f which makes α an isometry. For $x, y \in M^f$ we define the element $h(x,y)$ of E^f as follows. Let $L : E^f \to K$ be the K-linear map defined by $L(\gamma) = b(\gamma x, y)$ for $\gamma \in E^f$. Since the trace map $\mathrm{Tr}_{E^f/K}$ is surjective, the symmetric bilinear form

$$T : E^f \times E^f \to K,\ (\gamma, \gamma') \mapsto \mathrm{Tr}_{E^f/K}(\gamma\gamma')$$

is nondegenerate, and $T^* : E^f \to \mathrm{Hom}_K(E^f, K)$ is an isomorphism. Thus there exists a unique element $\gamma' \in E^f$ such that $T^*(\gamma) = L$. We define $h(x,y)$ to be the element γ'. In other words, $h(x,y)$ is a unique element satisfying the equation

$$\mathrm{Tr}_{E^f/K}(\gamma\, h(x,y)) = b(\gamma x, y) \qquad (*)$$

for all $\gamma \in E^f$. We now consider the map $h : M^f \times M^f \to E^f$. Taking $\gamma = 1$ in $(*)$, we obtain $b = \mathrm{Tr}_{E^f/K} \circ h$.

Claim 1*: h is E^f-linear in the first variable.* Let $x_1, x_2, y \in M^f$. For any $\gamma \in E^f$ we have

$$\begin{aligned} T(\gamma, h(x_1+x_2, y)) &= b(\gamma(x_1+x_2), y) = b(\gamma x_1, y) + b(\gamma x_2, y) \\ &= T(\gamma, h(x_1,y)) + T(\gamma, h(x_2,y)) = T(\gamma, h(x_1,y) + h(x_2,y)), \end{aligned}$$

which shows that $h(x_1+x_2, y) = h(x_1,y) + h(x_2,y)$ since T is nondegenerate. Furthermore, for any $\gamma, \gamma' \in E^f$ we have

$$T(\gamma, h(\gamma' x_1, y)) = b(\gamma\gamma' x_1, y) = \mathrm{Tr}_{E^f/K}(\gamma\gamma' h(x_1,y)) = T(\gamma, \gamma' h(x_1,y)),$$

which implies that $h(\gamma' x_1, y) = \gamma' h(x_1, y)$. This completes the proof of Claim 1.

Claim 2*: $h(y,x) = \sigma h(x,y)$ for any $x, y \in M^f$.* Let $x_1, x_2, y \in M^f$ and $\gamma \in E^f$. Note that $b(\gamma y, x) = b(y, \sigma(\gamma)x)$ since b makes α an isometry. We have

$$\begin{aligned} T(\gamma, h(y,x)) &= b(\gamma y, x) = b(y, \sigma(\gamma)x) = b(\sigma(\gamma)x, y) = \mathrm{Tr}_{E^f/K}(\sigma(\gamma) h(x,y)) \\ &= \mathrm{Tr}_{E^f/K}(\sigma(\sigma(\gamma)h(x,y))) = \mathrm{Tr}_{E^f/K}(\gamma\, \sigma(h(x,y))) = T(\gamma, \sigma h(x,y)). \end{aligned}$$

This shows that $h(y,x) = \sigma h(x,y)$.

Claims 1 and 2 mean that $h : M^f \times M^f \to E^f$ is a hermitian form. It remains to prove the uniqueness. Let h' be another hermitian form satisfying $b = \mathrm{Tr}_{E^f/K} \circ h'$. Then

$$T(\gamma, h'(x,y)) = \mathrm{Tr}_{E^f/K}(h'(\gamma x, y)) = b(\gamma x, y) = T(\gamma, h(x,y))$$

for any $x, y \in M^f$ and $\gamma \in E^f$. Therefore $h' = h$. The proof is complete. □

7.4 Isometries of inner product spaces over $\mathbb{R}$

In §4.6, we defined an invariant of an inner product space over $\mathbb{R}$ called the index. This subsection gives the definition of the index for an isometry, and study it. We begin by determining the forms of irreducible monic polynomials over $\mathbb{R}$. The symbol $\mathbb{T}$ denotes the unit circle in $\mathbb{C}$.

Proposition 7.21. *Let $h \in \mathbb{R}[X]$ be an irreducible monic polynomial.*

(i) *h is of type 1 if and only if $f(X) = X^2 - (\delta + \delta^{-1})X + 1$ for some $\delta \in \mathbb{T} \setminus \{1, -1\}$.*

(ii) *h is not $*$-symmetric if and only if $h(X) = X - \beta$ for some $\beta \in \mathbb{R} \setminus \{1, -1\}$ or $h(X) = X^2 - (\gamma + \bar{\gamma})X + \gamma\bar{\gamma}$ for some $\gamma \in \mathbb{C} \setminus (\mathbb{T} \cup \mathbb{R})$.*

Proof. An irreducible monic polynomial with real coefficients has one of the following forms:

$$\begin{aligned} &X - 1,\ X + 1, \\ &X^2 - (\delta + \delta^{-1})X + 1 \quad (\delta \in \mathbb{T} \setminus \{1, -1\}), \\ &X - \beta \quad (\beta \in \mathbb{R} \setminus \{1, -1\}), \\ &X^2 - (\gamma + \bar{\gamma})X + \gamma\bar{\gamma} \quad (\gamma \in \mathbb{C} \setminus (\mathbb{T} \cup \mathbb{R})). \end{aligned}$$

The polynomials $X - 1$ and $X + 1$ are of type 0; $X^2 - (\delta + \delta^{-1})X + 1$ is of type 1; and $X - \beta$ and $X^2 - (\gamma + \bar{\gamma})X + \gamma\bar{\gamma}$ are of type 2. Thus the assertions (i) and (ii) hold. □

Corollary 7.22. *Let $F \in \mathbb{R}[X]$ be a $*$-symmetric polynomial, and let $m(F)$ denote the number of roots of F whose absolute values are greater than 1 counted with multiplicity. Then $m(F) = \deg(F_2)/2$, where F_2 is the type 2 component of F in $\mathbb{R}[X]$.*

Proof. By Proposition 7.21, we have $m(F) = m(F_2)$, and F_2 can be expressed as

$$\begin{aligned} F_2(X) &= \prod_{i=1}^{k} (X - \beta_i)(X - \beta_i)^* \times \prod_{j=1}^{l} (X^2 - (\gamma_j + \overline{\gamma}_j)X + \gamma_j\overline{\gamma}_j)(X^2 - (\gamma_j + \overline{\gamma}_j)X + \gamma_j\overline{\gamma}_j)^* \\ &= \prod_{i=1}^{k} (X - \beta_i)(X - \beta_i^{-1}) \times \prod_{j=1}^{l} (X^2 - (\gamma_j + \overline{\gamma}_j)X + \gamma_j\overline{\gamma}_j)(X^2 - (\gamma_j^{-1} + \overline{\gamma}_j^{-1})X + \gamma_j^{-1}\overline{\gamma}_j^{-1}) \end{aligned}$$

where $\beta_i \in \mathbb{R} \setminus \{1, -1\}$ and $\gamma_j \in \mathbb{C} \setminus (\mathbb{T} \cup \mathbb{R})$. Hence $m(F) = \deg(F_2)/2$ as required. □

Let (V, b) be an inner product space over $\mathbb{R}$. Let t be an isometry of (V, b), and $F \in \mathbb{R}[X]$ its characteristic polynomial. Then F is $*$-symmetric and we have the orthogonal direct sum decomposition

$$V = \bigoplus_{f \in I(F;\mathbb{R})} V(f;t) \oplus \bigoplus_{\{g,g^*\} \subset I_2(F;\mathbb{R})} V(gg^*;t) \tag{26}$$

by Theorem 7.14. Note that $\mathrm{idx}(V(gg^*;t)) = 0$ for $g \in I_2(F;\mathbb{R})$ since $V(gg^*;t)$ is metabolic by Proposition 7.16.

Definition 7.23. The map $\mathrm{idx}_t : I(F;\mathbb{R}) \to \mathbb{Z}$ defined by

$$\mathrm{idx}_t(f) = \mathrm{idx}(V(f;t)) \quad (f \in I(F;\mathbb{R}))$$

is called the *index of* t (with respect to b). It is sometimes written by idx_t^b if the inner product b needs to be emphasized.

The index of an isometry has the following properties.

Proposition 7.24. *Suppose that t is semisimple. For each $f \in I(F;\mathbb{R})$, we have:*

(i) $-\deg(f^{m_f}) \le \mathrm{idx}_t(f) \le \deg(f^{m_f})$ *and* $\mathrm{idx}_t(f) \equiv \deg(f^{m_f}) \bmod 2$.

(ii) *If $f \in I_1(F;\mathbb{R})$ then* $(\deg(f^{m_f}) + \mathrm{idx}_t(f))/2 \equiv (\deg(f^{m_f}) - \mathrm{idx}_t(f))/2 \equiv 0 \bmod 2$ *(actually* $\deg(f^{m_f}) = 2m_f$ *by Proposition* 7.21*).*

Proof. Let (r_f, s_f) be the signature of the subspace $V(f;t) \subset V$. We remark that $\deg(f^{m_f}) = \dim(V;f) = r_f + s_f$ by Lemma 7.12, and $\mathrm{idx}_t(f) = r_f - s_f$. Thus the assertion (i) is clear. We prove the assertion (ii). Suppose that $f \in I_1(F;\mathbb{R})$, and identify V with the associated $\mathbb{R}[\Gamma]$-module M of F (see Lemma 7.18). Then $V(f;t) = M^f$, and Proposition 7.20 shows that there exists a hermitian product $h^f : M^f \times M^f \to E^f$ over $E^f = \mathbb{C}$ such that $b|_{M^f} = \mathrm{Tr}_{E^f/\mathbb{R}} \circ h^f$. Let (r'_f, s'_f) denote the signature of h^f. Then $r_f = 2r'_f \equiv 0$ and $r_f = 2r'_f \equiv 0 \bmod 2$ by Lemma 4.70. This is assertion (ii). □

Remark 7.25. In Proposition 7.24, the assumption for t to be semisimple can be removed in fact, see [4, §8].

The discussion so far yields the following relationship between the signature of the space V and the characteristic polynomial F of the isometry t.

Theorem 7.26. *Let t be a semisimple isometry of an inner product space (V,b) over $\mathbb{R}$ of signature (r,s). Let $F \in \mathbb{R}[X]$ denote the characteristic polynomial of t, and $m(F)$ the number of roots of F whose absolute values are greater than* 1 *counted with multiplicity. Then*

$$r, s \ge m(F) \text{ and if } F(1)F(-1) \ne 0 \text{ then } r \equiv s \equiv m(F) \bmod 2. \qquad \text{(Sign)}$$

Proof. Let (r_+, s_+) and (r_-, s_-) denote the signatures of the subspaces $V(X-1;t)$ and $V(X+1;t)$ respectively, and (r_f, s_f) the signature of $V(f;t)$ for each $f \in I_1(F;\mathbb{R})$ or $f = gg^*$ where $g \in I_2(F;\mathbb{R})$. Then we have

$$r = r_+ + r_- + \sum_{f \in I_1(F;\mathbb{R})} r_f + \sum_{\{g,g^*\} \subset I_2(F;\mathbb{R})} r_{gg^*}$$

by the orthogonal direct sum decomposition (26). Furthermore $r_{gg^*} = \deg((gg^*)^{m_g})/2$ since $V(gg^*;t)$ has index 0. Thus

$$\sum_{\{g,g^*\} \subset I_2(F;\mathbb{R})} r_{gg^*} = \sum_{\{g,g^*\} \subset I_2(F;\mathbb{R})} \deg((gg^*)^{m_g})/2 = \deg(F_2)/2 = m(F)$$

by Corollary 7.22, and we get

$$r = r_+ + r_- + \sum_{f \in I_1(F;\mathbb{R})} r_f + m(F).$$

In particular $r \ge m(F)$. Moreover, since $r_f \equiv 0 \bmod 2$ by Proposition 7.24 (ii), if $F(1)F(-1) \ne 0$ then $r_+ = r_- = 0$, and $r \equiv m(F) \bmod 2$. It follows similarly that $s \ge m(F)$ and if $F(1)F(-1) \ne 0$ then $s \equiv m(F) \bmod 2$. □

The condition (Sign) is denoted by $(\mathrm{Sign})_{r,s}$ if necessary. Changing from the situation so far, suppose that a $*$-symmetric polynomial $F \in \mathbb{R}[X]$ is given. For a given map $\mathfrak{i} : I(F;\mathbb{R}) \to \mathbb{Z}$, we consider when there exists an inner product space over $\mathbb{R}$ and its semisimple isometry t such that F is the characteristic polynomial of t and $\mathrm{idx}_t = \mathfrak{i}$.

Definition 7.27. Let r, s be non-negative integers. The symbol $\mathrm{Idx}(r, s; F)$ denotes the set of all maps $\mathfrak{i} : I(F;\mathbb{R}) \to \mathbb{Z}$ satisfying the following three conditions:

$$-\deg(f^{m_f}) \le \mathfrak{i}(f) \le \deg(f^{m_f}) \text{ and } \mathfrak{i}(f) \equiv \deg(f^{m_f}) \bmod 2 \text{ for each } f \in I(F;\mathbb{R}). \tag{27}$$

$$\frac{\deg(f^{m_f}) + \mathfrak{i}(f)}{2} \equiv \frac{\deg(f^{m_f}) - \mathfrak{i}(f)}{2} \equiv 0 \bmod 2 \text{ for each } f \in I_1(F;\mathbb{R}). \tag{28}$$

$$\sum_{f \in I(F;\mathbb{R})} \mathfrak{i}(f) = r - s. \tag{29}$$

Each map in $\mathrm{Idx}(r, s; F)$ is referred to as an *index map*.

For any semisimple isometry t of an inner product space over $\mathbb{R}$ of signature (r, s), with characteristic polynomial F, its index idx_t belongs to $\mathrm{Idx}(r, s; F)$. Indeed, the conditions (27), (28) follow from Proposition 7.24, and (29) from the decomposition (26). Conversely, any index map $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ is realized as the index of some isometry t. More precisely, the following theorem holds.

Theorem 7.28. *Let r, s be non-negative integers, and let $F \in \mathbb{R}[X]$ be a $*$-symmetric polynomial of degree $r+s$. Suppose that the condition $(\mathrm{Sign})_{r,s}$ holds. Then the set $\mathrm{Idx}(r, s; F)$ is not empty. Moreover, for any $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$, there exists an inner product b on the associated $\mathbb{R}[\Gamma]$-module M of F with transformation α such that it makes α an isometry with index $\mathfrak{i}$. As a result, we can write*

$$\mathrm{Idx}(r, s; F) = \left\{ \mathrm{idx}_t \;\middle|\; \begin{array}{l} t \text{ is a semisimple isometry of an inner product space} \\ \text{of signature } (r, s) \text{ with characteristic polynomial } F \end{array} \right\}.$$

Proof. We write $F(X) = (X-1)^{m_+}(X-1)^{m_-}F_1(X)F_2(X)$, where m_+, m_- are the multiplicities of $X-1, X+1$, and F_1, F_2 are the type $1, 2$ components over $\mathbb{R}$. Put $r' = r - m(F)$. Then $r' \ge 0$ and if $m_+ = m_- = 0$ then $r' \equiv 0 \bmod 2$ by (Sign). Moreover, since $r = \dim(V) - s \le \deg(F) - m(F)$ by (Sign) and $2m(F) = \deg(F_2)$ by Corollary 7.22, we have

$$r' \le (\deg(F) - m(F)) - m(F) = \deg(F) - \deg(F_2) = m_+ + m_- + \sum_{f \in I_1(F;\mathbb{R})} 2m_f.$$

Hence, there exists a partition $r' = r_+ + r_- + \sum_{f \in I_1(F;\mathbb{R})} r_f$ of r' into non-negative integers r_+, r_-, r_f $(f \in I_1(F;\mathbb{R}))$ such that

$$r_+ \le m_+,\ r_- \le m_-,\ r_f \le 2m_f \ \text{ and } r_f \equiv 0 \bmod 2 \quad (f \in I_1(F;\mathbb{R})).$$

We now define a map $\mathfrak{i} : I(F;\mathbb{R}) \to \mathbb{Z}$ by

$$\mathfrak{i}(X-1) = 2r_+ - m_+,\ \mathfrak{i}(X+1) = 2r_- - m_-, \ \text{ and } \mathfrak{i}(f) = 2r_f - 2m_f \quad (f \in I_1(F;\mathbb{R})).$$

Then, this map satisfies the conditions (27), (28) and (29), and belongs to $\mathrm{Idx}(r, s; F)$.

We then show the latter assertion. Let $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ be an index map. We will define an inner product on M in accordance with the decomposition (25). Note that any inner product on $M^{\pm}$ makes $\alpha|_{M^{\pm}} = \pm\mathrm{id}_{M^{\pm}}$ an isometry, and that $\frac{m_{\pm} + \mathfrak{i}(X \mp 1)}{2}$ and $\frac{m_{\pm} - \mathfrak{i}(X \mp 1)}{2}$ are non-negative

integers by (27). Let $b^{\pm}$ be an inner product on $M^{\pm}$ of signature $(\frac{m_{\pm}+\mathrm{i}(X\mp 1)}{2}, \frac{m_{\pm}-\mathrm{i}(X\mp 1)}{2})$. For $f \in I_1(F;\mathbb{R})$, noting that $\frac{2m_f+\mathrm{i}(f)}{4}$ and $\frac{2m_f-\mathrm{i}(f)}{4}$ are non-negative integers by (28), we define an inner product b^f on M^f by $b^f := \mathrm{Tr}_{E^f/\mathbb{R}} \circ h^f$, where $h^f : M^f \times M^f \to E^f$ is a hermitian product with signature $(\frac{2m_f+\mathrm{i}(f)}{4}, \frac{2m_f-\mathrm{i}(f)}{4})$. Then b^f is an inner product of signature $(\frac{2m_f+\mathrm{i}(f)}{2}, \frac{2m_f-\mathrm{i}(f)}{2})$ by Lemma 4.70, and it makes $\alpha|_{M^f}$ an isometry as seen in the paragraph above Proposition 7.20. For $g \in I_2(F;\mathbb{R})$, we take a hermitian product $h^{gg^*} : M^{gg^*} \times M^{gg^*} \to E^{gg^*}$ arbitrary, and set $b^{gg^*} := \mathrm{Tr}_{E^{gg^*}/\mathbb{R}} \circ h^{gg^*}$. Note that $\mathrm{idx}(b^{gg^*}) = 0$ by Proposition 7.16. Now, let us define an inner product b on $M = M^+ \oplus M^- \oplus \bigoplus_{f\in I_1(F;\mathbb{R})} M^f \oplus \bigoplus_{\{g,g^*\}\subset I_2(F;\mathbb{R})} M^{gg^*}$ by

$$b := b^+ \oplus b^- \oplus \bigoplus_{f\in I_1(F;\mathbb{R})} b^f \oplus \bigoplus_{\{g,g^*\}\subset I_2(F;\mathbb{R})} b^{gg^*}.$$

Then b makes α an isometry and $\mathrm{idx}^b_\alpha = \mathfrak{i}$ by its construction. This completes the proof. □

Corollary 7.29. *Let r, s be non-negative integers, and let $F \in \mathbb{R}[X]$ be a $*$-symmetric polynomial of degree $r+s$. The set* $\mathrm{Idx}(r,s;F)$ *is not empty if and only if the condition* $(\mathrm{Sign})_{r,s}$ *holds.*

Proof. The if part is included in Theorem 7.28. Suppose that $\mathrm{Idx}(r,s;F) \neq \emptyset$. Then, Theorem 7.28 shows that there exists a semisimple isometry of an inner product space of signature (r,s) with characteristic polynomial F. Hence, the condition $(\mathrm{Sign})_{r,s}$ holds by Theorem 7.26. □

7.5 Spinor norm

This subsection gives a description of the spinor norm of an isometry. Let K be a field characteristic not 2.

Definition 7.30 (Zassenhaus)**.** Let t be an isometry of an inner product space (V,b) over K. The *spinor norm* $\mathrm{sn}(t) \in K^\times/K^{\times 2}$ of t is the square class defined by

$$\mathrm{sn}(t) := \det(b|_{V(X+1;t)}) \cdot \det\left(\frac{1+t}{2}\middle|_{V(X+1;t)^\perp}\right),$$

where $V(X+1;t) = \{v \in V \mid (t+1)^N.v = 0 \text{ for some } N \in \mathbb{Z}_{\geq 0}\}$. Note that the former factor is the determinant of the inner product $b|_{V(X+1;t)}$, but the latter factor is the determinant of the K-linear transformation $\frac{1+t}{2}|_{V(X+1;t)^\perp} : V(X+1;t)^\perp \to V(X+1;t)^\perp$.

In the situation of Definition 7.30, if the characteristic polynomial of t is written as $F(X) = (X-1)^{m_+}(X+1)^{m_-}F_{12}(X)$, where m_+, m_- are the multiplicities of $X-1, X+1$, and F_{12} is the product of type 1 and 2 components, then

$$\begin{aligned}
\det\left(\frac{1+t}{2}\middle|_{V(X+1;t)^\perp}\right) &= (-2)^{\deg(F)-m_+} \cdot \det\left(-1-t\middle|_{V(X+1;t)^\perp}\right) \\
&= (-2)^{\deg(F)-m_+} \cdot (-1-1)^{m_-} F_{12}(-1) \\
&= (-2)^{\deg(F_{12})} F_{12}(-1) \\
&= F_{12}(-1)
\end{aligned}$$

in $K^\times/K^{\times 2}$ since $\deg(F_{12})$ is even. Thus, we get

$$\mathrm{sn}(t) = \det(b|_{V(X+1;t)}) \cdot F_{12}(-1). \tag{30}$$

Let (V, b) be an inner product space over K. For a reflection $\sigma_z \in \mathrm{O}(V)$ orthogonal to an anisotropic vector $z \in V$, we have $V(X+1;\sigma_z) = Kz$ and $\frac{1+\sigma_z}{2}|_{V(X+1;\sigma_z)^\perp} = \mathrm{id}_{V(X+1;\sigma_z)^\perp}$. Hence $\mathrm{sn}(\sigma_z) = b(z,z)$ in $K^\times/K^{\times 2}$. Zassenhaus showed in his paper [49] that

$$\mathrm{sn}(tt') = \mathrm{sn}(t)\,\mathrm{sn}(t')$$

for any isometries $t, t' \in \mathrm{O}(V)$. In other words, the spinor norm $\mathrm{sn} : \mathrm{O}(V) \to K^\times/K^{\times 2}$ is a group homomorphism. As a corollary, if an isometry t is expressed as a product of reflections, say $t = \sigma_{z_m} \cdots \sigma_{z_1}$ where each $z_i \in V$ is an anisotropic vector, then

$$\mathrm{sn}(t) = b(z_1, z_1) \cdots b(z_m, z_m) \quad \text{in } K^\times/K^{\times 2}. \tag{31}$$

Remark 7.31. It can be checked by using Lemma 4.17 that any isometry of V can be expressed as a product of reflections. The spinor norm was originally defined by equation (31). When we adopt this definition, it is clear that the spinor norm $\mathrm{sn} : \mathrm{O}(V) \to K^\times/K^{\times 2}$ is a group homomorphism, but it is non-trivial whether $\mathrm{sn}(t)$ is well-defined because it is defined by using an expression as a product of reflections, which is not unique. One way to show the well-definedness is to introduce the *Clifford algebra*, see [35, §55].

Proposition 7.32. *Let t be an isometry of an inner product space (V, b) over K. Suppose that the characteristic polynomial $F \in K[X]$ satisfies $F(1)F(-1) \neq 0$. Then $\det(b) = F(1)F(-1)$ in $K^\times/K^{\times 2}$.*

Proof. We remark that $V(X+1;t) = 0$ and $V(X+1;-t) = V(X-1;t) = 0$ since $F(-1) \neq 0$ and $F(1) \neq 0$. Then we have

$$\mathrm{sn}(t)\,\mathrm{sn}(-t) = \det\left(\frac{1+t}{2}\right)\det\left(\frac{1-t}{2}\right) = (-2)^{-\dim V}F(-1)\cdot 2^{-\dim V}F(1) = F(1)F(-1)$$

in $K^\times/K^{\times 2}$. On the other hand, we have

$$\mathrm{sn}(t)\,\mathrm{sn}(-t) = \mathrm{sn}(t)^2\,\mathrm{sn}(-\mathrm{id}_V) = \mathrm{sn}(-\mathrm{id}_V) = \det(b)$$

because $V(X+1;-\mathrm{id}_V) = V$. Hence $\det(b) = F(1)F(-1)$ in $K^\times/K^{\times 2}$. (There is a more elementary proof without spinor norms, see e.g. [4, Proposition 5.1].) □

Spinor norms of isometries of an even unimodular lattice over the valuation ring of a local field are as follows.

Theorem 7.33. *Let K be a non-archimedean local field of characteristic not 2, and $\mathcal{O}_K$ the valuation ring of K. For any even unimodular lattice (Λ, b) over $\mathcal{O}_K$, we have $\mathrm{sn}(\mathrm{SO}(\Lambda, b)) = 1 \cdot K^{\times 2}$ if $\mathrm{rk}\,\Lambda = 1$, and $\mathrm{sn}(\mathrm{SO}(\Lambda, b)) = \mathcal{O}_K^\times \cdot K^{\times 2}$ if $\mathrm{rk}\,\Lambda \geq 2$.*

Proof. See [35, Proposition 92:5] for the non-dyadic case, and see [20, Lemma 1] for the dyadic case. □

Corollary 7.34. *Let p be a prime number, and let (Λ, b) be an even unimodular lattice over $\mathbb{Z}_p$. For any isometry $t \in \mathrm{O}(\Lambda, b)$, we have*

$$v_p(\mathrm{sn}(t)) \equiv \begin{cases} 0 & \text{if } \det t = 1 \\ v_p(2) & \text{if } \det t = -1 \end{cases} \mod 2.$$

Proof. Let t be an isometry of Λ. If $\det t = 1$ then the congruence $v_p(\mathrm{sn}(t)) \equiv 0 \bmod 2$ follows from Theorem 7.33. Suppose that $\det t = -1$.

Case I*:* $p \neq 2$. In this case, there exists $z \in \Lambda$ such that $b(z,z)$ is a unit of $\mathbb{Z}_p$ by Theorem 5.18. Then, we have

$$v_p(\mathrm{sn}(\sigma_z \circ t)) \equiv v_p(\mathrm{sn}(\sigma_z)) + v_p(\mathrm{sn}(t)) \equiv v_p(b(z,z)) + v_p(\mathrm{sn}(t)) \equiv v_p(\mathrm{sn}(t)) \mod 2.$$

On the other hand, $v_p(\mathrm{sn}(\sigma_z \circ t)) \equiv 0 \bmod 2$ since $\det(\sigma_z \circ t) = 1$. Hence $v_p(\mathrm{sn}(t)) \equiv 0 \equiv v_p(2) \bmod 2$ as required.

Case II*:* $p = 2$. In this case, there exists $z \in \Lambda$ such that $b(z,z) = 2$ by Theorem 5.23. Indeed, if Λ contains a sublattice isomorphic to $\mathbb{H}_{\mathbb{Z}_2}$ then $b(e_1+e_2, e_1+e_2) = 2$, where e_1, e_2 is a hyperbolic basis of the sublattice. Then, we get

$$0 \equiv v_2(\mathrm{sn}(\sigma_z \circ t)) \equiv v_2(b(z,z)) + v_2(\mathrm{sn}(t)) \equiv v_2(2) + v_2(\mathrm{sn}(t)) \mod 2$$

as in Case I. This completes the proof. □

We will need the following proposition. It is stated without spinor norms but we use spinor norms for its proof, as in Proposition 7.32.

Proposition 7.35. *Let (V,b) be an inner product space over $\mathbb{Q}_p$ where p is a prime, $t \in \mathrm{O}(V,b)$ an isometry, and $F \in \mathbb{Q}_p[X]$ the characteristic polynomial of t. We write $F(X) = (X-1)^{m_+}(X+1)^{m_-}F_{12}(X)$ where $m_+, m_- \in \mathbb{Z}_{\geq 0}$ are non-negative integers and F_{12} is the product of type 1 and 2 components of F. If t preserves an even unimodular lattice on (V,b) then*

$$v_p(\det(b|_{V(X\mp 1;t)})) \equiv \begin{cases} v_p(F_{12}(\pm 1)) & \text{if } \det t = 1 \\ v_p(2F_{12}(\pm 1)) & \text{if } \det t = -1. \end{cases}$$

Proof. By (30), we have

$$v_p(\mathrm{sn}(t)) \equiv v_p(\det(b|_{V(X+1;t)})) + v_p(F_{12}(-1)) \mod 2,$$

and hence

$$v_p(\det(b|_{V(X+1;t)})) \equiv v_p(F_{12}(-1)) + v_p(\mathrm{sn}(t)) \mod 2.$$

Suppose that t preserves an even unimodular lattice on (V,b). Then

$$\begin{aligned} v_p(\det(b|_{V(X+1;t)})) &\equiv \begin{cases} v_p(F_{12}(-1)) + 0 & \text{if } \det t = 1 \\ v_p(F_{12}(-1)) + v_p(2) & \text{if } \det t = -1 \end{cases} \\ &\equiv \begin{cases} v_p(F_{12}(-1)) & \text{if } \det t = 1 \\ v_p(2F_{12}(-1)) & \text{if } \det t = -1 \end{cases} \mod 2 \end{aligned} \tag{32}$$

by Corollary 7.34. On the other hand, we have $\det(b) \in \mathbb{Z}_p^\times \cdot \mathbb{Q}_p^{\times 2}$ because b is an inner product of a unimodular lattice. Thus

$$\begin{aligned} 0 &\equiv v_p(\det b) \\ &\equiv v_p(\det(b|_{V(X-1;t)} \oplus b|_{V(X+1;t)} \oplus b|_{V(F_{12};t)})) \\ &\equiv v_p(\det(b|_{V(X-1;t)})) + v_p(\det(b|_{V(X+1;t)})) + v_p(\det(b|_{V(F_{12};t)})) \\ &\equiv v_p(\det(b|_{V(X-1;t)})) + v_p(\det(b|_{V(X+1;t)})) + v_p(F_{12}(1)F_{12}(-1)) \mod 2 \end{aligned}$$

where the last congruence follows from Proposition 7.32. Hence

$$v_p(\det(b|_{V(X-1;t)})) \equiv v_p(F_{12}(1)) + v_p(F_{12}(-1)) + v_p(\det(b|_{V(X+1;t)})) \mod 2.$$

Substituting (32), we obtain

$$v_p(\det(b|_{V(X-1;t)})) \equiv \begin{cases} v_p(F_{12}(1)) & \text{if } \det t = 1 \\ v_p(2F_{12}(1)) & \text{if } \det t = -1 \end{cases} \mod 2.$$

The proof is complete. □

8 Local theory

Our main concern is to know which polynomial occurs as the characteristic polynomial of an even unimodular lattice over $\mathbb{Z}$. In this section, we address the localized version of this problem. Let Γ be an infinite cyclic group. Let K be a non-archimedean local field, and assume that $\operatorname{char} K = 0$, though most of results in this section holds if we assume that $\operatorname{char} K \neq 2$ and field extensions are separable. The symbols v_K, $\mathcal{O}_K$, $\mathfrak{p}_K$, and κ denote the normalized valuation, valuation ring, maximal ideal, and residue field of K respectively.

8.1 Residue maps

Let E be a commutative K-algebra whose K-dimension is finite, with a nontrivial involution $\sigma : E \to E$. Moreover, we assume that E is a field or of type (sp) (see Definition 1.9). When E is a field, we say that E is *of type* (ur) if E/E^σ is an unramified extension, and *of type* (rm) otherwise.

Let $\mathcal{O}_E$ denote the integral closure of $\mathcal{O}_K$ in E. It coincides with the valuation ring of E if E is of type (ur) or (rm), see Theorem 1.35. Let $\alpha \in \mathcal{O}_E^\times$ be a unit with $\alpha\sigma(\alpha) = 1$, and let M be a finitely generated free E-module. The linear transformation $M \to M$ defined as the multiplication by α is also denoted by α. For any hermitian product $h : M \times M \to E$, the inner product $\operatorname{Tr}_{E/K} \circ h$ on M over K makes α an isometry (cf. the paragraph before Proposition 7.20), and the triple $(M, \operatorname{Tr}_{E/K} \circ h, \alpha)$ can be seen as a $K[\Gamma]$-inner product space. Moreover, this $K[\Gamma]$-inner product space is bounded (considering $A = \mathcal{O}_K[\Gamma]$ in Definition 6.22) because $\sum_{i=1}^m \mathcal{O}_E\, e_i \subset M$ is an α-stable lattice for a basis $e_1, \dots, e_m$ of M over E. Our aim of the first half of this section is to study its image $\partial[M, \operatorname{Tr}_{E/K} \circ h, \alpha] \in W_{\kappa[\Gamma]}(\kappa)$ under the residue homomorphism $\partial : W_{K[\Gamma]}(K) \to W_{\kappa[\Gamma]}(\kappa)$.

Proposition 8.1. *Let h be a hermitian product on M. The Witt class of the $K[\Gamma]$-inner product space $(M, \operatorname{Tr}_{E/K} \circ h, \alpha)$ is uniquely determined by $\det h \in \operatorname{Tw}(E, \sigma)$.*

Proof. Let h' be another hermitian product with $\det h' = \det h$. Then, there exists an isomorphism $\phi : (M, h) \to (M, h')$ of hermitian product spaces by Corollary 4.66 or Theorem 4.73. This isomorphism commutes with α since it is E-linear. Thus ϕ is also a $K[\Gamma]$-module isomorphism. Hence ϕ gives an isomorphism between $K[\Gamma]$-inner product spaces $(M, \operatorname{Tr}_{E/K} \circ h, \alpha)$ and $(M, \operatorname{Tr}_{E/K} \circ h', \alpha)$. In particular $[M, \operatorname{Tr}_{E/K} \circ h, \alpha] = [M, \operatorname{Tr}_{E/K} \circ h', \alpha]$. The proof is complete. □

This proposition leads to the following definition.

Definition 8.2. The map

$$\operatorname{Tw}(E, \sigma) \to W_{\kappa[\Gamma]}(\kappa), \quad \mu \mapsto \partial[M, \operatorname{Tr}_{E/K} \circ h, \alpha]$$

where h is a hermitian product on M of determinant μ, is defined independently of the choice of h by Proposition 8.1. This map is referred to as the *residue map* and denoted by $\partial_{M,\alpha} : \operatorname{Tw}(E, \sigma) \to W_{\kappa[\Gamma]}(\kappa)$.

We remark that the residue map is not a group homomorphism in general. Our purpose can be rephrased as studying the image of the residue map. To this end, the case where the E-module M is E itself is essential.

Notation 8.3. For $\mu \in (E^\sigma)^\times$, the symbol b_μ denotes the inner product $E \times E \to K$ defined by $b_\mu(x,y) = \mathrm{Tr}_{E/K}(\mu x\sigma(y))$ for $x, y \in E$.

The map $E \times E \to E$, $(x,y) \mapsto \mu x\sigma(y)$ is a hermitian product on the E-module E with determinant μ. Thus, we have

$$\partial_{E,\alpha}(\mu) = \partial[E, b_\mu, \alpha].$$

Proposition 8.4. *Suppose that E is of type* (sp)*, and let $\mu \in (E^\sigma)^\times$. The $K[\Gamma]$-inner product space (E, b_μ, α) is neutral, and in particular $\partial_{E,\alpha}(\mu) = 0$. The inner product space (E, b_μ) has an $\mathcal{O}_E$-stable unimodular lattice. Furthermore, if E^σ/K is an unramified extension and μ is a unit of $\mathcal{O}_{E^\sigma}$ then $\mathcal{O}_E$ is an $\mathcal{O}_E$-stable (and hence α-stable) unimodular lattice on (E, b_μ).*

Proof. We may assume that $E = E_0 \times E_0$ for some field E_0 isomorphic to E^σ. Then $X := \{(x,0) \in E \mid x \in E_0\}$ is a lagrangian of the $K[\Gamma]$-inner product space (E, b_μ, α). Thus (E, b_μ, α) is neutral, and $\partial_{E,\alpha}(\mu) = \partial[E, b_u, \alpha] = 0$.

We regard E as the K-algebra $K \otimes_{\mathcal{O}_K} \mathcal{O}_E$. Since X is also a lagrangian of the E-inner product space (E, b_μ) over K, the image of $[E, b_\mu]$ under the residue homomorphism $\partial : W_E(K) \to W_{\kappa \otimes_{\mathcal{O}_K} \mathcal{O}_E}(\kappa)$ is also zero. This implies that the space (E, b_μ) contains an $\mathcal{O}_E$-stable unimodular lattice by Theorem 6.32.

Suppose that E^σ/K is an unramified extension and μ is a unit of $\mathcal{O}_{E^\sigma}$. It remains to show that the lattice $(\mathcal{O}_E, b_\mu)$ is unimodular. Let $e_1, \dots, e_n \in \mathcal{O}_{E_0}$ be an $\mathcal{O}_K$-basis of the valuation ring $\mathcal{O}_{E_0}$ of E_0. Then $(e_1, 0), \dots, (e_n, 0), (0, e_1), \dots, (0, e_n) \in \mathcal{O}_E$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_E = \mathcal{O}_{E_0} \times \mathcal{O}_{E_0}$. The Gram matrix of $b_\mu : \mathcal{O}_E \times \mathcal{O}_E \to \mathbb{Z}$ with respect to this basis is of the form $\begin{pmatrix} O & G \\ G & O \end{pmatrix}$, where G is the Gram matrix of the inner product

$$T_\mu : E_0 \times E_0 \to K,\ (x,y) \mapsto \mathrm{Tr}_{E_0/K}(\mu xy)$$

with respect to the basis $e_1, \dots, e_n$. Since μ is a unit, the dual lattice of $\mathcal{O}_{E_0}$ with respect to T_μ is the codifferent ideal $\mathfrak{D}_{E_0/K}^{-1}$. On the other hand, it follows from Theorem 1.40 that $\mathfrak{D}_{E_0/K} = \mathcal{O}_{E_0}$ since E_0/K is unramified. Hence $(\mathcal{O}_{E_0}, T_\mu)$ is unimodular, and G is invertible over $\mathcal{O}_K$. Therefore $\begin{pmatrix} O & G \\ G & O \end{pmatrix}$ is also invertible over $\mathcal{O}_K$, and $(\mathcal{O}_E, b_\mu)$ is unimodular. This completes the proof. □

The case where E is a field is discussed in §§8.2 and 8.3.

8.2 Almost unimodular lattices on (E, b_μ)

Let E be a field with a nontrivial involution σ, and with $[E : K] < \infty$. As in the previous subsection, we fix a unit $\alpha \in \mathcal{O}_E^\times$ with $\alpha\sigma(\alpha) = 1$. This subsection gives a specific almost unimodular lattice on (E, b_μ, α) in order to compute $\partial[E, b_\mu, \alpha]$. The symbols v_E, $\mathcal{O}_E$, $\mathfrak{p}_E$, and λ denote the normalized valuation, valuation ring, maximal ideal, and residue field of E respectively. Let $D \in \mathbb{Z}_{\geq 0}$ denote the valuation of the different ideal $\mathfrak{D}_{E/K}$, that is, $D := v_E(\mathfrak{D}_{E/K})$.

Lemma 8.5. *Let $n \in \mathbb{Z}$ and $\mu \in (E^\sigma)^\times$. Then $\mathfrak{p}_E^n$ is an α-stable lattice on the inner product space (E, b_μ) over K, and we have $(\mathfrak{p}_E^n)^\vee = \mathfrak{p}_E^{-n-D-v_E(\mu)}$.*

Proof. Any nonzero fractional ideal of E is an α-stable lattice on (E, b_μ), and in particular, so is $\mathfrak{p}_E^n$. Since $(\mathfrak{p}_E^n)^\vee$ is also a fractional ideal of E, we can write $(\mathfrak{p}_E^n)^\vee = \mathfrak{p}_E^m$ for some $m \in \mathbb{Z}$. Our assertion is that $m = -n - D - v_E(\mu)$. Because

$$\mathcal{O}_K \supset b_\mu(\mathfrak{p}_E^n, \mathfrak{p}_E^m) = \mathrm{Tr}_{E/K}(\mu\mathfrak{p}_E^n\sigma(\mathfrak{p}_E^m)) = \mathrm{Tr}_{E/K}(\mu\mathfrak{p}_E^{n+m}),$$

we have $\mu\mathfrak{p}_E^{n+m} \subset \mathfrak{D}_{E/K}^{-1} = \mathfrak{p}_E^{-D}$ by the definition of the different ideal. This inclusion shows that $v_E(\mu)+n+m \geq -D$ and hence $m \geq -n-D-v_E(\mu)$. We now suppose that m were greater than $-n-D-v_E(\mu)$. Then $m-1 \geq -n-D-v_E(\mu)$ and thus $v_E(\mu)+n+m-1 \geq -D$. This inequality shows that $\mu\mathfrak{p}_E^{n+m-1} \subset \mathfrak{p}_E^{-D} = \mathfrak{D}_{E/K}^{-1}$, and

$$\mathrm{Tr}_{E/K}(\mu\mathfrak{p}_E^n\sigma(\mathfrak{p}_E^{m-1})) = \mathrm{Tr}_{E/K}(\mu\mathfrak{p}_E^{n+m-1}) \subset \mathcal{O}_K.$$

This would imply that $\mathfrak{p}_E^{m-1} \subset (\mathfrak{p}_E^n)^\vee = \mathfrak{p}_E^m$, but this is a contradiction. Therefore we obtain $m = -n - D - v_E(\mu)$. The proof is complete. □

Let $\bar{\sigma} : \lambda \to \lambda$ denote the involution induced by $\sigma : E \to E$. We remark that it can be trivial. In fact, we have:

Proposition 8.6. *The involution $\bar{\sigma}$ is nontrivial if and only if E is of type* (ur)*. In this case, the residue field of E^σ is the fixed subfield $\lambda^{\bar{\sigma}}$.*

Proof. Let λ' be the residue field of E^σ. If E is of type (rm) then $\lambda' = \lambda$ and $\bar{\sigma}$ is trivial. Suppose that E is of type (ur). Then the canonical homomorphism $\mathrm{Gal}(E/E^\sigma) \to \mathrm{Gal}(\lambda/\lambda')$ is an automorphism by Corollary 2.17. Thus $\bar{\sigma} \in \mathrm{Gal}(\lambda/\lambda')$ must be nontrivial since so is $\sigma \in \mathrm{Gal}(E/E^\sigma)$. In this case, we have $\lambda' = \lambda^\sigma$ because $[\lambda : \lambda^{\bar{\sigma}}] = 2 = [\lambda : \lambda']$. This completes the proof. □

Let $L \subset E$ be a maximal unramified extension in E/K. By Corollary 2.16, such a field is uniquely determined as an unramified field contained in E with residue field λ. For any $x \in \mathcal{O}_L$, we write $\bar{x} = x + \mathfrak{p}_L \in \lambda$. For a σ-invariant element $u \in \mathcal{O}_L$, the symbol $b_{\bar{u}}$ denotes the symmetric bilinear form $\lambda \times \lambda \to \kappa$ defined by

$$b_{\bar{u}}(\bar{x}, \bar{y}) = \mathrm{Tr}_{\lambda/\kappa}(\bar{u}\bar{x}\bar{\sigma}(\bar{y})) \quad (x, y \in \mathcal{O}_L) \tag{33}$$

as in Notation 8.3, although $\bar{\sigma}$ may be the identity. This symmetric bilinear form is nondegenerate if and only if $\bar{u} \neq 0$, or equivalently, u is a unit of $\mathcal{O}_L$.

Proposition 8.7. *Let π_K and π_E be uniformizers of K and E. Let $\mu \in (E^\sigma)^\times$.*

(i) *If $v_E(\mu) + D$ is even, set $n = -(v_E(\mu) + D)/2$ and $\Lambda = \mathfrak{p}_E^n$. Then Λ is an α-stable unimodular lattice in (E, b_μ) (clearly it is also $\mathcal{O}_E$-stable).*

(ii) *If $v_E(\mu)+D$ is odd, set $n = -(v_E(\mu)+D-1)/2$ and $\Lambda = \mathfrak{p}_E^n$. Then Λ is an α-stable almost unimodular lattice on (E, b_μ). Moreover, there is an isomorphism $(\Lambda^\vee/\Lambda, \pi_K\overline{b_\mu}, \alpha) \cong (\lambda, b_{\bar{u}}, \bar{\alpha})$ of $\kappa[\Gamma]$-inner product spaces, where $u \in \mathcal{O}_L$ is the σ-invariant unit defined by $u := u_\mu := \mathrm{Tr}_{E/L}(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))$.*

Proof. (i). Suppose that $v_E(\mu) + D$ is even, and set $n = -(v_E(\mu) + D)/2$ and $\Lambda = \mathfrak{p}_E^n$. Then it follows from Lemma 8.5 that

$$\Lambda^\vee = \mathfrak{p}_E^{-n-D-v_E(\mu)} = \mathfrak{p}^n = \Lambda,$$

which shows that Λ is unimodular.

(ii). Suppose that $v_E(\mu)+D$ is odd, and set $n=-(v_E(\mu)+D-1)/2$ and $\Lambda=\mathfrak{p}_E^n$. It follows from Lemma 8.5 that $\Lambda^\vee=\mathfrak{p}_E^{-n-D-v_E(\mu)}=\mathfrak{p}_E^{n-1}$. Hence we obtain

$$\Lambda=\mathfrak{p}^n\subset\mathfrak{p}^{n-1}=\Lambda^\vee \quad\text{and}\quad \pi_K\Lambda^\vee=\pi_K\mathfrak{p}_E^{n-1}\subset\mathfrak{p}_E^n=\Lambda.$$

These mean that Λ is almost unimodular. Put $u=\mathrm{Tr}_{E/L}(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))$. Then

$$\begin{aligned}\sigma(u)&=\sigma\left(\sum_{\tau\in\mathrm{Hom}_L^{\mathrm{al}}(E,\overline{L})}\tau(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))\right)\\&=\sum_{\tau\in\mathrm{Hom}_L^{\mathrm{al}}(E,\overline{L})}\sigma\circ\tau\circ\sigma^{-1}\circ\sigma(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))\\&=\sum_{\tau'\in\mathrm{Hom}_L^{\mathrm{al}}(E,\overline{L})}\tau'(\mu\pi_K\sigma(\pi_E^{n-1})\pi_E^{n-1})\\&=u,\end{aligned}$$

where $\overline{L}$ is an algebraic closure of L containing E, and an extension of σ to $\overline{L}$ is also written by σ. Moreover, we have

$$\begin{aligned}v_E(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))&=v_E(\mu)+v_E(\pi_K)+2(n-1)\\&=v_E(\mu)+v_E(\pi_K)-v_E(\mu)-D-1=v_E(\pi_K)-1-D\geq -D,\end{aligned}$$

which leads to $\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1})\in\mathfrak{p}_E^{-D}=\mathfrak{D}_{E/K}^{-1}$. On the other hand, because $\mathfrak{D}_{L/K}=\mathcal{O}_L$ by Theorem 1.40, it follows from Proposition 1.39 (i) that $\mathfrak{D}_{E/K}=\mathfrak{D}_{E/L}\mathfrak{D}_{L/K}=\mathfrak{D}_{E/L}$. Hence $\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1})\in\mathfrak{D}_{E/L}^{-1}$, which leads to $u=\mathrm{Tr}_{E/L}(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))\in\mathcal{O}_L$. It will be shown later that u is a unit.

We show that the map $\phi:\lambda\to\Lambda^\vee/\Lambda=\mathfrak{p}_E^{n-1}/\mathfrak{p}_E^n$ defined by

$$\phi(\bar{x})=x\pi_E^{n-1}+\mathfrak{p}_E^n\quad(x\in\mathcal{O}_L)$$

gives an isomorphism $(\lambda,b_{\bar{u}},\bar{\alpha})\to(\Lambda^\vee/\Lambda,\pi_K\overline{b_\mu},\alpha)$ of $\kappa[\Gamma]$-inner product spaces. It is clear that ϕ is a $\kappa[\Gamma]$-module isomorphism. Moreover, for $x,y\in\mathcal{O}_L$ we have

$$\begin{aligned}\pi_K\overline{b_\mu}(\phi(\bar{x}),\phi(\bar{y}))&=\pi_K\,\mathrm{Tr}_{E/K}(\mu x\pi_E^{n-1}\sigma(y\pi_E^{n-1}))+\mathfrak{p}_K\\&=\mathrm{Tr}_{L/K}\circ\mathrm{Tr}_{E/L}(\mu\pi_K x\pi_E^{n-1}\sigma(y\pi_E^{n-1}))+\mathfrak{p}_K\\&=\mathrm{Tr}_{L/K}\left(x\sigma(y)\cdot\mathrm{Tr}_{E/L}(\mu\pi_K\pi_E^{n-1}\sigma(\pi_E^{n-1}))\right)+\mathfrak{p}_K\\&=\mathrm{Tr}_{L/K}(ux\sigma(y))+\mathfrak{p}_K\\&=\mathrm{Tr}_{\lambda/\kappa}(\bar{u}\bar{x}\bar{\sigma}(\bar{y})),\end{aligned}$$

where the last equality is by Proposition 2.19. This means that ϕ is an isometry between $(\lambda,b_{\bar{u}})$ and $(\Lambda^\vee/\Lambda,\pi_K\overline{b_\mu})$. Hence $\phi:(\Lambda^\vee/\Lambda,\pi_K\overline{b_\mu},\alpha)\to(\lambda,b_{\bar{u}},\bar{\alpha})$ is an isomorphism of $\kappa[\Gamma]$-inner product spaces. In particular $b_{\bar{u}}$ is nondegenerate since so is $\pi_K\overline{b_\mu}$. Therefore u must be a unit of $\mathcal{O}_L$. This completes the proof. □

This proposition shows that $\partial_{E,\alpha}(\mu)=0$ or $[\lambda,b_{\bar{u}},\bar{\alpha}]$ for any $\mu\in\mathrm{Tw}(E,\sigma)$. In particular, if $m(X)\in\kappa[X]$ denotes the minimal polynomial of $\bar{\alpha}$ then $\partial_{E,\alpha}(\mu)\in W_{\kappa[\Gamma]}(\kappa;m)$, where the symbol $W_{\kappa[\Gamma]}(\kappa;m)$ is defined in the paragraph above Corollary 6.12.

8.3 Images of residue maps

We keep the notation of §8.2.

Lemma 8.8. *Suppose that $\bar{\alpha} \in \lambda$ is neither 1 nor -1.*

(i) *The induced involution $\bar{\sigma} : \lambda \to \lambda$ is nontrivial and $\lambda = \kappa(\bar{\alpha})$.*

(ii) *Let $b : \lambda \times \lambda \to \kappa$ be an inner product which makes $\bar{\alpha} : \lambda \to \lambda$ an isometry, and let $b_1 : \lambda \times \lambda \to \kappa$ be the inner product defined in* (33) *as $\bar{u} = 1$. Then $(\lambda, b, \bar{\alpha}) \cong (\lambda, b_1, \bar{\alpha})$ as $\kappa[\Gamma]$-inner product spaces.*

Proof. (i). We have

$$\bar{\alpha} \neq 1, -1 \iff \bar{\alpha}^2 - 1 \neq 0 \iff \bar{\alpha} - \bar{\alpha}^{-1} \neq 0 \iff \bar{\alpha} \neq \bar{\sigma}(\bar{\alpha}).$$

Let $\bar{\alpha} \neq 1, -1$. Then $\bar{\sigma}$ is nontrivial since $\bar{\alpha} \neq \bar{\sigma}(\bar{\alpha})$. Thus $\lambda^{\bar{\sigma}}$ is a proper subfield of λ and $[\lambda : \lambda^{\bar{\sigma}}] = 2$. If $[\lambda : \kappa(\bar{\alpha})]$ were greater than 1 then we would get

$$[\lambda^{\bar{\sigma}} : \kappa] = [\lambda : \kappa]/2 \geq [\lambda : \kappa]/[\lambda : \kappa(\bar{\alpha})] = [\kappa(\bar{\alpha}) : \kappa].$$

This means that $\kappa(\bar{\alpha}) \subset \lambda^{\bar{\sigma}}$ but this inclusion contradicts $\bar{\alpha} \neq \bar{\sigma}(\bar{\alpha})$. Hence we obtain $[\lambda : \kappa(\bar{\alpha})] = 1$, and $\lambda = \kappa(\bar{\alpha})$.

(ii). We write h_1 for the one-dimensional hermitian product $\lambda \times \lambda \to \lambda$ defined by $h_1(1, 1) = 1$. Then $b_1 = \mathrm{Tr}_{\lambda/\kappa} \circ h_1$. On the other hand, by assertion (i) and Proposition 7.20, there exists a hermitian product $h : \lambda \times \lambda \to \lambda$ such that $b = \mathrm{Tr}_{\lambda/\kappa} \circ h$. In order to show that $(\lambda, b, \bar{\alpha}) \cong (\lambda, b_1, \bar{\alpha})$, it is enough to give an isomorphism between hermitian product spaces (λ, h) and (λ, h_1). Let $\bar{w} \in \lambda$ be an element such that $\mathrm{N}_{\lambda/\lambda^{\bar{\sigma}}}(\bar{w}) = h(1, 1)$. Such an element exists by Corollary 2.5. Then, the multiplication by $\bar{w}$ gives an isomorphism from (λ, h) to (λ, h_1). Indeed

$$h_1(\bar{w}\bar{x}, \bar{w}\bar{y}) = \bar{w}\bar{x}\bar{\sigma}(\bar{w})\bar{\sigma}(\bar{y})h_1(1, 1) = h(1, 1)\bar{x}\bar{\sigma}(\bar{y}) = h(\bar{x}, \bar{y}) \quad (\bar{x}, \bar{y} \in \lambda).$$

Hence, we obtain the isomorphism $(\lambda, b, \bar{\alpha}) \cong (\lambda, b_1, \bar{\alpha})$ of $\kappa[\Gamma]$-inner product spaces. □

Let us compute the images of residue maps by using an almost unimodular lattice given in Proposition 8.7.

Proposition 8.9. *Suppose that E is of type* (ur).

(i) *If $\bar{\alpha} \neq 1, -1$ then $\mathrm{im}\, \partial_{E,\alpha} = \{0, [\kappa(\bar{\alpha}), b_1, \bar{\alpha}]\} \subset W_{\kappa[\Gamma]}(\kappa)$, and the class $[\kappa(\bar{\alpha}), b_1, \bar{\alpha}]$ has order 2.*

(ii) *If $\bar{\alpha} = \pm 1$ then $\mathrm{im}\, \partial_{E,\alpha} = \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim \omega \equiv 0 \bmod 2\}$.*

Proof. Since E/E^{σ} is unramified, the twisting group $\mathrm{Tw}(E, \sigma)$ can be written as $\mathrm{Tw}(E, \sigma) = \{\mu, \mu'\}$ where $\mu, \mu' \in (E^{\sigma})^{\times}$ with $v_E(\mu) \not\equiv v_E(\mu') \bmod 2$, see Theorem 2.22. Without loss of generality, we assume that $v_E(\mu) + D$ is odd and $v_E(\mu') + D$ is even. Proposition 8.7 shows that

$$\partial_{E,\alpha}(\mu) = \partial[E, b_\mu, \alpha] = [\lambda, b_{\bar{u}}, \bar{\alpha}] \quad \text{and} \quad \partial_{E,\alpha}(\mu') = \partial[E, b_{\mu'}, \alpha] = 0$$

where $u = u_\mu$ as in Proposition 8.7.

Suppose that $\alpha \neq 1, -1$. Then $\lambda = \kappa(\bar{\alpha})$ by Lemma 8.8 (i), and thus $\partial_{E,\alpha}(\mu) = [\kappa(\alpha), b_1, \bar{\alpha}]$. Moreover, we have $[\kappa(\alpha), -b_1, \bar{\alpha}] = [\lambda, -b_1, \bar{\alpha}] = [\lambda, b_1, \bar{\alpha}] = [\kappa(\alpha), b_1, \bar{\alpha}]$, where the second equation follows from Lemma 8.8 (ii). This means that the order of $[\kappa(\alpha), b_1, \bar{\alpha}]$ in $W_{\kappa[\Gamma]}(\kappa)$ is

at most 2. On the other hand, the class $[\kappa(\alpha), b_1, \alpha]$ in not zero because $\kappa(\alpha)$ is irreducible as a $\kappa[\Gamma]$-module. This completes the proof of the assertion (i).

Suppose that $\alpha = \pm 1$, and put $W' = \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim \omega \equiv 0 \bmod 2\}$. We have $[\lambda : \kappa] = [\lambda : \lambda^{\bar\sigma}][\lambda^{\bar\sigma} : \kappa] = 2[\lambda^{\bar\sigma} : \kappa]$, since $\bar\sigma$ is nontrivial by Proposition 8.6. Thus $\partial_{E,\alpha}(\mu) = [\lambda, b_{\bar u}, \bar\alpha] \in W'$. We remark that $W_{\kappa[\Gamma]}(\kappa; X \mp 1)$ is naturally isomorphic to the usual Witt group $W(\kappa)$. If $\operatorname{char}\kappa = 2$ then $W' = \{0\}$ by Theorem 6.38 (i), and hence we obtain $\operatorname{im}\partial_{E,\alpha} = W'$. Suppose that $\operatorname{char}\kappa \neq 2$. Then W' is a subgroup of $W_{\kappa[\Gamma]}(\kappa; X \mp 1)$ with order 2 by Theorem 6.38 (ii).

Claim: $\operatorname{disc}(b_1) \neq 1$ *in* $\kappa^\times/\kappa^{\times 2}$. Let $\overline{x_1}, \dots, \overline{x_{2n}} \in \lambda$ be a basis of λ over κ, and let τ be the generator of the Galois group $\operatorname{Gal}(\lambda/\kappa)$ defined by $\bar x \mapsto \bar x^{\#\kappa}$, see Proposition 2.4. Note that $\bar\sigma = \tau^n$. We define a matrix $A \in M_{2n}(\lambda)$ by $A := (\tau^{i-1}(\overline{x_j}))_{ij}$. Then $(b_1(\overline{x_i}, \overline{x_j}))_{ij} = {}^tAA^{\bar\sigma}$, where $A^{\bar\sigma} = (\bar\sigma\tau^{i-1}(x_j))_{ij}$. We remark that

$$\tau(\det A) = \det(\tau^i(\overline{x_j}))_{ij} = \operatorname{sgn}(1, 2, \dots, 2n) \cdot \det A = -\det A, \tag{$*$}$$

and

$$\det(A^{\bar\sigma}) = \bar\sigma(\det A) = \tau^n(\det A) = (-1)^n \det A.$$

Then, the discriminant of b_1 is calculated as

$$\operatorname{disc}(b_1) = (-1)^n \det(b_1) = (-1)^n \det({}^tA) \det(A^{\bar\sigma}) = (\det A)^2.$$

Furthermore, we have $(\det A)^{\#\kappa - 1} = \tau(\det A)/\det A = -1$ by $(*)$. This means that the square class $\operatorname{disc}(b_1) = \det(A)^2 \in \kappa^\times/\kappa^{\times 2}$ is not 1 by Proposition 2.2 (ii).

From Claim and Theorem 6.38 (ii), it follows that the class $\partial_{E,\alpha}(\mu) = [\lambda, b_1, \pm 1]$ is not zero in W'. This shows that $\operatorname{im}\partial_{E,\alpha} = W'$. The proof is complete. □

Proposition 8.10. *Suppose that E is of type* (rm). *Then $\bar\alpha = 1$ or -1. Let $\bar\alpha = \pm 1$.*

(i) *If* $\operatorname{char}\kappa \neq 2$ *then* $\operatorname{im}\partial_{E,\alpha} = \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim\omega \equiv [\lambda : \kappa] \bmod 2\}$.

(ii) *If* $\operatorname{char}\kappa = 2$ *then for any* $\mu \in (E^\sigma)^\times$ *we have*

$$\partial_{E,\alpha}(\mu) = \begin{cases} 0 & \text{if } [\lambda : \kappa]D \text{ is even} \\ \omega & \text{if } [\lambda : \kappa]D \text{ is odd} \end{cases}$$

where ω is the nontrivial element of $W_{\kappa[\Gamma]}(\kappa; X - 1) \cong W(\kappa)$.

Proof. The induced involution $\bar\sigma$ is the identity by Proposition 8.6. Thus $\bar\alpha = 1$ or -1 by Lemma 8.8 (i). Let $\bar\alpha = \pm 1$. We remark that $v_E = e(\mathfrak{p}_E/\mathfrak{p}_{E^\sigma}) v_{E^\sigma} = 2\, v_{E^\sigma}$ on E^σ by Corollary 1.36.

(i). Suppose that $\operatorname{char}\kappa \neq 2$, and put $W' = \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim\omega \equiv [\lambda : \kappa] \bmod 2\}$. The quadratic extension E/E^σ is tamely ramified (i.e., $\mathfrak{p}_E$ is tamely ramified over E^σ) since $\operatorname{char}\kappa \neq 2$. Thus $\mathfrak{D}_{E/E^\sigma} = \mathfrak{p}_E^{e(\mathfrak{p}_E/\mathfrak{p}_{E^\sigma})-1} = \mathfrak{p}_E$ by Theorem 1.40. Because

$$D = v_E(\mathfrak{D}_{E/K}) = v_E(\mathfrak{D}_{E/E^\sigma} \cdot \mathfrak{D}_{E^\sigma/K}) = v_E(\mathfrak{D}_{E/E^\sigma}) + v_E(\mathfrak{D}_{E^\sigma/K}) = 1 + 2\, v_{E^\sigma}(\mathfrak{D}_{E^\sigma/K}),$$

we have

$$v_E(\mu) + D = 2v_{E^\sigma}(\mu) + 1 + 2\, v_{E^\sigma}(\mathfrak{D}_{E^\sigma/K}) \equiv 1 \bmod 2$$

for any $\mu \in (E^\sigma)^\times$. Hence, it follows from Proposition 8.7 that $\partial_{E,\alpha}(\mu) = [\lambda, b_{\overline{u_\mu}}, \pm 1]$ for any $\mu \in (E^\sigma)^\times$. This shows that $\operatorname{im}\partial_{E,\alpha} \subset W'$.

Claim: We have $L \subset E^\sigma$, and $\operatorname{disc}(b_{\overline{u_\mu}}) = \mathrm{N}_{\lambda/\kappa}(\bar{\mu}) \operatorname{disc}(b_{\overline{u_1}})$ for any $\mu \in \mathcal{O}_L^\times$. Since E/E^σ is ramified, the unramified extension L is contained in E^σ. Let $\mu \in \mathcal{O}_L^\times$. We have

$$\overline{u_\mu} = \overline{\operatorname{Tr}_{E/L}(\mu \pi_K \pi_E^{n-1} \sigma(\pi_E^{n-1}))} = \overline{\mu \cdot \operatorname{Tr}_{E/L}(\pi_K \pi_E^{n-1} \sigma(\pi_E^{n-1}))} = \bar{\mu} \cdot \overline{u_1}$$

in λ, where $n = -(v_E(\mu) + D - 1)/2$ as in Proposition 8.7. Thus, for any $\bar{x}, \bar{y} \in \lambda$, we have

$$b_{\overline{u_\mu}}(\bar{x}, \bar{y}) = \operatorname{Tr}_{\lambda/\kappa}(\overline{u_\mu} \bar{x} \bar{\sigma}(\bar{y})) = \operatorname{Tr}_{\lambda/\kappa}(\bar{\mu} \overline{u_1} \bar{x} \bar{\sigma}(\bar{y})) = b_{\overline{u_1}}(\bar{\mu}\bar{x}, \bar{y}).$$

This shows that $\det(b_{\overline{u_\mu}}) = \mathrm{N}_{\lambda/\kappa}(\bar{\mu}) \cdot \det(b_{\overline{u_1}})$, and we obtain $\operatorname{disc}(b_{\overline{u_\mu}}) = \mathrm{N}_{\lambda/\kappa}(\bar{\mu}) \cdot \operatorname{disc}(b_{\overline{u_1}})$.

Let $\omega \in W'$. Since the norm map $\mathrm{N}_{\lambda/\kappa} : \lambda \to \kappa$ is surjective (Corollary 2.5), there exists $\mu \in \mathcal{O}_L^\times$ such that $\mathrm{N}_{\lambda/\kappa}(\bar{\mu}) = \operatorname{disc}(b_{\overline{u_1}})^{-1} \operatorname{disc}(\omega)$ (in $\kappa^\times/\kappa^{\times 2}$). Then, we have $\operatorname{disc}(b_{\overline{u_\mu}}) = \operatorname{disc}(\omega)$ by Claim. This implies $[\lambda, b_{\overline{u_\mu}}, \pm 1] = \omega$ by Theorem 6.38 (ii). Therefore $\operatorname{im} \partial_{E,\alpha} = W'$.

(ii). Suppose that $\operatorname{char} \kappa = 2$, and let $\mu \in (E^\sigma)^\times$. If D is even then so is $v_E(\mu) + D = 2 \cdot v_{E^\sigma}(\mu) + D$. In this case, Proposition 8.7 (i) shows that $\partial_{E,\alpha}(\mu) = 0$. If D is odd then so is $v_E(\mu) + D$. In this case, Proposition 8.7 (ii) shows that $\partial_{E,\alpha}(\mu) \equiv [\lambda, b_{\overline{u_\mu}}, 1]$. Thus

$$\partial_{E,\alpha}(\mu) = \begin{cases} 0 & \text{if } [\lambda : \kappa] \equiv 0 \bmod 2 \\ \text{nontrivial} & \text{if } [\lambda : \kappa] \equiv 1 \bmod 2 \end{cases}$$

by Theorem 6.38 (i). This completes the proof. □

Theorem 8.11. *Let E be a commutative K-algebra with a nontrivial involution σ. We assume that $[E : K] < \infty$ and E is a field or of type* (sp)*. Let M be a free E-module of rank m, and $\alpha \in \mathcal{O}_E^\times$ a unit with $\alpha\sigma(\alpha) = 1$.*

(i) *If E is of type* (sp) *then $\partial_{M,\alpha}$ is the zero map.*

(ii) *If E is of type* (ur) *then*

$$\operatorname{im} \partial_{M,\alpha} = \begin{cases} \{0, [\kappa(\bar{\alpha}), b_1, \bar{\alpha}]\} & \text{if } \bar{\alpha} \neq 1, -1 \\ \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim \omega \equiv 0 \bmod 2\} & \text{if } \bar{\alpha} = \pm 1. \end{cases}$$

In the case $\bar{\alpha} \neq 1, -1$, the Witt class $[\kappa(\bar{\alpha}), b_1, \bar{\alpha}]$ is of order 2.

(iii) *If E is of type* (rm) *then $\bar{\alpha} = 1$ or -1, and moreover,*

- *if $\operatorname{char} \kappa \neq 2$ and $\bar{\alpha} = \pm 1$ then $\operatorname{im} \partial_{M,\alpha} = \{\omega \in W_{\kappa[\Gamma]}(\kappa; X \mp 1) \mid \dim \omega \equiv m[\lambda : \kappa] \bmod 2\}$;*
- *if $\operatorname{char} \kappa = 2$ then for any $\mu \in \operatorname{Tw}(E, \sigma)$ we have*

$$\partial_{M,\alpha}(\mu) = \begin{cases} 0 & \text{if } m[\lambda : \kappa]D \text{ is even} \\ \text{the nontrivial class} & \text{if } m[\lambda : \kappa]D \text{ is odd} \end{cases} \quad \text{in } W_{\kappa[\Gamma]}(\kappa; X - 1).$$

Proof. By fixing a basis of M over E, we identify M with E^m. For $\mu \in (E^\sigma)^\times$, the value $\partial_{M,\alpha}(\mu)$ can be calculated as

$$\begin{aligned} \partial_{M,\alpha}(\mu) &= \partial[M, \operatorname{Tr}_{E/K} \circ \langle \mu, 1, \ldots, 1 \rangle_E, \alpha] \\ &= \partial[(E^m, b_\mu \oplus b_1 \oplus \cdots \oplus b_1, \alpha)] \\ &= \partial[E, b_\mu, \alpha] + (m-1)\partial[E, b_1, \alpha] \\ &= \partial_{E,\alpha}(\mu) + (m-1)\partial_{E,\alpha}(1). \end{aligned} \tag{$*$}$$

If E is of type (sp) then it is zero by Proposition 8.4. This shows the assertion (i). The assertions (ii) and (iii) follows from $(*)$ with Propositions 8.9 and 8.10 respectively. □

Remark 8.12. In the situation of Theorem 8.11, assume that E is of type (sp) or of type (ur), and M is the E-algebra E^m, the direct product of m copies of E. We write $\mathcal{O}_M$ for the integral closure of $\mathcal{O}_K$ in M, which is equal to $\mathcal{O}_E^m \subset M = E^m$.

(i) There exists $\mu \in (E^\sigma)^\times$ such that $(M, \mathrm{Tr}_{E/K} \circ \langle \mu, \dots, \mu \rangle_E)$ is an $\mathcal{O}_E$-stable unimodular lattice. Indeed, if E is of type (sp) then (E, b_μ) contains an $\mathcal{O}_E$-stable unimodular lattice for any $\mu \in (E^\sigma)^\times$ by Proposition 8.4; and if E is of type (ur) then there exists $\mu \in (E^\sigma)^\times$ such that $v_E(\mu) + D$ is even, and (E, b_μ) contains an $\mathcal{O}_E$-stable unimodular lattice by Proposition 8.7 (i). Hence, in either case, the space $(M, \mathrm{Tr}_{E/K} \circ \langle \mu, \dots, \mu \rangle_E) = (E, b_\mu)^{\oplus m}$ contains an $\mathcal{O}_E$-stable unimodular lattice.

(ii) Let $\mu_1, \dots, \mu_m \in (\mathcal{O}_{E^\sigma})^\times$ be units, and suppose that the extension E^σ/K is unramified. Then, in a similar manner as in (i), it follows from Propositions 8.4 and 8.7 that $\mathcal{O}_M$ is an α-stable unimodular lattice on $(M, \mathrm{Tr}_{E/K} \circ \langle \mu_1, \dots, \mu_m \rangle_E)$.

8.4 Characteristic polynomial of isometry

In the rest of this section, we deal with the problem of determining which polynomial occurs as the characteristic polynomial of an even unimodular lattice over $\mathcal{O}_K$. Let $F \in \mathcal{O}_K[X]$ be a $*$-symmetric polynomial, and write $F(X) = (X-1)^{m_+}(X+1)^{m_-}F_1(X)F_2(X)$ where $m_+, m_- \in \mathbb{Z}_{\geq 0}$ are non-negative integers and $F_i \in \mathcal{O}_K[X]$ is the type i component of F for $i = 1, 2$, see Definition 7.8. The product F_1F_2 will be abbreviated to F_{12}.

We give subscripts for irreducible factors of F_1 as follows. Note that for each $f \in I_1(F; K)$ the K-algebra $K[X]/(f)$ has the nontrivial involution σ defined by $X + (f) \mapsto (X + (f))^{-1}$. We define subsets $I_{1,\mathrm{ur}}(F; K)$ and $I_{1,\mathrm{rm}}(F; K)$ of $I_1(F; K)$ as

$$I_{1,\mathrm{ur}}(F; K) = \{ f \in I_1(F; K) \mid K[X]/(f) \text{ is of type (ur) } \},$$
$$I_{1,\mathrm{rm}}(F; K) = \{ f \in I_1(F; K) \mid K[X]/(f) \text{ is of type (rm) } \}.$$

Let $\mathcal{W}_{\mathrm{ur}}$ and $\mathcal{W}_{\mathrm{rm}}$ be sets of cardinalities $\#I_{1,\mathrm{ur}}(F; K)$ and $\#I_{1,\mathrm{rm}}(F; K)$ respectively. Then, fix bijections

$$\mathcal{W}_{\mathrm{ur}} \to I_{1,\mathrm{ur}}(F; K), \quad \mathcal{W}_{\mathrm{rm}} \to I_{1,\mathrm{rm}}(F; K)$$

and write f_w for the factor corresponding to $w \in \mathcal{W}_{\mathrm{ur}} \sqcup \mathcal{W}_{\mathrm{rm}}$. We also give subscripts for factors of F_2 as follows. Let $\mathcal{W}_{\mathrm{sp}}$ be a set of cardinality $\#I_2(F; K)/2$, Then there is a bijection between $\mathcal{W}_{\mathrm{sp}}$ and the set of all pairs of the form $\{g, g^*\}$ in $I_2(F; K)$. We fix such a bijection and write $\{g_w, g_w^*\}$ for the pair corresponding to $w \in \mathcal{W}_{\mathrm{sp}}$, and put $f_w = g_w g_w^*$. Under this notation, the polynomials F_1 and F_2 can be written as

$$F_1 = \prod_{w \in \mathcal{W}_{\mathrm{ur}}} f_w^{m_w} \times \prod_{w \in \mathcal{W}_{\mathrm{rm}}} f_w^{m_w}, \quad F_2 = \prod_{w \in \mathcal{W}_{\mathrm{sp}}} f_w^{m_w} = \prod_{w \in \mathcal{W}_{\mathrm{sp}}} (g_w g_w^*)^{m_w},$$

where m_w denotes the multiplicity of f_w in F.

In the following, the symbol M denotes the associated $K[\Gamma]$-module of F with transformation α. Set $\mathcal{W} := \mathcal{W}_{\mathrm{ur}} \sqcup \mathcal{W}_{\mathrm{rm}} \sqcup \mathcal{W}_{\mathrm{sp}}$. For each $w \in \mathcal{W}$, we write E_w, M_w, α_w for $E^{f_w}, M^{f_w}, \alpha^{f_w}$ in Notation 7.19. Then M can be expressed as

$$M = M^+ \times M^- \times \prod_{w \in \mathcal{W}_{\mathrm{ur}}} M_w \times \prod_{w \in \mathcal{W}_{\mathrm{rm}}} M_w \times \prod_{w \in \mathcal{W}_{\mathrm{sp}}} M_w,$$

where $M^\pm := M^{X \mp 1} = (K[X]/(X \mp 1))^{\times m_\pm}$. We can write

$$\mathcal{W}_{\mathrm{ur}} = \{ w \in \mathcal{W} \mid E_w \text{ is of type (ur) } \},$$
$$\mathcal{W}_{\mathrm{rm}} = \{ w \in \mathcal{W} \mid E_w \text{ is of type (rm) } \},$$
$$\mathcal{W}_{\mathrm{sp}} = \{ w \in \mathcal{W} \mid E_w \text{ is of type (sp) } \}.$$

By Proposition 8.10, if K is non-dyadic then $\mathcal{W}_{\mathrm{rm}}$ decomposes as $\mathcal{W}_{\mathrm{rm}} = \mathcal{W}_+ \sqcup \mathcal{W}_-$, where $\mathcal{W}_\pm := \{w \in \mathcal{W}_{\mathrm{rm}} \mid \overline{\alpha_w} = \pm 1\}$. For each $w \in \mathcal{W}_{\mathrm{ur}} \cup \mathcal{W}_{\mathrm{rm}}$, the residue field of E_w is denoted by λ_w.

Lemma 8.13. *Let $w \in \mathcal{W}_{\mathrm{ur}} \cup \mathcal{W}_{\mathrm{rm}}$. For any $c \in K$ we have*

$$v_K(f_w(c)) \equiv [\lambda_w : \kappa] v_{E_w}(c - \alpha_w).$$

Proof. Put $d = [E_w : K]$, and let $\beta_1, \dots, \beta_d \in \widetilde{E}_w$ be all conjugates of $\alpha_w \in E_w$, where $\widetilde{E}_w$ is the Galois closure of E_w/K. Then f_w can be written as $f_w(X) = \prod_{j=1}^d (X - \beta_j)$. For any finite extension L/K, we write $e(L/K)$ for the ramification index of corresponding maximal ideals. By using Corollary 1.36 and the fundamental identity (Proposition 1.22), we obtain

$$\begin{aligned} v_K(f_w(c)) &= e(\widetilde{E}_w/K)^{-1} \cdot v_{\widetilde{E}_w}(\textstyle\prod_{j=1}^d (c - \beta_j)) \\ &= e(\widetilde{E}_w/K)^{-1} \cdot d \cdot v_{\widetilde{E}_w}(c - \alpha_w) \\ &= e(\widetilde{E}_w/K)^{-1} \cdot d \cdot e(\widetilde{E}_w/E_w) \cdot v_{E_w}(c - \alpha_w) \\ &= e(E_w/K)^{-1} \cdot d \cdot v_{E_w}(c - \alpha_w) \\ &= [\lambda_w : \kappa] \cdot v_{E_w}(c - \alpha_w) \end{aligned}$$

for any $c \in K$, as required. □

Lemma 8.14. *Let $w \in \mathcal{W}$.*

(i) *If $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$ then $v_K(f_w(1)) \equiv v_K(f_w(-1)) \equiv 0 \bmod 2$.*

(ii) *Suppose that K is non-dyadic and $w \in \mathcal{W}_\pm$. Then $v_K(f_w(\mp 1)) = 0$. Moreover, for any $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ we have $\dim \partial_{M_w, \alpha_w}(\mu_w) \equiv m_w v_K(f_w(\pm 1)) \bmod 2$.*

Proof. (i). Suppose that $w \in \mathcal{W}_{\mathrm{sp}}$. We remark that $g_w(0)$ is a unit of $\mathcal{O}_K$ because $g_w(0)$ and $g_w(0)^{-1}$ are the constant terms of g_w and $g_w^* \in \mathcal{O}_K[X]$ respectively. Then

$$\begin{aligned} v_K(f_w(\pm 1)) &= v_K(g_w(\pm 1) g_w^*(\pm 1)) \\ &= v_K(g_w(\pm 1) g_w(0)^{-1} (-1)^{\deg g} g_w(\pm 1)) = 2 v_K(g_w(\pm 1)) \equiv 0 \mod 2. \end{aligned}$$

Suppose that $w \in \mathcal{W}_{\mathrm{ur}}$. Then $v_K(f_w(\pm 1)) = [\lambda_w : \kappa] v_{E_w}(1 \mp \alpha_w)$ by Lemma 8.13. Furthermore $[\lambda_w : \kappa]$ is even since the induced involution $\bar{\sigma} : \lambda_w \to \lambda_w$ is nontrivial (Proposition 8.6). Hence $v_K(f_w(\pm 1)) \equiv 0 \bmod 2$. This completes the proof of the assertion (i).

(ii). We have $v_K(f_w(\mp 1)) = [\lambda_w : \kappa] v_{E_w}(1 \mp \alpha_w)$ by Lemma 8.13, and $1 \pm \alpha_w \in \mathcal{O}_{E_w}^\times$ because $\overline{1 \pm \alpha_w} = 2 \neq 0$ in λ_w. Thus $v_K(f_w(\mp 1)) = 0$. To prove the latter assertion, let $\mu_w \in \mathrm{Tw}(E_w, \sigma)$, and let h_w be a hermitian product on M with determinant μ_w. Then $\dim \partial_{M_w, \alpha_w}(\mu_w) \equiv v_K(\det(\mathrm{Tr}_{E_w/K} \circ h_w)) \bmod 2$ by Proposition 6.35, and $\det(\mathrm{Tr}_{E_w/K} \circ h_w) = f_w(1)^{m_w} f_w(-1)^{m_w}$ in $K^\times / K^{\times 2}$ by Proposition 7.32. Thus

$$\begin{aligned} \dim \partial_{M_w, \alpha_w}(\mu_w) &\equiv v_K(\det(\mathrm{Tr}_{E_w/K} \circ h_w)) \\ &\equiv v_K(f_w(1)^{m_w} f_w(-1)^{m_w}) \\ &= m_w v_K(f_w(1)) + m_w v_K(f_w(-1)) \\ &= m_w v_K(f_w(\pm 1)) \mod 2, \end{aligned}$$

where the last equality follows from $v_K(f_w(\mp 1)) = 0$. This completes the proof. □

Lemma 8.14 yields a necessary condition for the existence of an inner product b on M such that (M, b) contains an α-stable unimodular lattice.

Proposition 8.15. *Suppose that K is non-dyadic. If there exists an inner product b on M such that (M,b) contains an α-stable unimodular lattice over $\mathcal{O}_K$ then $v_K(F(1)) \equiv v_K(F(-1)) \equiv 0 \bmod 2$. Here, we adopt the convention that $v_K(0) \equiv 0 \bmod 2$.*

Proof. Let b be an inner product on M such that (M,b) contains an α-stable unimodular lattice. If $F(1) = 0$ then $v_K(F(1)) \equiv 0 \bmod 2$ by our convention. Suppose that $F(1) \neq 0$. Note that for any $w \in \mathcal{W}$ there exists $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ and such that $\partial[M_w, b|_{M_w}, \alpha_w] = \partial_{M_w,\alpha_w}(\mu_w)$ by Proposition 7.20. We have

$$\begin{aligned} v_K(F(1)) &= v_K\left((1+1)^{m_-} \textstyle\prod_{w\in\mathcal{W}} f_w(1)^{m_w}\right) \\ &\equiv \sum_{w\in\mathcal{W}_+} m_w v_K(f_w(1)) + \sum_{w\in\mathcal{W}_-} m_w v_K(f_w(1)) \\ &\equiv \sum_{w\in\mathcal{W}_+} \dim(\partial[M_w, b|_{M_w}, \alpha_w]) \mod 2 \end{aligned}$$

by Lemma 8.14. On the other hand, we have $\partial[M,b,\alpha] = 0$ since (M,b) contains an α-stable unimodular lattice. Thus the image of $\partial[M,b,\alpha] \in W_{\kappa[\Gamma]}(\kappa)$ under the projection $W_{\kappa[\Gamma]}(\kappa) \to W_{\kappa[\Gamma]}(\kappa; X-1)$ is also 0, and in particular has dimension 0 mod 2. Moreover, the dimension of the image is given by $\dim \sum_{w\in\mathcal{W}_+} \dim(\partial[M_w, b|_{M_w}, \alpha_w])$ because $\dim(\partial[M_w, b|_{M_w}, \alpha_w]) \equiv 0 \bmod 2$ for any $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$ by Theorem 8.11 (or by Proposition 7.32 and Lemma 8.14 (i)). Therefore $v_K(F(1)) \equiv \sum_{w\in\mathcal{W}_+} \dim(\partial[M_w, b|_{M_w}, \alpha_w]) \equiv 0 \bmod 2$. Similarly we obtain $v_K(F(-1)) \equiv \sum_{w\in\mathcal{W}_-} \dim(\partial[M_w, b|_{M_w}, \alpha_w]) \equiv 0 \bmod 2$. The proof is complete. □

The congruence $v_K(F(1)) \equiv v_K(F(-1)) \equiv 0 \bmod 2$ is also a sufficient condition.

Theorem 8.16. *Suppose that K is non-dyadic. Let $F \in \mathcal{O}_K[X]$ be a $*$-symmetric polynomial, and M the associated $K[\Gamma]$-module of F with transformation α. Assume that $v_K(F(1)) \equiv v_K(F(-1)) \equiv 0 \bmod 2$. Then there exists an inner product b on M such that (M,b) contains an α-stable unimodular lattice over $\mathcal{O}_K$. Furthermore*

(a) *if $F(\pm 1) = 0$ then such an inner product can be chosen to satisfy $\det(b|_{M^\pm}) = u_\pm F_{12}(\pm 1)$ for any given $u_\pm \in \mathcal{O}_K^\times$; and*

(b) *if $\mathcal{W}_{\mathrm{rm}} = \emptyset$ then such an inner product can be chosen so that each of subspaces $(M^+, b|_{M^+})$, $(M^-, b|_{M^-})$, and $(M_w, b|_{M_w})$ for all $w \in \mathcal{W}$ contains an α-stable unimodular lattice.*

Proof. Let $u_+, u_- \in \mathcal{O}_K^\times$ be units. If $F(\pm 1) = 0$ we take an inner product $b^\pm$ on $M^\pm$ whose Gram matrix is $\mathrm{diag}(u_\pm F_{12}(\pm 1), 1, \dots, 1)$. Note that for any family $(\mu_w)_{w\in\mathcal{W}_\pm}$ consisting of $\mu_w \in \mathrm{Tw}(E_w, \sigma)$, we have

$$v_K(F_{12}(\pm 1)) = \sum_{w\in\mathcal{W}} m_w v_K(f_w(\pm 1)) \equiv \sum_{w\in\mathcal{W}_\pm} m_w v_K(f_w(\pm 1)) \equiv \sum_{w\in\mathcal{W}_\pm} \partial_{M_w,\alpha_w}(\mu_w) \mod 2 \quad (*)$$

by Lemma 8.14.

Claim: If $\mathcal{W}_\pm = \emptyset$ then $\partial[M^\pm, b^\pm, \pm 1] = 0$. If $\mathcal{W}_\pm \neq \emptyset$ then there exists a family $(\mu_w)_{w\in\mathcal{W}_\pm}$ consisting of $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ such that $\sum_{w\in\mathcal{W}_\pm} \partial_{M_w,\alpha_w}(\mu_w) = -\partial[M^\pm, b^\pm, \pm 1]$. Suppose that $\mathcal{W}_\pm = \emptyset$. Then $v_K(F_{12}(\pm 1)) \equiv 0 \bmod 2$ by $(*)$. Let $e_1, \dots, e_{m_\pm}$ be a basis of $(M^\pm, b^\pm)$ such that the corresponding Gram is $\mathrm{diag}(u_\pm F_{12}(\pm 1), 1, \dots, 1)$. Then the lattice

$$\mathcal{O}_K(\pi_K^{-v_K(F_{12}(\pm 1))/2} e_1) + \mathcal{O}_K e_2 + \cdots + \mathcal{O}_K e_{m_\pm}$$

is a unimodular lattice on $(M^{\pm}, b^{\pm})$. Hence $\partial[M^{\pm}, b^{\pm}, \pm 1] = 0$. Suppose that $\mathcal{W}_{\pm} \neq \emptyset$. For any family $(\mu_w)_{w \in \mathcal{W}_{\pm}}$, we have

$$\dim(-\partial[M^{\pm}, b^{\pm}, \pm 1]) \equiv v_K(\det b^{\pm}) \equiv v_K(F_{12}(\pm 1)) \equiv \sum_{w \in \mathcal{W}_{\pm}} \partial_{M_w, \alpha_w}(\mu_w) \mod 2,$$

where the first and last congruences follow from Proposition 6.35 and Equation $(*)$ respectively. Thus, Theorem 8.11 (iii) shows that we can take a suitable family $(\mu_w)_{w \in \mathcal{W}_{\pm}}$ so that $\sum_{w \in \mathcal{W}_{\pm}} \partial_{M_w, \alpha_w}(\mu_w) = -\partial[M^{\pm}, b^{\pm}, \pm 1]$. This completes the proof of Claim.

Let $(\mu_w)_{w \in \mathcal{W}_{\pm}}$ be a family as in Claim if $\mathcal{W}_{\pm} \neq \emptyset$. Furthermore, for each $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$, we take $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ satisfying $\partial_{M_w, \alpha_w}(\mu_w) = 0$. This is possible by Theorem 8.11 (i), (ii). Let $h_w : M_w \times M_w \to E_w$ be a hermitian product with determinant μ_w for each $w \in \mathcal{W}$, and define the inner product b on M by

$$b := b^+ \oplus b^- \oplus \bigoplus_{w \in \mathcal{W}} \mathrm{Tr}_{E_w/K} \circ h_w.$$

Then

$$\begin{aligned} \partial[M, b, \alpha] &= \partial[M^+, b^+, +1] + \partial[M^-, b^-, -1] + \sum_{w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}} \partial_{M_w, \alpha_w}(\mu_w) \\ &\quad + \sum_{w \in \mathcal{W}_+} \partial_{M_w, \alpha_w}(\mu_w) + \sum_{w \in \mathcal{W}_-} \partial_{M_w, \alpha_w}(\mu_w) \\ &= 0. \end{aligned}$$

This implies that (M, b) contains an α-stable unimodular lattice by Theorem 6.32. The assertions (a) and (b) are obvious by the construction of b. □

Corollary 8.17. *Suppose that K is non-dyadic. Let $F \in \mathcal{O}_K[X]$ be a $*$-symmetric polynomial. There exists a unimodular lattice having a semisimple isometry with characteristic polynomial F if and only if $v_K(F(1)) \equiv v_K(F(-1)) \equiv 0 \bmod 2$.*

Proof. The if part follows from Theorem 8.16. Suppose that there exists a unimodular lattice (Λ, b) having a semisimple isometry t with characteristic polynomial F. Then $\Lambda \otimes_{\mathcal{O}_K} K$ can be identified with the associated $K[\Gamma]$-module M of F with transformation t by Lemma 7.18. In this case $b \otimes K$ is an inner product on M such that Λ is a t-stable unimodular lattice on $(M, b \otimes K)$. Hence, we obtain $v_K(F(1)) \equiv v_K(F(-1)) \equiv 0 \bmod 2$ by Proposition 8.15. □

8.5 Dyadic case

Let us proceed to the dyadic case. We restrict ourselves to the case $K = \mathbb{Q}_2$ to avoid complexity. We refer to [22] for the general case.

Proposition 8.18. *Let (V, b) be an inner product space over $\mathbb{Q}_2$, and t an isometry of V. There exists a t-stable even unimodular lattice on V if and only if the following three conditions hold:*

(i) *V contains a t-stable unimodular lattice.*

(ii) *V contains an even unimodular lattice.*

(iii) $v_2(\mathrm{sn}(t)) \equiv \begin{cases} 0 \bmod 2 & \text{if } \det t = 1 \\ 1 \bmod 2 & \text{if } \det t = -1 \end{cases} \mod 2.$

Proof. If there exists a t-stable even unimodular lattice on V then the conditions (i) and (ii) hold clearly, and (iii) follows from Corollary 7.34.

Suppose conversely that the three conditions hold, and let Λ_0 be a t-stable lattice and Λ_1' an even unimodular lattice on V. If $\Lambda_1' \cong \left\langle \begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix} \right\rangle_{\mathbb{Z}_2}$ then a computation shows that every integral lattice on V is even, and in particular Λ_0 is a t-stable even unimodular lattice. So, by Theorem 5.23, we may assume that Λ_1' contains a hyperbolic sublattice H. Furthermore, we assume that Λ_0 is odd since we are done if it is even. Let e_1' and $e_2' \in V$ be vectors such that $2e_1'$ and e_2' form a hyperbolic basis of H. Put $N' = H^\perp \subset \Lambda_1'$ and $\Lambda_0' = N' + \mathbb{Z}_2(e_1' + e_2') + \mathbb{Z}_2(e_1' - e_2')$. Then Λ_0' is an odd lattice on V, and Corollary 5.22 shows that there exists $\tau \in \mathrm{O}(V, b)$ such that $\tau(\Lambda_0') = \Lambda_0$. We show that the even unimodular lattice $\Lambda_1 := \tau(\Lambda_1)$ on V is t-stable. Put $H = \tau(H')$, $e_1 = \tau(e_1')$ and $e_2 = \tau(e_2')$. Then $\Lambda_1 = N + \mathbb{Z}_2(2e_1) + \mathbb{Z}_2 e_2$ and $\Lambda_0 = N + \mathbb{Z}_2(e_1 + e_2) + \mathbb{Z}_2(e_1 - e_2)$. In addition, we consider lattices Λ_2 and Λ on V defined by $\Lambda_2 := N + \mathbb{Z}_2 e_1 + \mathbb{Z}_2(2e_2)$ and $\Lambda := N + \mathbb{Z}_2(2e_1) + \mathbb{Z}_2(2e_2)$ respectively. Then Λ_2 is an even unimodular lattice different from Λ_1, and Λ is contained in Λ_0, Λ_1 and Λ_2. Note that

$$\Lambda^\vee/\Lambda \cong (\mathbb{Z}_2(2e_1) + \mathbb{Z}_2(2e_2))^\vee/(\mathbb{Z}_2(2e_1) + \mathbb{Z}_2(2e_2)) \cong \mathbb{Z}_2/2\mathbb{Z}_2 \oplus \mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

see Proposition 5.15. This implies that $\Lambda^\vee/\Lambda$ has exactly 3 submodules except for 0 and $\Lambda^\vee/\Lambda$ itself, and Λ has at most 3 overlattices by Proposition 5.17. Hence, there is no overlattice of Λ other than Λ_0, Λ_1 and Λ_2.

Claim: We have $\Lambda = \{x \in \Lambda_0 \mid b(x,x) \in 2\mathbb{Z}_2\}$. Put $\Lambda' = \{x \in \Lambda_0 \mid b(x,x) \in 2\mathbb{Z}_2\}$. Since N is an even lattice, $b(2e_1, 2e_1) = b(2e_2, 2e_2) = 0$ and $b(2e_1, 2e_2) = 2$, we have $\Lambda \subset \Lambda'$. To prove the reverse inclusion, it is enough to show that any $x \in \mathbb{Z}_2(e_1 + e_2) + \mathbb{Z}_2(e_1 - e_2)$ belongs to Λ if $b(x,x) \in 2\mathbb{Z}_2$. Let $x = c_1(e_1 + e_2) + c_2(e_1 - e_2) \in \mathbb{Z}_2(e_1 + e_2) + \mathbb{Z}_2(e_1 - e_2)$ $(c_1, c_2 \in \mathbb{Z}_2)$, and suppose that $b(x,x) \in 2\mathbb{Z}_2$. Because

$$b(x,x) = b((c_1 + c_2)e_1 + (c_1 - c_2)e_2, (c_1 + c_2)e_1 + (c_1 - c_2)e_2) = (c_1 + c_2)(c_1 - c_2),$$

we have $(c_1 + c_2)(c_1 - c_2) \in 2\mathbb{Z}_2$. This means that $c_1 + c_2 \in 2\mathbb{Z}_2$ or $c_1 - c_2 \in 2\mathbb{Z}_2$, and hence both belong to $2\mathbb{Z}_2$. Therefore $x = (c_1 + c_2)e_1 + (c_1 - c_2)e_2 \in \mathbb{Z}_2(2e_1) + \mathbb{Z}_2(2e_2) \subset \Lambda$, and this completes the proof of Claim.

By Claim, the lattice Λ is preserved by t since so is Λ_0. Thus, the overlattices of Λ are permuted by t. Since Λ_0 is odd, and Λ_1, Λ_2 are even, we have $t(\Lambda_1) = \Lambda_1$ or $t(\Lambda_1) = \Lambda_2$. Suppose to the contrary that we had $t(\Lambda_1) = \Lambda_2$. Let s denote the reflection orthogonal to $e_1 + e_2$. Then $s(\Lambda_2) = \Lambda_1$, and $s \circ t$ preserves Λ_1. On the other hand, we have

$$\begin{aligned} v_2(\mathrm{sn}(s \circ t)) &= v_2(\mathrm{sn}(s)) + v_2(\mathrm{sn}(t)) \\ &= v_2(b(e_1 + e_2, e_1 + e_2)) + v_2(\mathrm{sn}(t)) \\ &\equiv \begin{cases} 0 \bmod 2 & \text{if } \det t = 1 \\ 1 \bmod 2 & \text{if } \det t = -1 \end{cases} \\ &\equiv \begin{cases} 0 \bmod 2 & \text{if } \det(s \circ t) = -1 \\ 1 \bmod 2 & \text{if } \det(s \circ t) = 1 \end{cases} \end{aligned}$$

by the assumption (iii). However, this contradicts Corollary 7.34. Therefore, we have $t(\Lambda_1) = \Lambda_1$ as required. The proof is complete. □

Theorem 8.19. *Let $F \in \mathbb{Z}_2[X]$ be a $*$-symmetric polynomial of even degree $2n$, and let $\delta \in \{1, -3\} \subset \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. Assume that*

(a) $v_2(F(1)) \equiv v_2(F(-1)) \equiv 0 \bmod 2$*; and*

(b) *if* $F(1)F(-1) \neq 0$ *then* $(-1)^n F(1)F(-1) = \delta$ *in* $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.

Then there exists an inner product b *on the associated* $\mathbb{Q}_2[\Gamma]$*-module* M *of* F *with transformation* α *such that* $\operatorname{disc} b = \delta$ *and* (M, b) *contains an* α*-stable even unimodular lattice over* $\mathbb{Z}_2$*. Furthermore, if* $F(1) = F(-1) = 0$ *then such an inner product can be chosen to satisfy*

$$\det M^{\pm} = \begin{cases} u_{\pm} F_{12}(\pm 1) & \text{if } m_+ \text{ is even} \\ 2u_{\pm} F_{12}(\pm 1) & \text{if } m_+ \text{ is odd} \end{cases}$$

for any given $u_+, u_- \in \mathcal{O}_K^\times$ *such that* $u_+ u_- = (-1)^n \delta$.

Proof. We take an inner product b on M as follows. First, set

$$\delta_{\pm} = \begin{cases} u_{\pm} F_{12}(\pm 1) & \text{if } m_+ \text{ is even} \\ 2u_{\pm} F_{12}(\pm 1) & \text{if } m_+ \text{ is odd} \end{cases}$$

and take inner products b^+ on M^+ and b^- on M^- satisfying

$$\det b^+ = \begin{cases} (-1)^n \delta F_{12}(1) F_{12}(-1) & \text{if } F(1) = 0 \text{ and } F(-1) \neq 0 \\ \delta_+ & \text{if } F(1) = F(-1) = 0, \end{cases}$$

$$\det b^- = \begin{cases} (-1)^n \delta F_{12}(1) F_{12}(-1) & \text{if } F(1) \neq 0 \text{ and } F(-1) = 0 \\ \delta_- & \text{if } F(1) = F(-1) = 0. \end{cases} \qquad (*)$$

Next, for each $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$ we fix $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ satisfying $\partial_{M_w, \alpha_w}(\mu_w) = 0$. This is possible by Theorem 8.11. Furthermore, we take $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ arbitrarily for each $w \in \mathcal{W}_{\mathrm{rm}}$. Then, for each $w \in \mathcal{W}$ we define an inner product b_w on M_w by $b_w := \mathrm{Tr}_{E_w/\mathbb{Q}_2} \circ h_w$, where h_w is a hermitian product on M_w over E_w with determinant μ_w, and define $b := b^+ \oplus b^- \oplus \bigoplus_{w \in \mathcal{W}} b_w$. Then, the discriminant of b is δ, and α is an isometry with respect to b.

Claim 1*: For any* b *constructed as above, the inner product space* (M, b) *with the isometry* α *satisfies the conditions* (i) *and* (iii) *in Proposition* 8.18. For (i), it is enough to show that $\partial[M, b, \alpha] = 0$ by Theorem 6.32. By Proposition 6.35, we have

$$\begin{aligned} \dim \partial[M^+ \oplus M^-, b^+ \oplus b^-, \alpha|_{M^+ \oplus M^-}] &\equiv v_2(\det(b^+ \oplus b^-)) \\ &\equiv v_2((-1)^n \delta F_{12}(1) F_{12}(-1)) \\ &\equiv v_2(F_{12}(1) F_{12}(-1)) \mod 2. \end{aligned}$$

On the other hand, since $\partial[M_w, b_w, \alpha|_{M_w}] = \partial_{M_w, \alpha_w}(\mu_w) = 0$ for $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$, we have

$$\begin{aligned} \dim \partial \left[\bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} M_w, \bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} b_w, \alpha|_{\bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} M_w} \right] &\equiv \dim \partial \left[\bigoplus_{w \in \mathcal{W}} M_w, \bigoplus_{w \in \mathcal{W}} b_w, \alpha|_{\bigoplus_{w \in \mathcal{W}} M_w} \right] \\ &\equiv v_2 \left(\det \left(\bigoplus_{w \in \mathcal{W}} b_w \right) \right) \\ &\equiv v_2(F_{12}(1) F_{12}(-1)) \mod 2 \end{aligned}$$

by Propositions 6.35 and 7.32. Hence

$$\dim \partial[M^+ \oplus M^- \oplus \bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} M_w, b^+ \oplus b^- \oplus \bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} b_w, \alpha|_{M^+ \oplus M^- \oplus \bigoplus_{w \in \mathcal{W}_{\mathrm{rm}}} M_w}] \equiv 0 \mod 2,$$

which means that

$$\partial[M^+ \oplus M^- \oplus \bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} M_w, b^+ \oplus b^- \oplus \bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} b_w, \alpha|_{M^+\oplus M^-\oplus\bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} M_w}] = 0$$

by Theorem 6.38 (i). Therefore

$$\begin{aligned}
&\partial\left[M^+ \oplus M^- \oplus \bigoplus_{w\in\mathcal{W}} M_w, b^+ \oplus b^- \oplus \bigoplus_{w\in\mathcal{W}} b_w, \alpha|_{M^+\oplus M^-\oplus\bigoplus_{w\in\mathcal{W}} M_w}\right] \\
&= \partial\left[M^+ \oplus M^- \oplus \bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} M_w, b^+ \oplus b^- \oplus \bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} b_w, \alpha|_{M^+\oplus M^-\oplus\bigoplus_{w\in\mathcal{W}_{\mathrm{rm}}} M_w}\right] \\
&\quad + \sum_{w\in\mathcal{W}_{\mathrm{sp}}\cup\mathcal{W}_{\mathrm{ur}}} \partial_{M_w,\alpha_w}(\mu_w) \\
&= 0.
\end{aligned}$$

Let us show (iii). If $F(-1) \neq 0$ then $v_2(\mathrm{sn}(\alpha)) \equiv v_2(F_{12}(-1)) \equiv 0 \bmod 2$ by (30) and the assumption (a). Suppose that $F(-1) = 0$. If $F(1) \neq 0$ then

$$v_2(\mathrm{sn}(\alpha)) \equiv v_2((-1)^n \delta F_{12}(1)F_{12}(-1)) + v_2(F_{12}(-1)) \equiv v_2(F_{12}(1)) \equiv 0 \mod 2$$

by (30), $(*)$, and the assumption (a). If $F(1) = 0$ then

$$v_2(\mathrm{sn}(\alpha)) \equiv \begin{cases} v_2(\delta_-) + v_2(F_{12}(-1)) \equiv 0 & \text{if } m_+ \text{ is even} \\ v_2(\delta_-) + v_2(F_{12}(-1)) \equiv 1 & \text{if } m_+ \text{ is odd} \end{cases} \mod 2$$

by (30) and $(*)$. Hence, the condition (iii) holds in any case, and Claim 1 has now been proved.
Claim 2: If b^+ and b^-, and $\mu_w \in \mathrm{Tw}(E_w, \sigma)$ for each $w \in \mathcal{W}_{\mathrm{rm}}$ are suitably chosen, then (M, b) satisfies the condition (ii) *in Proposition* 8.18*, that is, (M, b) contains an even unimodular lattice.*
In general, for each non-negative even integer $d \in 2\mathbb{Z}_{\geq 0}$ there is a unique $\theta_d \in \{0, 1\}$ such that any inner product space over $\mathbb{Q}_2$ of dimension d, discriminant δ, and Hasse-Witt invariant θ_d contains an even unimodular lattice. This is a consequence of Theorem 5.23. Suppose first that $\mathcal{W}_{\mathrm{rm}} \neq \emptyset$, and let $w_0 \in \mathcal{W}_{\mathrm{rm}}$. Let $\widehat{\mu}_{w_0} \in \mathrm{Tw}(E_{w_0}, \sigma)$ be an element different from μ_{w_0}, and $\widehat{h}_{w_0}$ a hermitian product on M_{w_0} with determinant $\widehat{\mu}_{w_0}$. Then, we define $\widehat{b}_{w_0} := \mathrm{Tr}_{E_{w_0}/\mathbb{Q}_2} \circ \widehat{h}_{w_0}$ and $\widehat{b} := b^+ \oplus b^- \oplus \widehat{b}_{w_0} \oplus \bigoplus_{w\neq w_0} b_w$. Because $\mathrm{hw}_2(b) \neq \mathrm{hw}_2(\widehat{b})$, we have $\mathrm{hw}_2(b) = \theta_{2n}$ or $\mathrm{hw}_2(\widehat{b}) = \theta_{2n}$. This means that the condition (ii) holds for (M, b) or $(M, \widehat{b})$.

Suppose then that $\mathcal{W}_{\mathrm{rm}} = \emptyset$. We first show that (M_w, b_w) contains an (α-stable) even unimodular lattice for each $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$. Let $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$. We may assume that (M_w, b_w) contains an $\mathcal{O}_E$-stable unimodular lattice Λ_w by Remark 8.12 (i). Note that there exists $\gamma \in \mathcal{O}_E$ such that $\gamma + \sigma(\gamma) = 1$. It is clear if $w \in \mathcal{W}_{\mathrm{sp}}$ and follows from Corollary 2.20 if $w \in \mathcal{W}_{\mathrm{ur}}$. Then, for any $x \in \Lambda_w$ we have

$$b(x, x) = b((\gamma + \sigma(\gamma))x, x) = b(\gamma x, x) + b(\sigma(\gamma)x, x) = 2b(\gamma x, x) \in 2\mathbb{Z}_2.$$

This shows that (M_w, b_w) contains an even unimodular lattice for each $w \in \mathcal{W}_{\mathrm{sp}} \cup \mathcal{W}_{\mathrm{ur}}$. So, in order to complete the proof of Claim 2, it is sufficient to show that $(M^+ \oplus M^-, b^+ \oplus b^-)$ contains an even unimodular lattice under a suitable choice of b^+ and b^-.

Case I. *$m_+ > 2$ or $m_- > 2$.* Suppose that $m_+ > 2$. Then there exists an inner product $\widehat{b}^+$ on M^+ with $\det \widehat{b}^+ = \det b^+$ and $\mathrm{hw}_2(\widehat{b}^+) \neq \mathrm{hw}_2(b^+)$. Because $\mathrm{hw}_2(b^+ \oplus b^-) = \theta_{m_+ + m_-}$ or $\mathrm{hw}_2(\widehat{b}^+ \oplus b^-) = \theta_{m_+ + m_-}$, either $(M^+ \oplus M^-, b^+ \oplus b^-)$ or $(M^+ \oplus M^-, \widehat{b}^+ \oplus b^-)$ contains an even

unimodular lattice. Similarly, if $m_- > 2$ then $(M^+ \oplus M^-, b^+ \oplus b^-)$ contains an even unimodular lattice for a suitable b^-.

Case II. $(m_+, m_-) = (2, 2)$. If $\delta_+ \neq -1$ or $\delta_- \neq -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then we can choose b^+ and b^- so that $\mathrm{hw}_2(b^+ \oplus b^-) = \theta_4$ as in Case I. If $\delta_+ = \delta_- = -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then b^+ and b^- are isomorphic to the hyperbolic plane and contain even unimodular lattices respectively.

Case III. $(m_+, m_-) = (2, 0)$ *or* $(0, 2)$. A similar proof of Case II works, and b^+ or b^- contains an even unimodular lattice if we choose b^+ or b^- suitably.

Case IV. $(m_+, m_-) = (1, 1)$. Since b has discriminant $\delta \in \{1, -3\}$ and $(\bigoplus_{w\in\mathcal{W}} M_w, \bigoplus_{w\in\mathcal{W}} b_w)$ contains an even unimodular lattice, we have $\mathrm{disc}(b^+ \oplus b^-) = \mathrm{disc}(b)^{-1} \cdot \mathrm{disc}(\bigoplus_{w\in\mathcal{W}} b_w) = 1$ or -3 by Theorem 5.23. If $\mathrm{disc}(b^+ \oplus b^-) = 1$ then $b^+ \oplus b^-$ is isomorphic to the hyperbolic plane and contains an even unimodular lattice. Suppose that $\mathrm{disc}(b^+ \oplus b^-) = -3$. Lemma 8.14 (i) implies that $v_2(F_{12}(1)) \equiv 0 \bmod 2$ since $\mathcal{W}_{\mathrm{rm}} = \emptyset$. The Hasse-Witt invariant of $b^+ \oplus b^-$ can be calculated as

$$\begin{aligned}\mathrm{hw}_2(b^+ \oplus b^-) &= (\delta_+, \delta_-)_2 = (\delta_+, -\delta_+\delta_-)_2 = (2u_+F_{12}(1), \mathrm{disc}(b^+ \oplus b^-))_2 \\ &= (2u_+F_{12}(1), -3)_2 = (2, -3)_2 + (u_+F_{12}(1), -3)_2 = 1\end{aligned}$$

by Theorem 4.61 (iii), and this means that $b^+ \oplus b^-$ is isomorphic to the lattice $\left\langle \begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix} \right\rangle_{\mathbb{Z}_2}$. Thus, the space $(M^+ \oplus M^-, b^+ \oplus b^-)$ contains an even unimodular lattice.

In any case, the space $(M^+ \oplus M^-, b^+ \oplus b^-)$ contains an even unimodular lattice if we choose b^+ and b^- suitably. This completes the proof of Claim 2.

Claims 1 and 2 mean that the inner product space (M, b) with the isometry α satisfies the conditions (i)–(iii) in Proposition 8.18 for a suitable inner product b. This implies that (M, b) contains an α-stable even unimodular lattice. The latter part of this theorem is obvious by the construction of b. □

Corollary 8.20. *Let $F \in \mathbb{Z}_2[X]$ be a $*$-symmetric polynomial of even degree. There exists an even unimodular lattice having a semisimple isometry with characteristic polynomial F if and only if the following conditions hold.*

(a) $v_2(F(1)) \equiv v_2(F(-1)) \equiv 0 \bmod 2$.

(b) *If $F(1)F(-1) \neq 0$ then $(-1)^{\deg(F)/2}F(1)F(-1) = 1$ or -3 in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.*

Proof. The if part follows from Theorem 8.19. Suppose that there exists an even unimodular lattice (Λ, b) having a semisimple isometry t with characteristic polynomial F, and put $V = \Lambda \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. If $\det t = -1$, i.e., F is -1-symmetric, then $F(1) = F(-1) = 0$, and the conditions (a) and (b) are clear. Suppose that $\det t = 1$, and write F as $F(X) = (X-1)^{m_+}(X+1)^{m_-}F_{12}(X)$ where m_+, m_- are the multiplicities of $X-1, X+1$, and F_{12} is the product of type 1 and 2 components. Note that m_+ and m_- are even since F is $+1$-symmetric and of even degree. We have

$$v_2(\det(b|_{V(X+1;t)})) + v_2(F_{12}(-1)) \equiv v_2(\mathrm{sn}(t)) \equiv 0 \mod 2 \qquad (*)$$

by Equation (30) and Corollary 7.34. On the other hand, we have

$$v_2(\det(b|_{V(X-1;t)})) + v_2(\det(b|_{V(X+1;t)})) + v_2(F_{12}(1)) + v_2(F_{12}(-1)) \equiv v_2(\det b) \equiv 0 \mod 2$$

by Proposition 7.32, and hence

$$v_2(\det(b|_{V(X-1;t)})) + v_2(F_{12}(1)) \equiv 0 \mod 2. \qquad (**)$$

If $F(-1) \neq 0$ then

$$v_2(F(-1)) \equiv v_2((-1-1)^{m_+}F_{12}(-1)) = m_+ + v_2(F_{12}(-1)) \equiv v_2(F_{12}(-1)) \equiv 0 \bmod 2$$

by Equation $(*)$. Similarly, if $F(1) \neq 0$ then $v_2(F(1)) \equiv v_2(F_{12}(1)) \equiv 0 \bmod 2$ by Equation $(**)$. Therefore, we get the condition (a). Suppose that $F(1)F(-1) \neq 0$. Then, we have

$$(-1)^{\deg(F)/2}F(1)F(-1) = (-1)^{\deg(F)/2}\det b = \operatorname{disc} b = 1 \text{ or } -3 \quad \text{in } \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2},$$

where the first and last equalities follow from Proposition 7.32 and Theorem 5.23 respectively. This is the condition (b), and the proof is complete. □

9 Local-global principle and obstruction

In this section, we fix non-negative integers $r, s \in \mathbb{Z}_{\geq 0}$ with $r \equiv s \bmod 8$ and a $*$-symmetric polynomial $F \in \mathbb{Z}[X]$ of degree $r+s$. Note that the congruence $r \equiv s \bmod 8$ is a necessary and sufficient condition for the existence of an even unimodular lattice (over $\mathbb{Z}$) of signature (r,s) (see Theorem 5.24). We will establish a criterion for the existence of an even unimodular lattice of signature (r,s) having a semisimple isometry with characteristic polynomial F and with a prescribed index $\mathfrak{i} \in \mathrm{Idx}(r,s;F)$. The key idea is to use local-global theory on the associated $\mathbb{Q}[\Gamma]$-module of F. We refer to an isometry with characteristic polynomial F and index $\mathfrak{i}$ as an $(F,\mathfrak{i})$-*isometry* for short.

9.1 Local conditions

If F is the characteristic polynomial of a semisimple isometry t of an even unimodular lattice (Λ, b) of signature (r,s), then F is also the characteristic polynomial of a semisimple isometry t of the inner product space $(\Lambda \otimes \mathbb{R}, b \otimes \mathbb{R})$ over $\mathbb{R}$ of signature (r,s). Thus, Theorem 7.26 shows that F must satisfy the condition $(\mathrm{Sign})_{r,s}$:

$$r, s \geq m(F) \text{ and if } F(1)F(-1) \neq 0 \text{ then } r \equiv s \equiv m(F) \bmod 2,$$

where $m(F)$ is the number of roots of F whose absolute values are greater than 1 counted with multiplicity. Namely, the localization at the infinite place yields the condition $(\mathrm{Sign})_{r,s}$. So, what condition is produced by the localizations at finite places? The answer is as follows.

Proposition 9.1. *Suppose that F is the characteristic polynomial of a semisimple isometry t of an even unimodular lattice (Λ, b) over $\mathbb{Z}$. Then $\deg(F)$ is even and*

$$|F(1)|, |F(-1)| \text{ and } (-1)^{(\deg F)/2}F(1)F(-1) \text{ are all squares.} \tag{Square}$$

Proof. The degree of F is even since any even unimodular lattice has even rank. Corollaries 8.17 and 8.20 show that $v_p(F(1)) \equiv v_p(F(-1)) \equiv 0 \mod 2$ for every prime p, since F is the characteristic polynomial of a semisimple isometry of the even unimodular lattice $(\Lambda \otimes \mathbb{Z}_p, b \otimes \mathbb{Z}_p)$ over $\mathbb{Z}_p$. Thus $|F(1)|$ and $|F(-1)|$ are squares in $\mathbb{Z}$ by considering their prime factorizations. If $F(1)$ or $F(-1)$ is zero then $(-1)^{(\deg F)/2}F(1)F(-1) = 0$ and we are done. Suppose that $F(1)F(-1) \neq 0$. Then $(-1)^{(\deg F)/2}F(1)F(-1) = \operatorname{disc}(b \otimes \mathbb{Q})$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ by Proposition 7.32. On the other hand, we have $\operatorname{disc}(b) = 1$ by Theorem 5.24. Therefore $(-1)^{(\deg F)/2}F(1)F(-1)$ is a square. This completes the proof. □

For the condition (Square), we have the following lemma.

Lemma 9.2. *The following assertions hold.*

(i) *Let f and $g \in \mathbb{Z}[X]$ be $*$-symmetric polynomials of even degrees. If f and g satisfy* (Square) *then so does fg. If g and fg satisfy* (Square)*, and $g(1)g(-1) \neq 0$, then f satisfies* (Square).

(ii) *Any $*$-symmetric polynomial in $\mathbb{Z}[X]$ of type 2 over $\mathbb{Q}$ satisfies* (Square).

Proof. (i). Straightforward.

(ii). Let $f \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of type 2. Then, there exists a monic polynomial $g \in \mathbb{Z}[X]$ such that $f = gg^*$. Note that $g(0)$ is a unit, i.e., $g(0) = 1$ or -1, because $g(0)$ and $g(0)^{-1}$ are the constant terms of g and $g^* \in \mathbb{Z}[X]$ respectively. Then

$$|f(\pm 1)| = |g(\pm 1)g^*(\pm 1)| = |g(\pm 1)g(0)^{-1}(\pm 1)^{\deg g} g(\pm 1)| = |g(\pm 1)|^2.$$

Moreover, we have

$$\begin{aligned}(-1)^{\deg(f)/2} f(1)f(-1) &= (-1)^{\deg g} g(1)g^*(1) \cdot g(-1)g^*(-1) \\ &= (-1)^{\deg g} g(1)g(0)^{-1}g(1) \cdot g(-1)g(0)^{-1}(-1)^{\deg g} g(-1) \\ &= (g(1)g(-1))^2.\end{aligned}$$

This completes the proof. □

It follows from this lemma that F satisfies (Square) if and only if F_0F_1 satisfies (Square), where F_i is the type i component over $\mathbb{Q}$. Furthermore, it can be easily seen that F satisfies $(\mathrm{Sign})_{r,s}$ if and only if F_0F_1 satisfies $(\mathrm{Sign})_{r',s'}$, where $r' := r - \deg(F_2)/2$ and $s' := s - \deg(F_2)/2$. One will see that the type 2 component has no substantial role in this section.

To consider when there exists an even unimodular lattice having a semisimple (F, i)-isometry, we use local-global theory for inner products on the associated $\mathbb{Q}[\Gamma]$-module of F.

Notation 9.3. We use the following notation.

(i) The set of all places of $\mathbb{Q}$ is denoted by $\mathcal{V}$. The infinite place of $\mathbb{Q}$ is denoted by ∞.

(ii) For a monic polynomial $f \in \mathbb{Z}[X]$, we write m_f for the multiplicity of f in F. We often write $m_\pm$ for $m_{X \mp 1}$ briefly. Furthermore, the sets $I(F;\mathbb{Q})$, $I_1(F;\mathbb{Q})$, and $I_2(F;\mathbb{Q})$ are abbreviated to I, I_1, and I_2 respectively. The product of the type 1 and 2 components of F is denoted by F_{12}. Under this notation, we can write

$$\begin{aligned}F(X) &= (X-1)^{m_+}(X+1)^{m_-}F_{12}(X), \\ F_{12}(X) &= \prod_{f \in I_1} f(X)^{m_f} \times \prod_{\{g,g^*\} \subset I_2} (g(X)g^*(X))^{m_g}.\end{aligned}$$

(iii) The symbol M denotes the associated $\mathbb{Q}[\Gamma]$-module of F with transformation α, and $M^f, M^\pm, E^f, \alpha^f, \sigma$ (f is a factor in I or of the form gg^* for some $g \in I_2$) are as in Notation 7.19. Furthermore, we define $M^1 := \prod_{f \in I_1} M^f$ and $M^2 := \prod_{\{g,g^*\} \subset I_2} M^{gg^*}$.

(iv) For a place $v \in \mathcal{V}$, we define $M_v := M \otimes \mathbb{Q}_v$. Similarly $M_v^f := M^f \otimes \mathbb{Q}_v$ for f which is in I or of the form gg^* for some $g \in I_2$, and $M_v^i := M^i \otimes \mathbb{Q}_v$ for $i = 1, 2$. Then

$$M_v = M_v^+ \oplus M_v^- \oplus \bigoplus_{f \in I_1} M_v^f \oplus \bigoplus_{\{g,g^*\} \subset I_2} M_v^{gg^*}.$$

Note that α is extended to a $\mathbb{Q}_v$-linear transformation on M_v in a unique way, and M_v is (isomorphic to) the associated $\mathbb{Q}_v[\Gamma]$-module of F.

We will consider when there exists an inner product b on M such that α becomes an isometry having a given index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice of signature (r, s). The following notation concerns localizations of this question.

Notation 9.4. Let $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ be an index map. We consider the following three properties (P1)–(P3) of an inner product b_v on M_v for each $v \in \mathcal{V}$. The first property is that

$$\alpha : M_v \to M_v \text{ is an isometry with respect to } b_v. \tag{P1}$$

Assume that b_v has the property (P1). The second property is that

$$\begin{aligned} &\text{if } v \neq \infty \text{ then there exists an } \alpha\text{-stable even unimodular lattice over } \mathbb{Z}_v \text{ on } (M_v, b_v), \text{ and} \\ &\text{if } v = \infty \text{ then the isometry } \alpha \text{ of } (M_\infty, b_\infty) \text{ has index } \mathfrak{i}. \end{aligned} \tag{P2}$$

The last property is that

$$\det(b_v|_{M_v^\pm}) = \delta_\pm \text{ in } \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}, \tag{P3}$$

where δ_+ and $\delta_- \in \mathbb{Q}^\times$ are nonzero rational numbers defined by

$$\delta_\pm := \begin{cases} (-1)^{(m_\pm - \mathfrak{i}(X \mp 1))/2} \, |F_{12}(\pm 1)| & \text{if } m_+ \text{ is even} \\ (-1)^{(m_\pm - \mathfrak{i}(X \mp 1))/2} \, 2|F_{12}(\pm 1)| & \text{if } m_+ \text{ is odd.} \end{cases}$$

Moreover, we write $\mathcal{B}_\mathfrak{i}$ for the set of families $\{b_v\}_{v \in \mathcal{V}}$ of inner products on M_v such that each b_v has the properties (P1)–(P3) and $\#\{v \in \mathcal{V} \mid \mathrm{hw}_v(b_v|_{M_v^f}) \neq 0\}$ is finite for all $f \in I$.

It will be seen in the next subsection that if b is an inner product on M such that α becomes an isometry having index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice of signature (r, s), then the family $\{b \otimes \mathbb{Q}_v\}_{v \in \mathcal{V}}$ obtained by localizations belongs to $\mathcal{B}_\mathfrak{i}$. We close this subsection by showing that $\mathcal{B}_\mathfrak{i} \neq \emptyset$ for any $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ if F satisfies the conditions $(\mathrm{Sign})_{r,s}$ and (Square).

Lemma 9.5. *Suppose that F satisfies the condition $(\mathrm{Sign})_{r,s}$, and let $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ be an index map. Put $n = \deg(F)/2$ and $s_\pm = (m_\pm - \mathfrak{i}(X \mp 1))/2$. Then the signature of $F_{12}(1)F_{12}(-1)$ is equal to $(-1)^{n+s_+ + s_-}$, or equivalently, we have*

$$(-1)^n F_{12}(1)F_{12}(-1) = (-1)^{s_+} \, |F_{12}(1)| \cdot (-1)^{s_-} \, |F_{12}(-1)|.$$

Proof. Let b_∞ be an inner product on M_∞ which makes α an isometry with index $\mathfrak{i}$. Such an inner product exists by Theorem 7.28. Let s_{12} denote the signature of the subspace $M_\infty^1 \oplus M_\infty^2$ of $M_\infty = (M_\infty, b_\infty)$. Then $s_+ + s_- + s_{12} = s$ since (M_∞, b_∞) has signature (r, s). Furthermore, since $n \equiv (r + s)/2 \equiv s \bmod 2$, we get $(-1)^{n+s_+ + s_-} = (-1)^{s+s_+ + s_-} = (-1)^{s_{12}}$.

On the other hand, it follows from Proposition 7.32 that the signature of $F_{12}(1)F_{12}(-1)$ is equal to $\det(b|_{M_\infty^1 \oplus M_\infty^2})$, which is $(-1)^{s_{12}}$. Hence, the signature of $F_{12}(1)F_{12}(-1)$ is equal to $(-1)^{n+s_+ + s_-}$. □

Theorem 9.6. *If F satisfies the conditions $(\mathrm{Sign})_{r,s}$ and (Square) then $\mathcal{B}_\mathfrak{i}$ is not empty for any $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$.*

Proof. Assume that F satisfies the conditions $(\mathrm{Sign})_{r,s}$ and (Square), and take $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ arbitrarily. Put $n = \deg(F)/2$ and $s_\pm = (m_\pm - \mathfrak{i}(X \mp 1))/2$ as in Lemma 9.5. By Theorem 7.28, there exists an inner product b_∞ with the properties (P1) and (P2). Such an inner product

satisfies (P3) automatically. Let p be a prime, and put $u_\pm = (-1)^{s_\pm} F_{12}(\pm 1)/|F_{12}(\pm 1)| \in \{1, -1\}$. Note that the property (P3) is equivalent to

$$\det(b_p|_{M_p^\pm}) = \begin{cases} u_\pm F_{12}(\pm 1) & \text{if } m_+ \text{ is even} \\ 2u_\pm F_{12}(\pm 1) & \text{if } m_+ \text{ is odd} \end{cases} \quad \text{in } \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}.$$

By the assumption (Square), we have $v_p(F(1)) \equiv v_p(F(-1)) \equiv 0 \bmod 2$, and if $F(1)F(-1) \neq 0$ then $(-1)^n F(1)F(-1) = 1$ mod squares.

Suppose that $p = 2$. Theorem 8.19 shows that there exists an inner product b_2 on M_2 of discriminant 1 with the properties (P1) and (P2), and moreover if $F(1) = F(-1) = 0$ then b_2 can be chosen to satisfy (P3). We claim that b_2 has property (P3) also in the cases where $F(1) = 0$ and $F(-1) \neq 0$, and where $F(1) \neq 0$ and $F(-1) = 0$. Suppose that $F(1) = 0$ and $F(-1) \neq 0$. In this case, we have $\det(b_2) = \det(b_2|_{M^+}) \det(b_2|_{M_2^1 \oplus M_2^2})$ since $M_2 = M_2^+ \oplus M_2^1 \oplus M_2^2$. On the other hand, we have $\det(b_2) = (-1)^n \operatorname{disc}(b_2) = (-1)^n$ and $\det(b_2|_{M_2^1 \oplus M_2^2}) = F_{12}(1)F_{12}(-1)$ by Proposition 7.32. Thus

$$\det(b_2|_{M^+}) = \det(b_2) \det(b_2|_{M_2^1 \oplus M_2^2}) = (-1)^n F_{12}(1)F_{12}(-1) = (-1)^{s_+} |F_{12}(1)||F_{12}(-1)|$$

mod squares, where the last equality is by Lemma 9.5. Furthermore, we have $|F_{12}(-1)| = |(-1-1)^{-m_+} F(-1)| = 2^{-m_+}|F(-1)|$. Here m_+ must be even since $m_- = 0$, and $|F(-1)|$ is a square by the assumption (Square). Hence $|F_{12}(-1)|$ is a square, and we obtain $\det(b_2|_{M^+}) = (-1)^{s_+} |F_{12}(1)|$ in $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$, which is the property (P3). Similarly, it can be seen that b_2 has property (P3) in the case where $F(1) \neq 0$ and $F(-1) = 0$.

Suppose that p is an odd prime. Then there exists an inner product b_p on M_p with properties (P1)–(P3) by Theorem 8.16. Moreover, if p is unramified in E^f then b_p can be chosen so that $(M_p^f, b_p|_{M_p^f})$ contains a unimodular lattice for each $f \in I$ by the latter assertion in Theorem 8.16. In this case, we have $\mathrm{hw}_p(b_p|_{M_p^f}) = 0$ by Corollary 5.19.

Let $\{b_v\}_{v \in \mathcal{V}}$ be the family consisting of inner products b_v chosen as above. Then each b_v has properties (P1)–(P3). Let $f \in I$, and put

$$\mathcal{V}' = \{\infty, 2\} \cup \{p \mid p \text{ is an odd prime ramified in } E^f\} \subset \mathcal{V}.$$

Then $\mathcal{V}'$ is a finite set by Corollary 1.41, and $\mathrm{hw}_p(b_p|_{M_p^f}) = 0$ for any $p \in \mathcal{V} \setminus \mathcal{V}'$ by construction. Hence $\#\{v \in \mathcal{V} \mid \mathrm{hw}_v(b_v|_{M_v^f}) \neq 0\} < \infty$. This shows that $\{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_\mathfrak{i}$. The proof is complete. □

9.2 Local-global principle

In the rest of this section, we assume that F satisfies the conditions $(\mathrm{Sign})_{r,s}$ and (Square), and fix an index map $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$. The aim of this subsection is to show the following theorem, which is the local-global principle for the desired inner product on the associated $\mathbb{Q}[\Gamma]$-module of F.

Theorem 9.7. *Let $r, s \in \mathbb{Z}_{\geq 0}$ be non-negative integers with $r \equiv s \bmod 8$, $F \in \mathbb{Z}[X]$ a $*$-symmetric polynomial of degree $r + s$ with the conditions $(\mathrm{Sign})_{r,s}$ and (Square), and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ an index map. The following conditions are equivalent:*

(i) *There exists an inner product b on M such that $\alpha : M \to M$ becomes an isometry having index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice over $\mathbb{Z}$.*

(ii) *There exists a family $\{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_\mathfrak{i}$ such that $\sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) = 0$ for any $f \in I$.*

We begin with the necessary condition, that is, (i) $\Rightarrow$ (ii) of Theorem 9.7.

Proposition 9.8. *Suppose that M admits an inner product b such that α becomes an isometry having index $\mathfrak{i}$ and (M,b) contains an α-stable even unimodular lattice over $\mathbb{Z}$. Then, the family $\{b\otimes\mathbb{Q}_v\}_{v\in\mathcal{V}}$ obtained by localizations belongs to $\mathcal{B}_{\mathfrak{i}}$. Moreover $\sum_{v\in\mathcal{V}}\mathrm{hw}_v((b\otimes\mathbb{Q}_v)|_{M_v^f})=0$ for any $f\in I$.*

Proof. Let $v\in\mathcal{V}$ be a place of $\mathbb{Q}$. it is obvious that $b\otimes\mathbb{Q}_v$ has properties (P1) and (P2). For (P3), it is sufficient to show that $\det(b|_{M^\pm})=\delta_\pm$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We remark that $\det(b|_{M^\pm})$ and $\delta_\pm$ have the same signature $(-1)^{(m_\pm-\mathfrak{i}(X\mp 1))/2}$ because the signature of $(M^\pm,b|_{M^\pm})$ is given by $((m_\pm+\mathfrak{i}(X\mp1))/2,(m_\pm-\mathfrak{i}(X\mp1))/2)$. Moreover, it follows from Proposition 7.35 that $v_p(\det(b|_{M^\pm}))\equiv v_p(\delta_\pm) \bmod 2$ for every prime p. By comparing the prime factorizations of $\det(b|_{M^\pm})$ and $\delta_\pm$, we obtain $\det(b|_{M^\pm})=\delta_\pm$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which means that $b\otimes\mathbb{Q}_v$ has property (P3). Moreover, for each $f\in I$, the reciprocity (Proposition 4.53) shows that $\mathrm{hw}_v((b\otimes\mathbb{Q}_v)|_{M_v^f})=0$ for almost all $v\in\mathcal{V}$ and $\sum_{v\in\mathcal{V}}\mathrm{hw}_v((b\otimes\mathbb{Q}_v)|_{M_v^f})=0$. This completes the proof. □

This proposition shows that (i) $\Rightarrow$ (ii) of Theorem 9.7, so it remains to prove the converse (ii) $\Rightarrow$ (i). Let f be a factor of F which is in I_1 or of the form gg^* for $g\in I_2$, and let $v\in\mathcal{V}$ be a place of $\mathbb{Q}$. The fixed subfield $(E^f)^\sigma\subset E^f$ of the involution σ is abbreviated to $E^{f,\sigma}$. The symbol $\mathcal{W}(f;v)$ denotes the set of all places of $E^{f,\sigma}$ above v. For $w\in\mathcal{W}(f;v)$, we write $(E^{f,\sigma})_w$ for the completion at w. We fix the isomorphism $E^{f,\sigma}\otimes_{\mathbb{Q}}\mathbb{Q}_v\cong\prod_{w\in\mathcal{W}(f;v)}(E^{f,\sigma})_w$ defined in Theorem 1.44, and identify them. Put $E_v^f=E^f\otimes_{\mathbb{Q}}\mathbb{Q}_v$ and $E_w^f=E^f\otimes_{E^{f,\sigma}}(E^{f,\sigma})_w$ for $w\in\mathcal{W}(f;v)$. Note that $\sigma:E^f\to E^f$ extends to an involution of E_w^f, and the fixed subfield $(E_w^f)^\sigma\subset E_w^f$ is canonically isomorphic to $(E^{f,\sigma})_w$. We identify them and often write $E_w^{f,\sigma}$. The algebra E_v^f is decomposed into the product of E_w^f:

$$\begin{aligned}E_v^f&=E^f\otimes_{E^{f,\sigma}}E^{f,\sigma}\otimes_{\mathbb{Q}}\mathbb{Q}_v=E^f\otimes_{E^{f,\sigma}}\left(\prod_{w\in\mathcal{W}(f;v)}(E^{f,\sigma})_w\right)\\&=\prod_{w\in\mathcal{W}(f;v)}E^f\otimes_{E^{f,\sigma}}(E^{f,\sigma})_w=\prod_{w\in\mathcal{W}(f;v)}E_w^f.\end{aligned}$$

Similarly, putting $M_w^f=M^f\otimes_{E^{f,\sigma}}(E^{f,\sigma})_w$ for $w\in\mathcal{W}(f;v)$, we have

$$M_v^f=\prod_{w\in\mathcal{W}(f;v)}M_w^f.$$

We write $\alpha_w^f=\alpha^f\otimes 1\in E_w^f=E^f\otimes_{E^{f,\sigma}}(E^{f,\sigma})_w$. The linear transformation $M_w^f\to M_w^f$ defined as the multiplication by α_w^f is the same as $\alpha|_{M_w^f}$.

Lemma 9.9. *Let b be an inner product on M such that $(M_p,b\otimes\mathbb{Q}_p)$ contains an α-stable even unimodular lattice Λ_p for every prime p. If $\Lambda_p=\mathcal{O}_{M_p}$ for almost all primes p then*

$$\Lambda:=\{x\in M\mid \iota_p(x)\in\Lambda_p \text{ for every prime } p\}$$

is an α-stable even unimodular lattice on (M,b). Here $\mathcal{O}_{M_p}$ is the integral closure of $\mathbb{Z}_p$ in the $\mathbb{Q}_p$-algebra M_p, and $\iota_p:M\to M_p=M\otimes\mathbb{Q}_p$ is the natural homomorphism.

Proof. Suppose that $\Lambda_p=\mathcal{O}_{M_p}$ for almost all primes p, and put $\mathcal{S}=\{p:\text{prime}\mid\Lambda_p\neq\mathcal{O}_{M_p}\}$. We first show that Λ is a finitely generated $\mathbb{Z}$-module on M. For each $p\in\mathcal{S}$, there exist integers

$N_p, N_p' \geq 0$ such that $p^{N_p'}\mathcal{O}_{M_p} \subset \Lambda_p \subset p^{-N_p}\mathcal{O}_{M_p}$, since Λ_p and $\mathcal{O}_{M_p}$ are finitely generated $\mathbb{Z}_p$-modules on M_p. Noting that $\mathbb{Z}_p\iota_p(\mathcal{O}_M) = \mathcal{O}_{M_p}$, we obtain

$$\left(\prod_{p\in\mathcal{S}} p^{N_p'}\right)\mathcal{O}_M \subset \Lambda \subset \left(\prod_{p\in\mathcal{S}} p^{-N_p}\right)\mathcal{O}_M.$$

Since $\left(\prod_{p\in\mathcal{S}} p^{-N_p}\right)\mathcal{O}_M$ is finitely generated over $\mathbb{Z}$, so is its submodule Λ. Furthermore, the $\mathbb{Q}$-span of Λ is M since so is that of $\left(\prod_{p\in\mathcal{S}} p^{N_p'}\right)\mathcal{O}_M$. Hence Λ is a finitely generated $\mathbb{Z}$-module on M.

We next show that (Λ, b) is integral and even. Let $x, y \in \Lambda$. For any prime p, we have $v_p(b(x,y)) = v_p((b\otimes\mathbb{Q}_p)(\iota_p(x),\iota_p(y))) \geq 0$ since $\iota_p(x)$ and $\iota_p(y)$ are in the integral lattice $(\Lambda_p, b\otimes\mathbb{Q}_p)$ over $\mathbb{Z}_p$. Thus $b(x,y)\in\mathbb{Z}$, and (Λ, b) is integral. Similarly, we have $v_2(b(x,x)) = v_2((b\otimes\mathbb{Q}_2)(\iota_2(x),\iota_2(x))) \geq 1$ since $(\Lambda_2, b\otimes\mathbb{Q}_2)$ is an even lattice. This shows that (Λ, b) is even.

It is easy to see that Λ is α-stable. So, it remains to prove that (Λ, b) is unimodular. We have $\Lambda \subset \Lambda^\vee$ since Λ is integral. Let $y \in \Lambda^\vee$, and let p be a prime. Then $(b\otimes\mathbb{Q}_p)(\iota_p(y), \mathbb{Z}_p\iota_p(\Lambda)) \subset \mathbb{Z}_p$. On the other hand, one can show that $\mathbb{Z}_p\iota_p(\Lambda) = \Lambda_p$ in M_p. Thus $\iota_p(y) \in (\mathbb{Z}_p\iota_p(\Lambda))^\vee = (\Lambda_p)^\vee = \Lambda_p$ since Λ_p is unimodular. This means that $y \in \bigcap_{p:\text{prime}} \iota_p^{-1}(\Lambda_p) = \Lambda$. Hence $\Lambda^\vee \subset \Lambda$, and Λ is unimodular. The proof is complete. □

Proposition 9.10. *Let $\{b_v\}_{v\in\mathcal{V}}$ be a family in $\mathcal{B}_\mathfrak{i}$ such that $\sum_{v\in\mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) = 0$ for all $f \in I$. Then M admits an inner product b such that α is an isometry of (M,b), the index of α with respect to b is $\mathfrak{i}$, and (M,b) contains an α-stable even unimodular lattice.*

Proof. Let b^+ and b^- be inner products M^+ and M^- such that $b^\pm \otimes \mathbb{Q}_v \cong b_v|_{M_v^\pm}$ for all $v \in \mathcal{V}$. Such inner products exist by Theorem 4.57, since $\det(b_v|_{M_v^\pm}) = \delta_\pm$ for all $v\in\mathcal{V}$ and $\sum_{v\in\mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^\pm}) = 0$.

Claim 1: *For almost all primes p, the integral closure $\mathcal{O}_{M_p^\pm}$ of $\mathbb{Z}_p$ in $M_p^\pm$ is an even unimodular lattice on $(M_p^\pm, b^\pm\otimes\mathbb{Q}_p)$.* Let $e_1,\dots,e_{m_\pm}$ be a $\mathbb{Z}$-basis of the integral closure $\mathcal{O}_{M^\pm}$ of $\mathbb{Z}$ in $M^\pm$. Then $\iota_p(e_1),\dots,\iota_p(e_{m_\pm})$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_{M_p^\pm}$ because $\mathcal{O}_{M^\pm}\otimes\mathbb{Z}_p = \mathcal{O}_{M_p^\pm}$. Let $G = (g_{ij})_{ij}$ be the Gram matrix of b with respect to the basis $e_1,\dots,e_{m_\pm}$. Then G is also the Gram matrix of $b^\pm\otimes\mathbb{Q}_p$ with respect to the basis $\iota_p(e_1),\dots,\iota_p(e_{m_\pm})$ for each p (by considering entries to be in $\mathbb{Z}_p$). We define

$$\mathcal{S} := \{p : \text{prime} \mid p \neq 2, \text{ and all entries of } G \text{ and } \det(G) \text{ are units of } \mathbb{Z}_p\}.$$

Then G is invertible over $\mathbb{Z}_p$ for any prime $p\in\mathcal{S}$. This means that $\mathcal{O}_{M_p^\pm}$ is a unimodular lattice, and furthermore it is an even lattice since $p\neq 2$. Because almost all primes belong to $\mathcal{S}$, the proof of Claim 1 is complete.

Let f be a factor of F which is in I_1 or of the form gg^* for $g\in I_2$, and let $\mathcal{W}(f)$ denote the set of places of $E^{f,\sigma}$. For each $w\in\mathcal{W}(f)$, there exists a hermitian product h_w^f such that $b_v|_{M_w^f} = \mathrm{Tr}_{E_w^f/\mathbb{Q}_v}\circ h_w^f$ by Proposition 7.20, where v is the place of $\mathbb{Q}$ below w. Put $\mu_w^f = \det(h_w^f) \in \mathrm{Tw}(E_w^f, \sigma)$.

Claim 2: *We have $\sum_{w\in\mathcal{W}(f)} \iota_w(\mu_w^f) = 0$ for $f\in I_1$, where $\iota_w : \mathrm{Tw}(E^f,\sigma)\to\mathbb{Z}/2\mathbb{Z}$ is defined in Notation* 3.30. Let $\widehat{h}^f : M^f\times M^f \to E^f$ be a hermitian product of determinant 1, and $\widehat{b}^f$ the inner product $\mathrm{Tr}_{E^f/\mathbb{Q}}\circ\widehat{h}^f : M^f\times M^f\to\mathbb{Q}$. For each $v\in\mathcal{V}$, it follows from Proposition 4.69 (ii) that

$$\begin{aligned}\mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_v}\left([\sigma,\mu_w^f]_{E_w^{f,\sigma}}\right) &= \mathrm{HW}_{K_v}\left(\mathrm{Tr}_{E_w^f/\mathbb{Q}_v}\circ h_w^f\right) + \mathrm{HW}_{K_v}\left(\mathrm{Tr}_{E_w^f/\mathbb{Q}_v}\circ(\widehat{h}^f\otimes E_w^f)\right)\\ &= \mathrm{HW}_{K_v}\left(b_v|_{M_w^f}\right) + \mathrm{HW}_{K_v}\left((\widehat{b}^f\otimes\mathbb{Q}_v)|_{M_w^f}\right).\end{aligned}$$

Summing over $w \in \mathcal{W}(f;v)$ yields

$$\begin{aligned}\sum_{w\in\mathcal{W}(f;v)} \mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_v}\left([\sigma,\mu_w^f]_{E_w^{f,\sigma}}\right) &= \sum_{w\in\mathcal{W}(f;v)} \mathrm{HW}_{K_v}\left(b_v|_{M_w^f}\right) + \sum_{w\in\mathcal{W}(f;v)} \mathrm{HW}_{K_v}\left((\widehat{b}^f\otimes\mathbb{Q}_v)|_{M_w^f}\right)\\ &= \mathrm{HW}_{K_v}\left(b_v|_{M_v^f}\right) + \mathrm{HW}_{K_v}\left((\widehat{b}^f\otimes\mathbb{Q}_v)|_{M_v^f}\right),\end{aligned}$$

where the last equality follows from Lemma 4.31 (iii). Thus

$$\begin{aligned}&\sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}(f;v)} \mathrm{inv}_{K_v}\left(\mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_v}\left([\sigma,\mu_w^f]_{E_w^{f,\sigma}}\right)\right)\\ &\quad= \sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}\left(\sum_{w\in\mathcal{W}(f;v)} \mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_v}\left([\sigma,\mu_w^f]_{E_w^{f,\sigma}}\right)\right)\\ &\quad= \sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}\circ\mathrm{HW}_{K_v}\left(b_v|_{M_v^f}\right) + \sum_{v\in\mathcal{V}} \mathrm{inv}_{K_v}\circ\mathrm{HW}_{K_v}\left((\widehat{b}^f\otimes\mathbb{Q}_v)|_{M_v^f}\right)\\ &\quad= 0,\end{aligned}$$

where the last equality follows by assumption and by the reciprocity (Proposition 4.53). This leads to $\sum_{w\in\mathcal{W}(f)} \iota_w(\mu_w^f) = 0$ as required, because we have the commutative diagram

$$\begin{array}{ccccc}
\mathrm{Tw}(E_w^f,\sigma) & \xrightarrow{[\sigma,\,\cdot\,]_{E_w^{f,\sigma}}} & \mathrm{Br}(E_w^{f,\sigma}) & \xrightarrow{\mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_v}} & \mathrm{Br}(\mathbb{Q}_v)\\
\downarrow{\scriptstyle \iota_w} & & \downarrow{\scriptstyle \mathrm{inv}} & & \downarrow{\scriptstyle \mathrm{inv}}\\
\mathbb{Z}/2\mathbb{Z} & \xrightarrow{\times\frac{1}{2}} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Q}/\mathbb{Z},
\end{array}$$

see §3.5.

Let $f \in I_1$. By Claim 2 and Theorem 4.74, there exists a hermitian product $h^f : M^f \times M^f \to E^f$ such that $h^f \otimes E_w \cong h_w^f$ for all $w \in \mathcal{W}(f)$. Let $e_1,\dots,e_{m^f}$ be the standard basis of $M^f = (E^f)^{m_f}$ over E^f. We may assume that $e_1,\dots,e_{m^f}$ is an orthogonal basis with respect to the hermitian product h^f by Proposition 4.65 (or by the proof of Theorem 4.74), i.e., $h^f = \langle\mu_1,\dots,\mu_{m_f}\rangle_{E^f}$ for some $\mu_1,\dots,\mu_{m_f} \in (E^{f,\sigma})^\times$. We define an inner product $b^f : M^f \times M^f \to \mathbb{Q}$ by $b^f := \mathrm{Tr}_{E/\mathbb{Q}}\circ h^f$. Note that

$$\begin{aligned}(M_v^f, b_v^f, \alpha|_{M_v^f}) &= \bigoplus_{w\in\mathcal{W}(f;v)} (M_w^f, \mathrm{Tr}_{E_w^f/\mathbb{Q}_v}\circ h_w^f, \alpha_w^f)\\ &\cong \bigoplus_{w\in\mathcal{W}(f;v)} (M_w^f, \mathrm{Tr}_{E_w^f/\mathbb{Q}_v}\circ(h^f\otimes E_w^f), \alpha_w^f)\\ &= (M_v^f, (b^f\otimes\mathbb{Q}_v), \alpha|_{M_v^f}) \qquad (*)\end{aligned}$$

as $\mathbb{Q}[\Gamma]$-inner product spaces for all $v \in \mathcal{V}$. Let $g \in I_2$. In this case, we put $h^{gg^*} = \langle 1,\dots,1\rangle_{E^{gg^*}}$ and define an inner product b^{gg*} on M^{gg^*} by $\mathrm{Tr}_{E^{gg^*}/\mathbb{Q}}\circ h^{gg^*}$. Then, for all $v \in \mathcal{V}$ we have $(M_v^{gg^*}, b_v^{gg^*}, \alpha|_{M_v^{gg^*}}) \cong (M_v^{gg^*}, (b^{gg^*}\otimes\mathbb{Q}_v), \alpha|_{M_v^{gg^*}})$ as in $(*)$, by Corollary 4.66.

Claim 3: *Let f be a factor of F which is in I_1 or of the form gg^* for $g \in I_2$. For almost all primes p, the integral closure $\mathcal{O}_{M_p^f}$ of $\mathbb{Z}_p$ in M_p^f is an even unimodular lattice on $(M_p^f, b^f\otimes\mathbb{Q}_p)$.*

We recall that h^f is expressed as $h^f = \langle\mu_1,\dots,\mu_{m_f}\rangle_{E^f}$ for some $\mu_1,\dots,\mu_{m_f} \in (E^{f,\sigma})^\times$. Put

$$\mathcal{T} = \left\{ p : \text{prime} \;\middle|\; \begin{array}{l} p \neq 2,\ p \text{ is unramified in } E^f, \text{ and } w(\mu_i^f) = 0 \text{ for all } w \in \mathcal{W}(f;p),\\ \text{where } w \text{ is identified with the corresponding valuation.}\end{array} \right\}.$$

Then, almost all primes belong to $\mathcal{T}$ by Corollary 1.41. Moreover, for every $p \in \mathcal{T}$, the integral closure $\mathcal{O}_{M_p^f} = \prod_{w \in \mathcal{W}(f;p)} \mathcal{O}_{M_w^f}$ is an even unimodular lattice on the space $(M_p^f, b^f \otimes \mathbb{Q}_p) = \bigoplus_{w \in \mathcal{W}(f;p)} (M_w^f, \mathrm{Tr}_{E_w^f/\mathbb{Q}_p} \circ (h^f \otimes E_w^f))$ by Remark 8.12 (ii). This completes the proof of Claim 3.

Now, we define an inner product b on $M = M^+ \otimes M^- \oplus \bigoplus_{f \in I_1} M^f \oplus \bigoplus_{\{g,g^*\} \subset I_2} M^{gg^*}$ by

$$b = b^+ \otimes b^- \oplus \bigoplus_{f \in I_1} b^f \oplus \bigoplus_{\{g,g^*\} \subset I_2} b^{gg^*}.$$

Then $(M_v, b \otimes \mathbb{Q}_v, \alpha) \cong (M_v, b_v, \alpha)$ as $\mathbb{Q}[\Gamma]$-inner product spaces by its construction. In particular, the index of the isometry α with respect to b is $\mathfrak{i}$, and $(M_p, b \otimes \mathbb{Q}_p)$ contains an α-stable even unimodular lattice Λ_p. Moreover, we may assume that $\Lambda_p = \mathcal{O}_{M_p}$ by Claims 1 and 3 for almost all primes p. Therefore, it follows from Lemma 9.9 that (M, b) contains an α-stable even unimodular lattice. This completes the proof. □

Proof of Theorem 9.7. The implication (i) ⇒ (ii) follows from Proposition 9.8, and Proposition 9.10 shows the converse (ii) ⇒ (i). □

9.3 Local-global obstruction 1

We keep the setting and notation of §§9.1 and 9.2. In particular $r, s \in \mathbb{Z}_{\geq 0}$ are non-negative integers with $r \equiv s \bmod 8$, $F \in \mathbb{Z}[X]$ is a $*$-symmetric polynomial of degree $r+s$ with the conditions $(\mathrm{Sign})_{r,s}$ and (Square), and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ is an index map.

Notation 9.11. Let $C(I)$ denote the $\mathbb{Z}/2\mathbb{Z}$-module consisting of all maps from $I = I(F; \mathbb{Q})$ to $\mathbb{Z}/2\mathbb{Z}$, that is, $C(I) := \{\gamma : I \to \mathbb{Z}/2\mathbb{Z}\} = (\mathbb{Z}/2\mathbb{Z})^{\oplus I}$. Moreover, we define a map $\eta : \mathcal{B}_{\mathfrak{i}} \to C(I)$ by

$$\eta(\beta)(f) = \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) \in \mathbb{Z}/2\mathbb{Z} \quad (\beta = \{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}},\ f \in I).$$

Under this notation, the condition (ii) in Theorem 9.7 can be rephrased as the one that there exists a family $\beta \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\beta) = \mathbf{0}$, where $\mathbf{0} \in C(I)$ is the zero map. So we study the image of the map $\eta : \mathcal{B}_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z}$. It will turn out that the image $\eta(\mathcal{B}_{\mathfrak{i}})$ coincides with a coset of some submodule in $C(I)$.

Notation 9.12. For a monic polynomial $f \in \mathbb{Z}[X]$, the symbol $\overline{I(f; \mathbb{Q}_p)}$ denotes the set of irreducible factors of reductions modulo p of polynomials in $I(f; \mathbb{Q}_p)$:

$$\overline{I(f; \mathbb{Q}_p)} := \left\{ \bar{h} \in \mathbb{F}_p[X] \;\middle|\; \begin{array}{l} \bar{h} \text{ is irreducible, and there exists a } *\text{-symmetric} \\ \text{irreducible factor of } f \text{ in } \mathbb{Z}_p[X] \text{ whose reduction} \\ \text{modulo } p \text{ is divisible by } \bar{h} \text{ in } \mathbb{F}_p[X] \end{array} \right\}.$$

Moreover, we define

$$\overline{I(X \mp 1; \mathbb{Q}_p)}' := \begin{cases} \overline{I(X \mp 1; \mathbb{Q}_p)} = \{X \mp 1\} & \text{if } m_\pm \geq 3; \text{ or } m_\pm = 2 \text{ and } \delta_\pm \neq -1 \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \\ \emptyset & \text{otherwise} \end{cases}$$

($m_\pm$ and $\delta_\pm$ are defined in Notations 9.3 and 9.4) and $\overline{I(f; \mathbb{Q}_p)}' := \overline{I(f; \mathbb{Q}_p)}$ for a monic polynomial with $f(1)f(-1) \neq 0$. Note that the set $\overline{I(X \mp 1; \mathbb{Q}_p)}'$ depends on the polynomial F and the value $\mathfrak{i}(X \mp 1)$ since so do $m_\pm$ and $\delta_\pm$. We define a set $\Pi_{\mathfrak{i}}^F(f, g)$ of primes for monic polynomials $f, g \in \mathbb{Z}[X]$ by

$$\Pi_{\mathfrak{i}}^F(f, g) := \{p : \text{prime} \mid \overline{I(f; \mathbb{Q}_p)}' \cap \overline{I(g; \mathbb{Q}_p)}' \neq \emptyset\}.$$

Remark 9.13. We give some remarks on Notation 9.12. Let p be a prime.

(i) The set $\overline{I(f;\mathbb{Q}_p)}$ is a subset of $I(f \bmod p;\mathbb{F}_p)$, but they do not necessarily coincide. For example, let us consider the case $f(X) = X^2 - 11X + 1$ and $p = 3$. Then f decomposes as

$$f(X) = (X - (11 + 3\sqrt{13})/2)(X - (11 - 3\sqrt{13})/2) \quad \text{in } \mathbb{Q}_3[X]$$

because 13 is a square in $\mathbb{Z}_3$. Thus f is of type 2 in $\mathbb{Q}_3[X]$ and $\overline{I(f;\mathbb{Q}_3)} = \emptyset$. On the other hand, we have $I(f \bmod 3;\mathbb{F}_3) = \{X - 1\}$ since $f(X) \bmod 3 = X^2 - 2X + 1 = (X - 1)^2$.

(ii) Let $f \in I_1$, and let $\bar{h} \in \mathbb{F}_p[X]$ be an irreducible polynomial. Then $\bar{h} \in \overline{I(f;\mathbb{Q}_p)}'$ if and only if there exists a place $w \in \mathcal{W}(f;p) \setminus \mathcal{W}_{\mathrm{sp}}(f;p)$ of $E^{f,\sigma}$ such that $\bar{h} \mid f_w \bmod p$, where f_w is the irreducible factor of f in $\mathbb{Q}_p[X]$ corresponding to w. In this case $\mathrm{Tw}(E^f_w, \sigma) \cong \mathbb{Z}/2\mathbb{Z}$.

(iii) The condition for $\overline{I(X \mp 1;\mathbb{Q}_p)}'$ to be not empty, $m_\pm \geq 3$ or $m_\pm = 2$ and $\delta_\pm \neq -1 \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, guarantees that there exist inner products $b_p^\pm$ and $\widehat{b}_p^\pm$ on $M_p^\pm$ such that $\det(b_p^\pm) = \det(\widehat{b}_p^\pm) = \delta_\pm$ and $\mathrm{hw}_p(b_p^\pm) \neq \mathrm{hw}_p(\widehat{b}_p^\pm)$, see Theorem 4.46.

For a subset J of I, we write $\mathbf{1}_J \in C(I)$ for the characteristic function:

$$\mathbf{1}_J(f) = \begin{cases} 1 & \text{if } f \in J \\ 0 & \text{if } f \notin J \end{cases} \quad (f \in I).$$

Let C_0 denote the submodule of $C(I)$ generated by the subset

$$\{\mathbf{1}_{\{f,g\}} \mid f, g \in I \text{ are distinct factors with } \Pi_{\mathfrak{i}}^F(f,g) \neq \emptyset\}.$$

Our first goal is to show that the image $\eta(\mathcal{B}_{\mathfrak{i}}) \subset C(I)$ is equal to a coset of C_0. For a prime p and for inner products $b_p^\pm$ on $M_p^\pm$ and b_w^f on M_w^f making α_w^f an isometry where $f \in I_1$ and $w \in \mathcal{W}(f;p)$, we write

$$\partial[b_p^\pm] = \partial[M_p^\pm, b_p^\pm, \pm 1], \quad \partial[b_w^f] = \partial[M_w^f, b_w^f, \alpha_w^f]$$

for short.

Lemma 9.14. *Let p be a prime.*

(i) *Let $b_p^\pm$ and $\widehat{b}_p^\pm$ be inner products on $M_p^\pm$ with determinant $\delta_\pm$. If $\mathrm{hw}_p(b_p^\pm) = \mathrm{hw}_p(b_p^\pm)$ then $\partial[b_p^\pm] = \partial[\widehat{b}_p^\pm]$. The converse is true unless $p = 2$.*

(ii) *Let $f \in I_1$ and $w \in \mathcal{W}(f;p)$. Let $h_w^f, \widehat{h}_w^f$ be hermitian products on M_w^f over E_w^f, and $b_w^f, \widehat{b}_w^f$ the inner products on M_w^f over $\mathbb{Q}_p$ defined by $b_w^f := \mathrm{Tr}_{E_w^f/\mathbb{Q}_p} \circ h_w^f$, $\widehat{b}_w^f := \mathrm{Tr}_{E_w^f/\mathbb{Q}_p} \circ \widehat{h}_w^f$. The following two conditions are equivalent.*

(a) $\mathrm{hw}_p(b_w^f) = \mathrm{hw}_p(\widehat{b}_w^f)$.

(b) $\det(h_w^f) = \det(\widehat{h}_w^f)$.

Moreover, if (a) *(or* (b)*) holds then $\partial[b_w^f] = \partial[\widehat{b}_w^f]$. The converse is true unless $p = 2$ and $w \in \mathcal{W}_{\mathrm{rm}}(f;2)$.*

Proof. (i). If $\mathrm{hw}_p(b_p^{\pm}) = \mathrm{hw}_p(\widehat{b}_p^{\pm})$ then $b_p^{\pm} \cong \widehat{b}_p^{\pm}$ by Theorem 4.45, and $\partial[b_p^{\pm}] = \partial[\widehat{b}_p^{\pm}]$. The converse in the case $p \neq 2$ follows from a direct computation with Corollary 4.62.

(ii). We have

$$\mathrm{HW}_{\mathbb{Q}_p}(b_w^f) - \mathrm{HW}_{\mathbb{Q}_p}(\widehat{b}_w^f) = \mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_p}\left([\sigma, \tfrac{\det(h_w^f)}{\det(\widehat{h}_w^f)}]_{E_w^{f,\sigma}}\right)$$

by Proposition 4.69. The left-hand side is zero if and only if the condition (a) holds. The right-hand side is zero if and only if the condition (b) holds because $[\sigma, \cdot]_{E_w^{f,\sigma}} : \mathrm{Tw}(E_w^f, \sigma) \to \mathrm{Br}(E_w^{f,\sigma})$ is injective by Theorem 3.20, and $\mathrm{cor}_{E_w^{f,\sigma}/\mathbb{Q}_p} : \mathrm{Br}(E_w^{f,\sigma}) \to \mathrm{Br}(\mathbb{Q}_p)$ is bijective by Proposition 3.27. Hence (a) and (b) are equivalent.

Suppose that the condition (a) holds. Then (b) also holds, and it implies that $h_w^f \cong \widehat{h}_w^f$ by Theorem 4.73. Thus $(M_w^f, b_w^f, \alpha_w^f) \cong (M_w^f, \widehat{b}_w^f, \alpha_w^f)$ as $\mathbb{Q}_p[\Gamma]$-inner product spaces, and in particular $\partial[b_p^f] = \partial[\widehat{b}_p^f]$. Conversely, suppose that $\partial[b_p^f] = \partial[\widehat{b}_p^f]$, and assume that $p \neq 2$ or $w \notin \mathcal{W}_{\mathrm{rm}}(f;2)$. If $w \in \mathcal{W}_{\mathrm{sp}}(f;p)$ then $\mathrm{Tw}(E_w^f, \sigma) = \{1\}$, and the condition (b) holds. In the other cases, Theorem 8.11 that $\partial_{M_w^f, \alpha_w^f} : \mathrm{Tw}(E_w^f, \sigma) \to W_{\kappa[\Gamma]}(\kappa)$ is injective. Thus, the equality $\partial_{M_w^f, \alpha_w^f}(\det(h_w^f)) = \partial[b_p^f] = \partial[\widehat{b}_p^f] = \partial_{M_w^f, \alpha_w^f}(\det(\widehat{h}_w^f))$ implies the condition (b). The proof is complete. □

We will also need the following lemma about the usual Witt group of a finite field, whose structure is described in Theorem 6.38.

Lemma 9.15. *Let κ be a finite field of characteristic not 2. Let $\omega_1, \omega_2 \in W(\kappa)$ be Witt classes, and let $\widehat{\omega}_i$ be a unique class different from ω_i with $\dim(\widehat{\omega}_i) \equiv \dim(\omega_i) \bmod 2$ for $i = 1, 2$. Then $\omega_1 + \omega_2 - \widehat{\omega}_1 - \widehat{\omega}_2 = 0$ in $W(\kappa)$.*

Proof. It can be seen from Theorem 6.38 (ii) that both of $\omega_1 - \widehat{\omega}_1$ and $\omega_2 - \widehat{\omega}_2$ are the unique nontrivial class of even dimension, and it has order 2. Hence

$$\omega_1 + \omega_2 - \widehat{\omega}_1 - \widehat{\omega}_2 = (\omega_1 - \widehat{\omega}_1) + (\omega_2 - \widehat{\omega}_2) = 0$$

as required. □

For $f \in I_1$ and a finite place w of $E^{f,\sigma}$, we write $\bar{\alpha}_w^f$ for the image of $\alpha_w^f \in \mathcal{O}_{E_w^f}$ under the natural surjection from $\mathcal{O}_{E_w^f}$ to its residue field.

Proposition 9.16. *For any $\beta \in \mathcal{B}_{\mathfrak{i}}$ and distinct $f, g \in I$ with $\Pi_{\mathfrak{i}}^F(f, g) \neq \emptyset$, there exists $\widehat{\beta} \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\beta) + \mathbf{1}_{\{f,g\}} = \eta(\widehat{\beta})$. In particular, the image $\mathrm{im}\,\eta \subset C(I)$ contains a coset of C_0.*

Proof. Let $\beta = \{b_v\}_v \in \mathcal{B}_{\mathfrak{i}}$, and let $f, g \in I$ be distinct factors with $\Pi_{\mathfrak{i}}^F(f, g) \neq \emptyset$. Take a prime $p \in \Pi_{\mathfrak{i}}^F(f, g)$. Suppose that $f, g \in I_1$. By the definition of $\Pi_{\mathfrak{i}}^F(f, g)$, there exist places $w_0 \in \mathcal{W}(f;p) \setminus \mathcal{W}_{\mathrm{sp}}(f;p)$ and $u_0 \in \mathcal{W}(g;p) \setminus \mathcal{W}_{\mathrm{sp}}(g;p)$ such that $f_{w_0} \bmod p$ and $g_{u_0} \bmod p$ have a common irreducible factor $\bar{h}$ in $\mathbb{F}_p[X]$. Note that $\bar{h}$ is the minimal polynomial of $\bar{\alpha}_{w_0}^f$ and $\bar{\alpha}_{u_0}^g$, which implies that $\partial[M_{w_0}^f, b_p|_{M_{w_0}^f}, \alpha_{w_0}^f]$ and $\partial[M_{u_0}^g, b_p|_{M_{u_0}^f}, \alpha_{u_0}^g]$ are in $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p; \bar{h})$.

By Proposition 7.20, there exist hermitian products $h_{w_0}^f$ on $M_{w_0}^f$ and $h_{u_0}^g$ on $M_{u_0}^g$ such that $b_p|_{M_{w_0}^f} = \mathrm{Tr}_{E_{w_0}^f/\mathbb{Q}_p} \circ h_{w_0}^f$ and $b_p|_{M_{u_0}^g} = \mathrm{Tr}_{E_{u_0}^g/\mathbb{Q}_p} \circ h_{u_0}^g$. Let $\widehat{h}_{w_0}^f$ and $\widehat{h}_{u_0}^g$ be hermitian products on $M_{w_0}^f$ and $M_{u_0}^g$ such that $\det(\widehat{h}_{w_0}^f) \neq \det(h_{w_0}^f)$ in $\mathrm{Tw}(E_{w_0}^f, \sigma)$ and $\det(\widehat{h}_{w_0}^f) \neq \det(h_{w_0}^f)$ in $\mathrm{Tw}(E_{u_0}^g, \sigma)$. Then we define inner products $\widehat{b}_p^f$ on $M_p^f = \bigoplus_{w \in \mathcal{W}(f;p)} M_w^f$ and $\widehat{b}_p^g$ on $M_p^g =$

$\bigoplus_{u\in\mathcal{W}(g;p)} M_u^g$ by

$$\begin{aligned}\widehat{b}_p^f &= \left(\mathrm{Tr}_{E_{w_0}^f/\mathbb{Q}_p}\circ\widehat{h}_{w_0}^f\right)\oplus \bigoplus_{w\in\mathcal{W}(f;p)\setminus\{w_0\}} b_p^f|_{M_w^f},\\ \widehat{b}_p^g &= \left(\mathrm{Tr}_{E_{u_0}^g/\mathbb{Q}_p}\circ\widehat{h}_{u_0}^g\right)\oplus \bigoplus_{u\in\mathcal{W}(g;p)\setminus\{u_0\}} b_p^g|_{M_u^f},\end{aligned} \tag{34}$$

and define $\widehat{b}_p$ on M_p by

$$\widehat{b}_p := b_p|_{M_p^+\oplus M_p^-}\oplus\widehat{b}_p^f\oplus\widehat{b}_p^g\oplus\left(\bigoplus_{k\in I_1\setminus\{f,g\}} b_p\,|_{M_p^k}\right)\oplus b_p|_{M_p^2}.$$

Claim: The inner product $\widehat{b}_p$ has properties (P1)–(P3). Properties (P1) and (P3) are clear. We first show that the class

$$\begin{aligned}\omega :&= \partial[\widehat{b}_p|_{M_{w_0}^f}]+\partial[\widehat{b}_p|_{M_{u_0}^g}]-\partial[b_p|_{M_{w_0}^f}]-\partial[b_p|_{M_{u_0}^g}]\\ &= \partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(\widehat{h}_{w_0}^f))+\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(\widehat{h}_{u_0}^g))-\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(h_{w_0}^f))-\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(h_{u_0}^g))\end{aligned}$$

is equal to 0. If $\bar{\alpha}_{w_0}^f\neq 1,-1$ then it follows from Theorem 8.11 (ii) that

$$\begin{aligned}\omega &= \left(\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(\widehat{h}_{w_0}^f))-\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(h_{w_0}^f))\right)\\ &\qquad+\left(\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(\widehat{h}_{u_0}^g))-\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(h_{u_0}^g))\right)\\ &= [\mathbb{F}_p(\bar{\alpha}_{w_0}^f),b_1,\bar{\alpha}_{w_0}^f]+[\mathbb{F}_p(\bar{\alpha}_{u_0}^g),b_1,\bar{\alpha}_{u_0}^g]\\ &= 2[\mathbb{F}_p(\bar{\alpha}_{w_0}^f),b_1,\bar{\alpha}_{w_0}^f]\\ &= 0.\end{aligned}$$

Suppose that $\bar{\alpha}_{w_0}^f=1$ or -1. Note that $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p;\bar{h})\cong W(\mathbb{F}_p)$ in this case. If $p=2$ then Theorem 6.38 (i) implies that $\omega=0$ since $\dim(\omega)\equiv 0 \bmod 2$. If p is an odd prime then Lemma 9.15 leads to $\omega=0$ since

$$\begin{aligned}\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(\widehat{h}_{w_0}^f))&\neq\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(h_{w_0}^f)),\\ \dim\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(\widehat{h}_{w_0}^f))&\equiv\dim\partial_{M_{w_0}^f,\alpha_{w_0}^f}(\det(h_{w_0}^f))\mod 2,\\ \partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(\widehat{h}_{u_0}^g))&\neq\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(h_{u_0}^g)),\\ \dim\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(\widehat{h}_{u_0}^g))&\equiv\dim\partial_{M_{u_0}^g,\alpha_{u_0}^g}(\det(h_{u_0}^g))\mod 2\end{aligned}$$

by Theorem 8.11 (ii) or (iii). Hence, we have $\omega=0$ in any case. We then show that $\widehat{b}_p$ has property (P2). By the construction of $\widehat{b}_p$, it follows that

$$\begin{aligned}\partial[M_p,\widehat{b}_p,\alpha] &= \partial[M_p,b_p,\alpha]-\partial[b_p|_{M_{w_0}^f}]-\partial[b_p|_{M_{u_0}^g}]+\partial[\widehat{b}_p|_{M_{w_0}^f}]+\partial[\widehat{b}_p|_{M_{u_0}^g}]\\ &= \partial[M_p,b_p,\alpha]+\omega.\end{aligned}$$

On the other hand, we have $\omega=0$ as proved now and $\partial[M_p,b_p,\alpha]=0$ because (M_p,b_p) contains an α-stable unimodular lattice by property (P2) for b_p. Hence $\partial[M_p,\widehat{b}_p,\alpha]=0$, which implies that $(M_p,\widehat{b}_p)$ contains an α-stable unimodular lattice by Theorem 6.32. If p is odd then the lattice is even and we are done.

Suppose that $p = 2$. It is sufficient to show that the three conditions (i)–(iii) of Proposition 8.18 hold for $V = M_2$, $b = \widehat{b}_2$, and $t = \alpha$. Note that the three conditions hold for (M_2, b_2, α) since it contains an α-stable even unimodular lattice. The condition (i) for $(M_2, \widehat{b}_2, \alpha)$ has already been proved. We write $\mathrm{sn}(\alpha; b_2)$ and $\mathrm{sn}(\alpha; \widehat{b}_2)$ for the spinor norms of $\alpha : M_2 \to M_2$ with respect to b_2 and $\widehat{b}_2$ respectively. Then

$$\begin{aligned}\mathrm{sn}(\alpha; \widehat{b}_2) &= \det(\widehat{b}_2^-) \cdot \det\left(\frac{1+\alpha}{2}\Big|_{M_2^+ \oplus M_2^1 \oplus M_2^2}\right) \\ &= \det(b_2^-) \cdot \det\left(\frac{1+\alpha}{2}\Big|_{M_2^+ \oplus M_2^1 \oplus M_2^2}\right) \\ &= \mathrm{sn}(\alpha; b_2),\end{aligned}$$

which implies that the condition (iii) holds for $(M_2, \widehat{b}_2, \alpha)$. For the condition (ii), it suffices to show that $\widehat{b}_2 \cong b_2$. Lemma 9.14 implies that

$$\mathrm{hw}_2(\widehat{b}_2|_{M^f_{w_0}}) - \mathrm{hw}_2(b_2|_{M^f_{w_0}}) = \mathrm{hw}_2(\mathrm{Tr}_{E^f_w/\mathbb{Q}_2} \circ \widehat{h}^f_{w_0}) - \mathrm{hw}_2(\mathrm{Tr}_{E^f_w/\mathbb{Q}_2} \circ h^f_{w_0}) = 1$$

since $\det(\widehat{h}^f_{w_0}) \neq \det(h^f_{w_0})$. Similarly we get $\mathrm{hw}_2(\widehat{b}_2|_{M^g_{u_0}}) - \mathrm{hw}_2(b_2|_{M^g_{u_0}}) = 1$. Thus

$$\mathrm{hw}_2(\widehat{b}_2) - \mathrm{hw}_2(b_2) = \mathrm{hw}_2(\widehat{b}_2|_{M^f_{w_0}}) + \mathrm{hw}_2(\widehat{b}_2|_{M^g_{u_0}}) - \mathrm{hw}_2(b|_{M^f_{w_0}}) - \mathrm{hw}_2(b|_{M^g_{u_0}}) = 0$$

where the first equality follows from Lemma 4.31 (iii). Hence $\widehat{b}_2$ and b_2 have the same dimension, same determinant, and same Hasse-Witt invariant, which means that $\widehat{b}_2 \cong b_2$ as required. Therefore $(M_2, \widehat{b}_2)$ contains an α-stable even unimodular lattice, that is, $\widehat{b}_2$ has property (P2). This completes the proof of Claim.

We now define

$$\widehat{\beta} := \{\widehat{b}_v\}_{v \in \mathcal{V}} \quad \text{where } \widehat{b}_v = b_v \text{ for } v \neq p.$$

Then each $\widehat{b}_v$ has the properties (P1)–(P3); this is clear for $v \neq p$ and proved now for $v = p$. Moreover, for each $f \in I$, the set $\{v \in \mathcal{V} \mid \mathrm{hw}_v(\widehat{b}_v|_{M^f_v}) \neq 0\}$ is contained in $\{p\} \cup \{v \in \mathcal{V} \mid \mathrm{hw}_v(b_v|_{M^f_v}) \neq 0\}$, and in particular, it is a finite set. Hence $\widehat{\beta} \in \mathcal{B}_{\mathfrak{i}}$. It remains to show that $\eta(\beta) + \mathbf{1}_{\{f,g\}} = \eta(\widehat{\beta})$. It is obvious that $\eta(\beta)(k) = \eta(\widehat{\beta})(k)$ for $k \neq f, g$, and we have

$$\eta(\widehat{\beta})(f) - \eta(\beta)(f) = \mathrm{hw}_p(\widehat{b}_p|_{M^f_p}) - \mathrm{hw}_p(b_p|_{M^f_p}) = \mathrm{hw}_p(\widehat{b}|_{M^f_{w_0}}) - \mathrm{hw}_p(b|_{M^f_{w_0}}) = 1.$$

The same calculation yields $\eta(\widehat{\beta})(g) - \eta(\beta)(g) = 1$, and thus $\eta(\beta) + \mathbf{1}_{\{f,g\}} = \eta(\widehat{\beta})$. The proof for the case $f, g \in I_1$ has been completed now.

Suppose that $f(X) = X \mp 1$. In this case, there exists an inner product $\widehat{b}^f_p = \widehat{b}^\pm_p$ on $M^\pm_p$ such that $\det(\widehat{b}^\pm_p) = \delta_\pm$ and $\mathrm{hw}_p(\widehat{b}^\pm_p) \neq \mathrm{hw}_p(b^\pm_p)$, see Remark 9.13 (iii). Let $\widehat{b}^g_p$ be an inner product defined similarly if $g(X) = X \pm 1$ and as in (34) if $g \in I_1$. We define

$$\begin{aligned}\widehat{b}_p &:= \widehat{b}^f_p \oplus \widehat{b}^g_p \oplus \left(\bigoplus_{k \in I \setminus \{f,g\}} b^k_p\right) \oplus b^2_p, \\ \widehat{\beta} &:= \{\widehat{b}_v\}_{v \in \mathcal{V}} \quad \text{where } \widehat{b}_v = b_v \text{ for } v \neq p.\end{aligned}$$

Then it can be shown similarly that $\widehat{\beta} \in \mathcal{B}_{\mathfrak{i}}$ and $\eta(\beta) + \mathbf{1}_{\{f,g\}} = \eta(\widehat{\beta})$. The proof is complete. □

We then prove that the image $\eta(\mathcal{B}_{\mathrm{i}})$ is contained in a coset of C_0. For $\beta = \{b_v\}_{v\in\mathcal{V}} \in \mathcal{B}_{\mathrm{i}}$ and $v \in \mathcal{V}$, we write $\eta_v(\beta) \in C(I)$ for the map defined by $\eta_v(\beta)(f) = \mathrm{hw}_v(b_v|_{M_v^f})$ $(f \in I)$. This map $\eta_v(\beta) : I \to \mathbb{Z}/2\mathbb{Z}$ is determined only by b_v and does not depend on any other $b_{v'}$. Note that $\eta(\beta)(f) = \sum_{v\in\mathcal{V}} \eta_v(\beta)(f)$. Furthermore, we define

$$V(\beta, \widehat{\beta}) := \{v \in \mathcal{V} \mid \eta_v(\beta) \neq \eta_v(\widehat{\beta})\}$$

for $\beta, \widehat{\beta} \in \mathcal{B}_{\mathrm{i}}$. This set $V(\beta, \widehat{\beta})$ is a finite set of primes. Indeed, $\eta_\infty(\beta) = \eta_\infty(\widehat{\beta})$ since $b_\infty \cong \widehat{b}_\infty$, and $\eta_v(\beta) = \mathbf{0} = \eta_v(\widehat{\beta})$ for almost all $v \in \mathcal{V}$ by the definition of $\mathcal{B}_{\mathrm{i}}$. The following lemma is crucial in proving $\eta(\mathcal{B}_{\mathrm{i}})$ is contained in a coset of C_0.

Lemma 9.17. *Let $\beta = \{b_v\}_v, \widehat{\beta} = \{\widehat{b}_v\}_v \in \mathcal{B}_{\mathrm{i}}$, and suppose that a prime p belongs to $V(\beta, \widehat{\beta})$. Then there exists $\widetilde{\beta} \in \mathcal{B}_{\mathrm{i}}$ such that $\eta(\widetilde{\beta}) - \eta(\beta) \in C_0$, $V(\widetilde{\beta}, \widehat{\beta}) \subset V(\beta, \widehat{\beta})$, and it satisfies the following conditions:*

$$\begin{aligned} &\partial[\widetilde{b}_p|_{M_p^+}] = \partial[\widehat{b}_p|_{M_p^+}],\ \partial[\widetilde{b}_p|_{M_p^-}] = \partial[\widehat{b}_p|_{M_p^-}], \\ &\partial[\widetilde{b}_p|_{M_w^f}] = \partial[\widehat{b}_p|_{M_w^f}] \quad \textit{for any } f \in I_1 \textit{ and } w \in \mathcal{W}(f;p). \end{aligned} \tag{35}$$

Proof. We first show that there exists $\beta'' = \{b''_v\}_v \in \mathcal{B}_{\mathrm{i}}$ such that $\eta(\beta'') - \eta(\beta) \in C_0$, $V(\beta'', \widehat{\beta}) \subset V(\beta, \widehat{\beta})$, $\partial[b''_p|_{M_p^+}] = \partial[\widehat{b}_p|_{M_p^+}]$, and $\partial[b''_p|_{M_p^-}] = \partial[\widehat{b}_p|_{M_p^-}]$. If $p = 2$ then it follows from Theorem 6.38 (i) that $\partial[b_2|_{M_2^\pm}] = \partial[\widehat{b}_2|_{M_2^\pm}]$ because they have the same dimension module 2 by Proposition 6.35. Thus β is the required family in this case. Suppose that $p \neq 2$, and $\partial[b_p|_{M_p^+}] \neq \partial[\widehat{b}_p|_{M_p^+}]$. Since we have $\partial[M_p, b_p, \alpha] = \partial[M_p, \widehat{b}_p, \alpha] = 0$, the images of them under the projection $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p) \to W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p; X-1)$ are also 0. Thus there exists $f \in I_1$ and $w_0 \in \mathcal{W}(f;p)$ such that $(X-1) \mid f_{w_0} \bmod p$ and $\partial[b_p|_{M_{w_0}^f}] \neq \partial[\widehat{b}_p|_{M_{w_0}^f}]$ in $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p; X-1)$. In this case $w_0 \notin \mathcal{W}_{\mathrm{sp}}(f;p)$ because otherwise both $\partial[b_p|_{M_{w_0}^f}]$ and $\partial[\widehat{b}_p|_{M_{w_0}^f}]$ would be 0. In particular $X-1 \in \overline{I(f;\mathbb{Q}_p)}$. On the other hand, we have $X-1 \in \overline{I(X-1;\mathbb{Q}_p)}'$. Indeed, neither $m_+ = 1$ nor $m_+ = 2$ and $\delta_+ = -1$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ occurs because Lemma 9.14 (i) implies that $\mathrm{hw}_p(b_p|_{M_p^+}) \neq \mathrm{hw}_p(\widehat{b}_p|_{M_p^+})$. Thus $p \in \Pi_{\mathrm{i}}^F(X-1, f)$. We now define

$$\begin{aligned} &b'_p := \widehat{b}_p|_{M_p^+} \oplus b_p|_{M_p^-} \oplus \left(\widehat{b}_p|_{M_{w_0}^f} \oplus \bigoplus_{w\in\mathcal{W}(f;p)\setminus\{w_0\}} b_p|_{M_w^f}\right) \oplus \left(\bigoplus_{k\in I_1\setminus\{f\}} b_p|_{M_p^k}\right) \oplus b_p|_{M_p^2}, \\ &\beta' := \{b'_v\}_{v\in\mathcal{V}} \quad \text{where } b'_v = b_v \text{ for } v \neq p. \end{aligned}$$

Then β' belongs to $\mathcal{B}_{\mathrm{i}}$, and $\eta(\beta') = \eta(\beta) + \mathbf{1}_{\{X-1,f\}}$ as in the proof of Proposition 9.16. Thus $\eta(\beta') - \eta(\beta) \in C_0$. It is clear that $V(\beta', \widehat{\beta}) \subset V(\beta, \widehat{\beta})$ and $\partial[b'_p|_{M_p^+}] = \partial[\widehat{b}_p|_{M_p^+}]$ by the definition of β'. If $\partial[b'_p|_{M_p^-}] \neq \partial[\widehat{b}_p|_{M_p^-}]$ then we repeat a similar procedure to obtain $\beta'' = \{b''_v\}_{v\in\mathcal{V}} \in \mathcal{B}_{\mathrm{i}}$ such that $\eta(\beta'') - \eta(\beta') \in C_0$, $V(\beta'', \widehat{\beta}) \subset V(\beta', \widehat{\beta})$, $\partial[b''_p|_{M_p^+}] = \partial[\widehat{b}_p|_{M_p^+}]$, and $\partial[b''_p|_{M_p^-}] = \partial[\widehat{b}_p|_{M_p^-}]$. This is the first goal since $\eta(\beta'') - \eta(\beta) = (\eta(\beta'') - \eta(\beta')) + (\eta(\beta') - \eta(\beta)) \in C_0$ and $V(\beta'', \widehat{\beta}) \subset V(\beta', \widehat{\beta}) \subset V(\beta, \widehat{\beta})$.

By considering β'' instead of β, we assume that $\partial[b_p|_{M_p^+}] = \partial[\widehat{b}_p|_{M_p^+}]$ and $\partial[b_p|_{M_p^-}] = \partial[\widehat{b}_p|_{M_p^-}]$ without loss of generality. Set $D_p(\beta, \widehat{\beta}) := \bigsqcup_{f\in I_1}\{w \in \mathcal{W}(f;p) \mid \partial[b_p|_{M_w^f}] \neq \partial[\widehat{b}_p|_{M_w^f}]\}$. If $\#D_p(\beta, \widehat{\beta}) = 0$ then β itself is the desired family. Suppose that $\#D_p(\beta, \widehat{\beta}) > 0$, and take $f \in I_1$ and $w_0 \in \mathcal{W}(f;p)$ satisfying $\partial[b_p|_{E_{w_0}^f}] \neq \partial[\widehat{b}_p|_{E_{w_0}^f}]$. Note that $w_0 \notin \mathcal{W}_{\mathrm{sp}}(f;p)$ as above. Let $\bar{h} \in \mathbb{F}_p[X]$ denote the unique irreducible factor of $(f_{w_0} \bmod p)$, where $f_{w_0} \in \mathbb{Z}_p[X]$ is the

irreducible factor of f in $\mathbb{Q}_p[X]$ corresponding to the place w_0. Since the images of $\partial[M_p, b_p, \alpha]$ and $\partial[M_p, \widehat{b}_p, \alpha]$ under the projection $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p) \to W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p; \bar{h})$ are the trivial class, there exists $g \in I_1$ and $u_0 \in \mathcal{W}(g;p) \setminus \mathcal{W}_{\mathrm{sp}}(g;p)$ such that $\bar{h} \mid (g_{u_0} \bmod p)$ and $\partial[b_p|_{E^g_{u_0}}] \neq \partial[\widehat{b}_p|_{E^g_{u_0}}]$ in $W_{\mathbb{F}_p[\Gamma]}(\mathbb{F}_p; \bar{h})$. Note that $p \in \Pi^F_{\mathrm{i}}(f,g)$. We now define an inner product $b^{(1)}_p$ on M_p as the one obtain by replacing $b_p|_{M^f_{w_0}}$ with $\widehat{b}_p|_{M^f_{w_0}}$ and $b_p|_{E^g_{u_0}}$ with $\widehat{b}_p|_{E^g_{u_0}}$ in

$$b_p = b_p|_{M_p^+ \oplus M_p^-} \oplus \left(\bigoplus_{k \in I_1} \bigoplus_{w \in \mathcal{W}(k;p)} b_p|_{M^k_w} \right) \oplus b_p|_{M^2_p},$$

and set $\beta^{(1)} := \{b^{(1)}_v\}_{v \in \mathcal{V}}$ where $b^{(1)}_v = b_v$ for $v \neq p$. Then, as in the proof of Proposition 9.16, we have $\beta^{(1)} \in \mathcal{B}_{\mathrm{i}}$, and

$$\eta(\beta^{(1)}) = \begin{cases} \eta(\beta) + \mathbf{1}_{\{f,g\}} & \text{if } f \neq g \\ \eta(\beta) & \text{if } f = g, \end{cases}$$

which implies that $\eta(\beta^{(1)}) - \eta(\beta) \in C_0$. Moreover, by the construction of $\beta^{(1)}$, we have $V(\beta^{(1)}, \widehat{\beta}) \subset V(\beta, \widehat{\beta})$ and $\#D_p(\beta^{(1)}, \widehat{\beta}) = \#D_p(\beta, \widehat{\beta}) - 2$. Therefore we obtain the desired family $\widetilde{\beta} \in \mathcal{B}_{\mathrm{i}}$ by repeating the same procedure until $\#D_p(\widetilde{\beta}, \widehat{\beta}) = 0$. The proof is complete. □

Proposition 9.18. *We have $\eta(\widehat{\beta}) - \eta(\beta) \in C_0$ for any $\beta, \widehat{\beta} \in \mathcal{B}_{\mathrm{i}}$. In other words, the image $\operatorname{im} \eta \subset C(I)$ is contained in a coset of C_0.*

Proof. Let $\beta = \{b_v\}_v, \widehat{\beta} = \{\widehat{b}_v\}_v \in \mathcal{B}_{\mathrm{i}}$. we can obtain $\widetilde{\beta} = \{\widetilde{b}_v\}_v \in \mathcal{B}_{\mathrm{i}}$ such that $\eta(\widetilde{\beta}) - \eta(\beta) \in C_0$, $V(\widetilde{\beta}, \widehat{\beta}) \subset V(\beta, \widehat{\beta})$, and satisfies (35) for all $p \in V(\beta, \widehat{\beta})$ by applying Lemma 9.17 repeatedly, since $V(\beta, \widehat{\beta})$ is a finite set of primes. It is sufficient to show that $\eta(\widehat{\beta}) - \eta(\widetilde{\beta}) \in C_0$. Since

$$\eta_p(\widehat{\beta})(f) - \eta_p(\widetilde{\beta})(f) = \begin{cases} \mathrm{hw}_p(\widehat{b}_p|_{M_p^\pm}) - \mathrm{hw}_p(\widetilde{b}_p|_{M_p^\pm}) & \text{if } f(X) = X \mp 1 \\ \sum_{w \in \mathcal{W}(f;p)} (\mathrm{hw}_p(\widehat{b}_p|_{M^f_w}) - \mathrm{hw}_p(\widetilde{b}_p|_{M^f_w})) & \text{if } f \in I_1 \end{cases}$$

for $f \in I$ and $p \in V(\beta, \widehat{\beta})$, Lemma 9.14 with (35) implies that $\eta_p(\widehat{\beta})(f) - \eta_p(\widetilde{\beta})(f) = 0$ unless $p \neq 2$. In other words $V(\widetilde{\beta}, \widehat{\beta}) \subset \{2\}$. Hence

$$\eta(\widehat{\beta}) - \eta(\widetilde{\beta}) = \sum_{p \in V(\widetilde{\beta}, \widehat{\beta})} (\eta_p(\widehat{\beta}) - \eta_p(\widetilde{\beta})) = \eta_2(\widehat{\beta}) - \eta_2(\widetilde{\beta}).$$

Put $J = \{f \in I \mid \eta_2(\widehat{\beta})(f) \neq \eta_2(\widetilde{\beta})(f)\}$. An element of J is $X - 1$, $X + 1$, or $f \in I_1$ with $\mathcal{W}_{\mathrm{rm}}(f;2) \neq \emptyset$ by Lemma 9.14. Thus, any element $f \in J$ has a $*$-symmetric irreducible factor whose reduction modulo 2 is divisible by $X - 1$ (in $\mathbb{F}_2[X]$). This shows that $2 \in \Pi^F_{\mathrm{i}}(f,g)$, and in particular $\mathbf{1}_{\{f,g\}} \in C_0$ for any distinct $f, g \in J$. We then show that the number of elements of J is even. Since $(M_2, \widehat{b}_2)$ and $(M_2, \widetilde{b}_2)$ contain even unimodular lattices of discriminant 1, they are isomorphic. Thus

$$0 = \mathrm{hw}_2(\widehat{b}_2) - \mathrm{hw}_2(\widetilde{b}_2) = \sum_{f \in I} \left(\mathrm{hw}_2(\widehat{b}_2|_{M^f_2}) - \mathrm{hw}_2(\widetilde{b}_2|_{M^f_2}) \right).$$

This shows that $\#J$ is even. Write $J = \{f_1, \dots, f_{2l}\}$. Then we obtain

$$\eta(\widehat{\beta}) - \eta(\widetilde{\beta}) = \eta_2(\widehat{\beta}) - \eta_2(\widetilde{\beta}) = \mathbf{1}_{\{f_1, f_2\}} + \cdots + \mathbf{1}_{\{f_{2l-1}, f_{2l}\}} \in C_0$$

as required. The proof is complete. □

Theorem 9.19. *The image $\eta(\mathcal{B}_{\mathrm{i}}) \subset C(I)$ coincides with a coset of C_0.*

Proof. This is a consequence of Propositions 9.16 and 9.18. □

9.4 Local-global obstruction 2

Definition 9.20. The *equivalence relation defined by* $(F, \mathfrak{i})$, written $\sim$, is the one on I generated by the binary relation $\{(f, g) \in I \times I \mid \Pi_{\mathfrak{i}}^F(f, g) \neq \emptyset\}$. We write $\Omega_{\mathfrak{i}}$ for the submodule $\{c \in C(I) \mid c(f) = c(g) \text{ if } f \sim g\}$ of $C(I)$. This is the submodule consisting of maps which are constant on each equivalence class with respect to $\sim$.

We now introduce an inner product $C(I) \times C(I) \to \mathbb{Z}/2\mathbb{Z}$ by

$$\gamma \cdot c = \sum_{f \in I} \gamma(f)c(f) \quad (\gamma, c \in C(I)).$$

Lemma 9.21. *We have* $\Omega_{\mathfrak{i}} = C_0^{\perp}$*, or equivalently* $\Omega_{\mathfrak{i}}^{\perp} = C_0$.

Proof. Let $c \in \Omega_{\mathfrak{i}}$. Then $\mathbf{1}_{\{f,g\}} \cdot c = c(f) + c(g) = 2c(f) = 0$ for any $f, g \in I$ with $\Pi_{\mathfrak{i}}^F(f, g) \neq \emptyset$. Since C_0 is generated by $\{\mathbf{1}_{\{f,g\}} \mid \Pi_{\mathfrak{i}}^F(f, g) \neq \emptyset\}$, we get $\Omega_{\mathfrak{i}} \subset C_0^{\perp}$.

Let $c \in C_0^{\perp}$. Let $J \subset I$ be an equivalence class with respect to $\sim$, and take $f, g \in J$ with $f \neq g$. Then, there exist distinct $h_1, \ldots, h_l \in J$ such that $\Pi_{\mathfrak{i}}^F(f, h_1), \Pi_{\mathfrak{i}}^F(h_j, h_{j+1})$ $(j = 1, \ldots, l-1)$, and $\Pi_{\mathfrak{i}}^F(h_l, g)$ are not empty. Thus

$$\begin{aligned} c(f) + c(g) &= \mathbf{1}_{\{f,g\}} \cdot c \\ &= (\mathbf{1}_{\{f,h_1\}} + \mathbf{1}_{\{h_1,h_2\}} + \cdots + \mathbf{1}_{\{h_{k-1},h_k\}} + \mathbf{1}_{\{h_k,g\}}) \cdot c \\ &= \mathbf{1}_{\{f,h_1\}} \cdot c + \mathbf{1}_{\{h_1,h_2\}} \cdot c + \cdots + \mathbf{1}_{\{h_{k-1},h_k\}} \cdot c + \mathbf{1}_{\{h_k,g\}} \cdot c \\ &= 0, \end{aligned}$$

which implies that $c(f) = c(g)$. Hence c is constant on J. This means that $c \in \Omega_{\mathfrak{i}}$, and therefore $C_0^{\perp} \subset \Omega_{\mathfrak{i}}$. This completes the proof. □

Definition 9.22. The homomorphism

$$\Omega_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z},\ c \mapsto \eta(\beta) \cdot c$$

is defined independently of the choice of $\beta \in \mathcal{B}_{\mathfrak{i}}$ since $\eta(\mathcal{B}_{\mathfrak{i}})$ is a coset of C_0 by Theorem 9.19 and $\Omega_{\mathfrak{i}} \subset C_0^{\perp}$ by Lemma 9.21. This homomorphism is called the *obstruction map* for $(F, \mathfrak{i})$ and denoted by $\mathrm{ob}_{\mathfrak{i}} : \Omega_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z}$. The submodule $\Omega_{\mathfrak{i}} \subset C(I)$ is called the *obstruction group* for $(F, \mathfrak{i})$. Note that the obstruction group $\Omega_{\mathfrak{i}}$ does not depend on $\mathfrak{i}$ unless $m_+ = 2$ or $m_- = 2$ since so does $\sim$.

We will prove that there exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry if and only if the obstruction map $\mathrm{ob}_{\mathfrak{i}} : \Omega_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z}$ is the zero map. Before that, let us see that the obstruction map factors through the quotient module $\Omega_{\mathfrak{i}}/\{\text{constant maps}\}$.

Proposition 9.23. *We have* $\eta(\beta) \cdot \mathbf{1}_I = 0$ *for any* $\beta \in \mathcal{B}_{\mathfrak{i}}$.

Proof. We define an inner product b on M as follows. Let $b^{\pm}$ be an inner product on $M^{\pm}$ which has Gram matrix $\mathrm{diag}(\delta_{\pm}, 1, \ldots, 1)$. For each f which is in I_1 or of the form gg^* for $g \in I_2$, take a hermitian product $h^f : M^f \times M^f \to E^f$ arbitrarily and set $b^f := \mathrm{Tr}_{E^f/\mathbb{Q}} \circ h^f$. Then, define the inner product b on M by $b := b^+ \oplus b^- \oplus \bigoplus_{f \in I_1} b^f \oplus \bigoplus_{\{g,g^*\} \subset I_2} b^{gg^*}$.

Let $\beta = \{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}}$. It follows from Lemma 4.31 (iii) that

$$\begin{aligned} &\mathrm{hw}_v(b_v) - \sum_{f \in I} \mathrm{hw}_v(b_v|_{M_v^f}) - \sum_{\{g,g^*\} \subset I_2} \mathrm{hw}_v(b_v|_{M_v^{gg^*}}) \\ &\quad = \mathrm{hw}_v(b \otimes \mathbb{Q}_v) - \sum_{f \in I} \mathrm{hw}_v(b^f \otimes \mathbb{Q}_v) - \sum_{\{g,g^*\} \subset I_2} \mathrm{hw}_v(b^{gg^*} \otimes \mathbb{Q}_v) \end{aligned}$$

for any $v \in \mathcal{V}$, since $\det(b_v|_{M_v^\pm}) = \delta_\pm = \det(b|_{M^\pm} \otimes \mathbb{Q}_v)$ and $\det(b_v|_{M_v^f}) = f(1)^{m_f} f(-1)^{m_f} = \det(b|_{M^f} \otimes \mathbb{Q}_v)$ for each $f \in I_1$ or $f = gg^*$ by Proposition 7.32. Furthermore, since $b_v|_{M_v^{gg^*}} \cong b|_{M^{gg^*}} \otimes \mathbb{Q}_v$ for each $g \in I_2$ by Corollary 4.66, we get

$$\mathrm{hw}_v(b_v) - \sum_{f \in I} \mathrm{hw}_v(b_v|_{M_v^f}) = \mathrm{hw}_v(b \otimes \mathbb{Q}_v) - \sum_{f \in I} \mathrm{hw}_v(b^f \otimes \mathbb{Q}_v).$$

Summing over $v \in \mathcal{V}$ yields

$$\sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v) - \sum_{f \in I} \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}) = \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b \otimes \mathbb{Q}_v) - \sum_{f \in I} \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b^f \otimes \mathbb{Q}_v) = 0,$$

where the last equality is by the reciprocity (Proposition 4.53). Since

$$\eta(\beta) \cdot \mathbf{1}_I = \sum_{f \in I} \eta(\beta)(f) = \sum_{f \in I} \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^f}),$$

it remains to show that $\sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v) = 0$. Let (Λ, B) be an even unimodular lattice over $\mathbb{Z}$ of signature (r, s). It follows from Theorems 5.18 and 5.23 that $B \otimes \mathbb{Q}_p \cong b_p$ for every prime p since they have the same discriminant and contain even unimodular lattices respectively. Furthermore $B \otimes \mathbb{Q}_\infty \cong b_\infty$ since they have the same signature. Hence $\sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v) = \sum_{v \in \mathcal{V}} \mathrm{hw}_v(B \otimes \mathbb{Q}_v) = 0$ by the reciprocity. This completes the proof. □

Definition 9.24. We refer to the quotient module $\widetilde{\Omega}_\mathfrak{i} := \Omega_\mathfrak{i} / \{\mathbf{0}, \mathbf{1}_I\}$ as the *reduced obstruction group* for $(F, \mathfrak{i})$. The obstruction map factors through $\widetilde{\Omega}_\mathfrak{i}$ by Proposition 9.23. The induces homomorphism $\widetilde{\Omega}_\mathfrak{i} \to \mathbb{Z}/2\mathbb{Z}$ is referred to as the *reduced obstruction map* for $(F, \mathfrak{i})$ and denoted $\widetilde{\mathrm{ob}}_\mathfrak{i} : \Omega_\mathfrak{i} \to \mathbb{Z}/2\mathbb{Z}$.

We conclude this section with the following theorem.

Theorem 9.25. *Let $r, s \in \mathbb{Z}_{\geq 0}$ be non-negative integers with $r \equiv s \bmod 8$, $F \in \mathbb{Z}[X]$ a $*$-symmetric polynomial of degree $r + s$ with the conditions* $(\mathrm{Sign})_{r,s}$ *and* (Square)*, and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ an index map. The following conditions are equivalent:*

(i) *There exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry.*

(ii) *The associated $\mathbb{Q}[\Gamma]$-module M of F with transformation α admits an inner product b such that α becomes an isometry having index $\mathfrak{i}$ and (M, b) contains an α-stable even unimodular lattice over $\mathbb{Z}$.*

(iii) *There exists a family $\beta \in \mathcal{B}_\mathfrak{i}$ such that $\eta(\beta) = \mathbf{0}$.*

(iv) *The obstruction map $\mathrm{ob}_\mathfrak{i} : \Omega_\mathfrak{i} \to \mathbb{Z}/2\mathbb{Z}$ is the zero map.*

(v) *The reduced obstruction map $\widetilde{\mathrm{ob}}_\mathfrak{i} : \widetilde{\Omega}_\mathfrak{i} \to \mathbb{Z}/2\mathbb{Z}$ is the zero map.*

Moreover, if both r and s are positive then the following condition is also equivalent:

(vi) *Any even unimodular lattice of signature (r, s) admits a semisimple $(F, \mathfrak{i})$-isometry.*

Proof. Suppose that there exists an even unimodular lattice (Λ, b) over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry t. By identifying $\Lambda \otimes \mathbb{Q}$ with M and t with α, we obtain (i) $\Rightarrow$ (ii). The reverse implication (ii) $\Rightarrow$ (i) is obvious. The equivalence (ii) $\Leftrightarrow$ (iii) is nothing but Theorem 9.7. (iii) $\Rightarrow$ (iv) is clear. We prove (iv) $\Rightarrow$ (iii). Suppose that the obstruction map

$\mathrm{ob}_{\mathfrak{i}} : \Omega_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z}$ vanishes, and take $\widetilde{\beta} \in \mathcal{B}_{\mathfrak{i}}$ arbitrarily. Then $\eta(\widetilde{\beta}) \in \Omega_{\mathfrak{i}}^{\perp} = C_0$ by Lemma 9.21. Thus $\eta(\mathcal{B}_{\mathfrak{i}}) = C_0$ by Theorem 9.19, and there exists $\beta \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\beta) = \mathbf{0}$. This shows (iv) $\Rightarrow$ (iii). The equivalence (iv) $\Leftrightarrow$ (v) is obvious. Moreover, if both r and s are positive then the equivalence (i) $\Leftrightarrow$ (vi) follows from the uniqueness of an even unimodular lattice of signature (r, s) (Theorem 5.25). The proof is complete. □

Remark 9.26. We give some historical remarks on Theorem 9.25. Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree. As mentioned in Introduction, Bayer-Fluckiger and Taelman [3] proved that when F is irreducible (or a power of a $*$-symmetric irreducible polynomial), the conditions (Sign) and (Square) are necessary and sufficient for the existence of an even unimodular lattice with a prescribed signature, having a semisimple isometry of characteristic polynomial F. For its proof, the local-global idea was introduced as well as the argument for the local existence of a unimodular lattice in terms of equivariant Witt groups. Afterwards, Bayer-Fluckiger [5, 6, 7] proceeded to the case where the polynomial F is reducible and $+1$-symmetric, and proved that the equivalence (i) $\Leftrightarrow$ (v) of Theorem 9.25 when F is $+1$-symmetric. However, the first proof given in her preprint [6] was difficult to follow, and did not take account of subtle conditions for obstruction that arise from the difference among the sets $\overline{I(f;\mathbb{Q}_p)}$, $\overline{I(f;\mathbb{Q}_p)}'$, and $I(f \bmod p;\mathbb{F}_p)$ for a monic polynomial of $f \in \mathbb{Z}[X]$, see Notation 9.12 and Remark 9.13. On the framework established by her, the author [45] improved the outlook of the proof, for example, by giving the intermediate result, Theorem 9.7, between (i) and (v). He also modified the definition of obstruction. Moreover, in [45], the result extended to the case where F is $*$-symmetric, which covers the -1-symmetric case, mainly by careful analysis at the prime 2. The descriptions in this thesis are more detailed and refined.

9.5 Some examples

This subsection gives some examples such that the obstruction vanishes. We keep the setting and notation of the previous subsections. In particular $F \in \mathbb{Z}[X]$ is a $*$-symmetric polynomial of degree $r + s$ with the conditions $(\mathrm{Sign})_{r,s}$ and (Square), and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ is an index map.

We say that an equivalence relation on I is *weakest* if all elements of I are equivalent one another.

Theorem 9.27. *There exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry if the equivalence relation on I defined by $(F, \mathfrak{i})$ is weakest.*

Proof. Suppose that equivalence relation on I defined by $(F, \mathfrak{i})$ is weakest. This means that $\Omega_{\mathfrak{i}}$ consists of the constant maps, and $\widetilde{\Omega}_{\mathfrak{i}}$ is a trivial group. Hence, the reduced obstruction map $\widetilde{\mathrm{ob}}_{\mathfrak{i}} : \widetilde{\Omega}_{\mathfrak{i}} \to \mathbb{Z}/2\mathbb{Z}$ is zero, which implies that there exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry by Theorem 9.25. □

For example, if F is a power of a $*$-symmetric irreducible polynomial $f \in \mathbb{Z}[X]$ then $I = \{f\}$ and the equivalence relation defined by $(F, \mathfrak{i})$ is clearly weakest. In this case, the obstruction vanishes independently of the index map $\mathfrak{i}$.

Theorem 9.28. *Suppose that $F \in \mathbb{Z}[X]$ is of the form $F(X) = (X - 1)(X + 1)f(X)^{m_f}$, where $f \in \mathbb{Z}[X]$ is a $*$-symmetric irreducible polynomial with $f(1)f(-1) \neq 0$ and m_f is non-negative integer. Then the obstruction map $\mathrm{ob}_{\mathfrak{i}}$ is zero. As a result, there exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry.*

Proof. Let $\beta = \{b_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}}$. For each $v \in \mathcal{V}$ we have $\mathrm{hw}_v(b_v|_{M_v^{\pm}}) = 0$ since $b_v|_{M_v^{\pm}}$ is one dimensional. This implies that $\eta(\beta)(X - 1) = 0$ and $\eta(\beta)(X + 1) = 0$. Moreover, noting that

$I = \{X-1, X+1, f\}$ we have

$$\eta(\beta)(f) = \eta(\beta)(f) + \eta(\beta)(X-1) + \eta(\beta)(X+1) = \eta(\beta) \cdot \mathbf{1}_I = 0$$

where the last equality is by Proposition 9.23. Therefore $\eta(\beta) = \mathbf{0}$, and the obstruction map $\mathrm{ob}_{\mathfrak{i}}$ is the zero map. As a result, there exists an even unimodular lattice over $\mathbb{Z}$ of signature (r, s) having a semisimple $(F, \mathfrak{i})$-isometry by Theorem 9.25. □

10 Computation of obstruction

This section gives some results for computing obstruction. In particular, Theorem 10.15, which compares two obstruction maps, together with results in §11, provides a systematic way to compute an obstruction map.

10.1 Computation of $\Pi(f, g)$

Definition 10.1. Let K be a field, and let $f(X) = \sum_{i=0}^{m} a_i X^i$ and $g(X) = \sum_{j=0}^{n} b_j X^j \in K[X]$ be polynomials of degrees m and n respectively. The *resultant* of f and g is the determinant of the $(m+n) \times (m+n)$ matrix

$$\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix},$$

and denoted by $\mathrm{Res}(f, g)$.

Under the setting in Definition 10.1, let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n \in \overline{K}$ be the roots of f and g respectively. Then it is known that

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j). \tag{36}$$

As a result, the resultant $\mathrm{Res}(f, g)$ vanishes if and only if f and g have a common root. If f and g are monic then Equation (36) can also be written as

$$\mathrm{Res}(f, g) = \prod_{i=1}^{m} g(\alpha_i) = (-1)^m \prod_{j=1}^{n} f(\beta_j).$$

Let f and $g \in \mathbb{Z}[X]$ be monic polynomials with coefficients in $\mathbb{Z}$. Note that $\mathrm{Res}(f, g)$ (considered as $f, g \in \mathbb{Q}[X]$) is an integer by definition. Moreover, for any prime p we have

$$\mathrm{Res}(f \bmod p, g \bmod p) \equiv \mathrm{Res}(f, g) \mod p.$$

Thus $(f \bmod p)$ and $(g \bmod p) \in \mathbb{F}_p[X]$ have a common factor if and only if $\mathrm{Res}(f, g) \equiv 0 \bmod p$.

Notation 10.2. For two monic polynomials f and $g \in \mathbb{Z}[X]$, we define

$$\Pi(f, g) := \{p : \text{prime} \mid \overline{I(f; \mathbb{Q}_p)} \cap \overline{I(g; \mathbb{Q}_p)} \neq \emptyset\},$$

where the set $\overline{I(f; \mathbb{Q}_p)}$ is defined in Notation 9.12. In the situation of Notation 9.12, we have $\Pi_{\mathfrak{i}}^F(f, g) \subset \Pi(f, g)$ and they coincide if $f(1)f(-1)g(1)g(-1) \neq 0$.

The set $\Pi(f,g)$ and the resultant $\mathrm{Res}(f,g)$ are related as follows.

Proposition 10.3. *Let f and $g \in \mathbb{Z}[X]$ be monic polynomials. Then*

$$\Pi(f,g) \subset \{p : \text{prime} \mid p \text{ is a factor of } \mathrm{Res}(f,g)\}.$$

Proof. Suppose that a prime p belongs to $\Pi(f,g)$. Then $(f \bmod p)$ and $(g \bmod p) \in \mathbb{F}_p[X]$ have a common factor, and thus $p \mid \mathrm{Res}(f,g)$. This shows the assertion. □

Example 10.4. Let $f(X) = X^4 - X^2 + 1$; this is the 12-th cyclotomic polynomial and irreducible (see §10.2). Then, the resultant $\mathrm{Res}(f, X-1) = -f(1) = -1$ has no prime factor. This means that $\Pi(f, X-1) = \emptyset$ by Proposition 10.3.

We will give an explicit description of the set $\Pi(f,g)$ when f and g are cyclotomic polynomials in §10.3. The following proposition will be useful.

Proposition 10.5. *Let $f \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial with $f(1)f(-1) \neq 0$, and let p be a prime.*

(i) *If $v_p(f(1))$ is odd then $X - 1 \in \overline{I(f;\mathbb{Q}_p)}$.*

(ii) *If $v_p(f(-1))$ is odd then $X + 1 \in \overline{I(f;\mathbb{Q}_p)}$.*

(iii) *If $(-1)^{\deg(f)/2} f(1)f(-1) \neq 1$ nor -3 in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then $X - 1 \in \overline{I(f;\mathbb{Q}_2)}$.*

Proof. We prove the assertions (i) and (ii) simultaneously. Suppose that $v_p(f(\pm 1))$ is odd. Hensel's lemma (Theorem 1.33) implies that f is factorized as $f = gh$, where g and $h \in \mathbb{Z}_p[X]$ are monic polynomials such that $g(X) \bmod p = (X \mp 1)^{\deg(g)}$ and $h(\pm 1) \not\equiv 0 \bmod p$. In order to get $X \mp 1 \in \overline{I(f;\mathbb{Q}_p)}$, it is sufficient to show that $I(g;\mathbb{Q}_p) \neq \emptyset$, or equivalently g is not of type 2 in $\mathbb{Q}_p[X]$. Suppose that g were of type 2. Then g decomposes as $g = kk^*$ in $\mathbb{Z}_p[X]$ for some $k \in \mathbb{Z}_p[X]$ with $k \neq k^*$. Note that $k(0) \in \mathbb{Z}_p^\times$ since $k(0)$ and $k(0)^{-1}$ are the constant terms of k and $k^* \in \mathbb{Z}_p[X]$ respectively. Then we would have

$$\begin{aligned} v_p(f(\pm 1)) &= v_p(g(\pm 1)) = v_p(k(\pm 1)k^*(\pm 1)) \\ &= v_p(k(\pm 1)k(0)^{-1}(\pm 1)^{\deg(k)}k(\pm 1)) = 2v_p(k(\pm 1)). \end{aligned}$$

This is a contradiction. Therefore g is not of type 2, and we obtain $X \mp 1 \in \overline{I(f;\mathbb{Q}_p)}$. This completes the proofs of (i) and (ii).

We proceed to the assertion (iii). Suppose that $(-1)^{\deg(f)/2} f(1)f(-1) \neq 1$ nor -3 in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. As above, Hensel's lemma implies that f is factorized as $f = gh$, where g and $h \in \mathbb{Z}_2[X]$ are monic polynomials such that $g(X) \bmod 2 = (X \mp 1)^{\deg(g)}$ and $h(\pm 1) \not\equiv 0 \bmod 2$, and it is enough to show that g is not of type 2. Let ϕ be the trace polynomial of h (see Definition 7.11). Then $h(1) - (-1)^{\deg(h)/2} h(-1) = \phi(2) - \phi(-2) \equiv 0 \bmod 4$, which implies that $(-1)^{\deg(h)/2} h(1)h(-1) \equiv 1 \bmod 4$. Thus $(-1)^{\deg(h)/2} h(1)h(-1) = 1$ or -3 in $\mathbb{Z}_2/8\mathbb{Z}_2$, and hence in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. We now suppose that g were of type 2. Then $(-1)^{\deg(g)/2} g(1)g(-1)$ is a square as in Lemma 9.2 (ii). Thus we would get

$$(-1)^{\deg(f)/2} f(1)f(-1) = (-1)^{\deg(g)/2} g(1)g(-1) \cdot (-1)^{\deg(h)/2} h(1)h(-1) = 1 \text{ or } -3$$

in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. This is a contradiction. Therefore g is not of type 2, and we obtain $X - 1 \in \overline{I(f;\mathbb{Q}_2)}$. The proof is complete. □

10.2 Cyclotomic polynomials modulo p

In this subsection, we study factorizations of cyclotomic polynomials modulo a prime number. For a positive integer $n \in \mathbb{Z}_{>0}$, we define $R_n := \{j \in \mathbb{Z} \mid 1 \leq j \leq n \text{ and } \gcd(j,n) = 1\}$. The function $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$ defined by $\varphi(n) = \#R_n$ is called *Euler's totient function*. Let n be a positive integer. The complex number $\zeta_n := \exp(2\pi\sqrt{-1}/n)$ is a primitive n-th root of unity (the letter π is the circle ratio). There are exactly $\varphi(n)$ primitive n-th roots of unity, and they are given by ζ_n^j for $j \in R_n$. The polynomial $\prod_{j \in R_n}(X - \zeta_n^j) \in \mathbb{C}[X]$ is called the *n-th cyclotomic polynomial* and denoted by $\Phi_n(X)$. It is known that $\Phi_n(X)$ is a monic polynomial with coefficients in $\mathbb{Z}$. Moreover, it is the minimal polynomial of ζ_n over $\mathbb{Q}$, and in particular irreducible in $\mathbb{Q}[X]$.

In the following, we fix a prime p, and write $\bar{f} \in \mathbb{F}_p[X]$ for the reduction modulo p of a polynomial $f \in \mathbb{Z}[X]$.

Proposition 10.6. *Let n be a positive integer, and write $n = p^e m$ where $e, m \in \mathbb{Z}_{\geq 0}$ and $\gcd(p,m) = 1$. Then $\overline{\Phi_n}(X) = \overline{\Phi_m}(X)^{\varphi(p^e)}$ in $\mathbb{F}_p[X]$.*

Proof. For each $j \in \mathbb{Z}$ with $0 \leq j \leq e$, the polynomial $\Phi_m(X^{p^e})$ vanishes at $X = \zeta_{p^j m}$ because the power $\zeta_{p^j m}^{p^e} = \zeta_m^{p^{e-j}}$ is a primitive m-th root of unity. This means that $\Phi_m(X^{p^e})$ is divisible by $\Phi_m(X)\Phi_{pm}(X)\cdots\Phi_{p^e m}(X)$ since $\Phi_{p^j m}(X)$ is the minimal polynomial of $\zeta_{p^j m}$. On the other hand, we have

$$\begin{aligned}
\deg(\Phi_m(X)\Phi_{pm}(X)\cdots\Phi_{p^e m}(X)) &= \varphi(m) + \sum_{j=1}^{e}\varphi(p^j m) = \varphi(m) + \sum_{j=1}^{e}\varphi(p^j)\varphi(m) \\
&= \varphi(m) + \sum_{j=1}^{e}\left(p^{j-1}(p-1)\varphi(m)\right) = \varphi(m) + (p-1)\varphi(m)\sum_{j=1}^{e}p^{j-1} \\
&= \varphi(m) + \varphi(m)(p^e - 1) = \varphi(m)p^e = \deg(\Phi_m(X^{p^e})).
\end{aligned}$$

Thus $\Phi_m(X)\Phi_{pm}(X)\cdots\Phi_{p^e m}(X) = \Phi_m(X^{p^e})$, and

$$\overline{\Phi_m}(X)\overline{\Phi_{pm}}(X)\cdots\overline{\Phi_{p^e m}}(X) = \overline{\Phi_m}(X^{p^e}) = \overline{\Phi_m}(X)^{p^e} \quad (\text{in } \mathbb{F}_p[X]).$$

By induction on e, we obtain $\overline{\Phi_n}(X) = \overline{\Phi_{p^e m}}(X) = \overline{\Phi_m}(X)^{\varphi(p^e)}$ as required. □

We then consider the factorization of $\overline{\Phi_m}(X)$ for a positive integer m with $\gcd(p,m) = 1$. It is clear that $\overline{\Phi_1}(X) = X - 1$ and $\overline{\Phi_2}(X) = X + 1$. Let $m \geq 3$ be a positive integer with $\gcd(p,m) = 1$. We write $\overline{\mathbb{F}_p}$ for the algebraic closure of $\mathbb{F}_p$, and $\mathbb{F}_q$ for the unique subfield of $\overline{\mathbb{F}_p}$ whose cardinality equals q, that is, $\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q = \alpha\}$, where q is a power of p.

Proposition 10.7. *Let $\bar{f} \in \mathbb{F}_p[X]$ be any irreducible factor of $\overline{\Phi_m}$, and let d denote the order of p in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$.*

(i) *Let $\bar{\zeta} \in \overline{\mathbb{F}_p}$ be any root of $\bar{f}$. Then the order of $\bar{\zeta}$ in $\overline{\mathbb{F}_p}^\times$ equals m.*

(ii) $\deg(\bar{f}) = d$.

(iii) *$\bar{f}$ is $+1$-symmetric if and only if there exists a non-negative integer r such that $p^r \equiv -1 \bmod m$.*

In particular, all irreducible factors of $\overline{\Phi_m}$ have degree d and are all $+1$-symmetric or all not.

Proof. (i). Let m' denote the order of $\bar{\zeta}$ in $\overline{\mathbb{F}_p}^\times$. Since $\bar{f}(X) \mid \overline{\Phi_m}(X) \mid (X^m - 1)$, we have $\bar{\zeta}^m = 1$, which shows that $m' \mid m$. Note that $X^m - 1 \in \mathbb{F}_p[X]$ is separable since it is coprime to its derivative mX^{m-1} in $\mathbb{F}_p[X]$ by the assumption $\gcd(p, m) = 1$. If m' were less than m then the polynomial

$$X^m - 1 = \prod_{r|m} \overline{\Phi_r}(X) = (X^{m'} - 1) \prod_{r|m, r\nmid m'} \overline{\Phi_r}(X)$$

would have $\bar{\zeta}$ as a multiple root since $\bar{\zeta}^{m'} - 1 = 0$ and $\overline{\Phi_m}(\bar{\zeta}) = 0$, but it contradicts separability. Therefore $m' = m$.

(ii). Let $\bar{\zeta} \in \overline{\mathbb{F}_p}$ be a root of $\bar{f}$. Since $p^d \equiv 1 \bmod m$ and $\bar{\zeta}^m = 1$, it follows that $\bar{\zeta}^{p^d} = \bar{\zeta}$. This shows that $\bar{\zeta} \in \mathbb{F}_{p^d}$, and $\mathbb{F}_p(\bar{\zeta}) \subset \mathbb{F}_{p^d}$. Thus

$$\deg(\bar{f}) = [\mathbb{F}_p(\bar{\zeta}) : \mathbb{F}_p] \leq [\mathbb{F}_{p^d} : \mathbb{F}_p] = d.$$

On the other hand, we have $\bar{\zeta}^{p^{\deg(\bar{f})}-1} = 1$ since the extension $\mathbb{F}_p(\bar{\zeta})/\mathbb{F}_p$ is of degree $\deg(\bar{f})$. Hence $p^{\deg(\bar{f})} - 1 \equiv 0 \bmod m$ by (i), and $p^{\deg(\bar{f})} \equiv 1 \bmod m$. Therefore $d \mid \deg(\bar{f})$, which shows that $d = \deg(\bar{f})$.

(iii). Suppose that $\bar{f}$ is $+1$-symmetric. Then $\bar{f}(\bar{\zeta}^{-1}) = \bar{f}^*(\bar{\zeta}^{-1}) = 0$ for a root $\bar{\zeta}$ of $\bar{f}$. In other words, $\bar{\zeta}^{-1}$ and $\bar{\zeta}$ are conjugate. Thus, there exists $r \in \mathbb{Z}_{\geq 0}$ such that $\bar{\zeta}^{p^r} = \bar{\zeta}^{-1}$, or equivalently $\bar{\zeta}^{p^r+1} = 1$. This implies that $p^r + 1 \equiv 0 \bmod m$ by (i), and $p^r \equiv -1 \bmod m$.

Conversely, suppose that there exists $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$. Then, for any root $\bar{\zeta}$ of $\bar{f}$, its inverse $\bar{\zeta}^{-1} = \bar{\zeta}^{p^r}$ is conjugate to $\bar{\zeta}$. Note that every root of $\bar{f}$ has multiplicity 1 since $\bar{f}$ is separable. Thus $\bar{f}$ is $*$-symmetric by Proposition 7.9. Furthermore, any root of $\bar{\zeta}$ is not 1 since its order in $\overline{\mathbb{F}_p}^\times$ is $m \geq 3$. Hence $X - 1$ is not a factor of $\bar{f}$, and $\bar{f}$ is $+1$-symmetric. □

The n-th cyclotomic polynomial decomposes in $\mathbb{F}_p[X]$ as follows.

Theorem 10.8. *Let n be a positive integer, and write $n = p^e m$ where $e, m \in \mathbb{Z}_{\geq 0}$ and $\gcd(p, m) = 1$.*

(i) $\overline{\Phi_n}(X) = \overline{\Phi_m}(X)^{\varphi(p^e)}$ *in* $\mathbb{F}_p[X]$.

(ii) *Suppose that $m \geq 3$, and let d denote the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then $\overline{\Phi_m}$ has exactly $\varphi(m)/d$ irreducible factors of degree d in $\mathbb{F}_p[X]$. Moreover, the irreducible factors are all $+1$ symmetric or all not, and the former case occurs if and only if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$.*

Proof. (i) is nothing but Proposition 10.6, and (ii) follows from Proposition 10.7. □

10.3 Computation of $\Pi(\Phi_n, \Phi_{n'})$

This subsection gives an explicit description of the set $\Pi(\Phi_n, \Phi_{n'})$. The goal is the following theorem.

Theorem 10.9. *Let n and n' be positive integers with $n > n'$.*

(i) *If n/n' is not a power of a prime, then $\Pi(\Phi_n, \Phi_{n'}) = \emptyset$.*

(ii) *Suppose that n/n' is a power of a prime p, and write $n = p^e m$ where $\gcd(p, m) = 1$. Then*

$$\Pi(\Phi_n, \Phi_{n'}) = \begin{cases} \{p\} & \text{if there exists } r \in \mathbb{Z}_{\geq 0} \text{ such that } p^r \equiv -1 \bmod m \\ \emptyset & \text{otherwise.} \end{cases}$$

Definition 10.10. Let n be a positive integer. The field $\mathbb{Q}(\zeta_n)$ is called the *n-th cyclotomic field*, and denoted by E_n, where $\zeta_n = \exp(2\pi\sqrt{-1}/n)$. If $n \geq 3$ then we write $\sigma : E_n \to E_n$ for the nontrivial involution σ on E_n determined by $\sigma(\zeta_n) = \zeta_n^{-1}$, and $(E_n)^\sigma$ for the fixed subfield $\{x \in E_n \mid \sigma(x) = x\}$. Note that $(E_n)^\sigma = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

The following general proposition is useful to observing ramifications of finite places.

Proposition 10.11. *Let A be a Dedekind domain, and K its field of fractions. Let L/K be a finite separable extension, and B the integral closure of A in L. Suppose that $L = K(\theta)$ for some $\theta \in B$, and let $\mathfrak{f}$ be the conductor of $A[\theta]$, that is, the biggest ideal of B which is contained in $A[\theta]$. Let $\mathfrak{p}$ be a nonzero prime ideal of A such that $\mathfrak{f}$ and $\mathfrak{p}B$ are coprime. Suppose that the minimal polynomial $F(X) \in A[X]$ of θ decomposes over the residue field $A/\mathfrak{p}$ as*

$$(F(X) \bmod \mathfrak{p}) = \overline{f_1}(X)^{e_1} \cdots \overline{f_l}(X)^{e_l}$$

where each e_j is a positive integer, and $\overline{f_1}, \ldots, \overline{f_l} \in (A/\mathfrak{p})[X]$ are distinct irreducible polynomials. Then the ideal $\mathfrak{p}$ decomposes in B as

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_l^{e_l}$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ are distinct prime ideals of B, and the inertia degree of $\mathfrak{P}_j$ equals $\deg(\overline{f_j})$ for each j.

Proof. See [32, Chapter I, Proposition 8.3]. □

Lemma 10.12. *Let $n \geq 3$ be a positive integer.*

(i) *A $\mathbb{Z}$-basis of the integer ring $\mathcal{O}_{E_n}$ of E_n is given by $1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$. Hence $\mathcal{O}_{E_n} = \mathbb{Z}[\zeta_n]$.*

(ii) *The integer ring $\mathcal{O}_{(E_n)^\sigma}$ of $(E_n)^\sigma$ is $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Proof. See e.g. [32, Chapter I, Proposition 10.2] for (i). We show the assertion (ii). The inclusion $\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subset \mathcal{O}_{(E_n)^\sigma}$ is obvious. Let $\alpha \in \mathcal{O}_{(E_n)^\sigma}$, and write

$$\alpha = b_{r-1} + b_{r-2}(\zeta_n + \zeta_n^{-1}) + \cdots + b_0(\zeta_n + \zeta_n^{-1})^{r-1},$$

where $r := \varphi(n)/2$, and $b_0, \ldots, b_{r-1} \in \mathbb{Q}$ are rational numbers. We show that $b_0, \ldots, b_{r-1}$ belong to $\mathbb{Z}$. Put $h(Y) = \sum_{j=0}^{r-1} b_{r-1-j} Y^j$ and $f(X) = X^{r-1} h(X + X^{-1})$. Then f can be written as

$$f(X) = a_0 + a_1 X + \cdots + a_{r-2} X^{r-2} + a_{r-1} X^{r-1} + a_{r-2} X^r + \cdots + a_1 X^{2r-3} + a_0 X^{2r-2},$$

where $a_0, \ldots, a_{r-1} \in \mathbb{Q}$ are rational numbers (determined by $b_0, \ldots, b_{r-1} \in \mathbb{Q}$). The coefficients $a_0, \ldots, a_{r-1}$ belong to $\mathbb{Z}$ by the assertion (i), since the value $f(\zeta_n) = \zeta_n^{r-1} h(\zeta_n + \zeta_n^{-1}) = \zeta_n^{r-1} \alpha$ is in $\mathcal{O}_{E_n}$. Hence $b_0, \ldots, b_{r-1}$ also belong to $\mathbb{Z}$ by Proposition 7.10. This means that $\alpha \in \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, and $\mathcal{O}_{(E_n)^\sigma} \subset \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. The proof is complete. □

Let $n \geq 3$ be a positive integer. We write Ψ_n for the minimal polynomial of $\zeta_n + \zeta_n^{-1}$. This is noting but the trace polynomial of Φ_n. By Proposition 10.11 and Lemma 10.12, a prime decomposes into prime ideals over E_n and $(E_n)^\sigma$ in the same way as the reductions of Φ_n and Ψ_n modulo the prime. So, we can know decompositions of prime ideals of $(E_n)^\sigma$ over E_n via decompositions of the reductions of Φ_n and Ψ_n.

Proposition 10.13. *Let $n \geq 3$ be an integer, and p a prime. Then $\mathcal{W}(\Phi_n; p) = \mathcal{W}_{\mathrm{rm}}(\Phi_n; p)$ if $n = p^e$ or $2p^e$ for some integer $e \geq 0$. Suppose that $n = p^e m$ where $e \geq 0$, $m \geq 3$, and $\gcd(p, m) = 1$. Then*

$$\mathcal{W}(\Phi_n; p) = \begin{cases} \mathcal{W}_{\mathrm{ur}}(\Phi_n; p) & \text{if there exists } r \in \mathbb{Z}_{\geq 0} \text{ such that } p^r \equiv -1 \bmod m \\ \mathcal{W}_{\mathrm{sp}}(\Phi_n; p) & \text{otherwise.} \end{cases}$$

Proof. We write $\bar{f}$ for the reduction modulo p for $f \in \mathbb{Z}[X]$. Suppose that $n = p^e$ or $2p^e$ for some integer $e \geq 0$. Then $\overline{\Phi_n}(X) = (X-1)^{\varphi(n)}$ or $(X+1)^{\varphi(n)}$ by Theorem 10.8 (i), and $\overline{\Psi_n}(Y) = (Y-2)^{\varphi(n)/2}$ or $(Y+2)^{\varphi(n)/2}$ because $\overline{\Psi_n}$ is the trace polynomial of $\overline{\Phi_n}$. Thus, it can be seen from Proposition 10.11 that there exists one and only one prime ideal of $(E_n)^\sigma$ above p which is ramified in E_n. In particular $\mathcal{W}(\Phi_n; p) = \mathcal{W}_{\mathrm{rm}}(\Phi_n; p)$.

Suppose that $n = p^e m$ where $e \geq 0$, $m \geq 3$, and $\gcd(p, m) = 1$. Then Theorem 10.8 (ii) shows that $\overline{\Phi_n}$ is factorized in $\mathbb{F}_p[X]$ as $\overline{\Phi_n} = \overline{f_1} \cdots \overline{f_l}$, where if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$ then $\overline{f_1}, \ldots, \overline{f_l} \in \mathbb{F}_p[X]$ are distinct $+1$-symmetric irreducible polynomials of degree d, and otherwise they are distinct polynomials of degree $2d$ which can be written as $\overline{f_j} = \overline{g_j}\ \overline{g_j}^*$ for some irreducible polynomial $\overline{g_j} \in \mathbb{F}_p[X]$ with $\overline{g_j}^* \neq \overline{g_j}^*$. Let $\overline{h_j}$ be the trace polynomial of $\overline{f_j}$. Then $\overline{h_1}, \ldots, \overline{h_l}$ are irreducible and $\overline{\Psi_n} = \overline{h_1} \cdots \overline{h_l}$. Thus Proposition 10.11 implies that there are l prime ideals of $(E_n)^\sigma$ above p. Moreover, they are all non-split and unramified in E_n if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$, and otherwise they are all split in E_n. This completes the proof. □

We use the following formula in proving Theorem 10.9.

Proposition 10.14 (Apostol)**.** *Let $n \in \mathbb{Z}_{>0}$ be a positive integer. Then*

$$\mathrm{Res}(\Phi_n, \Phi_1) = \begin{cases} -p & \text{if } n \text{ is a power of a prime } p \\ -1 & \text{otherwise.} \end{cases}$$

Let $n' \in \mathbb{Z}_{>0}$ be a positive integer such that $1 < n' < n$. Then

$$\mathrm{Res}(\Phi_n, \Phi_{n'}) = \begin{cases} p^{\varphi(n')} & \text{if } n/n' \text{ is a power of a prime } p \\ 1 & \text{otherwise.} \end{cases}$$

Proof. See [1]. □

Proof of Theorem 10.9. Let n and n' be positive integers with $n > n'$. If n/n' is not a power of a prime then $|\mathrm{Res}(\Phi_n, \Phi_{n'})| = 1$ by Proposition 10.14 and thus $\Pi(\Phi_n, \Phi_{n'}) = \emptyset$ by Proposition 10.3. This shows the assertion (i). We then show the assertion (ii). Suppose that n/n' is a power of a prime p, and write $n = p^e m$, $n' = p^{e'} m$ where $e > e' > 1$ and $\gcd(p, m) = 1$. Note that $\Pi(\Phi_n, \Phi_{n'}) \subset \{p\}$ by Propositions 10.14 and 10.3.

Suppose that $m = 1$ or 2. Then $\overline{\Phi_n}(X) = (X \mp 1)^{\varphi(p^e)}$, $\overline{\Phi_{n'}}(X) = (X \mp 1)^{\varphi(p^{e'})}$ in $\mathbb{F}_p[X]$ by Theorem 10.8 (i), and $\mathcal{W}(\Phi_n; p) = \mathcal{W}_{\mathrm{rm}}(\Phi_n; p)$, $\mathcal{W}(\Phi_{n'}; p) = \mathcal{W}_{\mathrm{rm}}(\Phi_{n'}; p)$ by Proposition 10.13. Hence $X \mp 1 \in \overline{I(\Phi_n; \mathbb{Q}_p)} \cap \overline{I(\Phi_{n'}; \mathbb{Q}_p)}$ and $p \in \Pi(\Phi_n, \Phi_{n'})$. Therefore $\Pi(\Phi_n, \Phi_{n'}) = \{p\}$.

Suppose that $m \geq 3$. If there is no integer $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$ then $\mathcal{W}(\Phi_n; p) = \mathcal{W}_{\mathrm{sp}}(\Phi_n; p)$ and $\mathcal{W}(\Phi_{n'}; p) = \mathcal{W}_{\mathrm{sp}}(\Phi_{n'}; p)$ by Proposition 10.13. Thus $\overline{I(\Phi_n; \mathbb{Q}_p)} = \overline{I(\Phi_{n'}; \mathbb{Q}_p)} = \emptyset$ and $p \notin \Pi(\Phi_n, \Phi_{n'})$. Therefore $\Pi(\Phi_n, \Phi_{n'}) = \emptyset$. If there exists $r \in \mathbb{Z}_{\geq 0}$ such that $p^r \equiv -1 \bmod m$ then $\overline{\Phi_n}(X) = \overline{\Phi_m}^{\varphi(p^e)}$, $\overline{\Phi_{n'}}(X) = \overline{\Phi_m}^{\varphi(p^{e'})}$ in $\mathbb{F}_p[X]$ and $\overline{\Phi_m}$ has a $+1$-symmetric irreducible factor $\bar{h} \in \mathbb{F}[X]$ by Theorem 10.8. Moreover $\mathcal{W}(\Phi_n; p) = \mathcal{W}_{\mathrm{ur}}(\Phi_n; p)$ and $\mathcal{W}(\Phi_{n'}; p) = \mathcal{W}_{\mathrm{ur}}(\Phi_{n'}; p)$ by Proposition 10.13. Thus there exist $+1$-symmetric factors f and $f' \in \mathbb{Z}_p[X]$ of Φ_n and $\Phi_{n'}$ in $\mathbb{Q}_p[X]$ respectively such that $\bar{h} \mid (f \bmod p)$ and $\bar{h} \mid (f' \bmod p)$. This implies that $\bar{h} \in \overline{I(\Phi_n; \mathbb{Q}_p)} \cap \overline{I(\Phi_{n'}; \mathbb{Q}_p)}$ and $p \in \Pi(\Phi_n, \Phi_{n'})$. Therefore $\Pi(\Phi_n, \Phi_{n'}) = \{p\}$. This completes the proof. □

10.4 Comparison

One practical way to compute an obstruction map is to compare it with another. Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree with the condition (Square). As in Notation 9.3, the symbols M and M_∞ denote the associated $\mathbb{Q}[\Gamma]$-module with transformation α and its localization at the infinite place ∞ respectively. Let r, s be non-negative integers with $r \equiv s \bmod 8$ such that F satisfies the condition $(\mathrm{Sign})_{r,s}$, and $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ an index map. Then, there exists an inner product $b_\mathfrak{i}$ on M_∞ which makes α an isometry with index $\mathfrak{i}$. For any $f \in I := I(F; \mathbb{Q})$, the index of the restriction $b_\mathfrak{i}|_{M_\infty^f}$ is given by $\sum_{g \in I(f;\mathbb{R})} \mathfrak{i}(g)$, and thus its isomorphism class is uniquely determined by $\mathfrak{i}$ independently of the choice of $b_\mathfrak{i}$. So we define the map $\eta_\infty(\mathfrak{i}) : I \to \mathbb{Z}/2\mathbb{Z}$ by

$$\eta_\infty(\mathfrak{i})(f) = \mathrm{hw}_\infty(b_\mathfrak{i}|_{M_\infty^f}) \quad (f \in I).$$

By Theorem 4.60, this map is explicitly as follows:

$$\eta_\infty(\mathfrak{i})(f) = \begin{cases} 0 & \text{if } (\deg(f^{m_f}) - \sum_{g \in I(f;\mathbb{R})} \mathfrak{i}(g))/2 \equiv 0 \text{ or } 1 \bmod 4 \\ 1 & \text{if } (\deg(f^{m_f}) - \sum_{g \in I(f;\mathbb{R})} \mathfrak{i}(g))/2 \equiv 2 \text{ or } 3 \bmod 4 \end{cases} \quad (f \in I). \tag{37}$$

Let r', s' be non-negative integers with $r' \equiv s' \bmod 8$ such that F satisfies the condition $(\mathrm{Sign})_{r',s'}$, and $\mathfrak{j} \in \mathrm{Idx}(r', s'; F)$ an index map. We remark that if

$$\mathfrak{i}(X-1) \equiv \mathfrak{j}(X-1) \quad \text{and} \quad \mathfrak{i}(X-1) \equiv \mathfrak{j}(X-1) \mod 4 \tag{38}$$

then two equivalence relations on I defined by $(F, \mathfrak{i})$ and $(F, \mathfrak{j})$ are the same, because they are determined by the values δ_+ and δ_- defined in Notation 9.4, see also Notation 9.12 and Definition 9.20. In this case, the obstruction group $\Omega_\mathfrak{i}$ for $(F, \mathfrak{i})$ is the same as that for $(F, \mathfrak{j})$.

Theorem 10.15. *Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree with the condition* (Square)*, and r, s, r', s' non-negative integers with $r \equiv s$ and $r' \equiv s' \bmod 8$ such that $(\mathrm{Sign})_{r,s}$ and $(\mathrm{Sign})_{r',s'}$ hold for F. Let $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$ and $\mathfrak{j} \in \mathrm{Idx}(r', s'; F)$ be index maps satisfying* (38)*. Then we have*

$$\mathrm{ob}_\mathfrak{i}(c) = \mathrm{ob}_\mathfrak{j}(c) + (\eta_\infty(\mathfrak{i}) - \eta_\infty(\mathfrak{j})) \cdot c$$

for all $c \in \Omega_\mathfrak{i}$. In particular, if $\mathrm{ob}_\mathfrak{j}$ is zero, then $\mathrm{ob}_\mathfrak{i}$ is zero precisely when the map

$$\Omega_\mathfrak{i} \to \mathbb{Z}/2\mathbb{Z},\ c \mapsto (\eta_\infty(\mathfrak{i}) - \eta_\infty(\mathfrak{j})) \cdot c$$

is zero.

Proof. Let $\beta_\mathfrak{i} = \{b_\mathfrak{i}\} \cup \{b_p\}_{p \in \mathcal{V} \setminus \{\infty\}} \in \mathcal{B}_\mathfrak{i}$. Then the family $\beta_\mathfrak{j} := \{b_\mathfrak{j}\} \cup \{b_p\}_{p \in \mathcal{V} \setminus \{\infty\}}$ belongs to $\mathcal{B}_\mathfrak{j}$, where $b_\mathfrak{j}$ is an inner product on M_∞ which makes α an isometry with index $\mathfrak{j}$. For any $f \in I$ we have

$$\begin{aligned} \eta(\beta_\mathfrak{i})(f) &= \mathrm{hw}_\infty(b_\mathfrak{i}|_{M_\infty^f}) + \sum_{p \in \mathcal{V} \setminus \{\infty\}} \mathrm{hw}_p(b_p|_{M_p^f}) \\ &= \left(\mathrm{hw}_\infty(b_\mathfrak{j}|_{M_\infty^f}) + \sum_{p \in \mathcal{V} \setminus \{\infty\}} \mathrm{hw}_p(b_p|_{M_p^f}) \right) + \mathrm{hw}_\infty(b_\mathfrak{i}|_{M_\infty^f}) - \mathrm{hw}_\infty(b_\mathfrak{j}|_{M_\infty^f}) \\ &= \eta(\beta_\mathfrak{j})(f) + (\eta_\infty(\mathfrak{i}) - \eta_\infty(\mathfrak{j}))(f). \end{aligned}$$

This implies that $\mathrm{ob}_\mathfrak{i}(c) = \mathrm{ob}_\mathfrak{j}(c) + (\eta_\infty(\mathfrak{i}) - \eta_\infty(\mathfrak{j})) \cdot c$ for all $c \in \Omega_\mathfrak{i}$ as required. □

Example 10.16. Let $F(X) = (X-1)^4 f(X)$, where $f(X) = \Phi_{12}(X) = X^4 - X^2 + 1$ as in Example 10.4. Note that the obstruction group Ω for $(F, \mathfrak{i})$ does not depend on the index map $\mathfrak{i}$, and is given by $\Omega = C(I)$ since $\Pi(f, X-1) = \emptyset$ as shown in Example 10.4, where $I = I(F; \mathbb{Q})$. Let Λ be the lattice E_8. Then there is no isometry of Λ with characteristic polynomial F (any isometry of Λ is semisimple because Λ has definite signature). To prove this, we first show that $\Lambda_{4,4}$ admits a semisimple isometry with characteristic F, where $\Lambda_{n,n}$ is the unique even unimodular lattice of signature (n, n) for $n \in \mathbb{Z}_{>0}$. It follows from Theorem 9.27 that $\Lambda_{2,2}$ admits a semisimple isometry t_f with characteristic polynomial f because f satisfies the conditions $(\mathrm{Sign})_{2,2}$ and (Square), and is irreducible. Thus the direct sum $t' := t_f \oplus \mathrm{id}_{\Lambda_{2,2}}$ is a semisimple isometry of $\Lambda_{4,4} = \Lambda_{2,2} \oplus \Lambda_{2,2}$ with characteristic polynomial F. Hence $\mathrm{ob}_{\mathfrak{j}} = 0$, where $\mathfrak{j} \in \mathrm{Idx}(4, 4; F)$ denotes the index of t'.

We now suppose to contrary that the E_8-lattice Λ admitted an isometry t with characteristic polynomial F. Then the index $\mathfrak{i} \in \mathrm{Idx}(8, 0; F)$ of t is uniquely determined: $\mathfrak{i}(g) = \deg(g)^{m_g}$ for every $g \in I(F; \mathbb{R})$ where m_g is the multiplicity of g in F. Thus we would get

$$(\eta_\infty(\mathfrak{i}) - \eta_\infty(\mathfrak{j})) \cdot \mathbf{1}_{\{X-1\}} = \eta_\infty(\mathfrak{i})(X-1) - \eta_\infty(\mathfrak{j})(X-1) = 0 - 1 = 1 \quad (\text{in } \mathbb{Z}/2\mathbb{Z}),$$

but this contradicts Theorem 10.15. Therefore, there is no isometry of Λ with characteristic polynomial F.

11 Isometries on even unimodular lattices of index 0

Let n be a positive integer. We write $\Lambda_{n,n}$ for an even unimodular lattice over $\mathbb{Z}$ of signature (n, n). Such a lattice is unique up to isomorphism, see Theorem 5.25. We show that any $*$-symmetric polynomial $F \in \mathbb{Z}[X]$ of degree $2n$ with the condition (Square) can be realized as the characteristic polynomial of an isometry of $\Lambda_{n,n}$ unless the multiplicity of $X-1$ or that of $X+1$ is one. In fact, a more stronger version will be proved as Theorem 11.9. Furthermore, it will be shown that the assumption on the multiplicities of $X-1$ and $X+1$ can be removed when F is a product of cyclotomic polynomials.

11.1 General case

Let $F \in \mathbb{R}[X]$ be a $*$-symmetric polynomial. As in §7.4, we write m_f for the multiplicity of a polynomial f in F and $m_\pm := m_{X \mp 1}$. Furthermore F_{12} is the product of type 1 and 2 components of F, and $m(F)$ is the number of roots of F whose absolute values are greater than 1 counted with multiplicity.

Let $P \in \mathbb{R}[X]$ be a $*$-symmetric polynomial with $P(1)P(-1) \neq 0$. Then P is $+1$-symmetric and of even degree. The signature of $(-1)^{\deg(P)/2} P(1)P(-1)$ is denoted by $e(P) \in \{1, -1\}$. If H is the trace polynomial of P then $(-1)^{\deg(P)/2} P(1)P(-1) = H(2)H(-2)$, and thus $e(P)$ is the signature of $H(2)H(-2)$. Note that if the coefficients of P are in $\mathbb{Z}$ and P satisfies the condition (Square) then $e(P) = 1$ since $(-1)^{\deg(P)/2} P(1)P(-1)$ is a square. Let $\mathbb{T}$ denote the unit circle in $\mathbb{C}$.

Lemma 11.1. *The number of roots of a $*$-symmetric polynomial $F \in \mathbb{R}[X]$ on $\mathbb{T} \setminus \{1, -1\}$ counted with multiplicity is equal to $2\sum_{f \in I_1(F;\mathbb{R})} m_f$. Moreover, we have $2\sum_{f \in I_1(F;\mathbb{R})} m_f \equiv 1 - e(F_{12}) \bmod 4$.*

Proof. Let N be the number of roots of F on $\mathbb{T} \setminus \{1, -1\}$ counted with multiplicity. The former assertion, $N = 2\sum_{f \in I_1(F;\mathbb{R})} m_f$, follows from Proposition 7.21 (i). Let H denote the trace polynomial of F_{12}, and N' the number of roots of H on the interval $(-2, 2)$. Then $N = 2N'$ because $\mathbb{T} \setminus \{1, -1\}$ is mapped two-to-one onto $(-2, 2)$ under the function $\mathbb{C} \to \mathbb{C}$, $x \mapsto x +$

x^{-1}. On the other hand, by considering the graph of H, it can be seen that N' is even if $H(2)H(-2) > 0$ and odd if $H(2)H(-2) < 0$. Since $e(F_{12})$ is the signature of $H(2)H(-2)$, we have $N' \equiv (1 - e(F_{12}))/2 \bmod 2$. Hence

$$N = 2N' \equiv 1 - e(F_{12}) \mod 4.$$

The proof is complete. □

Proposition 11.2. *Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree $2n$ with the condition* (Square).

(i) *Let $r, s \in \mathbb{Z}_{\geq 0}$ be non-negative integers with $r \equiv s \bmod 8$ and $r + s = 2n$ such that F satisfies the condition* $(\mathrm{Sign})_{r,s}$. *Then we have $\mathfrak{i}(X-1) + \mathfrak{i}(X+1) \equiv 1 - e(F_{12}) \mod 4$ for any $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$.*

(ii) *F satisfies the condition* $(\mathrm{Sign})_{n,n}$. *Moreover, for $i_+, i_- \in \mathbb{Z}$ with*

$$\begin{aligned} &-m_+ \leq i_+ \leq m_+,\ -m_- \leq i_- \leq m_-,\ i_+ \equiv i_- \equiv m_+ \bmod 2, \quad \textit{and} \\ &i_+ + i_- \equiv 1 - e(F_{12}) \bmod 4, \end{aligned} \tag{39}$$

there exists $\mathfrak{i} \in \mathrm{Idx}(n, n; F)$ such that $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_- \bmod 4$.

Proof. (i). Let $\mathfrak{i} \in \mathrm{Idx}(r, s; F)$. We have

$$\mathfrak{i}(X-1) + \mathfrak{i}(X+1) + \textstyle\sum_{f \in I_1(F;\mathbb{R})} \mathfrak{i}(f) = r - s \equiv 0 \mod 4$$

by (29). On the other hand, each $f \in I_1(F; \mathbb{R})$ satisfies $2m_f - \mathfrak{i}(f) \equiv 0 \bmod 4$ by (28). Thus

$$\begin{aligned} \mathfrak{i}(X-1) + \mathfrak{i}(X+1) &\equiv -\textstyle\sum_{f \in I_1(F;\mathbb{R})} \mathfrak{i}(f) \equiv -\sum_{f \in I_1(F;\mathbb{R})} 2m_f \\ &\equiv 2\textstyle\sum_{f \in I_1(F;\mathbb{R})} m_f \equiv 1 - e(F_{12}) \mod 4, \end{aligned}$$

where the last congruence is by Lemma 11.1.

(ii). By Corollary 7.29, it suffices to prove the latter assertion. Let $i_+, i_- \in \mathbb{Z}$ be integers satisfying (39), and take $i'_+ \in \{-1, 0, 1, 2\}$ and $i'_- \in \{-2, -1, 0, 1\}$ so that $i'_+ \equiv i_+$ and $i'_- \equiv i_-$ mod 4. Then $-3 \leq i'_+ + i'_- \leq 3$. Moreover, since $i'_+ + i'_- \equiv i_+ + i_- \equiv 1 - e(F_{12}) \bmod 4$ we have

$$i'_+ + i'_- = 1 - e(F_{12}) \text{ or } e(F_{12}) - 1. \tag{$*$}$$

We now put

$$\begin{aligned} r_0 &= (m_+ + i'_+)/2 + (m_- + i'_-)/2, \quad & s_0 &= (m_+ - i'_+)/2 + (m_- - i'_-)/2, \\ r_{12} &= n - r_0, & s_{12} &= n - s_0. \end{aligned}$$

Then the map $\mathfrak{i}_0 : \{X-1, X+1\} \to \mathbb{Z}$ defined by $\mathfrak{i}_0(X-1) = i'_+$ and $\mathfrak{i}_0(X+1) = i'_-$ belongs to $\mathrm{Idx}(r_0, s_0; F_0)$, where F_0 is the type 0 component of F (to be precise, $\mathfrak{i}_0|_{I_0(F_0;\mathbb{R})} \in \mathrm{Idx}(r_0, s_0; F_0)$).

We show that F_{12} satisfies the condition $(\mathrm{Sign})_{r_{12},s_{12}}$. Note that $m(F) = (2n - m_+ - m_- - 2\sum_{f \in I_1(F;\mathbb{R})} m_f)/2$. Then

$$r_{12} - m(F_{12}) = (n - r_0) - m(F) = \sum_{f \in I_1(F;\mathbb{R})} m_f - (i'_+ + i'_-)/2. \tag{$**$}$$

Here $\sum_{f \in I_1(F;\mathbb{R})} m_f \geq (1 - e(F_{12}))/2$ since $\sum_{f \in I_1(F;\mathbb{R})} m_f \geq 0$ and $\sum_{f \in I_1(F;\mathbb{R})} m_f \equiv (1 - e(F_{12}))/2 \bmod 2$ by Lemma 11.1. Hence, it follows from Equations $(*)$ and $(**)$ that

$$\begin{aligned} &r_{12} - m(F_{12}) \geq (1 - e(F_{12}))/2 - (1 - e(F_{12}))/2 = 0, \\ &r_{12} - m(F_{12}) \equiv (1 - e(F_{12}))/2 - (1 - e(F_{12}))/2 \equiv 0 \mod 2. \end{aligned}$$

Similarly, we get $s_{12} - m(F_{12}) \geq 0$ and $s_{12} - m(F_{12}) \equiv 0 \bmod 2$, and therefore F_{12} satisfies the condition $(\mathrm{Sign})_{r_{12},s_{12}}$.

Let $\mathfrak{i}_1 \in \mathrm{Idx}(r_{12}, s_{12}; F_{12})$ be an index map. Then the sum $\mathfrak{i} := \mathfrak{i}_0 \oplus \mathfrak{i}_1 : I(F;\mathbb{R}) \to \mathbb{Z}$ belongs to $\mathrm{Idx}(n,n;F)$. This is the desired index map since $\mathfrak{i}(X \mp 1) = i'_{\pm} \equiv i_{\pm} \bmod 4$. The proof is complete. □

We reformulate Notation 9.12 and Definition 9.20.

Definition 11.3. Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree, and $m_{\pm}$ the multiplicity of $X \mp 1$ in F. Let $i_+, i_- \in \mathbb{Z}$ be integers with $i_{\pm} \equiv m_{\pm} \bmod 2$. We define

$$\delta_{\pm}(F; i_+, i_-) := \begin{cases} (-1)^{(m_{\pm}-i_{\pm})/2} \, |F_{12}(\pm 1)| & \text{if } m_+ \text{ is even} \\ (-1)^{(m_{\pm}-i_{\pm})/2} \, 2|F_{12}(\pm 1)| & \text{if } m_+ \text{ is odd.} \end{cases}$$

Moreover

$$\overline{I(X \mp 1; \mathbb{Q}_p)}' := \begin{cases} \{X \mp 1\} & \text{if } m_{\pm} \geq 3; \text{ or } m_{\pm} = 2 \text{ and } \delta_{\pm}(F; i_+, i_-) \neq -1 \in \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2} \\ \emptyset & \text{otherwise} \end{cases}$$

and $\overline{I(f;\mathbb{Q}_p)}' := \overline{I(f;\mathbb{Q}_p)}$ for a monic polynomial with $f(1)f(-1) \neq 0$ as in Notation 9.12. We then define a set $\Pi^F_{i_+,i_-}(f,g)$ of primes for monic polynomials $f, g \in \mathbb{Z}[X]$ by

$$\Pi^F_{i_+,i_-}(f,g) := \{p : \text{prime} \mid \overline{I(f;\mathbb{Q}_p)}' \cap \overline{I(g;\mathbb{Q}_p)}' \neq \emptyset\}.$$

The *equivalence relation defined by* $(F; i_+, i_-)$ is the one on $I(F;\mathbb{Q})$ generated by the binary relation $\{(f,g) \in I(F;\mathbb{Q}) \times I(F;\mathbb{Q}) \mid \Pi^F_{i_+,i_-}(f,g) \neq \emptyset\}$. Note that $\Pi^F_{i_+,i_-}(f,g) = \Pi^F_{\mathfrak{i}}(f,g)$ if $\mathfrak{i}$ is an index map with $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_- \bmod 4$.

In the following, $F \in \mathbb{Z}[X]$ is a $*$-symmetric polynomial of even degree $2n$ with the condition (Square), and i_+, i_- are integers satisfying (39). Note that $m_+ + m_- = \deg(F_0)$ is even since so are $\deg(F)$ and $\deg(F_{12})$. Note also that the condition (Square) holds for the factor $(X-1)^{m_+}(X+1)^{m_-}F_1(X)$ by Lemma 9.2. For a subset J in $I := I(F;\mathbb{Q})$, we define $F_J := \prod_{f \in J} f^{m_f}$, where m_f is the multiplicity of f in F. If J is empty then F_J is defined to be the constant 1. The subset $J \setminus \{X-1, X+1\}$ of J is denoted by J°.

Lemma 11.4. *Suppose that $m_+ \neq 1$ and $m_- \neq 1$. Let J be an equivalence class in I with respect to the equivalence relation defined by $(F; i_+, i_-)$. If $|F_{J^{\circ}}(\pm 1)|$ is not a square then $X \mp 1 \in J$ i.e., $F_J(\pm 1) = 0$.*

Proof. Suppose that $|F_{J^{\circ}}(\pm 1)|$ is not a square, and let p be a prime such that $v_p(F_{J^{\circ}}(\pm 1))$ is odd. We remark that there is no $g \in I_1 \setminus J$ such that $v_p(g(\pm 1))$ is odd; because otherwise Proposition 10.5 implies that $p \in \Pi^F_{i_+,i_-}(F_{J^{\circ}}, g)$, and we would have $g \in J$. Hence

$$v_p(F_{12}(\pm 1)) \equiv v_p(F_1(\pm 1)) \equiv v_p(F_{J^{\circ}}(\pm 1)) \equiv 1 \mod 2.$$

This implies that $|F(\pm 1)| = 0$ since $|F(\pm 1)|$ is a square, and thus $m_{\pm} \geq 2$ by the assumption $m_{\pm} \neq 1$. Moreover, if $m_{\pm} = 2$ then $\delta_{\pm}(F; i_+, i_-) \neq -1$ in $\mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$ since $v_p(\delta_{\pm}(F; i_+, i_-)) \equiv v_p(F_{12}(\pm 1)) \equiv 1 \bmod 2$. Therefore $\overline{I(X \mp 1; \mathbb{Q}_p)}' = \{X \mp 1\}$, which leads to $p \in \Pi^F_{i_+,i_-}(F_{J^{\circ}}, X \mp 1)$, and $X \mp 1 \in J$. This means that $F_J(\pm 1) = 0$, and the proof is complete. □

Proposition 11.5. *Suppose that $m_+ \neq 1$ and $m_- \neq 1$. For any equivalence class J in I with respect to the equivalence relation defined by $(F; i_+, i_-)$, the corresponding factor F_J has even degree and satisfies the condition* (Square).

Proof. We begin with the case $F(1)F(-1) \neq 0$, i.e., $m_+ = m_- = 0$. Let J be an equivalence class in I. The degree of F_J is even since F_J has no type 0 component. We first show that $|F_J(1)|$ and $|F_J(-1)|$ are squares simultaneously. Suppose that $|F_J(\pm 1)|$ were not a square, and let p be prime such that $v_p(F_J(\pm 1))$ is odd. Note that $v_p(F_1(\pm 1))$ is even since the condition (Square) holds for F_1. Then there exists $g \in I \setminus J$ such that $v_p(g(\pm 1))$ is odd. In this case, we have $X \mp 1 \in \overline{I(F_J;\mathbb{Q}_p)} = \overline{I(F_J;\mathbb{Q}_p)}'$ and $X \mp 1 \in \overline{I(g;\mathbb{Q}_p)} = \overline{I(g;\mathbb{Q}_p)}'$ by Proposition 10.5. Thus $p \in \Pi^F_{i_+,i_-}(F_J, g)$, and g would be contained in the equivalence class J, but this is a contradiction. Hence $|F_J(1)|$ and $|F_J(-1)|$ are squares.

We then show that $(-1)^{n_J}F_J(1)F_J(-1)$ is a square, where $n_J := \deg(F_J)/2$. Suppose that $(-1)^{n_J}F_J(1)F_J(-1)$ were not a square. Since $|F_J(1)|$ and $|F_J(-1)|$ are squares as proved now, we have $(-1)^{n_J}F_J(1)F_J(-1) = -1$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and hence in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. Thus there exists $g \in I \setminus J$ such that $(-1)^{\deg(g)/2}g(1)g(-1) \neq 1$ nor -3 in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ because $(-1)^{\deg(F_1)/2}F_1(1)F_1(-1) = 1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. In this case, we have $X-1 \in \overline{I(F_J;\mathbb{Q}_2)} = \overline{I(F_J;\mathbb{Q}_2)}'$ and $X-1 \in \overline{I(g;\mathbb{Q}_2)} = \overline{I(g;\mathbb{Q}_2)}'$ by Proposition 10.5. Thus $2 \in \Pi^F_{i_+,i_-}(F_J, g)$, and g would be contained in the equivalence class J, but this is a contradiction. Hence $(-1)^{n_J}F_J(1)F_J(-1)$ is a square. This completes the case $F(1)F(-1) \neq 0$.

We proceed to the case $F(1)F(-1) = 0$. Let $J \subset I$ be an equivalence class. Note that F_{J° has even degree. If m_+ and m_- are even then it is obvious that $\deg(F_J)$ is even. If m_+ and m_- are odd then $m_+, m_- \geq 3$ by the assumption $m_+, m_- \neq 1$. This implies that $J = J^\circ$ or $\{X-1, X+1\} \subset J$, and $\deg(F_J)$ is even. We now show that F_J satisfies the condition (Square). If F_{J° satisfies (Square) then so does F_J. Hence, it is enough to consider the case where F_{J° does not satisfy (Square). Lemma 11.4 implies that if $|F_{J^\circ}(1)|$ or $|F_{J^\circ}(-1)|$ is not a square then F_J satisfies (Square). Suppose then that $|F_{J^\circ}(1)|$ and $|F_{J^\circ}(-1)|$ are squares but $(-1)^{\deg(F_{J^\circ})/2}F_{J^\circ}(1)F_{J^\circ}(-1) = -1$ mod squares. If $m_+ \geq 3$ or $m_- \geq 3$ then $\overline{I(X-1;\mathbb{Q}_2)}' = \{X-1\}$ or $\overline{I(X+1;\mathbb{Q}_2)}' = \{X-1\}$, and $2 \in \Pi^F_{i_+,i_-}(F_J, X-1)$ or $2 \in \Pi^F_{i_+,i_-}(F_J, X+1)$ by Proposition 10.5. Thus $X-1 \in J$ or $X+1 \in J$, and $F_J(1)F_J(-1) = 0$. This leads to the condition (Square) for F_J. Suppose that $(m_+, m_-) = (2,2)$, $(2,0)$ or $(0,2)$. Note that there is no $g \in I_1 \setminus J$ such that $(-1)^{\deg(g)/2}g(1)g(-1) \neq 1$ nor -3 since otherwise we would have $g \in J$ by Proposition 10.5. This shows that in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ we have

$$\begin{aligned}
&(-1)^{\deg(F_{12})/2}F_{12}(1)F_{12}(-1)\\
&= (-1)^{\deg(F_{J^\circ})/2}F_{J^\circ}(1)F_{J^\circ}(-1) \times \prod_{g \in I_1 \setminus J} (-1)^{\deg(g)/2}g(1)g(-1) \times (-1)^{\deg(F_2)/2}F_2(1)F_2(-1)\\
&= -\prod_{g \in I_1 \setminus J} (-1)^{\deg(g)/2}g(1)g(-1)\\
&\in \{-1, 3\}.
\end{aligned}$$

Thus

$$\begin{aligned}
\delta_+(F;i_+,i_-)\delta_-(F;i_+,i_-) &= (-1)^{(m_+-i_+)/2}|F_{12}(1)|(-1)^{(m_+-i_+)/2}|F_{12}(-1)|\\
&= (-1)^n F_{12}(1)F_{12}(-1)\\
&= (-1)^{(m_++m_-)/2}(-1)^{\deg(F_{12})/2}F_{12}(1)F_{12}(-1)\\
&= \begin{cases} 1 \text{ or } -3 & \text{if } (m_+,m_-) = (2,0) \text{ or } (0,2)\\ -1 \text{ or } 3 & \text{if } (m_+,m_-) = (2,2) \end{cases}
\end{aligned}$$

in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, where the second equality is obtained by applying Lemma 9.5 after taking $\mathfrak{i}$ as in Proposition 11.2 (ii). Hence, if $(m_+, m_-) = (2,0)$ then $\delta_+(F;i_+,i_-) \neq -1$; if $(m_+, m_-) = (0,2)$ then $\delta_-(F;i_+,i_-) \neq -1$; and if $(m_+, m_-) = (2,2)$ then $\delta_-(F;i_+,i_-) \neq -1$ or $\delta_-(F;i_+,i_-) \neq -1$

in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. These imply that $X-1 \in \overline{I(X-1;\mathbb{Q}_2)}'$ or $X-1 \in \overline{I(X+1;\mathbb{Q}_2)}'$, and $X-1 \in J$ or $X+1 \in J$. Therefore $(-1)^{\deg(F_J)/2}F_J(1)F_J(-1)=0$, which leads to the condition (Square) for F_J. The proof is complete. □

Let $J_\pm$ denote the equivalence class in I (with respect to the equivalence relation defined by $(F;i_+,i_-)$) containing $X \mp 1$. If $m_\pm = 0$ then $J_\pm$ is defined to be the empty set. Note that J_+ and J_- coincide or have no intersection.

Lemma 11.6. *Suppose that $m_+ \neq 1$ and $m_- \neq 1$. Then $\delta_+(F_{J_+};i_+,i_-) = \delta_+(F;i_+,i_-)$ and $\delta_-(F_{J_-};i_+,i_-) = \delta_-(F;i_+,i_-)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. As a result, for any equivalence class J in I with respect to the equivalence relation defined by $(F;i_+,i_-)$, the equivalence relation on $J = I(F_J;\mathbb{Q})$ defined by $(F_J;i_+,i_-)$ is weakest.*

Proof. Suppose first that $J_+ \neq J_-$. Then $F_{12} = F_{J_+^\circ}F_{J_-^\circ} \times \prod_{H \neq J_+,J_-} F_H \times F_2$, where H ranges over all equivalence classes other than J_+ and J_-. Note that $|F_{J_-^\circ}(1)|$ must be a square since otherwise $X-1$ would belong to J_- by Lemma 11.4, but this contradicts $J_+ \neq J_-$. Furthermore $|F_H(1)|$ for $H \neq J_+, J_-$ and $|F_2(1)|$ are also squares by Proposition 11.5 and Lemma 9.2 (ii). Thus, we obtain

$$|F_{12}(1)| = |F_{J_+^\circ}(1)||F_{J_-^\circ}(1)| \times \prod_{H \neq J_+,J_-} |F_H(1)| \times |F_2(1)| = |F_{J_+^\circ}(1)| \quad \text{in } \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

If $J_+ = J_-$ then $F_{12} = F_{J_+^\circ} \times \prod_{H \neq J_+} F_H \times F_2$, and it also follows from Proposition 11.5 and Lemma 9.2 (ii) that $|F_{12}(1)| = |F_{J_+^\circ}(1)|$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Furthermore, the multiplicity of $X-1$ in F_{J_+} is m_+. Hence $\delta_+(F_{J_+};i_+,i_-) = \delta_+(F;i_+,i_-)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Similarly, we have $\delta_-(F_{J_-};i_+,i_-) = \delta_-(F;i_+,i_-)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

For the latter assertion, it suffices to check that $\Pi^{F_J}_{i_+,i_-}(f,g) = \Pi^F_{i_+,i_-}(f,g)$ for any $f,g \in J$. If $f,g \notin \{X-1, X+1\}$ then $\Pi^{F_J}_{i_+,i_-}(f,g)$ and $\Pi^F_{i_+,i_-}(f,g)$ are equal to $\Pi(f,g)$ (defined in Notation 10.2), and they coincide. So it is enough to prove this assertion for J_+ and J_-, but it follows from the equalities $\delta_+(F_{J_+};i_+,i_-) = \delta_+(F;i_+,i_-)$ and $\delta_-(F_{J_-};i_+,i_-) = \delta_-(F;i_+,i_-)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which we proved above. □

The following lemma is a special case of the main theorem 11.9.

Lemma 11.7. *Suppose that $m_+ \neq 1$ and $m_- \neq 1$. Let $i_+, i_- \in \mathbb{Z}$ be integers with (39). If $J_+ \cup J_-$ is one equivalence class in I with respect to the equivalence relation defined by $(F;i_+,i_-)$ then there exists $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ with $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_-$ mod 4 such that $\Lambda_{n,n}$ admits a semisimple $(F,\mathfrak{i})$-isometry.*

Proof. Let H be an equivalence class in I other than J_+ and J_-, and put $n_H = \deg(F_H)/2$. Then F_H satisfies the conditions $(\mathrm{Sign})_{n_H,n_H}$ and (Square) by Proposition 11.2 (ii) and Proposition 11.5. Moreover, the equivalence relation on $H = I(F_H;\mathbb{Q})$ defined by $(F_H;i_+,i_-)$ is weakest by Lemma 11.6. Let $\mathfrak{i}_H \in \mathrm{Idx}(n_H,n_H;F_H)$ be an index map. Theorem 9.27 shows that Λ_{n_H,n_H} has a semisimple $(F_H,\mathfrak{i}_H)$-isometry t_H.

Suppose that $J := J_+ \cup J_-$ is one equivalence class in I. Then $F_1 = F_J \times \prod_{H \neq J} F_H$, where H ranges over all equivalence classes other than J. Note that $e(F_H) = 1$ for each $H \neq J$ and $e(F_2) = 1$ since F_H and F_2 satisfy the condition (Square). Thus

$$e(F_{12}) = e(F_J) \times \prod_{H \neq J} e(F_H) \times e(F_2) = e(F_J). \tag{40}$$

Furthermore, the multiplicities of $X-1$ and $X+1$ in F_J are m_+ and m_- respectively. Hence, there exists $\mathfrak{i}_J \in \mathrm{Idx}(n_J,n_J;F_J)$ with $\mathfrak{i}_J(X-1) \equiv i_+$ and $\mathfrak{i}_J(X+1) \equiv i_-$ mod 4 by Proposition

11.2 (ii), where $n_J := \deg(F_J)/2$. Lemma 11.6 and Theorem 9.27 imply that Λ_{n_J,n_J} has a semisimple $(F_J, \mathfrak{i}_J)$-isometry t_J.

We now define an isometry t on $\Lambda_{n,n} = \Lambda_{n_J,n_J} \oplus \bigoplus_{H\neq J} \Lambda_{n_H,n_H}$ by $t := t_J \oplus \bigoplus_{H\neq J} t_H$, and define $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ to be the index of t. Then $\mathfrak{i}(X-1) \equiv \mathfrak{i}_J(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv \mathfrak{i}_J(X+1) \equiv i_-$ mod 4. This completes the proof. □

The following proposition is an essential part of the proof of the main theorem.

Proposition 11.8. *Let $i_+, i_- \in \mathbb{Z}$ be integers with* (39)*. Suppose that $m_+ = m_- = 2$. Then there exists $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ with $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_-$ mod 4 such that $\Lambda_{n,n}$ admits a semisimple $(F,\mathfrak{i})$-isometry.*

Proof. If $J_- \cup J_+$ is one equivalence class then we are done by Lemma 11.7. So we assume that J_+ and J_- are distinct non-empty equivalence classes. Then $|F_{J_+^\circ}(-1)|$ and $|F_{J_-^\circ}(1)|$ are squares by Lemma 11.4. Thus, we have

$$\begin{aligned}(-1)^{\deg(F_{J_+^\circ})/2} F_{J_+^\circ}(1)F_{J_+^\circ}(-1) &= e(F_{J_+^\circ})|F_{J_+^\circ}(1)||F_{J_+^\circ}(-1)| = e(F_{J_+^\circ})|F_{J_+^\circ}(1)|,\\ (-1)^{\deg(F_{J_-^\circ})/2} F_{J_-^\circ}(1)F_{J_-^\circ}(-1) &= e(F_{J_-^\circ})|F_{J_-^\circ}(1)||F_{J_-^\circ}(-1)| = e(F_{J_-^\circ})|F_{J_-^\circ}(-1)|\end{aligned} \tag{$*$}$$

in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We also have the relation

$$e(F_{12}) = e(F_{J_+^\circ})e(F_{J_-^\circ}) \times \prod_{H\neq J_+,J_-} e(F_H) \times e(F_2) = e(F_{J_+^\circ})e(F_{J_-^\circ})$$

as in Equation (40).

Case I*:* $e(F_{12}) = 1$. We have $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,1)$ or $(-1,-1)$. Furthermore $(i_+,i_-) \equiv (0,0)$ or $(2,2)$ mod 4 by (39).

Case I-(a)*:* $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,1)$ *and* $(i_+,i_-) \equiv (0,0)$ mod 4. By applying Proposition 11.2 (ii) as $F = F_{J_+}$ and $(i_+,i_-) = (0,0)$, we get $\mathfrak{i}_{J_+} \in \mathrm{Idx}(n_{J_+}, n_{J_+}; F_{J_+})$ with $\mathfrak{i}_{J_+}(X-1) = 0$. Similarly, there exists $\mathfrak{i}_{J_-} \in \mathrm{Idx}(n_{J_-}, n_{J_-}; F_{J_-})$ with $\mathfrak{i}_{J_-}(X+1) = 0$. Then we can obtain the desired $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ as in Lemma 11.7.

Case I-(b)*:* $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (-1,-1)$ *and* $(i_+,i_-) \equiv (2,2)$ mod 4. By applying Proposition 11.2 (ii) as $F = F_{J_+}$ and $(i_+,i_-) = (2,0)$, we get $\mathfrak{i}_{J_+} \in \mathrm{Idx}(n_{J_+}, n_{J_+}; F_{J_+})$ with $\mathfrak{i}_{J_+}(X-1) = 2$. Similarly, there exists $\mathfrak{i}_{J_-} \in \mathrm{Idx}(n_{J_-}, n_{J_-}; F_{J_-})$ with $\mathfrak{i}_{J_-}(X+1) = 2$. So we are done as in Case I-(a).

Case I-(c)*:* $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,1)$ *and* $(i_+,i_-) \equiv (2,2)$ mod 4. We show that this case does not occur. Note that in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ we have

$$(-1)^{\deg(F_{J_+^\circ})/2} F_{J_+^\circ}(1)F_{J_+^\circ}(-1) = |F_{J_+^\circ}(1)|, \quad (-1)^{\deg(F_{J_-^\circ})/2} F_{J_-^\circ}(1)F_{J_-^\circ}(-1) = |F_{J_-^\circ}(-1)|$$

by $(*)$ and

$$\delta_+(F; i_+, i_-) = |F_{J_+^\circ}(1)|, \quad \delta_-(F; i_+, i_-) = |F_{J_-^\circ}(-1)|$$

by Lemma 11.6. These equations imply that

$$\begin{aligned} X-1 &\in \overline{I(F_{J_+^\circ}; \mathbb{Q}_2)}' && \text{if } |F_{J_+^\circ}(1)| = -1 \text{ in } \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2},\\ X-1 &\in \overline{I(F_{J_-^\circ}; \mathbb{Q}_2)}' && \text{if } |F_{J_-^\circ}(-1)| = -1 \text{ in } \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2},\\ X-1 &\in \overline{I(X-1; \mathbb{Q}_2)}' && \text{if } |F_{J_+^\circ}(1)| \neq -1 \text{ in } \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2},\\ X-1 &\in \overline{I(X+1; \mathbb{Q}_2)}' && \text{if } |F_{J_-^\circ}(-1)| \neq -1 \text{ in } \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}\end{aligned}$$

by Proposition 10.5 (iii) and the definition of the set $\overline{I(f;\mathbb{Q}_2)}'$. Hence, if $|F_{J_+^\circ}(1)| = -1$ and $|F_{J_-^\circ}(-1)| = -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then $2 \in \Pi^F_{i_+,i_-}(F_{J_+^\circ}, F_{J_-^\circ})$, and we would have $J_+ = J_-$; if $|F_{J_+^\circ}(1)| = -1$ and $|F_{J_-^\circ}(-1)| \neq -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then $2 \in \Pi^F_{i_+,i_-}(F_{J_+^\circ}, X+1)$, and we would have $J_+ = J_-$; if $|F_{J_+^\circ}(1)| \neq -1$ and $|F_{J_-^\circ}(-1)| = -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then $2 \in \Pi^F_{i_+,i_-}(X-1, F_{J_+^\circ})$, and we would have $J_+ = J_-$; if $|F_{J_+^\circ}(1)| \neq -1$ and $|F_{J_-^\circ}(-1)| \neq -1$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ then $2 \in \Pi^F_{i_+,i_-}(X-1, X+1)$, and we would have $J_+ = J_-$. Therefore Case I-(c) does not occur.

Case I-(d)*:* $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (-1,-1)$ *and* $(i_+, i_-) \equiv (0,0) \bmod 4$. This case does not occur for similar reasons to Case I-(c). So we are done in Case I.

Case II*:* $e(F_{12}) = -1$. We have $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,-1)$ or $(-1,1)$. Furthermore $(i_+, i_-) \equiv (2,0)$ or $(0,2) \bmod 4$ by (39). Hence there are 4 cases; (a) $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,-1), (i_+, i_-) \equiv (0,2)$; (b) $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (-1,1), (i_+, i_-) \equiv (2,0)$; (c) $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (1,-1), (i_+, i_-) \equiv (2,0)$; and (d) $(e(F_{J_+^\circ}), e(F_{J_-^\circ})) = (-1,1), (i_+, i_-) \equiv (0,2)$. As in Case I, we obtain the desired $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ in the cases (a) and (b), and it can be seen that the cases (c) and (d) do not occur. This completes the proof. □

Theorem 11.9. *Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial of even degree, and $i_+, i_- \in \mathbb{Z}$ integers with* (39)*. Suppose that $m_+ \neq 1$ and $m_- \neq 1$, where $m_\pm$ is the multiplicity of $X \mp 1$ in F. Then there exists $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ with $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_-$ mod 4 such that $\Lambda_{n,n}$ admits a semisimple $(F,\mathfrak{i})$-isometry.*

Proof. Suppose first that m_+ and m_- are odd. Then $m_+, m_- \geq 3$ by the assumption $m_+, m_- \neq 1$. Thus $\Pi^F_{i_+,i_-}(X-1, X+1) = \Pi(X-1, X+1) \ni 2$. This implies that $J_+ = J_-$, and Lemma 11.7 leads to the assertion.

Suppose then that m_+ and m_- are even. If $m_+ = 0$ or $m_- = 0$ then $J_+ = \emptyset$ or $J_+ = \emptyset$, and we arrive at the assertion by Lemma 11.7. Suppose that $m_+, m_- \geq 2$, and put $n'_\pm = (m_\pm - 2)/2$. Then F can be written as

$$F(X) = (X-1)^{2n'_+}(X+1)^{2n'_-}\widetilde{F}(X),$$

where $\widetilde{F}(X) := (X-1)^2(X+1)^2F_{12}(X)$. Let $\Lambda'_\pm$ and $\widetilde{\Lambda}$ denote the even unimodular lattices of signatures $(n'_\pm, n'_\pm)$ and $(\widetilde{n}, \widetilde{n})$, where $\widetilde{n} := n - n'_+ - n'_-$. By Proposition 11.8, there exists $\widetilde{\mathfrak{i}} \in I(\widetilde{n}, \widetilde{n}; \widetilde{F})$ with $\widetilde{\mathfrak{i}}(X-1) \equiv i_+$ and $\widetilde{\mathfrak{i}}(X+1) \equiv i_-$ mod 4 such that $\widetilde{\Lambda}$ admits a semisimple $(\widetilde{F}, \widetilde{\mathfrak{i}})$-isometry $\widetilde{t}$. We now define an isometry t of $\Lambda_{n,n} = \Lambda'_+ \oplus \Lambda'_- \oplus \widetilde{\Lambda}$ by $t = \mathrm{id}_{\Lambda'_+} \oplus (-\mathrm{id}_{\Lambda'_-}) \oplus \widetilde{t}$. Then t is a semisimple isometry of $\Lambda_{n,n}$ with characteristic polynomial F. Moreover, if $\mathfrak{i}$ denotes the index of t then $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_-$ mod 4 by the construction of t. This completes the proof. □

On the question of whether the assumption $m_+, m_- \neq 1$ in Theorem 11.9 can be removed, the author has neither proof nor counterexample. However, it is possible if the polynomial F is a product of cyclotomic polynomials.

11.2 Cyclotomic case

The aim of this subsection is to show the following theorem, which removes the assumption on m_+ and m_- in Theorem 11.9 by assuming that F is a product of cyclotomic polynomials.

Theorem 11.10. *Let $F \in \mathbb{Z}[X]$ be a product of cyclotomic polynomials. Assume that* $\deg(F)$ *is even, say $2n$. Let $i_+, i_- \in \mathbb{Z}$ be integers with* (39)*. Then there exists $\mathfrak{i} \in \mathrm{Idx}(n,n;F)$ with $\mathfrak{i}(X-1) \equiv i_+$ and $\mathfrak{i}(X+1) \equiv i_-$ mod 4 such that $\Lambda_{n,n}$ admits a semisimple $(F,\mathfrak{i})$-isometry.*

In the following, we assume that F is a product of cyclotomic polynomials of degree $2n$. For a map $\mathfrak{i} : I(F;\mathbb{R}) \to \mathbb{Z}$ and a factor $f \in I_1(F;\mathbb{Q})$ of F in $\mathbb{Q}[X]$, we write $\mathfrak{i}(f)$ for the sum $\sum_{g \in I_1(f;\mathbb{R})} \mathfrak{i}(g)$ (although it may be a slight abuse of notation).

Lemma 11.11. *Let $r, s \in \mathbb{Z}_{\geq 0}$ be non-negative integers with $r + s = 2n$. Suppose that F satisfies the condition $(\mathrm{Sign})_{r,s}$. Let $\mathfrak{j} \in \mathrm{Idx}(r, s; F)$ be an index map, and let $f \in I_1(F;\mathbb{Q})$ be a $+1$-symmetric irreducible factor of F other than $X + 1$.*

(i) *If $\mathfrak{j}(f) < \deg(f^{m_f})$ then F satisfies the condition $(\mathrm{Sign})_{r+2,s-2}$ and there exists $\mathfrak{i} \in \mathrm{Idx}(r+2, s-2; F)$ such that*

$$\mathfrak{i}(h) = \begin{cases} \mathfrak{j}(h) + 4 & \text{if } h = f \\ \mathfrak{j}(h) & \text{if } h \neq f \end{cases} \quad \text{for } h \in I(F;\mathbb{Q}).$$

(ii) *If $\mathfrak{j}(f) > -\deg(f^{m_f})$ then F satisfies the condition $(\mathrm{Sign})_{r-2,s+2}$ and there exists $\mathfrak{i} \in \mathrm{Idx}(r-2, s+2; F)$ such that*

$$\mathfrak{i}(h) = \begin{cases} \mathfrak{j}(h) - 4 & \text{if } h = f \\ \mathfrak{j}(h) & \text{if } h \neq f \end{cases} \quad \text{for } h \in I(F;\mathbb{Q}).$$

Proof. We remark that f is a cyclotomic polynomial other than $X - 1$ and $X + 1$. This means that f is of type 1 over $\mathbb{R}$. In other words, it can be written as $f = \prod_{g \in I_1(f;\mathbb{R})} g$. The multiplicity of each $g \in I_1(f;\mathbb{R})$ in F is m_f. We prove the assertion (i). It is enough to show the existence of $\mathfrak{i}$ by Corollary 7.29. Suppose that $\mathfrak{j}(f) < \deg(f^{m_f})$. Then there exists $g_0 \in I(f;\mathbb{R})$ such that $\mathfrak{j}(g_0) < \deg(g_0^{m_f})$. Noting that $\mathfrak{j}(g_0) \equiv \deg(g_0^{m_f}) \bmod 4$ by (28), we get $\mathfrak{j}(g_0) \geq \deg(g_0^{m_f}) - 4$. Thus, the map $\mathfrak{i} : I(F;\mathbb{R}) \to \mathbb{Z}$ defined by

$$\mathfrak{i}(g) = \begin{cases} \mathfrak{j}(g) + 4 & \text{if } g = g_0 \\ \mathfrak{j}(g) & \text{if } g \neq g_0 \end{cases} \quad \text{for } g \in I(F;\mathbb{R})$$

satisfies the conditions (27) and (28). Furthermore

$$\sum_{g \in I(F;\mathbb{R})} \mathfrak{i}(g) = r - s + 4 = (r+2) - (s-2).$$

These mean that the map $\mathfrak{i}$ belongs to $\mathrm{Idx}(r+2, s-2; F)$, and it is the desired index map. The assertion (ii) is obtained similarly. □

In the situation of this lemma, we have

$$\eta_\infty(\mathfrak{i})(f) \neq \eta_\infty(\mathfrak{j})(f) \quad \text{and} \quad \eta_\infty(\mathfrak{i})(h) = \eta_\infty(\mathfrak{j})(h) \text{ for all } h \in I(F;\mathbb{Q}) \setminus \{f\}$$

by (37).

Proposition 11.12. *Suppose that the multiplicities of $X - 1$ and $X + 1$ in F are 1. Then $\Lambda_{n,n}$ admits a semisimple isometry with characteristic polynomial F.*

Proof. We can write

$$F(X) = (X-1)(X+1) f_1(X)^{m_1} f_2(X)^{m_2} \cdots f_l(X)^{m_l},$$

where $f_1, \ldots, f_l$ are distinct cyclotomic polynomials and $m_1, \ldots, m_l$ are positive integers. Let $\mathfrak{i} \in \mathrm{Idx}(n, n; F)$ be an index map, and take $\beta_\mathfrak{i} = \{b_\mathfrak{i}\} \cup \{b_p\}_{p \in \mathcal{V} \setminus \{\infty\}} \in \mathcal{B}_\mathfrak{i}$. The following claim is essential.

Claim: If $\eta(\beta_{\mathfrak{i}}) \neq \mathbf{0}$ *then there exists* $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ *and* $\beta_{\mathfrak{j}} \in \mathcal{B}_{\mathfrak{j}}$ *such that* $\mathfrak{j}(X-1) = \mathfrak{i}(X-1), \mathfrak{j}(X+1) = \mathfrak{i}(X+1)$ *and* $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) \subsetneq \mathrm{Supp}(\eta(\beta_{\mathfrak{i}}))$. Suppose that $\eta(\beta_{\mathfrak{i}}) \neq \mathbf{0}$. Since $\eta(\beta_{\mathfrak{i}})(X-1) = 0$ and $\eta(\beta_{\mathfrak{i}})(X+1) = 0$ as in the proof of Theorem 9.28, and $\eta(\beta_{\mathfrak{i}}) \cdot \mathbf{1}_I = 0$ by Proposition 9.23, there exist $k, k' \in \{1, \ldots, l\}$ such that $\eta(\beta_{\mathfrak{i}})(f_k) = \eta(\beta_{\mathfrak{i}})(f_{k'}) = 1$. We assume $k = 1$ and $k' = 2$ without loss of generality. Note that we have $|\mathfrak{i}(f_1) + \mathfrak{i}(f_2)| \leq \deg(f_1^{m_1}) + \deg(f_2^{m_2})$ and the equality holds if and only if one of the following two conditions holds:

$$\mathfrak{i}(f_1) = \deg(f_1^{m_1}) \quad \text{and} \quad \mathfrak{i}(f_2) = \deg(f_2^{m_2}), \tag{41}$$

$$\mathfrak{i}(f_1) = -\deg(f_1^{m_1}) \quad \text{and} \quad \mathfrak{i}(f_2) = -\deg(f_2^{m_2}). \tag{42}$$

Case I: $|\mathfrak{i}(f_1) + \mathfrak{i}(f_2)| < \deg(f_1^{m_1}) + \deg(f_2^{m_2})$. We may assume that $\mathfrak{i}(f_1) < \deg(f_1^{m_1})$. If $\mathfrak{i}(f_2) > -\deg(f_2^{m_2})$ then it can be seen that there exists $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ such that

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) + 4 & \text{if } h = f_1 \\ \mathfrak{i}(h) - 4 & \text{if } h = f_2 \\ \mathfrak{i}(h) & \text{if } h \neq f_1, f_2 \end{cases} \qquad (h \in I(F; \mathbb{Q}))$$

by using Lemma 11.11 twice. We now define a family $\beta_{\mathfrak{j}}$ of inner products by $\beta_{\mathfrak{j}} := \{b_{\mathfrak{j}}\} \cup \{b_p\}_{p \in \mathcal{V} \setminus \{\infty\}}$, where $b_{\mathfrak{j}}$ is an inner product on M_∞ such that $\mathrm{idx}_\alpha^{b_{\mathfrak{j}}} = \mathfrak{j}$. Then $\beta_{\mathfrak{j}}$ belongs to $\mathcal{B}_{\mathfrak{j}}$. Moreover, we have

$$\eta(\beta_{\mathfrak{j}})(h) - \eta(\beta_{\mathfrak{i}})(h) = \eta_\infty(\mathfrak{j})(h) - \eta_\infty(\mathfrak{i})(h) = \begin{cases} 1 & \text{if } h = f_1, f_2 \\ 0 & \text{if } h \neq f_1, f_2 \end{cases}$$

by (37). Hence $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) = \mathrm{Supp}(\eta(\beta_{\mathfrak{i}})) \setminus \{f_1, f_2\} \subsetneq \mathrm{Supp}(\eta(\beta_{\mathfrak{i}}))$ as required. If $\mathfrak{i}(f_2) = -\deg(f_2^{m_2})$ then $\mathfrak{i}(f_1) > -\deg(f_1^{m_1})$ by the assumption $|\mathfrak{i}(f_1) + \mathfrak{i}(f_2)| < \deg(f_1^{m_1}) + \deg(f_2^{m_2})$. In this case, there exists $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ such that

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) - 4 & \text{if } h = f_1 \\ \mathfrak{i}(h) + 4 & \text{if } h = f_2 \\ \mathfrak{i}(h) & \text{if } h \neq f_1, f_2 \end{cases} \qquad (h \in I(F; \mathbb{Q}))$$

by Lemma 11.11. Hence, as above, we obtain $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) \subsetneq \mathrm{Supp}(\eta(\beta_{\mathfrak{i}}))$ for $\beta_{\mathfrak{j}} := \{b_{\mathfrak{j}}\} \cup \{b_p\}_p \in \mathcal{B}_{\mathfrak{j}}$.

Case II: $|\mathfrak{i}(f_1) + \mathfrak{i}(f_2)| = \deg(f_1^{m_1}) + \deg(f_2^{m_2})$ *and* (41) *holds.* In this case, we remark that if

$$\text{there exists } i \geq 3 \text{ such that } \mathfrak{i}(f_i) \leq -2 \text{ and } \deg(f_i^{m_i}) \geq 4 \tag{$\star$}$$

then we arrive at Claim. Indeed, if ($\star$) holds then it can be shown that there exists $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ such that

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) - 4 & \text{if } h = f_1, f_2 \\ \mathfrak{i}(h) + 8 & \text{if } h = f_i \\ \mathfrak{i}(h) & \text{if } h \neq f_1, f_2, f_i \end{cases} \qquad (h \in I(F; \mathbb{Q}))$$

by using Lemma 11.11 repeatedly. Therefore, as in Case I, we obtain $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) = \mathrm{Supp}(\eta(\beta_{\mathfrak{i}})) \setminus \{f_1, f_2\} \subsetneq \mathrm{Supp}(\eta(\beta_{\mathfrak{i}}))$ for $\beta_{\mathfrak{j}} := \{b_{\mathfrak{j}}\} \cup \{b_p\}_p \in \mathcal{B}_{\mathfrak{j}}$. We also remark that

$$\begin{aligned} \textstyle\sum_{i=3}^{l} \mathfrak{i}(f_i) &= -(\mathfrak{i}(X-1) + \mathfrak{i}(X+1)) - (\mathfrak{i}(f_1) + \mathfrak{i}(f_2)) \\ &\leq 2 - (\deg(f_1^{m_1}) + \deg(f_2^{m_2})) \end{aligned} \tag{43}$$

by the assumption (41).

Case II-(a): $\deg(f_1^{m_1}) + \deg(f_2^{m_2}) \geq 10$. It follows from equation (43) that $\sum_{i=3}^{l} \mathfrak{i}(f_i) \leq -8$. Because the number of cyclotomic polynomials of degree 2 is three (that is, Φ_3, Φ_4 and Φ_6), the inequality $\sum_{i=3}^{l} \mathfrak{i}(f) \leq -8$ shows that $(\star)$ holds. Thus we are done.

Case II-(b): $\deg(f_1^{m_1}) + \deg(f_2^{m_2}) = 8$. It follows from equation (43) that $\sum_{i=3}^{l} \mathfrak{i}(f_i) \leq -6$. If $\deg(f_1^{m_1}) = 2$ or $\deg(f_1^{m_2}) = 2$ then the number of cyclotomic polynomials of degree 2 which are contained in $\{f_i \mid i = 3, \ldots, l\}$ is at most two. Thus, the inequality $\sum_{i=3}^{l} \mathfrak{i}(f_i) \leq -6$ leads to $(\star)$ as in Case II-(a). Suppose that $\deg(f_1^{m_1}) = \deg(f_2^{m_2}) = 4$ and $(\star)$ does not hold. In this case, we have $l = 5$, $\{f_3, f_4, f_5\} = \{\Phi_3, \Phi_4, \Phi_6\}$, $m_3 = m_4 = m_5 = 1$, and $\mathfrak{i}(\Phi_3) = \mathfrak{i}(\Phi_4) = \mathfrak{i}(\Phi_6) = -2$. By Lemma 11.11, we can take $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ such that

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) - 4 & \text{if } h = f_1, f_2 \\ \mathfrak{i}(h) + 4 & \text{if } h = \Phi_3, \Phi_6 \\ \mathfrak{i}(h) & \text{if } h \neq f_1, f_2, \Phi_3, \Phi_6 \end{cases} \qquad (h \in I(F; \mathbb{Q}))$$

We define $\beta'_{\mathfrak{j}} := \{b_{\mathfrak{j}}\} \cup \{b_p\}_p \in \mathcal{B}_{\mathfrak{j}}$. Because $\Pi_{\mathfrak{j}}^F(\Phi_3, \Phi_6) = \Pi(\Phi_3, \Phi_6) = \{2\} \neq \emptyset$ by Theorem 10.9, there exists $\beta_{\mathfrak{j}} \in \mathcal{B}_{\mathfrak{j}}$ such that $\eta(\beta_{\mathfrak{j}}) = \eta(\beta'_{\mathfrak{j}}) + \mathbf{1}_{\{\Phi_3, \Phi_6\}}$ by Proposition 9.16. This is the desired family because $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) = \mathrm{Supp}(\eta(\beta_{\mathfrak{i}})) \setminus \{f_1, f_2\}$.

Case II-(c): $\deg(f_1^{m_1}) + \deg(f_2^{m_2}) = 6$. We assume that $\deg(f_1^{m_1}) = 2$ and $\deg(f_2^{m_2}) = 4$ without loss of generality, and suppose that $(\star)$ does not hold. Then $l = 4$, $m_3 = m_4 = 1$, $\deg(f_3) = \deg(f_4) = 2$, and $\mathfrak{i}(f_3) = \mathfrak{i}(f_4) = -2$. Note that $\{f_1, f_3, f_4\} = \{\Phi_3, \Phi_4, \Phi_6\}$. If $f_1 = \Phi_4$ then $\{f_3, f_4\} = \{\Phi_3, \Phi_6\}$, and we can obtain the desired index map $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ and family $\beta_{\mathfrak{j}} \in \mathcal{B}_{\mathfrak{j}}$ as in Case II-(b). Suppose that $f_1 \neq \Phi_4$. We may assume that $\{f_1, f_3\} = \{\Phi_3, \Phi_6\}$. Since $\eta(\beta_{\mathfrak{i}})(X - 1) = \eta(\beta_{\mathfrak{i}})(X + 1) = 0$ and $\eta(\beta_{\mathfrak{i}})(f_1) = \eta(\beta_{\mathfrak{i}})(f_2) = 1$, one of the following two cases occurs by Proposition 9.23: (i) $\eta(\beta_{\mathfrak{i}})(f_3) = \eta(\beta_{\mathfrak{i}})(f_4) = 1$; or (ii) $\eta(\beta_{\mathfrak{i}})(f_3) = \eta(\beta_{\mathfrak{i}})(f_4) = 0$. Note that $\Pi_{\mathfrak{i}}^F(f_1, f_3) = \Pi(\Phi_3, \Phi_6) = \{2\}$. Then, there exists a family $\beta'_{\mathfrak{i}} = \{b'_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}}$ such that $\eta(\beta'_{\mathfrak{i}}) = \eta(\beta_{\mathfrak{i}}) + \mathbf{1}_{\{f_1, f_3\}}$ by Proposition 9.16. In the case (i), this is the desired family because $\mathrm{Supp}(\eta(\beta'_{\mathfrak{i}})) = \{f_2, f_4\} \subsetneq \{f_1, f_2, f_3, f_4\} = \mathrm{Supp}(\eta(\beta_{\mathfrak{i}}))$. In the case (ii), there exists $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ such that

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) - 4 & \text{if } h = f_2 \\ \mathfrak{i}(h) + 4 & \text{if } h = f_4 \\ \mathfrak{i}(h) & \text{if } h \neq f_2, f_4 \end{cases} \qquad (h \in I(F; \mathbb{Q}))$$

by Lemma 11.11. We define $\beta_j := \{b_{\mathfrak{j}}\} \cup \{b'_p\}_p \in \mathcal{B}_{\mathfrak{j}}$. Then $\mathrm{Supp}(\eta(\beta_{\mathfrak{j}})) = \emptyset$ since $\mathrm{Supp}(\eta(\beta'_{\mathfrak{i}})) = \{f_2, f_4\}$. Hence we are done.

Case II-(d): $\deg(f_1^{m_1}) + \deg(f_2^{m_2}) = 4$. This case is similar to Case II-(c). We have $m_1 = m_2 = 1$ and $\deg(f_1) = \deg(f_2) = 2$. Suppose that $(\star)$ does not hold. Then $l = 3$, $m_3 = 1$, $\deg(f_3) = 2$, and $\mathfrak{i}(f_3) = -2$. Thus $\{f_1, f_2, f_3\} = \{\Phi_3, \Phi_4, \Phi_6\}$, and moreover we have $\eta(\beta)(f_3) = 0$ by Proposition 9.23. If $\{f_1, f_2\} = \{\Phi_3, \Phi_6\}$ then a family $\beta'_{\mathfrak{i}} \in \mathcal{B}_{\mathfrak{i}}$ with $\eta(\beta'_{\mathfrak{i}}) = \eta(\beta_{\mathfrak{i}}) + \mathbf{1}_{\{f_1, f_2\}}$ is the desired one. Suppose that $\{f_1, f_2\} \neq \{\Phi_3, \Phi_6\}$. We may assume $\{f_1, f_3\} = \{\Phi_3, \Phi_6\}$. Let $\beta'_{\mathfrak{i}} = \{b'_v\}_{v \in \mathcal{V}} \in \mathcal{B}_{\mathfrak{i}}$ be a family with $\eta(\beta'_{\mathfrak{i}}) = \eta(\beta_{\mathfrak{i}}) + \mathbf{1}_{\{f_1, f_3\}}$, and define $\beta_{\mathfrak{j}} := \{b_{\mathfrak{j}}\} \cup \{b'_p\}_p \in \mathcal{B}_{\mathfrak{j}}$, where $\mathfrak{j} \in \mathrm{Idx}(n, n; F)$ is an index map satisfying

$$\mathfrak{j}(h) = \begin{cases} \mathfrak{i}(h) - 4 & \text{if } h = f_2 \\ \mathfrak{i}(h) + 4 & \text{if } h = f_3 \\ \mathfrak{i}(h) & \text{if } h \neq f_2, f_3 \end{cases} \qquad (h \in I(F; \mathbb{Q})).$$

Then $\mathrm{Supp}\, \eta(\beta_{\mathfrak{j}}) = \emptyset$, and we are done.

Case III: $|\mathfrak{i}(f_1)+\mathfrak{i}(f_2)| = \deg(f_1^{m_1})+\deg(f_2^{m_2})$ *and* (42) *holds.* In this case, Claim can be shown as in Case II. The proof of Claim is complete.

By applying Claim repeatedly, we obtain $\mathfrak{j} \in \mathrm{Idx}(n,n;F)$ and $\beta_{\mathfrak{j}} \in \mathcal{B}_{\mathfrak{j}}$ such that $\mathfrak{j}(X-1) = \mathfrak{i}(X-1), \mathfrak{j}(X+1) = \mathfrak{i}(X+1)$ and $\eta(\beta_{\mathfrak{j}}) = \mathbf{0}$. This means that $\Lambda_{n,n}$ admits a semisimple $(F,\mathfrak{j})$-isometry by Theorem 9.25. The proof is complete. □

Proof of Theorem 11.10. If m_+ and m_- are even then the theorem follows from Theorem 11.9. Suppose that m_+ and m_- are odd, and put $n'_\pm = (m_\pm - 1)/2$. Then F can be written as $F(X) = (X-1)^{2n'_+}(X+1)^{2n'_-}\widetilde{F}(X)$, where $\widetilde{F}(X) = (X-1)(X+1)F_{12}(X)$. Let $\Lambda'_\pm$ and $\widetilde{\Lambda}$ denote the even unimodular lattices of signatures $(n'_\pm, n'_\pm)$ and $(\widetilde{n},\widetilde{n})$, where $\widetilde{n} := n - n_+ - n_-$. By Proposition 11.12, there exists a semisimple isometry $\widetilde{t}$ of $\widetilde{\Lambda}$ with characteristic polynomial F. Let $\widetilde{b}$ denote the inner product of the lattice $\widetilde{\Lambda}$. Note that $(\widetilde{\Lambda}, -\widetilde{b})$ is also an even unimodular lattice of signature $(\widetilde{n},\widetilde{n})$, and $\widetilde{t}$ is a semisimple $(F,-\widetilde{\mathfrak{i}})$-isometry of $(\widetilde{\Lambda},-\widetilde{b})$, where $\widetilde{\mathfrak{i}} := \mathrm{idx}_{\widetilde{t}}^{\widetilde{b}}$.

Suppose that $e(F_{12}) = 1$. Since $\widetilde{\mathfrak{i}}(X-1) \equiv \widetilde{\mathfrak{i}}(X+1) \equiv 1 \bmod 2$ by Proposition 7.24 and $\widetilde{\mathfrak{i}}(X-1)+\widetilde{\mathfrak{i}}(X+1) \equiv 0 \bmod 4$ by Proposition 11.2 (i), we have $(\widetilde{\mathfrak{i}}(X-1), \widetilde{\mathfrak{i}}(X+1)) \equiv (1,-1)$ or $(-1,1) \bmod 4$. Similarly, we have $(i_+,i_-) \equiv (1,-1)$ or $(-1,1) \bmod 4$ by the assumption (39). Hence, we assume without loss of generality that $(\widetilde{\mathfrak{i}}(X-1), \widetilde{\mathfrak{i}}(X+1)) \equiv (i_+,i_-) \bmod 4$ by replacing $\widetilde{b}$ by $-\widetilde{b}$ if necessary. We now define an isometry t of $\Lambda_{n,n} = \Lambda'_+ \oplus \Lambda'_- \oplus \widetilde{\Lambda}$ by $t := \mathrm{id}_{\Lambda'_+} \oplus (-\mathrm{id}_{\Lambda'_-}) \oplus \widetilde{t}$. Then t is a semisimple isometry of $\Lambda_{n,n}$ with characteristic polynomial F, and its index is the desired index map by construction. In the case $e(F_{12}) = -1$, we can obtain the desired index map similarly. The proof is complete. □

Chapter IV
Automorphisms of K3 surfaces

12 K3 surfaces

This section gives a minimal explanation of K3 surfaces to describe the relationship between automorphisms of K3 surfaces and isometries of a K3 lattice, assuming knowledge of complex manifolds. We refer to [47] for complex manifolds, and [2] and [23] for more details on K3 surfaces.

12.1 Preliminaries

Before describing K3 surfaces, we make some preliminaries independent of complex manifold theory.

Primitive submodules Let Λ be a finitely generated free $\mathbb{Z}$-module. A submodule N of Λ is said to be *primitive* in Λ if the quotient Λ/N is torsion-free.

Lemma 12.1. *Let K be a subfield of $\mathbb{C}$, and let W be a K-subspace of $\Lambda \otimes K$. Then the intersection $\Lambda \cap W$ is primitive in Λ.*

Proof. Let $x \in \Lambda$ be a nonzero element, and suppose that $nx \in \Lambda \cap W$ for some $n \in \mathbb{Z}_{>0}$. Then $x = n^{-1}(nx) \in W$, and $x \in \Lambda \cap W$. This means that $\Lambda/(\Lambda \cap W)$ is torsion-free. □

For a submodule N of Λ, we write $\mathbb{Q} \cdot N$ or just $\mathbb{Q}N$ for the $\mathbb{Q}$-span of N in $\Lambda \otimes \mathbb{Q}$. A submodule N is primitive in Λ if and only if $N = \mathbb{Q}N \cap \Lambda$. Note that if Λ is equipped with an inner product $b : \Lambda \times \Lambda \to \mathbb{Q}$ then we have $\mathbb{Q} \cdot N^\perp = (\mathbb{Q}N)^\perp$ in $\Lambda \otimes \mathbb{Q}$.

Proposition 12.2. *Let N be a submodule of Λ, and suppose that Λ is equipped with an inner product $b : \Lambda \times \Lambda \to \mathbb{Q}$.*

(i) *$N^\perp = \{y \in \Lambda \mid b(y, x) = 0$ for all $x \in N\}$ is primitive.*

(ii) *If N is primitive then $N^{\perp\perp} = N$.*

Proof. (i). The submodule $N^\perp$ is the intersection of Λ and the $\mathbb{Q}$-subspace $\{y \in \Lambda \otimes \mathbb{Q} \mid b(y, x) = 0$ for all $x \in N\}$ of $\Lambda \otimes \mathbb{Q}$. Thus, it is primitive by Lemma 12.1.

(ii). Since $N^{\perp\perp}$ is primitive by (i), we have $N^{\perp\perp} = \mathbb{Q} \cdot N^{\perp\perp} \cap \Lambda$. Furthermore $\mathbb{Q} \cdot N^{\perp\perp} = (\mathbb{Q} \cdot N^\perp)^\perp = (\mathbb{Q} \cdot N)^{\perp\perp} = \mathbb{Q} \cdot N$. Hence $N^{\perp\perp} = \mathbb{Q} \cdot N^{\perp\perp} \cap \Lambda = \mathbb{Q}N \cap \Lambda = N$ if N is primitive. □

Weyl groups Let (Λ, b) be an even lattice of signature $(3, n)$, where $n \in \mathbb{Z}_{>0}$. We consider that the Euclidean topology is given on the $\mathbb{R}$-vector space $\Lambda_{\mathbb{R}} := \Lambda \otimes \mathbb{R}$. The innner product obtained by extending b linearly on $\Lambda_{\mathbb{R}}$ is also denoted by b. Let E be a nondegenerate subspace of $\Lambda_{\mathbb{R}}$ of signature $(2, 0)$, and put $V = E^{\perp} \subset \Lambda_{\mathbb{R}}$. Since V is of signature $(1, n)$, the cone $\{x \in V \mid b(x, x) > 0\}$ has exactly two connected components. Let us fix one component $\mathscr{C}^+$ arbitrarily, and refer to it as the *positive cone*. The rest component is given by $-\mathscr{C}^+$. Note that any isometry of V maps $\mathscr{C}^+$ onto $\mathscr{C}^+$ itself or onto $-\mathscr{C}^+$.

Put $\Delta = \{r \in \Lambda \cap V \mid b(r, r) = -2\}$. This set may be infinite, or empty. For $r \in \Delta$, the hyperplane $H_r := (\mathbb{R}r)^{\perp}_V$ in V orthogonal to $r \in \Delta$ has signature $(1, n-1)$. This implies that the intersection of H_r and $\mathscr{C}^+$ is not empty. Thus, the reflection orthogonal to $r \in \Delta$ preserves $\mathscr{C}^+$ since it fix a point of $H_r \cap \mathscr{C}^+$. The subgroup $\mathscr{W}$ of $\mathrm{O}(\Lambda) \cap \mathrm{O}(V) \subset \mathrm{O}(\Lambda_{\mathbb{R}})$ generated by reflections orthogonal to vectors in Δ is called the *Weyl group* with respective to Δ. Any isometry in the Weyl group preserves $\mathscr{C}^+$ since so does each reflection.

In this situation, it can be shown that the action of $\mathscr{W}$ on $\mathscr{C}^+$ is *properly discontinuous*, see [23, Lemma 2.12]. This implies that the family $\{H_r\}_{r \in \Delta}$ is locally finite in $\mathscr{C}^+$, and the union $\bigcup_{r \in \Delta} H_r$ is a closed set in $\mathscr{C}^+$, see Lemma 2.5 and Corollary 2.6 of [23]. A connected component of $\mathscr{C}^+ \setminus \bigcup_{r \in \Delta} H_r$ is called a *chamber*. If y is a point in $\mathscr{C}^+ \setminus \bigcup_{r \in \Delta} H_r$ and $\mathscr{K}$ is the chamber containing y, by letting $\Delta^+ = \{r \in \Delta \mid b(y, r) > 0\}$, this chamber can be written as

$$\mathscr{K} = \{x \in \mathscr{C}^+ \mid b(x, r) > 0 \text{ for all } r \in \Delta^+\}.$$

The following fact will be needed.

Theorem 12.3. *Let $\mathscr{K}$ be a chamber in $\mathscr{C}^+$.*

(i) $\mathscr{C}^+ \setminus \bigcup_{r \in \Delta} H_r = \bigcup_{w \in \mathscr{W}} w(\mathscr{K})$.

(ii) *If $w \in \mathscr{W}$ satisfies $w(\mathscr{K}) = \mathscr{K}$ then $w = \mathrm{id}$.*

Namely, the Weyl group acts simply transitively on the set of chambers.

Proof. See [23, Theorem 2.9]. □

12.2 Basic facts

For a complex manifold Σ, the l-th singular cohomology group with coefficients in a ring R is denoted by $H^l(\Sigma, R)$. In the case $R = \mathbb{R}$ or $\mathbb{C}$, singular cohomology groups are often identified with de Rham cohomology groups. Furthermore $H^{i,j}(\Sigma)$ denote the Dolbeault cohomology group. We call a 2-dimensional manifold a *surface*.

Definition 12.4. A *K3 surface* is a compact complex surface Σ such that its canonical bundle is trivial and $\dim_{\mathbb{C}}(H^{0,1}(\Sigma)) = 0$.

A nonsingular quartic surface in the projective space $\mathbb{P}^3$ is a K3 surface, see [23, Example 4.1]. A K3 surface can be nonprojective. By Siu [43], it is shown that every K3 surface is Kähler.

In the following, Σ is a K3 surface. Since the canonical bundle is trivial, there exists a nowhere vanishing holomorphic 2-form ω_Σ, and it is unique up to scalar multiplication. We have $H^{2,0}(\Sigma) = \mathbb{C}\omega_\Sigma$, where we also use the symbol ω_Σ for its cohomology class. Let $\langle \cdot, \cdot \rangle : H^2(\Sigma, \mathbb{Z}) \times H^2(\Sigma, \mathbb{Z}) \to \mathbb{Z}$ denote the intersection form, that is, the symmetric bilinear form defined by the evaluation of the cup product on the fundamental class.

Theorem 12.5. *Let Σ be a K3 surface. Then $H^2(\Sigma, \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank 22. Moreover, the intersection form makes $H^2(\Sigma, \mathbb{Z})$ an even unimodular lattice of signature $(3, 19)$.*

Proof. See [23, Theorem 4.5]. □

For any subfield K of $\mathbb{C}$, we identify $H^2(\Sigma,\mathbb{Z})\otimes K$ with $H^2(\Sigma,K)$ naturally and regard $H^2(\Sigma,\mathbb{Z})$ as a submodule of $H^2(\Sigma,K)$. If $K\subset L\subset\mathbb{C}$ then we consider that $H^2(\Sigma,K)\subset H^2(\Sigma,L)\subset H^2(\Sigma,\mathbb{C})$. Furthermore $H^2(\Sigma,\mathbb{R})$ is regarded as the real part of $H^2(\Sigma,\mathbb{C})$. The intersection form is extended linearly on $H^2(\Sigma,\mathbb{C})$, which is denoted by $\langle\,\cdot\,,\,\cdot\,\rangle$ again. Let $\bar{\cdot}: H^2(\Sigma,\mathbb{C})\to H^2(\Sigma,\mathbb{C})$ denote the complex conjugate. Because $\langle\omega_\Sigma,\omega_\Sigma\rangle=\int_\Sigma\omega_\Sigma\wedge\omega_\Sigma$ and $\langle\omega_\Sigma,\overline{\omega_\Sigma}\rangle=\int_\Sigma\omega_\Sigma\wedge\overline{\omega_\Sigma}$, we have

$$\langle\omega_\Sigma,\omega_\Sigma\rangle=0\quad\text{ and }\quad\langle\omega_\Sigma,\overline{\omega_\Sigma}\rangle>0. \tag{44}$$

These equations are called the *Riemann condition*. Let $E\subset H^2(\Sigma,\mathbb{R})$ denote the real part of $H^{2,0}(\Sigma,\mathbb{C})\oplus H^{0,2}(\Sigma,\mathbb{C})=\mathbb{C}\omega_\Sigma\oplus\mathbb{C}\overline{\omega_\Sigma}$, which is generated by $(\omega_\Sigma+\overline{\omega_\Sigma})/2$ and $(\omega_\Sigma-\overline{\omega_\Sigma})/2\sqrt{-1}$. The Riemann condition (44) means that E is of signature $(2,0)$ (with respect to the intersection form).

Since Σ is Kähler as mentioned before, it follows from Hodge theory that the cohomology group $H^2(\Sigma,\mathbb{C})$ decomposes as

$$H^2(\Sigma,\mathbb{C})=H^{2,0}(\Sigma)\oplus H^{1,1}(\Sigma)\oplus H^{0,2}(\Sigma)$$

(the Hodge decomposition), and $H^{1,1}(\Sigma)$ is orthogonal to the 2-dimensional subspace $H^{2,0}(\Sigma)\oplus H^{0,2}(\Sigma)$. Let $H^{1,1}_{\mathbb{R}}(\Sigma)$ denote the real part of $H^{1,1}(\Sigma)$. Then, the decomposition $H^2(\Sigma,\mathbb{R})=H^{1,1}_{\mathbb{R}}(\Sigma)\oplus E$ is an orthogonal direct sum decomposition. The signature of $H^{1,1}_{\mathbb{R}}(\Sigma)$ is $(1,19)$ since $H^2(\Sigma,\mathbb{R})$ and E have signature $(3,19)$ and $(2,0)$ respectively. The submodule $P_\Sigma:=H^2(\Sigma,\mathbb{Z})\cap H^{1,1}_{\mathbb{R}}(\Sigma)$ of $H^2(\Sigma,\mathbb{Z})$ is called the *Picard lattice* or *Néron-Severi lattice*. The restriction of the intersection form on the Picard lattice can be degenerate, though we call it the Picard 'lattice'.

As in the latter part of §12.1, the cone $\{x\in H^{1,1}_{\mathbb{R}}(\Sigma)\mid\langle x,x\rangle>0\}$ has exactly two connected components since $H^{1,1}_{\mathbb{R}}(\Sigma)$ is of signature $(1,19)$. The one containing a Kähler class is called the *positive cone* and deonted by $\mathscr{C}^+_\Sigma$. Put $\Delta_\Sigma=\{r\in P_\Sigma\mid\langle r,r\rangle=-2\}$ and $\Delta^+_\Sigma=\{r\in\Delta_\Sigma\mid r\text{ is effective}\}$. Here, a cohomology class $r\in P_\Sigma$ is *effective* if it is the first Chern class of the line bundle defined by an effective divisor. Then Δ_Σ is decomposed as $\Delta_\Sigma=\Delta^+_\Sigma\sqcup-\Delta^+_\Sigma$ (see [23, Lemma 4.16]), and

$$\mathscr{K}_\Sigma:=\{x\in\mathscr{C}^+_\Sigma\mid\langle x,r\rangle>0\text{ for all }r\in\Delta^+_\Sigma\}$$

is a chamber in $\mathscr{C}^+_\Sigma$. We refer to this chamber as the *Kähler cone* of Σ. It is known that the every point in the Kähler cone is a Kähler class, see Definition 4.17 and Theorem 7.5 of [23].

We close this subsection with a criterion for projectivity of a K3 surface in terms of the Picard lattice. The following general result for compact complex surfaces is known.

Theorem 12.6. *A compact complex surface Σ is projective if and only if there exists $x\in H^2(\Sigma,\mathbb{Z})\cap H^{1,1}(\Sigma)$ such that $\langle x,x\rangle>0$, where $\langle\,\cdot\,,\,\cdot\,\rangle$ is the intersection form.*

Proof. The Lefschetz theorem on $(1,1)$-classes (see [2, Chapter IV, Theorem 2.13]) means that $P_\Sigma=\{c_1(\mathcal{L})\mid\mathcal{L}\text{ is a line bundle on }\Sigma\}$, where $c_1(\mathcal{L})$ is the first Chern class of $\mathcal{L}$. Then the theorem follows from [2, Chapter IV, Theorem 6.2]. □

Corollary 12.7. *A K3 surface Σ is projective if and only if the Picard lattice P_Σ is nondegenerate and has signature $(1,\mathrm{rk}(P_\Sigma)-1)$.*

Proof. This follows from Theorem 12.6 by noting that the Picard lattice P_Σ of a K3 surface Σ is contained in the space $H^{1,1}_{\mathbb{R}}(\Sigma)$ of signature $(1,19)$. □

12.3 Torelli theorem and surjectivity of the period mapping

For an isomorphism $\phi : \Sigma' \to \Sigma$ of $K3$ surfaces, we use the same symbol ϕ^* for the induced homomorphisms $H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma', \mathbb{Z})$ and $H^2(\Sigma, \mathbb{C}) \to H^2(\Sigma', \mathbb{C})$. It preserves structures on the cohomology groups mentioned in §12.2. Namely, ϕ^* is an isometry (with respect to intersection forms), $\phi^*(\mathbb{C}\omega_\Sigma) = \mathbb{C}\omega_{\Sigma'}$, and $\phi^*(\mathscr{K}_\Sigma) = \mathscr{K}_{\Sigma'}$. The Torelli theorem states that such an isometry between cohomology groups comes from an isomorphism between K3 surfaces.

Theorem 12.8 (Torelli theorem for K3 surfaces)**.** *Let Σ, Σ' be K3 surfaces. Suppose that there exists an isometry $t : H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma', \mathbb{Z})$ with $t(\omega_\Sigma) \in \mathbb{C}\omega_{\Sigma'}$ and $t(\mathscr{K}_\Sigma) = \mathscr{K}_{\Sigma'}$. Then there exists a unique isomorphism $\phi : \Sigma' \to \Sigma$ of complex manifolds such that $\phi^* = t$.*

Proof. See [23, Theorem 6.1]. □

We explain the period mapping of K3 surfaces.

Definition 12.9. A *K3 lattice* is an even unimodular lattice of signature $(3, 19)$. Such a lattice is unique up to isomorphism (Theorem 5.25).

As seen in §12.2, the second cohomology group of any K3 surface is a K3 lattice with the intersection form. In the following, we fix a K3 lattice (Λ, b). For a nonzero vector $\omega \in \Lambda_\mathbb{C} := \Lambda \otimes \mathbb{C}$, we write $[\omega]$ for its image under the projection $\Lambda_\mathbb{C} \setminus \{0\} \to \mathbb{P}(\Lambda_\mathbb{C})$, where $\mathbb{P}(\Lambda_\mathbb{C})$ is the projective space. The symbol b also denotes the inner product $b \otimes \mathbb{C}$ on $\Lambda_\mathbb{C}$. The set

$$\Omega_{\mathrm{K3}} := \{[\omega] \in \mathbb{P}(\Lambda_\mathbb{C}) \mid b(\omega, \omega) = 0 \text{ and } b(\omega, \overline{\omega}) > 0\}$$

is called the *period domain* of K3 surfaces. If Σ is a K3 surface and $\tau_\Sigma : H^2(\Sigma, \mathbb{Z}) \to \Lambda$ is a lattice isometry, then the Riemann condition (44) means that $[\tau_\Sigma(\omega_\Sigma)]$ belongs to Ω_{K3}.

Definition 12.10. A *marked K3 surface* is a pair (Σ, τ_Σ) consisting of a K3 surface Σ and a lattice isometry $\tau_\Sigma : H^2(\Sigma, \mathbb{Z}) \to \Lambda$. Two marked K3 surfaces (Σ, τ_Σ) and $(\Sigma', \tau_{\Sigma'})$ are *isomorphic* if there exists an isomorphism $\phi : \Sigma' \to \Sigma$ such that $\tau_\Sigma = \tau_{\Sigma'} \circ \phi^*$. Let $\mathcal{M}$ denote the set of isomorphism classes of marked K3 surfaces. The map $\mathcal{M} \to \Omega_{K3}$ defined by sending a marked K3 surface (Σ, τ_Σ) to $[\tau_\Sigma(\omega_\Sigma)] \in \Omega_{\mathrm{K3}}$ is called the *period mapping* of marked K3 surfaces.

Theorem 12.11 (Surjectivity of the period mapping)**.** *The period mapping is surjective. In other words, for any $[\omega] \in \Omega_{\mathrm{K3}}$, there exists a marked K3 surface (Σ, τ_Σ) such that $[\tau_\Sigma(\omega_\Sigma)] = [\omega]$.*

Proof. See Theorem 6.9 and Section 7 of [23]. □

Definition 12.12. We refer to a vector $\omega \in \Lambda_\mathbb{C}$ with $[\omega] \in \Omega_{\mathrm{K3}}$ as a *Hodge vector*. An isometry t of Λ is called a *Hodge isometry* with respect to a Hodge vector ω if $[t(\omega)] = [\omega]$, i.e., if ω is an eigenvector of t.

By using a Hodge vector, we introduce a Kähler cone for Λ formally as a chamber. Let $\omega \in \Lambda_\mathbb{C}$ be a Hodge vector. Let $H^{2,0}$, $H^{0,2}$, and $H^{1,1}$ be subspaces of $\Lambda_\mathbb{C}$ defined as

$$H^{2,0} = \mathbb{C}\omega, \quad H^{0,2} = \mathbb{C}\overline{\omega}, \quad H^{1,1} = (H^{2,0} + H^{0,2})^\perp.$$

Then $\Lambda_\mathbb{C}$ decomposes as $\Lambda_\mathbb{C} = H^{2,0} \oplus H^{1,1} \oplus H^{0,2}$, and the real part $H^{1,1}_\mathbb{R}$ of $H^{1,1}$ is of signature $(1, 19)$. Let $\mathscr{C}^+$ be the positive cone, that is, one of two connected components of $\{x \in H^{1,1}_\mathbb{R} \mid b(x, x) > 0\}$ chosen arbitrarily. Put $P = \Lambda \cap H^{1,1}_\mathbb{R}$ and $\Delta = \{r \in P \mid b(r, r) = -2\}$. The submodule $P \subset \Lambda$ will be referred to as the *Picard lattice* of Λ (with respect to ω), and the Weyl group with respect to Δ will be referred to as the *Weyl group of Λ determined by ω*, which is in fact determined by the class $[\omega]$. As mentioned in the latter part of §12.1, the hyperplanes

orthogonal to vectors in Δ partition $\mathscr{C}^+$ into chambers. If we fix a chamber $\mathscr{K}$, this chamber is called the *Kähler cone* for Λ. Note that we make the choice of the positive cone $\mathscr{C}^+$ when we fix a Kähler cone $\mathscr{K}$.

Let us fix a Hodge vector ω and Kähler cone $\mathscr{K}$ for Λ. By Theorem 12.11, there exists a marked K3 surface (Σ, τ'_Σ) with $[\tau'_\Sigma(\omega_\Sigma)] = [\omega]$ in $\mathbb{P}(\Lambda_\mathbb{C})$. Then, the positive cone $\mathscr{C}^+_\Sigma$ is mapped onto $\mathscr{C}^+$ or $-\mathscr{C}^+$ under τ'_Σ, since τ'_Σ is an isometry. Put $\tau''_\Sigma = -\tau'_\Sigma$ if $\tau'_\Sigma(\mathscr{C}^+_\Sigma) = -\mathscr{C}^+$ and $\tau''_\Sigma = \tau'_\Sigma$ if $\tau'_\Sigma(\mathscr{C}^+_\Sigma) = \mathscr{C}^+$. Then $\tau''_\Sigma(\mathscr{C}^+_\Sigma) = \mathscr{C}^+$, and the Kähler cone $\mathscr{K}_\Sigma$ is mapped onto a chamber $\mathscr{K}'$ in $\mathscr{C}^+$ under τ''_Σ. Since the Weyl group $\mathscr{W}$ of Λ determined by ω acts transitivity on the set of chambers by Theorem 12.3, there exists $w \in \mathscr{W}$ such that $w(\mathscr{K}') = \mathscr{K}$. We have $w(\omega) = \omega$ since w is a composition of reflections orthogonal to vectors in $H^{1,1}_\mathbb{R}$. Put $\tau_\Sigma = w \circ \tau''_\Sigma$. Then the marked K3 surface (Σ, τ_Σ) has the condition

$$[\tau_\Sigma(\omega_\Sigma)] = [\omega] \quad \text{and} \quad \tau_\Sigma(\mathscr{K}_\Sigma) = \mathscr{K}.$$

This means that, in Theorem 12.11, a marked K3 surface (Σ, τ_Σ) can be chosen to have this condition for any Hodge vector ω and Kähler cone $\mathscr{K}$.

Theorem 12.13. *Let Λ be a K3 lattice, $\omega \in \Lambda_\mathbb{C}$ a Hodge vector, and $\mathscr{K}$ a Kähler cone for Λ. Let t be a Hodge isometry with respect to ω that preserves the Kähler cone $\mathscr{K}$. Then there exists a marked K3 surface (Σ, τ_Σ) and automorphism ϕ of Σ such that $\tau_\Sigma(\omega_\Sigma) \in \mathbb{C}\omega$, $\tau_\Sigma(\mathscr{K}_\Sigma) = \mathscr{K}$, and $\phi^* = \tau_\Sigma^{-1} \circ t \circ \tau_\Sigma$.*

Proof. As explained now, there exists a marked K3 surface (Σ, τ_Σ) such that $\tau_\Sigma(\omega_\Sigma) = \mathbb{C}\omega$ and $\tau_\Sigma(\mathscr{K}_\Sigma) = \mathscr{K}$. Then $\tau_\Sigma^{-1} \circ t \circ \tau_\Sigma$ preserves the vector ω_Σ up to constant and the Kähler cone $\mathscr{K}_\Sigma$. Hence, there exists an automorphism $\phi : \Sigma \to \Sigma$ such that $\phi^* = \tau_\Sigma^{-1} \circ t \circ \tau_\Sigma$ by the Torelli theorem 12.8. This completes the proof. □

13 Dynamical degrees of K3 surface automorphisms

In this section, we deal with the problem of which number can be realized as the dynamical degree of an automorphism of a K3 surface. The main idea is to reduce this problem to the problem of lattice isometries by Theorem 12.13, and use results established in Chapter III.

13.1 Salem numbers and Salem polynomials

This subsection gives a brief description of Salem numbers and Salem polynomials. We refer to [38] and [44] for more detail.

Definition 13.1. A real algebraic integer $\beta > 1$ is called a *Salem number* if it is conjugate to β^{-1} and all of its conjugates other than β and β^{-1} have absolute value 1. The minimal polynomial of a Salem number over $\mathbb{Q}$ is called a *Salem polynomial*.

Any Salem number is a unit since its inverse is also an algebraic integer by definition. A Salem number can be characterized as a real algebraic unit $\beta > 1$ such that all of its conjugates other than β and β^{-1} have absolute value 1 (β is assumed to be a unit, and the condition that β is conjugate to β^{-1} is dropped). Indeed, if such a real algebraic unit β were not conjugate to β^{-1} then the product of all conjugates of β, the constant term of its minimal polynomial or -1 times that value, would have absolute value greater than 1. However, this is a contradiction since β is unit. Hence β is conjugate to β^{-1}, and it is a Salem number. In the following, the unit circle in $\mathbb{C}$ is denoted by $\mathbb{T}$.

Proposition 13.2. *Every Salem polynomial is a $+1$-symmetric irreducible polynomial of even degree.*

Proof. Let β be a Salem number, and S its minimal polynomial. It is clear that S is irreducible. If β has no conjugate other than β^{-1} then $S(X) = X^2 - (\beta + \beta^{-1})X + 1$, and we are done. Suppose that β has a conjugate $\delta \in \mathbb{T}$ other than β^{-1}. Let L be the Galois closure of $\mathbb{Q}(\beta)/\mathbb{Q}$, and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be an automorphism with $\sigma(\beta) = \delta$. Then δ^{-1} is also a conjugate of β since $\sigma(\beta^{-1}) = \sigma(\beta)^{-1} = \delta^{-1}$. Furthermore $\delta \neq \delta^{-1}$ since $\delta \neq 1, -1$. Hence, the set of roots of S is of the form $\{\beta, \beta^{-1}, \delta_1, \delta_1^{-1}, \ldots, \delta_{n-1}, \delta_{n-1}^{-1}\}$, where $\delta_1, \ldots, \delta_{n-1} \in \mathbb{T} \setminus \{1, -1\}$. This means that S can be written as $S(X) = (X^2 - (\beta + \beta^{-1})X + 1) \times \prod_{j=1}^{n-1}(X^2 - (\delta_j + \delta_j^{-1})X + 1)$. Therefore S is $+1$-symmetric and of even degree. □

Remark 13.3. Sometimes, a Salem number is assumed to have degree at least 4, or equivalently, assumed to have at least one conjugate on the unit circle $\mathbb{T}$. In this case, it coincides with Salem's definition ([38, p.26]). However, as in [25], it will be useful to allow Salem numbers of degree 2 in our context.

For any even number d, there exist infinitely many Salem numbers of degree d, see e.g. [18, §7]. On the other hand, for a positive integer d and a positive real number r, there are at most finitely many Salem numbers of degree d smaller than r, because the coefficients of the minimal polynomials of such Salem numbers are bounded. Hence, one can speak of the i-th smallest Salem number of degree d. In his website [31], Mossinghoff gives a complete list of Salem numbers of small degrees, below certain bounds. The smallest Salem number of degree 10 is called *Lehmer's number*, and it is the smallest known Salem number.

Let S be a Salem polynomial. By Proposition 13.2, there is the trace polynomial R of S (see Definition 7.11). Because $\mathbb{T} \setminus \{1, -1\}$ is mapped two-to-one onto the interval $(-2, 2)$ under the function $\mathbb{C} \to \mathbb{C}$, $x \mapsto x + x^{-1}$, all roots of R except for $\beta + \beta^{-1} > 2$ lie on $(-2, 2)$. By considering the graph of R, the value $S(1) = R(2)$ is always negative. The following lemma will be needed.

Lemma 13.4. *Let S be a Salem polynomial of degree d.*

(i) *If $d \equiv 0 \bmod 4$ then S does not satisfy the condition* (Square).

(ii) *Suppose that $d \equiv 2 \bmod 4$. Then S satisfies the condition* (Square) *if $|S(1)|$ and $|S(-1)|$ are squares.*

Proof. Put $n = d/2$, and let R be the trace polynomial of S. By consider the graph of R, the value $(-1)^n S(1)S(-1) = R(2)R(-2)$ is negative if $d \equiv 0 \bmod 4$, and positive if $d \equiv 2 \bmod 4$. In particular, if $d \equiv 0 \bmod 4$ then $(-1)^n S(1)S(-1)$ cannot be a square. This shows the assertion (i). Suppose that $d \equiv 2 \bmod 4$. Then $(-1)^n S(1)S(-1) = |(-1)^n S(1)S(-1)| = |S(1)||S(-1)|$. Hence, if $|S(1)|$ and $|S(-1)|$ are squares then so is $(-1)^n S(1)S(-1)$. This shows the assertion (ii). □

13.2 Dynamical degrees

Here, we discuss dynamical degrees of K3 surface automorphisms.

Definition 13.5. Let Σ be a conpact complex surface, and ϕ an automorphism of Σ.

(i) The (first) *dynamical degree* of ϕ, denoted $d(\phi)$, is the spectral radius of the induced homomorphism $\phi^* : H^2(X, \mathbb{C}) \to H^2(X, \mathbb{C})$, that is,

$$d(\phi) = \max\{|\mu| \mid \mu \in \mathbb{C} \text{ is an eigenvalue of } \phi^* : H^2(X, \mathbb{C}) \to H^2(X, \mathbb{C})\}.$$

(ii) If Σ is a K3 surface, then there exists a complex number δ such that $\phi^*\omega_\Sigma = \delta\omega_\Sigma$ since $\phi^*\omega_\Sigma$ is again a nowhere vanishing holomorphic 2-form. This complex number δ is called the *determinant of ϕ*.

Remark 13.6. It is known as the Gromov–Yomdin theorem that the *topological entropy* of an automorphism ϕ of a compact Kähler manifold Σ of dimension n is given by the logarithm of the spectral radius of the induced homomorphism $\phi^* : \bigoplus_{i=0}^{2n} H^i(\Sigma, \mathbb{R}) \to \bigoplus_{i=0}^{2n} H^i(\Sigma, \mathbb{R})$, see [15, Theorem 2.1]. As a result, if Σ is a compact Kähler surface then the topological entropy is given by $\log d(\phi)$. By S. Cantat, it is shown that if a compact complex surface Σ admits an automorphism with positive entropy then Σ is a torus, a K3 surface, an Enriques surface, or a rational surface, see [12, Proposition 1].

Note that the determinant δ of a K3 surface automorphism ϕ lies on the unit circle $\mathbb{T}$ because we have

$$\langle \omega_\Sigma, \overline{\omega_\Sigma} \rangle = \langle \phi^*(\omega_\Sigma), \phi^*(\overline{\omega_\Sigma}) \rangle = \langle \delta \omega_\Sigma, \overline{\delta} \overline{\omega_\Sigma} \rangle = |\delta|^2 \langle \omega_\Sigma, \overline{\omega_\Sigma} \rangle$$

and $\langle \omega_\Sigma, \overline{\omega_\Sigma} \rangle > 0$ by the Riemann condition (44). The reason why δ is referred to as the determinant is that it coincides with the determinant of the complex derivative $D_p\phi : T_p\Sigma \to T_p\Sigma$ of ϕ at a fixed point p of ϕ if exists, see [25, Section 3]. It will turn out that the dynamical degree of a K3 surface automorphism is 1 or a Salem number. More precisely, we prove the following theorem.

Theorem 13.7. *Let ϕ be an automorphism of a K3 surface Σ with determinant $\delta \in \mathbb{T}$. Suppose that the dynamical degree β of ϕ is greater than* 1.

(i) *β is a Salem number of degree at most* 22*, and the characteristic polynomial F of ϕ^* is the product of the minimal polynomial S of β and a product C of cyclotomic polynomials (C can be* 1*).*

(ii) *Σ is projective if and only if δ is a root of C. Equivalently, Σ is nonprojective if and only if δ is a root of S.*

(iii) *ϕ^* is semisimple.*

This theorem is a consequence of ϕ^* being a Hodge isometry of $H^2(\Sigma, \mathbb{Z})$ with respect to ω_Σ that preserves the positive cone $\mathscr{C}_\Sigma^+$. We begin with the following lemma.

Lemma 13.8. *Let $F \in \mathbb{Z}[X]$ be a $*$-symmetric polynomial with coefficients in $\mathbb{Z}$.*

(i) *If every root of F has absolute value* 1 *then F is a product of cyclotomic polynomials.*

(ii) *If F has exactly one root β with $|\beta| > 1$ then β or $-\beta$ is a Salem number, and F is of the form $F = SC$ where S is the minimal polynomial of β and C is a product of cyclotomic polynomials.*

Proof. The assertion (i) follows from Kronecker's Theorem (see e.g. [17] for the proof): an algebraic integer whose all conjugates have absolute value 1 is a root of unity. We show the assertion (ii). Suppose that F has exactly one root β with $|\beta| > 1$. Since the constant term of F is 1 or -1, the number β is an algebraic unit. Furthermore β is a real number because its complex conjugate is also a root of F with absolute value greater than 1. Note that any root of F is accompanied by its inverse since F is $*$-symmetric. This implies that all roots of F other than β and β^{-1} lie on the unit circle $\mathbb{T}$. In particular, all conjugates of β (resp. $-\beta$) other than β and β^{-1} (resp. $-\beta$ and $-\beta^{-1}$) lie on $\mathbb{T}$. This means that the positive one of β and $-\beta$ is a Salem number. Let $S \in \mathbb{Z}[X]$ denote the minimal polynomial of β over $\mathbb{Q}$. Then F factors as $F = SC$ in $\mathbb{Z}[X]$, where $C \in \mathbb{Z}[X]$ is a monic polynomial. In this case, all roots of C lie on $\mathbb{T}$ since β and β^{-1} are roots of S. Furthermore, Lemma 7.3 (iv) shows that C is $*$-symmetric because S is $*$-symmetric by Proposition 13.2. Therefore C is a product of cyclotomic polynomials by the assertion (i). This complete the proof. □

Let (Λ, b) be a K3 lattice, and $\omega \in \Lambda_{\mathbb{C}} := \Lambda \otimes \mathbb{C}$ is a Hodge vector, i.e., satisfies $b(\omega, \omega) = 0$ and $b(\omega, \overline{\omega}) > 0$. We define subspaces $H^{2,0}, H^{1,1}, H^{0,2} \subset \Lambda_{\mathbb{C}}$ and the Picard lattice P as in the paragraph below Definition 12.12. Moreover, fix a positive cone $\mathscr{C}^+$ and Kähler cone $\mathscr{K}$. In the following, a Hodge isometry means a Hodge isometry with respect to ω.

Proposition 13.9. *Let t be a Hodge isometry of Λ with spectral radius greater than 1. If t preserves the positive cone $\mathscr{C}^+$ then the characteristic polynomial F of t can be expressed as $F = SC$, where S is a Salem polynomial and C is a product of cyclotomic polynomials (this factor can be 1). In particular, the spectral radius of t is a Salem number of degree at most 22.*

Proof. Note that F is a $*$-symmetric polynomial with coefficients in $\mathbb{Z}$ since t is a lattice isometry. Since the spectral radius of t is greater than 1, the polynomial F has at least one root β with $|\beta| > 1$. Let $\delta \in \mathbb{T}$ be the eigenvalue of t corresponding to the Hodge vector ω. Then F decomposes in $\mathbb{R}[X]$ as $F(X) = G(X)(X^2 - (\delta + \delta^{-1})X + 1)$, where $G(X) \in \mathbb{R}[X]$. The factor G is the characteristic polynomial of $t|_{H^{1,1}_{\mathbb{R}}}$, and β is a root of G. Since $H^{1,1}_{\mathbb{R}}$ is of signature $(1, 19)$, Theorem 7.26 shows that β is the only root with $|\beta| > 1$ of G, and hence of F. Thus, it follows from Lemma 13.8 that β or $-\beta$ is a Salem number, and F can be expressed as $F = SC$, where S is the minimal polynomial of β and C is a product of cyclotomic polynomials. It remains to show that β is positive. Suppose that t preserves the positive cone $\mathscr{C}^+$, and let $v \in H^{1,1}_{\mathbb{R}}$ be an eigenvector of t corresponding to β. We have $b(v, v) = 0$ because $b(v, v) = b(tv, tv) = \beta^2 b(v, v)$. So we can assume that v lies on the closure $\overline{\mathscr{C}^+}$ (in fact on the boundary) of $\mathscr{C}^+$ by considering $-v$ instead of v if necessary. Then β must be positive since $t(\overline{\mathscr{C}^+}) = \overline{\mathscr{C}^+}$. This completes the proof. □

The submodule

$$T := P^{\perp} \subset \Lambda$$

is called the *trancendental lattice* of Λ. It can be degenerate as well as the Picard lattice P.

Lemma 13.10. *The trancendental lattice T is the minimum primitive submodule in Λ such that its $\mathbb{C}$-span $\mathbb{C}T \subset \Lambda_{\mathbb{C}}$ contains $H^{2,0}$.*

Proof. Primitivity of T follows from Corollary 12.2. Since $P \subset H^{1,1}$ we have

$$\mathbb{C}T = \mathbb{C} \cdot P^{\perp} = (\mathbb{C}P)^{\perp} \supset (H^{1,1})^{\perp} \supset H^{2,0}.$$

Let T' be a primitive submodule in Λ such that $H^{2,0} \subset \mathbb{C}T'$. We show that $(T')^{\perp} \subset P$. Let $x \in \Lambda$ be orthogonal to T'. Then x is orthogonal to $H^{2,0}$, that is, $b(x, \omega) = 0$. Furthermore $b(x, \overline{\omega}) = \overline{b(\overline{x}, \omega)} = \overline{b(x, \omega)} = 0$. Thus x belongs to $(H^{2,0} \oplus H^{0,2})^{\perp} = H^{1,1}$, and to $P = \Lambda \cap H^{1,1}$. This means that $(T')^{\perp} \subset P$. Therefore $T = P^{\perp} \subset (T')^{\perp\perp} = T'$ (in Λ), where the last equality follows from Proposition 12.2 since T' is primitive. This completes the proof. □

Lemma 13.11. *Let t be a Hodge isometry of Λ and $\delta \in \mathbb{T}$ the eigenvalue of t corresponding to ω. Let g be the minimal polynomial of δ over $\mathbb{Q}$. Then*

$$\mathbb{R}T \subset \{x \in \Lambda_{\mathbb{R}} \mid g(t).x = 0\}. \tag{45}$$

Moreover, the equality holds if δ has multiplicity 1 as an eigenvalue of t.

Proof. Put $T' = \{x \in \Lambda \mid g(t).x = 0\}$. Since g is with coefficients in $\mathbb{Q}$, for any subfield K of $\mathbb{C}$ we have

$$KT' = \{x \in \Lambda_K \mid g(t).x = 0\}. \tag{$*$}$$

We first show that $T \subset T'$. Since T' can be expressed as $T' = \Lambda \cap \mathbb{Q}T'$ by $(*)$, it is primitive. Moreover $\mathbb{C}T' = \{x \in \Lambda_{\mathbb{C}} \mid g(t).x = 0\}$, and hence $\mathbb{C}T'$ contains the subspace $\mathbb{C}\omega = H^{2,0}$ since

ω is an eigenvector of t corresponding to the eigenvalue δ. Thus, it follows from Lemma 13.10 that $T \subset T'$. Hence we obtain $\mathbb{R}T \subset \mathbb{R}T' = \{x \in \Lambda_{\mathbb{R}} \mid g(t).x = 0\}$ by $(*)$.

Suppose then that δ has multiplicity 1 as an eigenvalue of t. Let $L \subset \mathbb{C}$ be the Galois closure of $\mathbb{Q}(\delta)/\mathbb{Q}$. Note that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ acts on $\Lambda_L \subset \Lambda_{\mathbb{C}}$ naturally. We have $LT' = \{x \in \Lambda_L \mid g(t).x = 0\} = \sum_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} L\sigma(\omega)$ by the assumption that δ has multiplicity 1. On the other hand, the vector ω belongs to $\mathbb{C}T$ by Lemma 13.10, and we can assume that $\omega \in LT$ since $\delta \in L$. Then $\sigma(\omega) \in \sigma(LT) = L\sigma(T) = LT$ for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, which implies that $LT' = \sum_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} L\sigma(\omega) \subset LT$. Therefore $T' = \Lambda \cap LT' \subset \Lambda \cap LT = T$, and $\{x \in \Lambda_{\mathbb{R}} \mid g(t).x = 0\} = \mathbb{R}T' \subset \mathbb{R}T$. This shows that the equality holds in (45). □

Proposition 13.12. *Let t be a Hodge isometry of Λ that preserves the positive cone $\mathscr{C}^+$, and let $\delta \in \mathbb{T}$ be the eigenvalue of t corresponding to ω. Suppose that the spectral radius β of t is greater than 1. Then β is a Salem number, and the characteristic polynomial F of t is the product of the minimal polynomial S of β and a product C of cyclotomic polynomial by Proposition 13.9.*

(i) *If δ is a root of C then P is nondegenerate and has signature $(1, \mathrm{rk}(P) - 1)$.*

(ii) *If δ is a root of S then P is nondegenerate and has signature $(0, 22 - \deg(S))$. Moreover $\mathbb{R}T = \{x \in \Lambda_{\mathbb{R}} \mid S(t).x = 0\}$.*

(iii) *t is semisimple.*

Proof. Put $V = \Lambda_{\mathbb{R}}$, and define $V(f;t) := \{x \in V \mid f(t)^N.x = 0 \text{ for some } N \in \mathbb{Z}_{\geq 0}\}$ for a factor f of F. Then $V = V(S;t) \oplus V(C;t)$, which is an orthogonal direct sum decomposition, see §7.2. Put $d_S = \deg(S)$ and $d_C = \deg(C)$. Since the signature of V is $(3, 19)$, Proposition 7.24 implies that those of the subspaces $V(S;t)$ and $V(C;t)$ are $(1, d_S - 1)$ and $(2, d_C - 2)$; or $(3, d_S - 3)$ and $(0, d_C)$. Let $g \in \mathbb{Z}[X]$ be the minimal polynomial of δ over $\mathbb{Q}$.

(i). Suppose that δ is a root of C. Then C is divisible by g, and Lemma 13.11 implies that $\mathbb{R}T \subset V(C;t)$. In this case, the signature of $V(C;t)$ is $(2, d_C - 2)$ since $V(C;t)$ contains $V(X^2 - (\delta + \delta^{-1})X + 1;t)$, the real part of $H^{2,0} \oplus H^{0,2}$. The inclusion $\mathbb{R}T \subset V(C;t)$ yields $\mathbb{R}P = (\mathbb{R}T)^{\perp} \supset V(C;t)^{\perp} = V(S;t)$, and the signature of $V(S;t)$ is $(1, d_S - 1)$ since that of $V(C;t)$ is $(2, d_C - 2)$. This shows that P is nondegenerate and has signature $(1, \mathrm{rk}(P) - 1)$.

(ii). Suppose that δ is a root of S. Then $g = S$, and Lemma 13.11 implies that $\mathbb{R}T = \{x \in V \mid S(t).x = 0\}$ since δ is a simple root of F. In this case, the signature of $V(S;t)$ is $(3, d_S - 3)$, and that of the orthogonal complement $(\mathbb{R}T)^{\perp} = \mathbb{R}P$ is $(0, 22 - d_S)$. This completes the proof of the assertion (ii).

(iii). Note that any isometry of an inner product space over $\mathbb{R}$ of definite signature is semisimple. Suppose first that δ is a root of S. Then the subspace $V(C;t)$ is negative definite by (ii). Thus $t|_{V(C;t)}$ is semisimple. Furthermore $t|_{V(S;t)}$ is also semisimple since S has multiplicity 1 in F. Therefore $t : V \to V$ is semisimple.

Suppose then that δ is a root of C. Then, the Picard lattice P is nondegenerate and has signature $(1, \mathrm{rk}(P) - 1)$ by (i), and V decomposes as $V = \mathbb{R}P \oplus \mathbb{R}T$ (orthogonal direct sum). The subspace $\mathbb{R}P$ decomposes as $\mathbb{R}P = V(S;t) \oplus U$, where U is the orthogonal complement of $V(S;t)$ in $\mathbb{R}P$. Since $V(S;t)$ is of signature $(1, d_S - 1)$, the complement U is negative define. Thus $\phi|_{\mathbb{R}P}$ is semisimple as in the nonprojective case. Moreover $t|_{\mathbb{R}T}$ is also semisimple because Lemma 13.11 shows that $\mathbb{R}T$ is a subspace of the space $\{x \in V \mid g(t).x = 0\}$, on which t acts semisimply. Therefore $t : V \to V$ is semisimple. The proof is complete. □

Proof of Theorem 13.7. Let ϕ be an automorphism of a K3 surface Σ with determinant $\delta \in \mathbb{T}$, and suppose that the dynamical degree β of ϕ is greater than 1. Then $\phi^* : H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma, \mathbb{Z})$ is a Hodge isometry with respect to $\omega_\Sigma \in H^2(\Sigma, \mathbb{C})$ which preserves the positive cone $\mathscr{C}_\Sigma^+$ (in fact it preserves the Kähler cone $\mathscr{K}_\Sigma$). Thus Proposition 13.9 shows the assertion (i). Moreover,

the assertion (ii) follows from Corollary 12.7 and Proposition 13.12 (i), (ii). The assertion (iii) follows from Proposition 13.12 (iii). □

13.3 Nonprojective realizability

Definition 13.13. We use the following terminology focusing on the case of K3 surfaces.

(i) We refer to a polynomial $F(X) \in \mathbb{Z}[X]$ of degree 22 as a *complemented Salem polynomial* if F can be expressed as $F(X) = S(X)C(X)$, where $S(X)$ is a Salem polynomial and $C(X)$ is a product of cyclotomic polynomials. In this case, S is called the *Salem factor* of F.

(ii) A Salem number β is *projectively* (resp. *nonprojectively*) *realizable* if there exists an automorphism of a projective (resp. nonprojective) K3 surface with dynamical degree β.

Theorem 13.7 (i) shows that a realizable Salem number has degree at most 22, and moreover, Theorem 13.7 (ii) implies that if a Salem number β is projectively realizable then $\deg(\beta) \leq 20$; and if β is nonprojectively realizable then $\deg(\beta) \geq 4$. This subsection is devoted to proving the following theorem, which is the main theorem of this chapter.

Theorem 13.14. *Let β be a Salem number of degree d with $4 \leq d \leq 22$, and S its minimal polynomial. Let $\mathcal{C}_{10}$ and $\mathcal{C}_{18}$ be the sets consisting of integers defined by*

$$\mathcal{C}_{10} := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 21, 22, 24, 28, 30, 36, 42\},$$
$$\mathcal{C}_{18} := \{1, 2, 3, 4, 6, 12\}.$$

(i) *Suppose that $d = 22$. Then β is nonprojectively realizable if and only if $|S(1)|$ and $|S(-1)|$ are squares.*

(ii) *Suppose that $d = 4, 6, 8, 12, 14, 16$, or 20. Then β is nonprojectively realizable.*

(iii) *Suppose that $d = 10$ or 18. Then β is nonprojectively realizable if and only if there exists $l \in \mathcal{C}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$. Here Φ_l is the l-th cyclotomic polynomial and the set $\Pi(S, \Phi_l)$ is defined in Notation 10.2.*

Remark 13.15. The question of which Salem number is realizable has been considered since the appearance of the paper [18] by B.H. Gross and C.T. McMullen. They proved in [18] that a Salem number of degree 22 is nonprojectively realizable if $|S(1)| = |S(-1)| = 1$, where S is the corresponding Salem polynomial, and speculated that the assertion (i) of Theorem 13.14 holds. The proof of (i) was given by E. Bayer-Fluckiger and L. Taelman in [3] for the first time. The assertion (ii) was proved by Bayer-Fluckiger [6, 7] for $d = 4, 6, 8, 12, 14$, and 16 and by the author [45] for $d = 20$, see also Remark 9.26. In this thesis, we give the proof of Theorem 13.14 in a consistent way.

In order to prove Theorem 13.14, we use results established in Chapter III, in particular §§9, 10, and 11. Note that every complemented Salem polynomial is $*$-symmetric and satisfies the condition $(\mathrm{Sign})_{3,19}$. Let $F = SC$ be a complemented Salem polynomial with Salem factor S. For a root δ of S with $|\delta| = 1$, we define the index map $\mathfrak{i}_\delta \in \mathrm{Idx}(3, 19; F)$ by

$$\mathfrak{i}_\delta = \begin{cases} 2 & \text{if } f(X) = X^2 - (\delta + \delta^{-1})X + 1 \\ -\deg(f^{m_f}) & \text{if } f(X) \neq X^2 - (\delta + \delta^{-1})X + 1 \end{cases} \quad \text{for } f \in I(F; \mathbb{R}).$$

The following proposition is a reason why the nonprojective case is more tractable than the projective case. Roughly speaking, in the nonprojective case, we do not need to take care of the condition of preserving the Kähler cone in Theorem 12.13 when considering only the dynamical degree.

Proposition 13.16. *Let β be a Salem number with $4 \leq \deg \beta \leq 22$, and S its minimal polynomial. The following are equivalent:*

(i) *β is nonprojectively realizable.*

(ii) *There exists a conjugate δ of β with $|\delta| = 1$ and a complemented Salem polynomial F with Salem factor S such that a K3 lattice admits a semisimple (F, i_δ)-isometry.*

(iii) *There exists a conjugate δ of β with $|\delta| = 1$ and a complemented Salem polynomial F with Salem factor S such that it satisfies* (Square) *and the obstruction map for (F, i_δ) vanishes.*

(iv) *For any conjugate δ of β with $|\delta| = 1$, there exists a complemented Salem polynomial F with Salem factor S such that it satisfies* (Square) *and the obstruction map for (F, i_δ) vanishes.*

(v) *For any conjugate δ of β with $|\delta| = 1$, there exists a complemented Salem polynomial F with Salem factor S such that a K3 lattice admits a semisimple (F, i_δ)-isometry.*

Proof. Let us prove that

$$\text{(i)} \Leftrightarrow \text{(ii)} \quad \text{and} \quad \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(iv)} \Rightarrow \text{(v)} \Rightarrow \text{(ii)}.$$

(i) $\Rightarrow$ (ii). Suppose that β is nonprojectively realizable, and let ϕ be an automorphism of a nonprojective K3 surface Σ with dynamical degree β. Then, the induced homomorphism ϕ^* is is an isometry of the K3 lattice $H^2(\Sigma, \mathbb{Z})$. Let $\delta \in \mathbb{T}$ be the determinant of ϕ. Theorem 13.7 implies that the characteristic polynomial of ϕ^*, say F, is a complemented Salem polynomial with Salem factor S; δ is a conjugate of β since Σ is nonprojective; and $\phi^* : H^2(\Sigma, \mathbb{Z}) \to H^2(\Sigma, \mathbb{Z})$ is a semisimple (F, i_δ)-isometry. This means that (ii) holds.

(ii) $\Rightarrow$ (i). Let δ be a conjugate of β with $|\delta| = 1$, and F a complemented Salem polynomial F with Salem factor S. Suppose that a K3 lattice Λ admits a semisimple (F, i_δ)-isometry t. Let $\omega \in \Lambda_{\mathbb{C}} := \Lambda \otimes \mathbb{C}$ be an eigenvector of t corresponding to β. Since the index of t is i_δ, we have $b(\omega, \omega) = 0$ and $b(\omega, \overline{\omega}) > 0$, where b is extended on $\Lambda_{\mathbb{C}}$ linearly. This means that ω is a Hodge vector, and t is an Hodge isometry with respect to ω. Let us fix a positive cone $\mathscr{C}^+$ and Kähler cone $\mathscr{K}$ for Λ. Then $t(\mathscr{C}^+) = \mathscr{C}^+$ or $t(\mathscr{C}^+) = -\mathscr{C}^+$ since t is an isometry, and we have the former case because an eigenvector of t corresponding to the positive real eigenvalue β lies on the boundary of $\mathscr{C}^+$. Thus t sends the Kähler cone $\mathscr{K}$ to another chamber $\mathscr{K}'$ in $\mathscr{C}^+$. let $\mathscr{W}$ be the Weyl group determined by ω. Then, there exists $w \in \mathscr{W}$ such that $w(\mathscr{K}') = \mathscr{K}$ by Theorem 12.3. Put $\widetilde{t} = w \circ t$. Then $\widetilde{t}$ is a Hodge isometry of Λ with respect to ω that preserves $\mathscr{K}$ as in the discussion above Theorem 12.13.

So, by Theorem 12.13, it is sufficient to show that the spectral radius of $\widetilde{t}$ remains β. Let P and T be the Picard lattice and trancendental lattice of Λ (with respect to ω). Since t is a Hodge isometry preserving $\mathscr{C}^+$, the Picard lattice P is nondegenerate and negative definite by Proposition 13.12 (ii). In particular, we have the orthogonal direct sum decomposition $\Lambda_{\mathbb{R}} = \mathbb{R}P \oplus \mathbb{R}T$. Since any isometry in $\mathscr{W}$ acts on $\mathbb{R}T$ as identity, we can write $\widetilde{t}|_{\Lambda_{\mathbb{R}}} = (t|_{\mathbb{R}P} \circ w|_{\mathbb{R}P}) \oplus t|_{\mathbb{R}T}$. The characteristic polynomial of $t|_{\mathbb{R}T}$ is S because $\mathbb{R}T = \{x \in \Lambda_{\mathbb{R}} \mid S(t).x = 0\}$ by Proposition 13.12 (ii). On the other hand, that of $t|_{\mathbb{R}P} \circ w|_{\mathbb{R}P}$ is a product of cyclotomic polynomial polynomial since P is negative definite. Therefore, the characteristic polynomial of $\widetilde{t}$ is a complemented Salem polynomial with Salem factor S, and the spectral radius of $\widetilde{t}$ is equal to β. This completes the proof of (ii) $\Rightarrow$ (i).

The implications (ii) $\Rightarrow$ (iii) and (iv) $\Rightarrow$ (v) follow from Theorem 9.25. Furthermore (v) $\Rightarrow$ (ii) is obvious. So it remains to prove (iii) $\Rightarrow$ (iv). Let δ' be a conjugate of β with $|\delta'| = 1$, and suppose that there exists a complemented Salem polynomial F with Salem factor S such that

it satisfies (Square) and the obstruction map for $(F, \mathrm{i}_{\delta'})$ vanishes. Let δ be another conjugate of β with $|\delta| = 1$. Then, Theorem 10.15 shows that the obstruction map for (F, i_δ) is also zero because $\eta_\infty(\mathrm{i}_\delta) = \eta_\infty(\mathrm{i}_{\delta'})$. This completes the proof. □

In the following, β is a Salem number of degree d with $4 \leq d \leq 22$, and S is its minimal polynomial. Furthermore, we fix a conjugate δ of β with $|\delta| = 1$. Let us begin with the case $d = 22$.

Theorem 13.17. *Suppose that $d = 22$. Then β is nonprojectively realizable if and only if $|S(1)|$ and $|S(-1)|$ are squares.*

Proof. Suppose that β is nonprojectively realizable, and let ϕ be an automorphism of a nonprojective K3 surface Σ with dynamical degree β. Then S is the characteristic polynomial of the semisimple isometry ϕ^* on the K3 lattice $H^2(\Sigma, \mathbb{Z})$. Hence S satisfies the condition (Square) by Proposition 9.1, and in particular $|S(1)|$ and $|S(-1)|$ are squares. Suppose conversely that $|S(1)|$ and $|S(-1)|$ are squares. Then S satisfies (Square) by Lemma 13.4 (ii). Since S is irreducible, Theorem 9.27 implies that a K3 lattice admits a semisimple (F, i_δ)-isometry. Therefore β is nonprojectively realizable by Proposition 13.16. □

The case $d = 20$ is as follows.

Theorem 13.18. *If $d = 20$ then β is nonprojectively realizable.*

Proof. Put $F(X) = (X-1)(X+1)S(X)$. Then F is a complemented Salem polynomial with the condition (Square) clearly, and the obstruction map for (F, i_δ) vanishes by Theorem 9.28. Hence β is nonprojectively realizable by Proposition 13.16. □

We proceed to the case $d \leq 18$.

Theorem 13.19. *Suppose that $d \leq 18$. If S does not satisfy the condition* (Square) *then β is nonprojectively realizable. In particular, if $d = 4, 8, 12,$ or 16 then β is nonprojectively realizable.*

Proof. Suppose first that $|S(1)|$ is not a square. Put $F(X) = (X-1)^{21-d}(X+1)S(X)$. Then F is a complemented Salem polynomial with the condition (Square). Since the multiplicity of $X-1$ in F, $21-d$, is greater than 3, Proposition 10.5 (i) implies that $\Pi^F_{\mathrm{i}_\delta}(S, X-1)$ is not empty. Thus, the obstruction group for (F, i_δ) is generated by $\mathbf{1}_{\{S, X-1\}}$ and $\mathbf{1}_{\{X+1\}}$. Now, let $\{b_v\}_{v \in \mathcal{V}}$ be a family in $\mathcal{B}_{\mathrm{i}_\delta}$, where $\mathcal{B}_{\mathrm{i}_\delta}$ is defined in Notation 9.4. Since the multiplicity of $X+1$ in F is 1, we have

$$\eta(\{b_v\}_v) \cdot \mathbf{1}_{\{X+1\}} = \eta(\{b_v\}_v)(X+1) = \sum_{v \in \mathcal{V}} \mathrm{hw}_v(b_v|_{M_v^-}) = 0$$

where we use notation in §9. Moreover

$$\eta(\{b_v\}_v) \cdot \mathbf{1}_{\{S, X-1\}} = \eta(\{b_v\}_v) \cdot \mathbf{1}_{\{S, X-1\}} + \eta(\{b_v\}_v) \cdot \mathbf{1}_{\{X+1\}} = \eta(\{b_v\}_v) \cdot \mathbf{1}_{\{S, X-1, X+1\}} = 0,$$

where the last equation is by Proposition 9.23. These mean that the obstruction map for (F, i_δ) vanishes. Hence β is nonprojectively realizable by Proposition 13.16. Similarly, if $|S(-1)|$ is not a square then it can be checked that β is nonprojectively realizable by putting $F(X) = (X-1)(X+1)^{21-d}S(X)$.

Suppose then that $|S(1)|$ and $|S(-1)|$ are squares but $(-1)^{d/2}S(1)S(-1)$ is not a square. In this case, we put $F(X) = (X-1)^{22-d}S(X)$. This is a complemented Salem polynomial with the condition (Square). Since $(-1)^{d/2}S(1)S(-1) = -1$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and $22 - d \geq 3$, Proposition 10.5 (iii) implies that $\Pi^F_{\mathrm{i}_\delta}(S, X-1)$ contains 2 and is not empty. This means that the equivalence

Table 13.1: Integers l with $\varphi(l) \leq 12$

$\varphi(l)$	l
1	$1, 2$
2	$3, 4, 6$
4	$5, 8, 10, 12$
6	$7, 9, 14, 18$
8	$15, 16, 20, 24, 30$
10	$11, 22$
12	$21, 28, 36, 42$

relation on $I(F;\mathbb{Q}) = \{X-1, S\}$ defined by $(F, \mathfrak{i}_\delta)$ is weakest. So β is nonprojectively realizable by Theorem 9.27 and Proposition 13.16.

Therefore, if S does not satisfy the condition (Square) then β is nonprojectively realizable. In particular, if $d = 4, 8, 12$, or 16 then S does not satisfy (Square) by Lemma 13.4 (i), and β is nonprojectively realizable. □

Remark 13.20. In the proof of Theorem 13.19, the complemented Salem polynomial F can be chosen in a different way. For example, put $F(X) = (X-1)^{(22-d)/2}(X-1)^{(22-d)/2}S(X)$. If $d \leq 16$ then one can show that the equivalence relation on $I(F;\mathbb{Q}) = \{X-1, X+1, S\}$ defined by $(F, \mathfrak{i}_\delta)$ is weakest, and conclude that β is nonprojectively realizable.

Theorem 13.21. *If $d = 6$ or 14, then β is nonprojectively realizable.*

Proof. If S does not satisfy (Square) then we are done by Theorem 13.19. Suppose that S satisfies (Square), and let Λ_S and Λ_C denote even unimodular lattices of signature $(3, d-3)$ and $(0, 22-d)$ respectively. Such lattices exist by Theorem 5.25. Note that S satisfies $(\mathrm{Sign})_{3,d-3}$. We define the index map $\mathfrak{j}_\delta \in \mathrm{Idx}(3, d-3; S)$ by

$$\mathfrak{j}_\delta(f) = \begin{cases} 2 & \text{if } f(X) = X^2 - (\delta + \delta^{-1})X + 1 \\ -2 & \text{if } f(X) \neq X^2 - (\delta + \delta^{-1})X + 1 \end{cases} \quad \text{for } f \in I(S;\mathbb{R}).$$

Since S is irreducible, Theorem 9.27 implies that Λ_S has a semisimple $(S, \mathfrak{j}_\delta)$-isometry t_S. Let t be the isometry of the K3 lattice $\Lambda_S \oplus \Lambda_C$ defined by $t := t_S \oplus \mathrm{id}_{\Lambda_C}$. Then t is a semisimple $(S(X)(X-1)^{22-d}, \mathfrak{i}_\delta)$-isometry by its construction. Therefore β is nonprojectively realizable by Proposition 13.16. □

The cases $d = 10$ and 18 are more complicated. For $d = 10$ or 18, let $\widetilde{\mathcal{C}}_d$ denote the set of integers $l \geq 1$ such that $\varphi(l) < 22-d$, or $\varphi(l) = 22-d$ and Φ_l satisfies (Square). Integers l with $\varphi(l) \leq 12$ are listed in Table 13.1.

Lemma 13.22. *Suppose that $d = 10$ or 18, and let $F = SC$ be a complemented Salem polynomial with Salem factor S. Suppose that F and S satisfies the condition* (Square)*. Then C is also satisfies* (Square)*, and any irreducible factor of C can be written as Φ_l for some $l \in \widetilde{\mathcal{C}}_d$.*

Proof. It follows from Lemma 9.2 (i) that C is satisfies (Square). Let Φ_l be an irreducible factor of C, where $l \in \mathbb{Z}_{>0}$. Then $\varphi(l) = \deg(\Phi_l) \leq \deg(C) = 22-d$. Moreover, if $\varphi(l) = 22-d$ then $\Phi_l = C$, and it satisfies (Square). This completes the proof. □

Put $\mathcal{C}_{10} = \widetilde{\mathcal{C}}_{10} \setminus \{20\}$ and $\mathcal{C}_{18} = \widetilde{\mathcal{C}}_{18}$. These sets can be expressed explicitly as

$$\mathcal{C}_{10} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 21, 22, 24, 28, 30, 36, 42\},$$
$$\mathcal{C}_{18} = \{1, 2, 3, 4, 6, 12\},$$

as defined in Theorem 13.14.

Proposition 13.23. *Suppose that $d = 10$ or 18. If β is nonprojectively realizable then there exists $l \in \mathcal{C}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$.*

Proof. If S does not satisfy (Square), then $\Pi(S, \Phi_1) \neq \emptyset$ or $\Pi(S, \Phi_2) \neq \emptyset$ by Proposition 10.5, and we are done. So we assume that S satisfies (Square). Suppose that β is nonprojectively realizable. Then, by Proposition 13.16, there exists a complemented Salem polynomial $F = SC$ with the condition (Square) such that the obstruction map $\mathrm{ob}_{\mathfrak{i}_\delta}$ for $(F, \mathfrak{i}_\delta)$ is zero. We remark that C satisfies (Square), and any irreducible factor of C can be written as Φ_l for some $l \in \widetilde{\mathcal{C}}_d$ by Lemma 13.22.

Let Λ_S and Λ_C be even unimodular lattices of signature $(d/2, d/2)$ and $((22-d)/2, (22-d)/2)$ respectively. Let $\mathfrak{j}_S \in \mathrm{Idx}(d/2, d/2; S)$ be an index map. Then Λ_S admits a semisimple $(S, \mathfrak{j}_S)$-isometry t_S by Theorem 9.27 since S is irreducible. On the other hand, Theorem 11.10 shows that there exists $\mathfrak{j}_C \in \mathrm{Idx}((22-d)/2, (22-d)/2; F)$ with

$$\mathfrak{j}_C(X-1) \equiv \mathfrak{i}_\delta(X-1) \text{ and } \mathfrak{j}_C(X+1) \equiv \mathfrak{i}_\delta(X+1) \bmod 4 \qquad (*)$$

such that Λ_C admits a semisimple $(C, \mathfrak{j}_C)$-isometry t_C. Then $t := t_S \oplus t_C$ is a semisimple $(F, \mathfrak{j})$-isometry on the even unimodular lattice $\Lambda_S \oplus \Lambda_C$, where $\mathfrak{j} := \mathfrak{j}_S \oplus \mathfrak{j}_C \in \mathrm{Idx}(11, 11; F)$. In particular, the obstruction map $\mathrm{ob}_{\mathfrak{j}}$ for $(F, \mathfrak{j})$ vanishes. Note that the equivalence relation on $I(F; \mathbb{Q})$ defined by $(F, \mathfrak{j})$ is the same as the one defined by $(F, \mathfrak{i}_\delta)$ because of the relation $(*)$. Let $\sim$ denote the equivalence relation on $I(F; \mathbb{Q})$, and Ω the obstruction group.

Now, suppose that $\Pi(S, \Phi_l)$ were empty for all $l \in \widetilde{\mathcal{C}}_d$. Then $\{S\} \subset I(F; \mathbb{Q})$ forms an equivalence class with respect to $\sim$, since any irreducible factor of C can be written as Φ_l for some $l \in \widetilde{\mathcal{C}}_d$. This would mean that $\mathbf{1}_{\{S\}}$ belongs to Ω. On the other hand, a calculation yields

$$(\eta_\infty(\mathfrak{i}_\delta) - \eta_\infty(\mathfrak{j})) \cdot \mathbf{1}_{\{S\}} = 1 - 0 = 1 \quad (\text{in } \mathbb{Z}/2\mathbb{Z}).$$

This contradicts Theorem 10.15 since $\mathrm{ob}_{\mathfrak{i}_\delta}$ and $\mathrm{ob}_{\mathfrak{j}}$ are zero. Therefore, there exists $l \in \widetilde{\mathcal{C}}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$. This complete the proof of the case $d = 18$ since $\mathcal{C}_{18} = \widetilde{\mathcal{C}}_{18}$.

Suppose that $d = 10$. It remains to prove that the following case does not occur: 20 is the only integer in $\widetilde{\mathcal{C}}_{10}$ such that $\Pi(S, \Phi_{20}) \neq \emptyset$. Suppose that this case occurred. Then C must be divisible by Φ_{20} by the same reason as above, and F can be expressed as $F = S\Phi_{20}C'$, where C' is the remaining factor of C. Note that $\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$ satisfies (Square), and we may assume that $\mathfrak{j}(\Phi_{20}) = 0$. Because $S\Phi_{20}$ has degree 18 and satisfies (Square), any factor of C' can be written as Φ_l for some $l \in \mathcal{C}_{18}$ by the same reason as Lemma 13.22. By using Theorem 10.9, it can be checked that $\Pi(\Phi_{20}, \Phi_l) = \emptyset$ for all $l \in \mathcal{C}_{18}$. This would mean that $\{S, \Phi_{20}\} \subset I(F; \mathbb{Q})$ forms an equivalence class with respect to $\sim$, and $\mathbf{1}_{\{S, \Phi_{20}\}} \in \Omega$. On the other hand, we have

$$\begin{aligned}(\eta_\infty(\mathfrak{i}_\delta) - \eta_\infty(\mathfrak{j})) \cdot \mathbf{1}_{\{S, \Phi_{20}\}} &= \eta_\infty(\mathfrak{i}_\delta)(S) - \eta_\infty(\mathfrak{j})(S) + \eta_\infty(\mathfrak{i}_\delta)(\Phi_{20}) - \eta_\infty(\mathfrak{j})(\Phi_{20}) \\ &= 1 - 0 + 0 - 0 \\ &= 1.\end{aligned}$$

However, this contradicts Theorem 10.15. Hence, there exists $l \in \mathcal{C}_{10} = \widetilde{\mathcal{C}}_{10} \setminus \{20\}$ such that $\Pi(S, \Phi_l) \neq \emptyset$. This completes the proof. □

Proposition 13.24. *Suppose that $d = 10$ or 18. If there exists $l \in \mathcal{C}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$ then β is nonprojectively realizable.*

Proof. If S does not satisfy (Square) then β is nonprojectively realizable by Theorem 13.19. So we assume that S satisfies (Square). Suppose that there exists $l \in \mathcal{C}_d$ such that $\Pi(S, \Phi_l) \neq \emptyset$.

Case $d = 18$. We define a complemented Salem polynomial F as

$$F(X) = \begin{cases} S(X)\Phi_l(X)^4 & \text{if } l = 1, 2 \\ S(X)\Phi_l(X)^2 & \text{if } l = 3, 4, 6 \\ S(X)\Phi_l(X) & \text{if } l = 12. \end{cases}$$

Then F satisfies (Square), and $\Pi^F_{\mathrm{i}_\delta}(S, \Phi_l) = \Pi(S, \Phi_l) \neq \emptyset$. Thus, the equivalence relation on $I(F; \mathbb{Q}) = \{S, \Phi_l\}$ defined by (F, i_δ) is weakest, and hence β is nonprojectively realizable by Theorem 9.27 and Proposition 13.16.

Case $d = 10$. We define a complemented Salem polynomial F as

$$F(X) = \begin{cases} S(X)\Phi_l(X)^{12/\varphi(l)} & \text{if } \varphi(l) = 1, 2, 6, 12 \\ S(X)\Phi_l(X)(X-1)^4(X+1)^4 & \text{if } \varphi(l) = 4 \text{ but } l \neq 12, \text{ i.e., } l = 5, 8, 10 \\ S(X)\Phi_{12}(X)^3 & \text{if } l = 12 \\ S(X)\Phi_l(X)\Phi_3(X)^2 & \text{if } l = 15, 24 \\ S(X)\Phi_{16}(X)(X-1)^4 & \text{if } l = 16 \\ S(X)\Phi_{30}(X)\Phi_6(X)^2 & \text{if } l = 30 \\ S(X)\Phi_{11}(X)(X-1)^2 & \text{if } l = 11 \\ S(X)\Phi_{22}(X)(X+1)^2 & \text{if } l = 22. \end{cases}.$$

Then F satisfies (Square), and it can be checked that the equivalence relation on $I(F; \mathbb{Q})$ defined by (F, i_δ) is weakest by using Theorem 10.9. Hence, we conclude that β is nonprojectively realizable by Theorem 9.27 and Proposition 13.16. □

Proof of Theorem 13.14. Assertion (i) is proved in Theorem 13.17. Assertion (ii) follows from Theorem 13.18 if $d = 20$, Theorem 13.19 if $d = 4, 8, 12, 16$, and Theorem 13.21 if $d = 6, 14$. Assertion (iii) is a consequence of Propositions 13.23 and 13.24. □

Example 13.25. Let $\beta_{10} \approx 1.17628$ be the smallest Salem number of degree 10, that is, Lehmer's number. Its minimal polynomial S is given by

$$S(X) = 1 + X - X^3 - X^4 - X^5 - X^6 - X^7 + X^9 + X^{10}.$$

Let us check that β_{10} is nonprojectively realizable. The factorizations $S(X)$ and $\Phi_4(X)$ into irreducible factors modulo 3 are given as

$$\begin{aligned} S(X) \bmod 3 &= (1 + X^2)(1 + X + 2X^2 + X^3 + X^5 + 2X^6 + X^7 + X^8), \\ \Phi_4(X) \bmod 3 &= 1 + X^2 \end{aligned}$$

in $\mathbb{F}_3[X]$. In particular $\Phi_4(X) = 1 + X^2$ over $\mathbb{Q}_3$, and $\overline{I(\Phi_4; \mathbb{Q}_3)} = \{1 + X^2\}$. Moreover, Hensel's lemma (Theorem 1.33) implies that there is an irreducible factor $f \in \mathbb{Z}_3[X]$ of S over $\mathbb{Q}_3$ such that $f(X) \bmod 3 = 1 + X^2$. This factor f must be $*$-symmetric, because otherwise $\underline{f(X)f^*}(X) \bmod 3 = (1 + X^2)^2$ would divide $S \bmod 3$ in $\mathbb{F}_3[X]$. This means that $1 + X^2 \in \overline{I(S; \mathbb{Q}_3)}$, and $3 \in \Pi(S, \Phi_4)$. Hence β_{10} is nonprojectively realizable by Theorem 13.14 (iii). The proof of this fact was given by McMullen [27] for the first time, and it is different from the proof here.

Example 13.26 ([7, Example 22.3]). Let $\beta_{18} \approx 1.18837$ be the smallest Salem number of degree 18. Its minimal polynomial S is given by

$$\begin{aligned} S(X) = 1 - X + X^2 - X^3 - X^6 + X^7 - X^8 + X^9 \\ - X^{10} + X^{11} - X^{12} - X^{15} + X^{16} - X^{17} + X^{18}. \end{aligned}$$

By direct computation, we get

$$\begin{aligned} &\mathrm{Res}(S, \Phi_1) = -1, \quad \mathrm{Res}(S, \Phi_2) = 1, \quad \mathrm{Res}(S, \Phi_3) = 1, \\ &\mathrm{Res}(S, \Phi_4) = 1, \quad \mathrm{Res}(S, \Phi_6) = 1, \quad \mathrm{Res}(S, \Phi_{12}) = 169 = 13^2. \end{aligned}$$

Hence, it follows from Proposition 10.3 that $\Pi(S_{18}, \Phi_l) = \emptyset$ for $l = 1, 2, 3, 4, 6$. Moreover, Proposition 10.13 implies that $I(\Phi_{12}; \mathbb{Q}_{13}) = \emptyset$, and $\Pi(S_{18}, \Phi_{12}) = \emptyset$ (the fact $I(\Phi_{12}; \mathbb{Q}_{13}) = \emptyset$ can also be seen from the factorization $(\Phi_{12}(X) \bmod 13) = (X-2)(X-7)(X+2)(X+7)$ in $\mathbb{F}_{13}[X]$). Therefore, the Salem number β_{18} is not nonprojective realizable by Theorem 13.14 (iii). On the other hand, it is shown by McMullen [28] that β_{18} is projectively realizable.

Bayer-Fluckiger gives an example of a Salem number of degree 18 that is not realizable as the dynamical degree of an automorphism of a K3 surface, projective or not, see [7, §26]. As for the case of degree 10, there is no known Salem number that is not nonprojectively realizable. A Salem number of degree 10 is not nonprojectively realizable if and only if $\Pi(S, \Phi_l) = \emptyset$ for all $l \in \mathcal{C}_{10}$ by Theorem 13.14 (iii), where S is the corresponding Salem polynomial. This condition is so strong that there seems to be no number satisfying it.

13.4 Other results

This subsection gives a survey of dynamical degrees, in particular greater than 1, of automorphisms of compact complex surfaces. As mentioned in Remark 13.6, if a compact complex surface Σ admits an automorphism with dynamical degree greater than 1 then Σ is a torus, a rational surface, a K3 surface, or an Enriques surface.

We begin with tori. If ϕ is an automorphism of a 2-dimensional complex torus then its dynamical dynamical degree $d(\phi)$ is 1 or a Salem number of degree at most 6. P. Reschke proved:

Theorem 13.27 ([36, Theorem 1.1])**.** *Let β be a Salem number of degree at most 6, and S its minimal polynomial. The number β is realizable as the dynamical degree of a 2-dimensional complex torus if and only if one of the following conditions holds:*

(i) $\deg(\beta) = 6$*, and both $|S(1)|$ and $|S(-1)|$ are squares.*

(ii) $\deg(\beta) = 4$*, and one of the following three conditions holds: $|S(1)|$ is a square; $|S(-1)|$ are square; or both $2|S(1)|$ and $2|S(-1)|$ are squares.*

(iii) $\deg(\beta) = 2$.

Partial results of this theorem are also given in [25], [27]. Reschke also gives a more detail theorem in [37], for example, taking projectivity into account.

Next, we explain the case of rational surfaces. We refer to [26] and [46] for more detail. Let N be the integer at least 3, and let $\mathbb{Z}^{1,N}$ denote the lattice $\langle 1, -1, \ldots, -1 \rangle_{\mathbb{Z}}$ over $\mathbb{Z}$ of signature $(1, N)$. Let $e_0, e_1, \ldots, e_N$ be the standard basis of $\mathbb{Z}^{1,N}$, and put $z_0 = e_0 - e_1 - e_2 - e_3$ and $z_i = e_i - e_{i+1}$ for $i = 1, \ldots, N-1$. The subgroup of $\mathrm{O}(\mathbb{Z}^{1,N})$ generated by reflections

$\sigma_{z_0}, \sigma_{z_1}, \ldots, \sigma_{z_N}$ orthogonal to $z_0, z_1, \ldots, z_N$ is called the *Weyl group* of $\mathbb{Z}^{1,N}$, and denoted by $\mathscr{W}_N$. We define

$$\mathcal{S} := \{\text{the special radius of } w \mid w \in \mathscr{W}_N,\ N \geq 3\}.$$

Let ϕ be an automorphism of a rational surface Σ. If $d(\phi) > 1$ then there exists an integer $N \geq 10$, an isometry $\tau : \mathbb{Z}^{1,N} \to H^2(\Sigma, \mathbb{Z})$, and an element $w \in \mathscr{W}_N$ such that the diagram

$$\begin{array}{ccc} \mathbb{Z}^{1,N} & \xrightarrow{w} & \mathbb{Z}^{1,N} \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ H^2(\Sigma, \mathbb{Z}) & \xrightarrow{\phi^*} & H^2(\Sigma, \mathbb{Z}) \end{array} \tag{46}$$

commutes. In particular $d(\phi) \in \mathcal{S}$. In the situation of (46), we say that w is *realized by* ϕ. McMullen [26] showed that for any $N \geq 10$, every *Coxeter element*, that is, the product of $\sigma_{z_0}, \sigma_{z_1}, \ldots, \sigma_{z_N}$ taken one a time any order, is realized by a rational surface automorphism. The case $d = 10$ yields a rational surface automorphism whose dynamical degree is Lehmer's number. He also proved that the dynamical degree of any automorphism of a compact complex surface is greater than or equal to Lehmer's number unless it is 1. T. Uehara gave the following decisive result.

Theorem 13.28 ([46, Theorem 1.1])**.** *We have*

$$\{d(\phi) \mid \phi \textit{ is a rational surface automorphism}\} = \mathcal{S}.$$

Finally, the cases of K3 surfaces and of Enriques surfaces. It is known that the second cohomology group modulo torsion of any Enriques surface is an even unimodular lattice of signature $(1, 9)$, with respect to the intersection form. As a consequence, the dynamical degree of any automorphism of an Enriques surface is 1 or a Salem number of degree at most 10. The study of dynamical degrees greater than 1 began by determining the minimum value. K. Oguiso [33] showed that the smallest Salem number of degree 14, which is the third smallest known Salem number, is realizable as the dynamical degree of an automorphism of a nonprojective K3 surface. He also showed that Lehmer's number cannot be realized as the dynamical degree of any automorphism of an Enriques surface. Afterwards, by McMullen, it was proved that Lehmer's number is realizable as the dynamical degree of a nonprojective K3 surface automorphism in [27], and of a projective K3 surface automorphism in [28], see also [8]. S. Brandhorst and N.D. Elkies [10] gave an explicit equation for a projective K3 surface having an automorphism whose dynamical degree is Lehmer's number. As for Enriques surfaces, after several works, e.g. [13], [24], [42], Oguiso and X. Yu determined the minimum value of dynamical degrees of Enriques surface automorphisms.

Theorem 13.29 ([34, Theorem 1.1])**.** *Let $\beta \approx 1.58234$ be the fourth smallest Salem number of degree 6 (its minimal polynomial is $1 - X^2 - 2X^3 - X^4 + X^6$). Then β is the minimum Salem number which is realized as the dynamical degree of an Enriques surface automorphism.*

For projective K3 surfaces or Enriques surfaces, works cited above enable us to determine the realizability of a given Salem number (in a computer-aided way), but a characterization, such as Theorem 13.14, 13.27, or 13.28, has not yet been obtained. However, there is a result of another type by Brandhorst.

Theorem 13.30 ([9, Theorem 1.2])**.** *Let β be a Salem number of degree d, and S its minimal polynomial. There exists a positive integer $N \in \mathbb{Z}_{>0}$ such that the power β^N is realized as the dynamical degree of an automorphism of a K3 surface (resp. Enriques surface, 2-dimensional*

torus) if and only if $d < 22$ *(resp.* $10, 6$*); or* $d = 22$ *(resp.* $10, 6$*) and* $(-1)^{d/2}S(1)S(-1)$ *is a square. If additionally* $d \leq 20$ *(resp.* $10, 4$*) then there exists* $N' \in \mathbb{Z}_{>0}$ *such that* $\beta^{N'}$ *is realized as the dynamical degree of an automorphism of a projective K3 surface (resp. Enriques surface,* 2*-dimensional torus).*

Although the topics are restricted to those related to dynamical degrees here, we remark that other interesting results of dynamical systems are also contained in papers cited above.

Bibliography

[1] T.M. Apostol, *Resultants of cyclotomic polynomials.* Proc. Amer. Math. Soc. **24** (1970), 457–462.

[2] W.P. Barth, K. Hulek, C.A.M. Peters and A. Van de Ven, Compact Complex Surfaces. Second edition. Springer-Verlag, Berlin, 2004.

[3] E. Bayer-Fluckiger and L. Taelman, *Automorphisms of even unimodular lattices and equivariant Witt groups.* J. Eur. Math. Soc. **22** (2020), 3467–3490.

[4] E. Bayer-Fluckiger, *Isometries of quadratic spaces.* J. Eur. Math. Soc. (JEMS) **17** (2015), no. 7, 1629–1656.

[5] E. Bayer-Fluckiger, *Isometries of lattices and Hasse principles.* arXiv:2001.07094.

[6] E. Bayer-Fluckiger, *Isometries of lattices and automorphisms of K3 surfaces.* arXiv:2107.07583.

[7] E. Bayer-Fluckiger, *Automorphisms of K3 surfaces, signatures, and isometries of lattices.* arXiv:2209.06698.

[8] S. Brandhorst and V. González-Alonso, *Automorphisms of minimal entropy on supersingular K3 surfaces.* J. Lond. Math. Soc. (2) **97** (2018), no.2, 282–305.

[9] S. Brandhorst, *On the stable dynamical spectrum of complex surfaces.* Math. Ann. **377** (2020), no. 1-2, 421–434.

[10] S. Brandhorst and N.D. Elkies, *Equations for a K3 Lehmer map.* J. Algebraic Geom. **32** (2023), no.4, 641–675.

[11] R. Brusamarello, P. Chuard-Koulmann and J. Morales, *Orthogonal groups containing a given maximal torus.* J. Algebra **266** (2003), no. 1, 87–101.

[12] S. Cantat, *Dynamique des automerphismes des surfaces projectives complexes.* C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 10, 901–906.

[13] I. Dolgachev, *Salem numbers and Enriques surfaces.* Exp. Math. **27** (2018), no.3, 287–301.

[14] P.K. Draxl, Skew Fields. Cambridge University Press, Cambridge, 1983.

[15] S. Friedland, *Entropy of algebraic maps.* Proceedings of the Conference in Honor of Jean-Pierre Kahane (Orsay, 1993). J. Fourier Anal. Appl. 1995, Special Issue, 215–228.

[16] G. Fujisaki, Fields and Galois Theory (in Japanese). Iwanami Shoten, Publishers, 1991.

[17] G. Greiter, *A simple proof for a theorem of Kronecker.* Amer. Math. Monthly **85** (1978), no.9, 756–757.

[18] B.H. Gross and C.T. McMullen, *Automorphisms of even unimodular lattices and unramified Salem numbers.* J. Algebra **257** (2002), no. 2, 265–290.

[19] D. Harari, Galois cohomology and class field theory. Universitext, Springer, Cham, 2020.

[20] J.S. Hsia, *Spinor norms of local integral rotations. I.* Pacific J. Math. **57** (1975), no.1, 199–206.

[21] I. Kaplansky, *Modules over Dedekind rings and valuation rings.* Trans. Amer. Math. Soc. **72** (1952), 327–340.

[22] M. Kirschmer, *Automorphisms of even unimodular lattices over number fields.* J. Number Theory **197**(2019), 121–134.

[23] S. Kondō, $K3$ Surfaces. EMS Tracts Math., **32**. EMS Publishing House, Berlin, 2020.

[24] Y. Matsumoto, H. Ohashi and S. Rams, *On automorphisms of Enriques surfaces and their entropy.* Math. Nachr. **291** (2018), no.13, 2084–2098.

[25] C.T. McMullen, *Dynamics on K3 surfaces: Salem numbers and Siegel disks.* J. Reine Angew. Math. **545** (2002), 201–233.

[26] C.T. McMullen, *Dynamics on blowups of the projective plane.* Publ. Math. Inst. Hautes Études Sci. **105** (2007), 49–89.

[27] C.T. McMullen, *K3 surfaces, entropy and glue.* J. Reine Angew. Math. **658** (2011), 1–25.

[28] C.T. McMullen, *Automorphisms of projective K3 surfaces with minimum entropy.* Invent. Math. **203** (2016), no. 1, 179–215.

[29] J. Milnor, *On isometries of inner product spaces.* Invent. Math. **8** (1969), 83–97.

[30] J. Milnor and D. Husemoller, Symmetric Bilinear Forms. Springer-Verlag, Heidelberg New York, 1973.

[31] M.J. Mossinghoff, More Salem numbers, lists of polynomials with small Mahler measure, Lehmer's problem, `http://wayback.cecm.sfu.ca/~mjm/Lehmer/lists/`.

[32] J. Neukirch, Algebraic Number Theory. Springer-Verlag, Berlin, 1999.

[33] K. Oguiso, *The third smallest Salem number in automorphisms of K3 surfaces.* Algebraic geometry in East Asia-Seoul 2008, 331–360, Adv. Stud. Pure Math., **60**, Math. Soc. Japan, Tokyo, 2010.

[34] K. Oguiso, and X. Yu, *Minimum positive entropy of complex Enriques surface automorphisms.* Duke Math. J. **169** (2020), no. 18, 3565–3606.

[35] O.T. O'Meara, Introduction to Quadratic Forms. Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[36] P. Reschke, *Salem numbers and automorphisms of complex surfaces.* Math. Res. Lett. **19** (2012), no. 2, 475–482.

[37] P. Reschke, *Salem numbers and automorphisms of abelian surfaces.* Osaka J. Math. **54** (2017), no. 1, 1–15.

[38] R. Salem, Algebraic Numbers and Fourier Analysis. D. C. Heath and Co., Boston, MA, 1963.

[39] W. Scharlau, Quadratic and Hermitian Forms. Springer-Verlag, Berlin, 1985.

[40] J.P. Serre, A Course in Arithmetic. Springer Sience+Business Media New York, 1973.

[41] J.P. Serre, Local Fields. Springer Sience+Business Media New York, 1979.

[42] I. Shimada, *On an Enriques surface associated with a quartic Hessian surface.* Canad. J. Math. **71** (2019), no.1, 213–246.

[43] Y.T. Siu, *Every $K3$ surface is Kähler.* Invent. Math. **73** (1983), no. 1, 139–150.

[44] C. Smyth, *Seventy years of Salem numbers.* Bull. Lond. Math. Soc. **47** (2015), no. 3, 379–395.

[45] Y. Takada, *Lattice isometries and K3 surface automorphisms: Salem numbers of degree 20.* J. Number Theory **252** (2023), 195–242.

[46] T. Uehara, *Rational surface automorphisms with positive entropy.* Ann. Inst. Fourier (Grenoble) **66** (2016), no. 1, 377–432.

[47] R.O. Wells, Jr, Differential Analysis on Complex Manifolds. Third edition. Grad. Texts in Math., **65** Springer, New York, 2008.

[48] K. Yamazaki, Rings and Modules (in Japanese). Iwanami Shoten, Publishers, 1990.

[49] H. Zassenhaus, *On the spinor norm.* Arch. Math. **13** (1962), 434–451.