Ideal Lattices in Cyclotomic Fields

Alexandre Lemire Paquin

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal,Quebec

2013-12-01

A thesis submitted to McGill University in partial fulfilment of the requirements for an M.Sc. degree

ACKNOWLEDGEMENTS

I would like to thank my family for their support, my supervisor Eyal Goren for his advice and, the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Fonds de recherche québécois sur la nature et les technologies (FQRNT) for their financial support.

ABSTRACT

We study lattices arising from ideals in cyclotomic fields. We begin with some general theory about lattices. We introduce certain important lattices, namely the root lattices and the Niemeier lattices. We then describe how to obtain lattices using ideals in number fields and we determine some of their basic properties. We continue our study by specializing to cyclotomic fields. We determine all the root lattices and all the Niemeier lattices that are similar to ideals in cyclotomic fields as well as all the cyclotomic fields in which they can be obtained. We give many examples and even a few examples of even unimodular lattices in dimension 32. We mainly follow the work of E. Bayer (see the references).

RÉSUMÉ

Nous étudions les réseaux qui surviennent d'idéaux dans des corps cyclotomiques. Nous commençons avec de la théorie générale sur les réseaux. Nous introduisons certains importants réseaux, les réseaux racines et les réseaux de Niemeier. Nous décrivons ensuite comment obtenir des réseaux en utilisant des idéaux dans des corps de nombres et nous déterminons quelques-unes de leurs propriétés. Nous continuons notre étude en nous spécialisant aux corps cyclotomiques. Nous déterminons tous les réseaux racines et les réseaux de Niemeier qui sont similaires à des idéaux dans des corps cyclotomiques ainsi que tous les corps cyclotomiques dans lesquels ils peuvent être obtenus. Nous donnons plusieurs exemples et même quelque exemples de réseaux unimodulaires pairs en dimension 32. Nous suivons principalement certains travaux de E. Bayer (voir les références).

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1
Introduction

The study of lattices is of some importance for chemistry and physics. For example, 3-dimensional lattices are used to investigate the structure of crystals (see [OH80]) and the Leech lattice is involved in superstring theory (see [Cha85]). Furthermore, lattices have many connections to different topics within mathematics. Among other things, they are closely related to coding theory, group theory, the theory of quadratic forms, the theory of modular forms and algebraic number theory (see [CS99]). The interest for lattices in all these fields gives a motivation to study different ways of constructing them. In this thesis, we present a particular way of constructing lattices via number fields, with an emphasis on examples coming from cyclotomic fields.

In chapter 2, we give some basic definitions about lattices and introduce some of their basic invariants like the discriminant and the signature. In particular, the positive definite lattices, or Euclidean lattices, are particularly interesting since they are related to the geometrical problems of determining the densest packing of spheres in space, the thinnest covering of space with balls and the maximal number of spheres that can be put around a sphere. In the cases where these problems are solved (in small dimensions), the answer is often obtained from root lattices or their dual. The root lattices are integral lattices generated by their elements of squared norm 1 and 2. They are all classified: they are given by all the orthogonal direct sums of the indecomposable root lattices $\mathbb{Z}$, A_n $(n \geq 1)$, D_n $(n \geq 3)$ and E_n $(n = 6, 7, 8)$. Other interesting examples of lattices are the unimodular lattices. The theta series of these lattices satisfies a particular functional equation and in the case of even unimodular

lattices this equation implies that the theta series is a modular form (for the whole group $\mathrm{SL}_2(\mathbb{Z})$). These modular forms are known and this allows to determine the theta series of these lattices. This is very useful in classifying the even unimodular lattices. Such a classification is known in dimensions ≤ 24. Even unimodular lattices exist in dimensions a multiple of 8. In dimension 8, there is a unique such lattice up to isomorphism; the root lattice E_8. In dimension 16, there are only 2 such lattices; the root lattice $2E_8$ and the lattice D_{16}^+. In dimension 24, there are 24 such lattices, called the Niemeier lattices, one of them being the Leech lattice. The Leech lattice is the only Niemeier lattice with no roots, all other Niemeier lattices having in fact a complete root system. In higher dimensions, there are so much even unimodular lattices that a general classification seems unlikely to ever be achieved. However, in dimension 32, the even unimodular lattices with complete root systems form a very small subset of all the even unimodular lattices in this dimension and they are all classified.

In chapter 3, we describe the connection with algebraic number theory. We obtain lattices by considering ideals in number fields and the trace pairing. These lattices are important since, for example, the ring of integers of a number field can be seen as a lattice and its dual lattice is the codifferent ideal, which tells the ramification of primes. We determine formulas for the discriminant and the signature of these lattices. Then we determine when the construction gives a rational lattice, when it gives an integral lattice and when it gives an unimodular lattice. If one is interested in euclidean lattices, these can only be obtained when the number field is either totally real or a CM-field.

In chapter 4, we concentrate our study on cyclotomic fields which are an important class of examples of CM-fields. The main question we ask is : Which lattices can be obtained from ideals in cyclotomic fields? It turns out that these lattices are

characterized by some properties of their automorphism group (not only by the structure of the group but also by how it acts on the lattice). This enables us to determine all the root lattices that arise from ideals in cyclotomic fields and all the cyclotomic fields in which they can be obtained (our result corrects and completes a theorem in [Bay99]). We also present the determination due to E. Bayer of all the Niemeier lattices that arise from cyclotomic fields and of the cyclotomic fields in which they can be obtained. We conclude with a short discussion on higher dimensions.

CHAPTER 2
General theory of lattices

2.1 Basic definitions

We will need the following notion of non-degeneracy.

Definition 2.1.1. Let V be a finite dimensional vector space over a field K. A symmetric bilinear pairing

$$(-,-) : V \times V \to K$$

is said to be *non-degenerate* if the only $x \in V$ such that $(x, y) = 0$ for all $y \in V$ is $x = 0$.

Definition 2.1.2. Let $\mathscr{L}$ be a free $\mathbb{Z}$-module of finite rank with a symmetric $\mathbb{Z}$-bilinear pairing

$$(-,-) : \mathscr{L} \times \mathscr{L} \to \mathbb{R}.$$

If the induced bilinear pairing on the real vector space $V = \mathscr{L} \otimes_{\mathbb{Z}} \mathbb{R}$ is non-degenerate then we say that $\mathscr{L}$ (or $\{\mathscr{L},(-,-)\}$) is a *lattice*.

There is a natural notion of sublattice.

Definition 2.1.3. Let $\{\mathscr{L},(-,-)\}$ be a lattice and S be a submodule of $\mathscr{L}$. If S is a lattice with the pairing obtained from the restriction of $(-,-)$ to $S \times S$ then we say that S is a sublattice of $\mathscr{L}$.

Definition 2.1.4. Let $\{\mathscr{L},(-,-)\}$ and $\{\mathscr{L}',(-,-)'\}$ be two lattices. A homomorphism of $\mathbb{Z}$-module

$$f : \mathscr{L} \to \mathscr{L}'$$

is a *morphism of lattices* if it satisfies

$$(f(x), f(y))' = (x, y) \text{ for all } x, y \in \mathscr{L}.$$

If f is a bijection then f is an *isomorphism of lattices* and the lattices $\mathscr{L}$ and $\mathscr{L}'$ are said to be *isomorphic*, or *congruent*, and we write $\mathscr{L} \cong \mathscr{L}'$. An isomorphism from a lattice to itself is called an *automorphism* of the lattice. The group of all automorphisms of $\mathscr{L}$ is denoted by $\mathrm{Aut}(\mathscr{L})$.

Next, we relax the notion of congruence of lattices by allowing a scaling factor.

Definition 2.1.5. Let $\{\mathscr{L},(-,-)\}$ and $\{\mathscr{L}',(-,-)'\}$ be two lattices. Suppose there exists an isomorphism of $\mathbb{Z}$-module

$$f : \mathscr{L} \to \mathscr{L}'$$

satisfying

$$(f(x), f(y))' = \alpha(x, y) \text{ for all } x, y \in \mathscr{L}$$

for some $\alpha \neq 0$ in $\mathbb{R}$. Then we say $\mathscr{L}$ and $\mathscr{L}'$ are *equivalent*, or *similar*.

Given a lattice of rank n and a lattice of rank m, we can build a lattice of rank $n + m$ in the following way.

Definition 2.1.6. Let $\{\mathscr{L},(-,-)\}$ and $\{\mathscr{L}',(-,-)'\}$ be two lattices. The (*external*) *orthogonal direct sum* $\mathscr{L} \oplus \mathscr{L}'$ of $\mathscr{L}$ and $\mathscr{L}'$ is the free $\mathbb{Z}$-module $\mathscr{L} \times \mathscr{L}'$ with pairing $< -, - >$ defined by

$$< (x, x'), (y, y') >:= (x, y) + (x', y')'$$

for $x, y \in \mathscr{L}$ and $x', y' \in \mathscr{L}'$.

There is a very close notion of *internal orthogonal direct sum*.

Definition 2.1.7. Let $\{\mathscr{L},(-,-)\}$ be a lattice and $\mathscr{L}_1$, $\mathscr{L}_2$ two sublattices of $\mathscr{L}$. Suppose that the following two conditions are satisfied:

i) every $x \in \mathscr{L}$ can be written uniquely as sum $y + z$ of an element $y \in \mathscr{L}_1$ and of an element $z \in \mathscr{L}_2$,

ii) $(y, z) = 0$ for all $y \in \mathscr{L}_1$ and for all $z \in \mathscr{L}_2$.

Then we say that $\mathscr{L}$ is the (*internal*) *orthogonal direct sum* of its two sublattices $\mathscr{L}_1$, $\mathscr{L}_2$ and we write $\mathscr{L} = \mathscr{L}_1 \oplus \mathscr{L}_2$.

The internal orthogonal direct sum of two sublattices $\mathscr{L}_1$ and $\mathscr{L}_2$ of a lattice $\mathscr{L}$ is easily identified with their external orthogonal direct sum, and conversely, the external direct sum of two lattices $\mathscr{L}_1$ and $\mathscr{L}_2$ is the internal direct sum of the two sublattices $\mathscr{L}_1 \equiv \{(x,0) \mid x \in \mathscr{L}_1\}$ and $\mathscr{L}_2 \equiv \{(0,x) \mid x \in \mathscr{L}_2\}$.

Definition 2.1.8. A lattice $\mathscr{L}$ is said to be *decomposable* if it can be written as an orthogonal direct sum of two of its sublattices. Otherwise, it is said to be *indecomposable*.

Every lattice $\mathscr{L}$ can be written as an orthogonal direct sum of indecomposable sublattices and there are at most $\mathrm{rk}(\mathscr{L})$ of them in every such decomposition.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis (or more briefly a *basis*) for $\mathscr{L}$. The matrix representing $(-,-)$ in this basis is then $A = ((\alpha_i, \alpha_j))_{1 \leq i,j \leq n}$. We call A a *Gramm matrix* for the lattice. Also let $\{\beta_1, \ldots, \beta_n\}$ be a basis for $\mathscr{L}'$ and $A' = ((\beta_i, \beta_j))_{1 \leq i,j \leq n}$. It is easy to show that if $\mathscr{L}$ is similar to $\mathscr{L}'$ with α as in definition 1.1.5 then there exists a matrix U with integer entries and determinant ± 1 such that $A' = \alpha U A U^t$, where t denotes transposition. Thus if $\mathscr{L}$ and $\mathscr{L}'$ are congruent lattices then $\det(A) = \det(A')$. In particular, taking $\mathscr{L} = \mathscr{L}'$ and $(-,-) = (-,-)'$ with the identity isomorphism, we see that the determinant of a Gramm Matrix is the same for any choice of basis. We then define the *discriminant* of the lattice $\mathscr{L}$ by

$$\mathrm{disc}(\mathscr{L}) := |\det(A)|.$$

Remark 2.1.9. The non-degeneracy condition in the definition of a lattice is equivalent to $\mathrm{disc}(\mathscr{L}) \neq 0$.

2.2 Quadratic forms and the signature

Given a basis for a lattice $\mathscr{L}$, the corresponding Gramm matrix A is a real symmetric matrix. Real symmetric matrices are in one-to-one correspondence with quadratic forms over the real numbers. By a quadratic form over a commutative ring R, we mean a homogeneous polynomial of degree 2 in a given number of variables

and with coefficients in R. The correspondence is as follows: starting with a real $n \times n$ symmetric matrix A, we get the quadratic form $q(x) = xAx^t$, where $x = (x_1, \ldots, x_n)$, and starting with a quadratic form $q(x)$ in n variables, there is a unique symmetric $n \times n$ matrix A such that $q(x) = xAx^t$. When the matrix A is a Gramm matrix for a lattice, we know that $\det(A) \neq 0$ by the non-degeneracy of the pairing. A quadratic form with matrix A such that $\det(A) \neq 0$ is said to be *non-degenerate*.

If we have two quadratic forms in the same number of variables, one with matrix A and the other one with matrix A', and if A and A' are related by $A' = UAU^t$ for some invertible real matrix U then we say that the two quadratic forms are $\mathbb{R}$-*equivalent*. If we can take the matrix U with integer entries and determinant ± 1 then we say that the two quadratic forms are *integrally equivalent*. Thus changing basis or changing the lattice for a congruent one gives integrally equivalent quadratic forms. In other words, to each congruence class of lattices we can associate an integral equivalence class of quadratic forms over $\mathbb{R}$. Conversely, given a non-degenerate quadratic form over $\mathbb{R}$ in n variables, the associated symmetric matrix A can be used to define a lattice by $\mathscr{L} = \mathbb{Z}^n$ and $(x, y) = xAy^t$ for $x, y \in \mathbb{Z}^n$. It is easy to see that integrally equivalent quadratic forms then define congruent lattices and that the associations just defined are inverse of each other. Therefore there is a bijective correspondence between congruence classes of lattices and integral equivalence classes of non-degenerate quadratic forms over $\mathbb{R}$.

The above correspondence becomes particularly interesting when restricted to *integral* lattices and *integral* quadratic forms. A lattice is said to be *integral* when the pairing is integer valued. This is equivalent to say that any Gramm matrix has entries only in $\mathbb{Z}$. A quadratic form is said to be *integral* when the associated matrix has entries in $\mathbb{Z}$. We thus have a bijective correspondence between congruence classes of integral lattices and integral equivalence classes of non-degenerate integral

quadratic forms. Classification of integral quadratic forms is a classical subject in mathematics (see [CS99], chapter 15).

An important invariant for the classification of quadratic forms is the *signature*. Given a quadratic form over $\mathbb{R}$, it is $\mathbb{R}$-equivalent to a form

$$x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2$$

for some integers $r, s \geq 0$ (see [Ser73]). If the quadratic form is non-degenerate in n variables then $r+s = n$. The *signature* of the quadratic form is the couple (r, s). This is well defined and $\mathbb{R}$-equivalent quadratic forms have the same signature. Therefore using the correspondence between congruence classes of lattices and integral equivalence classes of non-degenerate quadratic forms, we have a well defined notion of signature for a lattice $\mathscr{L}$ (we denote it by $\text{sign}(\mathscr{L})$), and congruent lattices have the same signature. More generally, if $\mathscr{L}$ is equivalent to $\mathscr{L}'$ with an $\alpha > 0$ then $\text{sign}(\mathscr{L}) = \text{sign}(\mathscr{L}')$. When $\alpha < 0$, if $\text{sign}(\mathscr{L}) = (r, s)$ then $\text{sign}(\mathscr{L}') = (s, r)$.

Definition 2.2.1. Let $\mathscr{L}$ be a lattice and $\text{sign}(\mathscr{L}) = (r, s)$. If $r = 0$ or $s = 0$ then we say that $\mathscr{L}$ is *definite* (*positive definite* if $s = 0$ and *negative definite* if $r = 0$). Otherwise, we say that $\mathscr{L}$ is *indefinite*.

Example 2.2.2. Let $0 \leq r \leq n$ be an integer. Define a non-degenerate symmetric bilinear form on $\mathbb{R}^n$ by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = x_1 y_1 + \cdots + x_r y_r - x_{r+1} y_{r+1} - \cdots - x_n y_n.$$

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $\mathbb{R}^n$ and $\mathscr{L} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. If we restrict to $\mathscr{L}$ the bilinear form on $\mathbb{R}^n$ then $\mathscr{L}$ is a lattice. The signature of $\mathscr{L}$ is $(r, n-r)$. Let's show that in fact any lattice is isomorphic to such a lattice. Supppose a lattice $\mathscr{L}$ of rank n with pairing $(-,-)$ is given. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for $\mathscr{L}$ and let A be the corresponding Gramm matrix. The quadratic form associated to A is $\mathbb{R}$-equivalent to a form $x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2$. That is, there exists an invertible matrix U such that $UAU^t = D$ where D is a diagonal matrix with diagonal entries

$d_i = 1$ for $i \leq r$ and $d_i = -1$ for $i > r$. Define now $\beta_i \in \mathbb{R}^n$ as the i^{th} row of U^{-1}. Let $\mathscr{L}' = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$ and define an isomorphism of $\mathbb{Z}$-module $f : \mathscr{L} \to \mathscr{L}'$ by $f(\alpha_i) = \beta_i$. Then for any $x = \sum_{i=1}^n x_i\alpha_i \in \mathscr{L}$ and for any $y = \sum_{i=1}^n y_i\alpha_i \in \mathscr{L}$ we have $f(x) \cdot f(y) = (x_1, \ldots, x_n)U^{-1}D(U^{-1})^t(y_1, \ldots, y_n)^t$ and thus $f(x) \cdot f(y) = (x, y)$. Therefore $\mathscr{L}$ and $\mathscr{L}'$ are isomorphic.

In particular, the preceding example tells us that any positive definite lattice $\mathscr{L}$ can be seen as $\mathscr{L} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \subseteq \mathbb{R}^n$ for some basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{R}^n$ and where $\mathbb{R}^n$ is endowed with the usual inner product. For this reason, we shall refer sometimes to positive definite lattices as *Euclidean lattices*. From now on, unless otherwise stated, $\mathbb{R}^n$ will always be endowed with the usual inner product and the induced norm will be denoted $||\cdot||$. Also, when we will say that $\mathscr{L} \subseteq \mathbb{R}^n$ is a lattice, it will be understood that $\mathscr{L}$ is an additive subgroup of $\mathbb{R}^n$ and that the pairing is the restriction to $\mathscr{L}$ of the usual inner product (in general, the rank of $\mathscr{L}$ could be smaller than n but sometimes it will be clear from the context that we assume that the rank of $\mathscr{L}$ is n).

2.3 Euclidean lattices

Let $\mathscr{L} \subseteq \mathbb{R}^n$ be a lattice. If $\{\alpha_1, \ldots, \alpha_m\}$ is a $\mathbb{Z}$-basis for $\mathscr{L}$ then the corresponding Gramm matrix is $A = (\alpha_i \cdot \alpha_j)_{1 \leq i,j \leq m}$. If the vectors $\alpha_1, \ldots, \alpha_m$ are linearly dependent over $\mathbb{R}$ then it is easy to see that $\det(A) = 0$. Thus a $\mathbb{Z}$-basis for a lattice $\mathscr{L}$ must be formed by linearly independent vectors. Conversely, if $\{\alpha_1, \ldots, \alpha_m\}$ is a set of linearly independent vectors in $\mathbb{R}^n$ and if $\mathscr{L} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$ then $\mathscr{L}$ is a lattice. Indeed, we can see this by completing the set $\{\alpha_1, \ldots, \alpha_m\}$ to a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{R}^n$, where the α_j's for $j > m$ satisfy $\alpha_i \cdot \alpha_j = 0$ when $i \neq j$ and $\alpha_j \cdot \alpha_j = 1$. Then $\det((\alpha_i \cdot \alpha_j)_{1 \leq i,j \leq m}) = \det((\alpha_i \cdot \alpha_j)_{1 \leq i,j \leq n}) \neq 0$.

Remark 2.3.1. We just saw that $m \leq n$ linearly independent vectors in $\mathbb{R}^n$ generate a lattice over $\mathbb{Z}$ in the positive definite case. In the indefinite case, this is not true in general. For example, consider $\mathbb{R}^2$ with pairing

$$(x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 - x_2 y_2.$$

Then the restriction of this pairing to $\mathbb{Z}(1,1)$ is trivial. Therefore $\mathbb{Z}(1,1)$ is not a lattice.

We now give two important results about Euclidean lattices.

Proposition 2.3.2. *$\mathscr{L} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$ for linearly independent vectors $\alpha_1, \ldots, \alpha_m$ in $\mathbb{R}^n$ if and only if $\mathscr{L}$ is a discrete additive subgroup of $\mathbb{R}^n$.*

Proof. Suppose that $\mathscr{L} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$ for linearly independent vectors $\alpha_1, \ldots, \alpha_m$ in $\mathbb{R}^n$. Complete the set $\{\alpha_1, \ldots, \alpha_m\}$ to a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{R}^n$ if necessary. Define a norm on $\mathbb{R}^n$ by

$$||\sum_{i=1}^{n} x_i \alpha_i||' := ||(x_1, \ldots, x_n)||.$$

Any two norms on $\mathbb{R}^n$ are equivalent, that is there exists positive constants C and D such that $C||v||' \leq ||v|| \leq D||v||'$ for all $v \in \mathbb{R}^n$. Clearly, if v is a non-zero element in $\mathscr{L}$ then $||v||' \geq 1$. Therefore for any v non-zero element in $\mathscr{L}$ we have $C \leq ||v||$. It follows that $\mathscr{L}$ is discrete.

Now suppose that $\mathscr{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. Let $m = \dim (\mathbb{R}\mathscr{L})_{\mathbb{R}}$. So we can choose m linearly independent vectors $\alpha_1, \ldots, \alpha_m$ in $\mathscr{L}$ and we have $\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m \subseteq \mathscr{L}$. Let $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$. Let's show that the index $[\mathscr{L} : A]$ is finite. If x is any element in $\mathscr{L}$ then $x = r_1\alpha_1 + \cdots + r_m\alpha_m$ for some real numbers $r_1, \ldots, r_m$. For each $1 \leq i \leq m$, we can write $r_i = m_i + r_i'$ for some $m_i \in \mathbb{Z}$ and some $0 \leq r_i' < 1$. Then

$$x = \sum_{i=1}^{m} m_i \alpha_i + \sum_{i=1}^{m} r_i' \alpha_i.$$

It follows that x is congruent to $\sum_{i=1}^{m} r_i' \alpha_i$ modulo A. We have

$$||\sum_{i=1}^{n} r_i' \alpha_i|| \leq D||\sum_{i=1}^{n} r_i' \alpha_i||' = D\sqrt{(r_1')^2 + \cdots + (r_m')^2} < D\sqrt{m}.$$

So each class modulo A contains a representative of norm smaller than $D\sqrt{m}$. But since $\mathscr{L}$ is a discrete subgroup, any bounded set contains only a finite number of elements. Therefore there is only a finite number of classes modulo A. Thus $\mathscr{L}$ is a torsion free abelian group containing a free subgroup A of rank m and of finite index. It follows that $\mathscr{L}$ is also free of rank m. Hence we have $\mathscr{L} = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m$ for some $\beta_1, \ldots, \beta_m \in \mathbb{R}^n$ and the β_i's are linearly independent because $\dim(\mathbb{R}\mathscr{L})_{\mathbb{R}} = m$. ■

Proposition 2.3.3. *Let $\mathscr{L}$ be a Euclidean lattice. Then $\mathscr{L}$ can be written uniquely as an orthogonal direct sum of indecomposable sublattices $\mathscr{L}_1$, $\mathscr{L}_2$, ..., $\mathscr{L}_k$. That is, if also $\mathscr{L} = \mathscr{J}_1 \oplus \mathscr{J}_2 \oplus \cdots \oplus \mathscr{J}_t$ for some indecomposable sublattices $\mathscr{J}_1$, $\mathscr{J}_2$, ..., $\mathscr{J}_t$ of $\mathscr{L}$ then $t = k$ and for all $1 \leq i \leq t$, $\mathscr{J}_i = \mathscr{L}_j$ for some $1 \leq j \leq t$.*

Proof. Let $(-,-)$ be the pairing on $\mathscr{L}$. We will call an element $x \in \mathscr{L}$ *reducible* if there are non-zero y and z in $\mathscr{L}$ with $(y,z) = 0$ such that $x = y + z$, and we will call it *irreducible* otherwise. We define an equivalence relation on the set of non-zero irreducible elements of $\mathscr{L}$ in the following way: x is equivalent to y if and only if there is a chain of irreducible elements $x = z_1, z_2, \ldots, z_q = y$ such that $(z_i, z_{i+1}) \neq 0$ for $1 \leq i \leq q-1$. Denote by C_i for $i \geq 1$ the classes of equivalence. Also let K_i be the additive subgroup of $\mathscr{L}$ generated by C_i. From the last proposition, each K_i is a sublattice of $\mathscr{L}$. If $i \neq j$ then for all $x \in K_i$ and $y \in K_j$ we have $(x,y) = 0$. As the rank of $\mathscr{L}$ is finite, there are only a finite number of K_i's, say K_1, K_2, ..., K_t (and then also there are only a finite number of C_i's, C_1, C_2, ..., C_t). We then have $K_1 \oplus K_2 \oplus \cdots \oplus K_t \subseteq \mathscr{L}$. But any $x \in \mathscr{L}$ is a sum of irreducible elements because if $x = y + z$ for some non-zero y and z with $(y,z) = 0$ then $(x,x) = (y,y) + (z,z)$ and so $(y,y) < (x,x)$ and $(z,z) < (x,x)$. Hence $\mathscr{L} = K_1 \oplus K_2 \oplus \cdots \oplus K_t$.

Now, assume that $\mathscr{L} = \mathscr{J}_1 \oplus \mathscr{J}_2 \oplus \cdots \oplus \mathscr{J}_s$ for some indecomposable sublattices $\mathscr{J}_1$, $\mathscr{J}_2$, ..., $\mathscr{J}_s$ of $\mathscr{L}$. If x is in C_i then x is in some $\mathscr{J}_j$ because x is irreducible. It then follows that $C_i \subseteq \mathscr{J}_j$ and hence also $K_i \subseteq \mathscr{J}_j$. We can conclude from this

that $\mathscr{J}_j$ is equal to the orthogonal direct sum of the K_l's it contains. But since $\mathscr{J}_j$ is indecomposable, we must have $\mathscr{J}_j = K_i$. ■

Remark 2.3.4. The last proposition is not true for indefinite lattices. For example, consider the lattice $\mathscr{L} = \mathbb{Z}^2$ with pairing

$$(x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 - 2x_2 y_2.$$

Then we both have

$$\mathscr{L} = \mathbb{Z}(1, 0) \oplus \mathbb{Z}(0, 1)$$

and

$$\mathscr{L} = \mathbb{Z}(2, 1) \oplus \mathbb{Z}(1, 1).$$

Remark 2.3.5. If f is an automorphism of $\mathscr{L}$ and $\mathscr{L} = \mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k$ for some indecomposable sublattices $\mathscr{L}_1$, $\mathscr{L}_2$, ..., $\mathscr{L}_k$ then we have

$$\mathscr{L} = f(\mathscr{L}_1) \oplus f(\mathscr{L}_2) \oplus \cdots \oplus f(\mathscr{L}_k)$$

and so, from the uniqueness of the decomposition, f permutes the elements of $\{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}$. We shall make use of this remark later on.

We continue with some basic definitions.

Definition 2.3.6. Let $\alpha_1 = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n}), \alpha_2 = (\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2n}), \ldots, \alpha_m = (\alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{mn}) \in \mathbb{R}^n$ be a basis for the Euclidean lattice $\mathscr{L}$. The $m \times n$ matrix $M = (\alpha_{ij})$ is called a *generator matrix* for $\mathscr{L}$ (with respect to the basis $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathscr{L}$).

Clearly, if M is a generator matrix with respect to some basis then the Gramm matrix associated to this basis is MM^t. If M is a square matrix then the discriminant of the lattice is $\det(M)^2$.

For two lattices $\mathscr{L}$ and $\mathscr{L}'$ in $\mathbb{R}^n$, we can reformulate the notions of congruence and equivalence in term of their generator matrices M and M'. We have that $\mathscr{L}$ and $\mathscr{L}'$ are equivalent lattices if and only if there exists a nonzero constant c, a matrix U with integer entries and determinant ± 1 and a real orthogonal matrix B such that

$$M' = cUMB.$$

Then they are congruent if and only if we can take $c = 1$.

Definition 2.3.7. Let $\mathscr{L}$ be a lattice of rank n in $\mathbb{R}^n$ and M a generator matrix. The columns of M^{-1} generate a lattice $\mathscr{L}^*$ called the *dual* of $\mathscr{L}$.

If $\{\beta_1, \beta_2, \ldots, \beta_n\}$ are the columns of M^{-1} and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are the rows of M then, for all $1 \leq i, j \leq n$, $\beta_i \cdot \alpha_j = 0$ or 1 and so $\mathscr{L}^* \subseteq \{x \in \mathbb{R}^n \mid x \cdot u \in \mathbb{Z}, \forall u \in \mathscr{L}\}$. Also if $x \in \{x \in \mathbb{R}^n \mid x \cdot u \in \mathbb{Z}, \forall u \in \mathscr{L}\}$ then $x \cdot \alpha_i = k_i \in \mathbb{Z}$ for all $1 \leq i \leq n$ and so $xM^{tr} = (k_1, k_2, \ldots, k_n)$. It follows that $x = (k_1, k_2, \ldots, k_n)(M^{-1})^{tr}$ and hence that x is a $\mathbb{Z}$-linear combination of the columns of M^{-1}. Thus

$$\mathscr{L}^* = \{x \in \mathbb{R}^n \mid x \cdot u \in \mathbb{Z}, \forall u \in \mathscr{L}\}.$$

Remark 2.3.8. We have $\mathrm{disc}(\mathscr{L}^*) = \mathrm{disc}(\mathscr{L})^{-1}$. Also if $\mathscr{L}$ is integral then $\mathscr{L} \subseteq \mathscr{L}^*$ and $|\mathscr{L}^*/\mathscr{L}| = \mathrm{disc}(\mathscr{L})$.

Definition 2.3.9. A positive definite lattice $\mathscr{L}$ is called *unimodular* if $\mathscr{L} = \mathscr{L}^*$.

Therefore a positive definite lattice $\mathscr{L}$ is unimodular if and only if $\mathscr{L}$ is integral and $\mathrm{disc}(\mathscr{L}) = 1$.

Definition 2.3.10. An integral lattice $\mathscr{L}$ with pairing $(-,-)$ is called *even* if $(x, x) \in 2\mathbb{Z}$ for all $x \in \mathscr{L}$. Otherwise, it is called *odd*.

Remark 2.3.11. An integral lattice $\mathscr{L}$ is even if and only if the diagonal entries of any Gramm matrix are even.

We now turn our attention to a particular class of integral lattices: the *root lattices*.

2.4 Root lattices

Definition 2.4.1. Let $\mathscr{L}$ be a positive definite integral lattice with pairing $(-,-)$. Every $x \in \mathscr{L}$ such that $(x, x) = 1$ or 2 is called a *root* of $\mathscr{L}$. If $\mathscr{L}$ is generated by its roots, it is called a *root lattice*.

We now give a list of examples that can be used to classify the root lattices.

Example 2.4.2. Let $\mathbb{Z} \subseteq \mathbb{R}$. This is an odd root lattice.

Example 2.4.3. Let $A_n := \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid x_0 + x_1 + \cdots + x_n = 0\} \subseteq \mathbb{R}^{n+1}$ for $n \geq 1$. For $0 \leq i \leq n$, let $e_i \in \mathbb{R}^{n+1}$ be the vector with 1 in the x_i coordinate and 0 elsewhere. Then

$$A_n = \mathbb{Z}(e_1 - e_0) + \mathbb{Z}(e_2 - e_1) + \cdots + \mathbb{Z}(e_n - e_{n-1}).$$

The generator matrix for A_n with respect to the basis $\{e_1 - e_0, e_2 - e_1, \ldots, e_n - e_{n-1}\}$ is the $n \times (n+1)$ matrix

$$\begin{pmatrix} -1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & -1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & -1 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \ldots & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & -1 & 1 \end{pmatrix}.$$

The Gramm matrix corresponding to this generator matrix is the $n \times n$ matrix

$$\begin{pmatrix} 2 & -1 & 0 & \ldots & 0 & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 \\ 0 & -1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & -1 & 0 \\ 0 & \vdots & \ddots & -1 & 2 & -1 \\ 0 & 0 & \ldots & 0 & -1 & 2 \end{pmatrix}.$$

So A_n is an n-dimensional even root lattice. We have $\mathrm{disc}(A_n) = n + 1$.

Example 2.4.4. Let $D_n := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \text{ is even}\} \subseteq \mathbb{R}^n$ for $n \geq 3$. For $1 \leq i \leq n$, let $e_i \in \mathbb{R}^n$ be the vector with 1 in the x_i coordinate and 0 elsewhere. Then

$$D_n = \mathbb{Z}(e_1 + e_2) + \mathbb{Z}(e_2 - e_1) + \mathbb{Z}(e_3 - e_2) + \cdots + \mathbb{Z}(e_n - e_{n-1}).$$

The generator matrix for D_n with respect to the basis $\{e_1 + e_2, e_2 - e_1, e_3 - e_2, \ldots, e_n - e_{n-1}\}$ is the $n \times n$ matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \dots & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & -1 & 1 \end{pmatrix}.$$

The Gramm matrix corresponding to this generator matrix is the $n \times n$ matrix

$$\begin{pmatrix} 2 & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 2 & -1 & 0 & \dots & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & \ddots & -1 & 0 \\ 0 & 0 & \vdots & \ddots & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & -1 & 2 \end{pmatrix}.$$

So D_n is an n-dimensional even root lattice. We have $\mathrm{disc}(D_n) = 4$.

Example 2.4.5. Let $E_8 := \{(x_1, \dots, x_8) \mid \text{all } x_i \in \mathbb{Z} \text{ or all } x_i \in \mathbb{Z} + \frac{1}{2}, x_1 + \dots + x_8 \text{ is even}\} \subseteq \mathbb{R}^8$. A generator matrix for E_8 is then

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

The Gramm matrix corresponding to this generator matrix is

$$\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

We have $\mathrm{disc}(E_8) = 1$ and so E_8 is an unimodular even root lattice in 8 dimensions.

Example 2.4.6. Let $E_7 := \{(x_1, \ldots, x_8) \in E_8 \mid x_1 + \cdots + x_8 = 0\} \subseteq \mathbb{R}^8$. A generator matrix for E_7 is then

$$\begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

The Gramm matrix corresponding to this generator matrix is

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}.$$

So E_7 is a 7-dimensional even root lattice. We have $\mathrm{disc}(E_7) = 2$.

Example 2.4.7. Let $E_6 := \{(x_1, \ldots, x_8) \in E_8 \mid x_1 + x_8 = x_2 + \cdots + x_7 = 0\} \subseteq \mathbb{R}^8$.

A generator matrix for E_6 is then

$$\begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

The Gramm matrix corresponding to this generator matrix is

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}.$$

So E_6 is a 6-dimensional even root lattice. We have $\mathrm{disc}(E_6) = 3$.

Theorem 2.4.8. *The root lattices $\mathbb{Z}$, A_n ($n \geq 1$), D_n ($n \geq 3$), E_6, E_7 and E_8 are indecomposable and any root lattice is isomorphic to an orthogonal direct sum of them.*

Proof. See [Hum72].

The root lattices are often the answers to some interesting geometrical problems related to lattices. We briefly describe these problems and some of the known results about them in the next section.

2.5 Some geometrical problems

The reader is referred to [CS99] for a reference. In what follows, $m(\mathscr{L})$ will denote the minimal length of a non-zero element of the lattice $\mathscr{L}$.

The sphere packing problem: The classical sphere packing problem asks for the greatest density of an arrangement of congruent nonoverlapping balls in $\mathbb{R}^n$. When the centers of the balls form a lattice, we call the packing a *lattice packing*. Any lattice $\mathscr{L}$ of rank n in $\mathbb{R}^n$ induces a packing by centering balls of radius $\frac{m(\mathscr{L})}{2}$ (the *packing radius*) at the points of $\mathscr{L}$. The density of such a lattice packing is then

$$\frac{V_n(m(\mathscr{L})/2)^n}{\sqrt{disc(\mathscr{L})}},$$

where V_n is the volume of a ball of radius 1 in $\mathbb{R}^n$. The general packing problem is solved only for $n = 1$, 2 and 3. In dimension 1, the problem is trivial; one can choose the packing induced from the lattice $\mathbb{Z}$. In dimension 2, the densest packing is in fact a lattice packing and it is obtained from the *hexagonal lattice* ($\cong A_2$). In dimension 3, the densest packing is again a lattice packing and it is obtained from the *face-centered cubic lattice* ($\cong A_3$). The proof of this result involves complex computer calculations (see [LHF11]). The problem is open for $n \geq 4$. However, the problem of finding the densest packing among the lattice packings is solved also in dimensions 4 to 8. The densest lattice packing in dimension 4 is obtained from the

lattice D_4, in dimension 5 from the lattice D_5, in dimension 6 from the lattice E_6, in dimension 7 from the lattice E_7 and in dimension 8 from the lattice E_8. The problem is open for $n \geq 9$.

The covering problem: The classical covering problem asks for the most efficient covering of the space $\mathbb{R}^n$ by congruent balls. By the most efficient covering we mean the covering minimizing the average number of balls that contain a point of the space (the *thickness*). When the centers of the balls form a lattice, the thickness is given by

$$\frac{V_n R^n}{\sqrt{\text{disc}(\mathscr{L})}},$$

where R is the radius of the balls in the covering. The problem is solved only in dimension 1 and 2. The problem is of course trivial in dimension 1; one can choose the covering induced from the lattice $\mathbb{Z}$. In dimension 2, the thinnest covering is obtained from the hexagonal lattice. In dimensions 3 to 5, only the thinnest coverings among the coverings induced from lattices are known. In dimension 3, the thinnest covering induced from a lattice is obtained from the *body-centered cubic lattice* ($\cong A_3^*$). In dimension 4, it is obtained from the lattice A_4^* and in dimension 5, from the lattice A_5^*.

The kissing number problem: The *kissing number* τ of a sphere in a sphere packing is the number of spheres that touches it. In a lattice packing, τ is the same for every sphere and it is equal to the number of elements of minimal non-zero norm in the lattice. The kissing number problem is to determine the highest possible τ when looking over all sphere packings in $\mathbb{R}^n$. The problem is solved only in dimensions 1, 2, 3, 8 and 24. The problem is of course trivial in dimension 1; one can choose the lattice $\mathbb{Z}$ with kissing number 2. In dimension 2, the highest kissing number is 6 and it is obtained from the hexagonal lattice. In dimension 3, the highest kissing number is 12 and it is obtained from the face-centered cubic

lattice. In dimension 8, the highest kissing number is 240 and it is obtained from the lattice E_8. In dimension 24, the highest kissing number is 196560 and it is obtained from the *Leech lattice*. The Leech lattice can be constructed in many different ways (see [CS99], and we will realize it using ideals in cyclotomic fields in chapter 4). It can be characterized as the only even unimodular lattice with no element of squared norm 2 (see [CS99], chapter 12). We will say more about even unimodular lattices in the next section.

In dimension 4, the highest kissing number is not known but it is either 24 or 25. However, if one looks only among lattice packings then the highest kissing number is known to be 24 and it is obtained from the lattice D_4. The highest kissing number among lattice packings is also known in dimensions 5 to 7. In dimension 5, it is 40 and it is obtained from the lattice D_5. In dimension 6, it is 72 and it is obtained from the lattice E_6. In dimension 7, it is 126 and it is obtained from the lattice E_7. The problem is open in other dimensions.

We give a table of the kissing numbers of the indecomposable root lattices and their dual for further uses. The kissing number of a lattice is one of the coefficients of its *theta series*. We talk about this in the next section.

Table 2–1: Kissing numbers of the indecomposable root lattices and their dual

Lattice	Kissing number
A_n $(n \geq 1)$	$n(n+1)$
A_n^* $(n \geq 1)$	2 $(n = 1)$, $2(n+1)$ $(n \geq 1)$
D_n $(n \geq 3)$	$2n(n-1)$
D_n^* $(n \geq 3)$	8 $(n = 3)$, 24 $(n = 4)$, $2n$ $(n \geq 5)$
E_6	72
E_6^*	54
E_7	126
E_7^*	56
E_8	240

2.6 Theta series and even unimodular lattices

Definition 2.6.1. Let $\mathscr{L} \subseteq \mathbb{R}^n$ be a lattice. For $z \in \mathbb{H} = \{\tau \in \mathbb{C} \mid Im(z) > 0\}$, we define the *theta series* of $\mathscr{L}$ by

$$\Theta_{\mathscr{L}}(z) := \sum_{x \in \mathscr{L}} q^{\frac{1}{2}x \cdot x},$$

where $q = e^{2\pi i z}$.

This is a well defined function and it is holomorphic on $\mathbb{H}$ (see [Ebe94], Lemma 2.2). We have

$$\Theta_{\mathscr{L}}(z) = 1 + \tau q^{2\rho^2} + \cdots,$$

where τ is the kissing number of $\mathscr{L}$ and ρ its packing radius. If $\mathscr{L}$ is integral and $N(m) = |\{x \in \mathscr{L} \mid x \cdot x = m\}|$ (the number of elements of $\mathscr{L}$ of squared norm m) then

$$\Theta_{\mathscr{L}}(z) = \sum_{m=0}^{\infty} N(m) q^{\frac{m}{2}}.$$

Example 2.6.2. If $\mathscr{L} = \mathbb{Z}^n$ then the coefficient $N(m)$ is the number of ways of writing m as a sum of n squares.

There is an identity relating the theta series of a lattice to the theta series of its dual. It can be derived from the Poisson summation formula (see [Ebe94]).

Proposition 2.6.3. *Let $\mathscr{L} \subseteq \mathbb{R}^n$ be a lattice. Then for all $z \in \mathbb{H}$ we have*

$$\Theta_{\mathscr{L}}(-\tfrac{1}{z}) = (\tfrac{z}{i})^{\frac{n}{2}} \frac{1}{\sqrt{disc(\mathscr{L})}} \Theta_{\mathscr{L}^*}(z).$$

Corollary 2.6.4. *Let $\mathscr{L} \subseteq \mathbb{R}^n$ be an even unimodular lattice. Then $n \equiv 0 \ (mod\ 8)$.*

Proof. Suppose the contrary. Since $\mathscr{L} \oplus \mathscr{L}$ and $\mathscr{L} \oplus \mathscr{L} \oplus \mathscr{L} \oplus \mathscr{L}$ are also even unimodular lattices, we can assume that $n \equiv 4 \ (mod\ 8)$. Then the identity for the dual implies

$$\Theta_{\mathscr{L}}(-\tfrac{1}{z}) = -z^{\frac{n}{2}} \Theta_{\mathscr{L}}(z).$$

The group $\mathrm{SL}_2(\mathbb{Z})$ of 2×2 matrices with integral coefficients and determinant 1 acts on $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(these two elements generate $\mathrm{SL}_2(\mathbb{Z})$). The theta series $\Theta_{\mathscr{L}}$ is invariant under T and thus

$$\Theta_{\mathscr{L}}((TS) \cdot z) = -z^{\frac{n}{2}}\Theta_{\mathscr{L}}(z).$$

A simple computation then gives

$$\Theta_{\mathscr{L}}(z) = \Theta_{\mathscr{L}}((TS)^3 \cdot z) = -\Theta_{\mathscr{L}}(z)$$

and so we have a contradiction. ■

Let $\mathscr{L} \subseteq \mathbb{R}^n$ be an even unimodular lattice. Knowing that we must have $n \equiv 0 \ (mod\ 8)$ and again using the identity for the dual, we get

$$\Theta_{\mathscr{L}}(-\tfrac{1}{z}) = z^{\frac{n}{2}}\Theta_{\mathscr{L}}(z).$$

It follows from this that $\Theta_{\mathscr{L}}$ is a modular form of weight $\frac{n}{2}$.

Definition 2.6.5. Let k be an integer. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a *modular form of weight k* if the following two conditions are satisfied :

i) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

ii) f has a power series expansion in $q = e^{2\pi iz}$.

Important examples of modular forms are the (normalized) *Eisenstein series* $\mathscr{E}_k$ (k an even integer and $k > 2$). Here we content ourselves by giving the power series expansion of $\mathscr{E}_k$ (for more details see [Ebe94] or [Ser73]):

$$\mathscr{E}_k(z) = 1 - \tfrac{2k}{B_k}\sum_{r=1}^{\infty}\sigma_{k-1}(r)q^r,$$

where $\sigma_{k-1}(r) = \sum_{d|r} d^{k-1}$ and B_k is the k^{th} *Bernoulli number*. The Bernoulli numbers are defined by

$$\tfrac{x}{e^x-1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

The Eisenstein series can be used to determine the $\mathbb{C}$-vector spaces M_k of modular forms of weight k. We denote by M_k^0 the $\mathbb{C}$-vector space of *cusp forms* of weight k. These are defined as the modular forms of weight k with coefficient $a_0 = 0$ in their power series expansion $\sum_{r=0}^{\infty} a_r q^r$. Hence M_k^0 is the kernel of a linear functional on M_k and so $dim(M_k/M_k^0) = 0$ or 1. If $k > 2$ and k is even, the expansion for $\mathscr{E}_k$ shows that $\mathscr{E}_k \notin M_k^0$ and thus

$$M_k = M_k^0 \oplus \mathbb{C}\mathscr{E}_k.$$

The following theorem then determines the space M_k for any integer k.

Theorem 2.6.6. *([Ebe94], Theorem 2.4)*

i) We have $M_k = 0$ for k odd, for $k < 0$ and for $k = 2$.

ii) We have $M_0 = \mathbb{C}$, $M_0^0 = 0$ and, for $k = 4, 6, 8, 10$, $M_k^0 = 0$ and $M_k = \mathbb{C}\mathscr{E}_k$.

iii) Multiplication by $\mathscr{E}_4^3 - \mathscr{E}_6^2$ defines an isomorphism of M_{k-12} onto M_k^0.

Corollary 2.6.7. *([Ebe94], Proposition 2.5) Let $\mathscr{L} \subseteq \mathbb{R}^8$ be an even unimodular lattice. Then $\mathscr{L} \cong E_8$.*

Proof. The theta series $\Theta_{\mathscr{L}}$ of $\mathscr{L}$ is a modular form of weight 4 and so $\Theta_{\mathscr{L}} \in M_4 = \mathbb{C}\mathscr{E}_4$. Since the constant term of $\Theta_{\mathscr{L}}$ is 1, we have $\Theta_{\mathscr{L}} = \mathscr{E}_4$. We then obtain from the expansion of $\mathscr{E}_4$ that $\mathscr{L}$ has 240 roots ($B_4 = -\frac{1}{30}$). The root sublattice of $\mathscr{L}$ must then be isomorphic to E_8 since any other root lattice in dimension ≤ 8 contains less roots (see Theorem 1.4.8 and Table 2-1, p.19). Then the index of the root sublattice of $\mathscr{L}$ in $\mathscr{L}$ is 1 because both are unimodular and of the same rank. We conclude that $\mathscr{L} \cong E_8$. ■

Corollary 2.6.8. *Let $\mathscr{L} \subseteq \mathbb{R}^{16}$ be an even unimodular lattice. Then $\mathscr{L} \cong E_8 \oplus E_8$ or the root sublattice of $\mathscr{L}$ is D_{16}.*

Proof. The theta series $\Theta_{\mathscr{L}}$ of $\mathscr{L}$ is a modular form of weight 8 and so $\Theta_{\mathscr{L}} \in M_8 = \mathbb{C}\mathscr{E}_8$. Since the constant term of $\Theta_{\mathscr{L}}$ is 1, we have $\Theta_{\mathscr{L}} = \mathscr{E}_8$. We then obtain from the expansion of $\mathscr{E}_8$ that $\mathscr{L}$ has 480 roots ($B_8 = -\frac{1}{30}$). The root sublattice of $\mathscr{L}$ must

then be isomorphic to $E_8 \oplus E_8$ or D_{16} since any other root lattice in dimension ≤ 16 contains less roots (see Theorem 1.4.8 and Table 2-1, p.19). If the root sublattice is $E_8 \oplus E_8$ then its index in $\mathscr{L}$ is 1 because both are unimodular and of the same rank, and so $\mathscr{L} \cong E_8 \oplus E_8$. ■

There indeed exists an even unimodular lattice of rank 16 and root sublattice D_{16} (and it is unique up to isomorphism, see [Ebe94], Example 3.1). We can obtain it by using the technique of *gluing*.

Definition 2.6.9. Let $\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k$ be positive definite integral lattices Suppose the lattice $\mathscr{L}$ is generated by $\mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k$ and some m vectors $y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)} \in \mathscr{L}_1^* \oplus \mathscr{L}_2^* \oplus \cdots \oplus \mathscr{L}_k^*$ $(1 \leq j \leq m)$ having integral inner products with each other and being closed under addition modulo $\mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k$. Let $[y^{(j)}]$ be the class of $y^{(j)}$ in the dual quotient $\mathscr{L}_1^*/\mathscr{L}_1 \oplus \mathscr{L}_2^*/\mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k^*/\mathscr{L}_k$. Then we say that the *components* $\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k$ have been *glued* together by the *glue vectors* $\{[y^{(1)}], [y^{(2)}], \ldots, [y^{(m)}]\}$ to obtain the lattice $\mathscr{L}$ and we write $\mathscr{L} = (\mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k)^+$.

Example 2.6.10. Consider the lattice D_{16} and the vector

$$y = (\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}) \in D_{16}^*.$$

Let D_{16}^+ be the lattice obtained by gluing D_{16} with the glue vector $[y]$. Then $D_{16}^+ = D_{16} \cup (y + D_{16})$ and it is an even unimodular lattice with root sublattice D_{16}.

The idea in the proofs of Corollary 2.6.7 and Corollary 2.6.8 is that we could determine the root sublattice of any even unimodular lattice of rank 8 and 16 and this enabled us to classify them. The same idea allows also to classify the even unimodular lattices in rank 24. We now say a bit more about this. We first introduce the notion of *theta series with spherical coefficients*.

Definition 2.6.11. Let $P \in \mathbb{C}[x_1, \ldots, x_n]$ be a complex polynomial in n variables and $\mathscr{L} \subseteq \mathbb{R}^n$ be a lattice.

i) P is called *spherical* if $\Delta P = 0$, where $\Delta = \sum_{i=1}^{n} \frac{\partial}{\partial x_i^2}$ is the Laplace operator.

ii) For $z \in \mathbb{H} = \{\tau \in \mathbb{C} \mid Im(z) > 0\}$, we define the *theta series with spherical coefficients* of $\mathscr{L}$ at the spherical polynomial P by

$$\Theta_{\mathscr{L},P}(z) := \sum_{x \in \mathscr{L}} P(x) q^{\frac{1}{2}x \cdot x},$$

where $q = e^{2\pi i z}$.

Proposition 2.6.12. *([Ebe94], Corollary 3.3) Let $\mathscr{L} \subseteq \mathbb{R}^n$ be an even unimodular lattice and P be a spherical polynomial in n variables of degree r. Then $\Theta_{\mathscr{L},P}$ is a modular form of weight $\frac{n}{2} + r$ and a cusp form if $r > 0$.*

Corollary 2.6.13. *Let $n = 8$, 16 or 24 and let $\mathscr{L} \subseteq \mathbb{R}^n$ be an even unimodular lattice. Then for any $y \in \mathbb{R}^n$ we have*

$$\sum_{x \in R} (x \cdot y)^2 = \frac{2|R|}{n}(y \cdot y),$$

where $R = \{x \in \mathscr{L} \mid x \cdot x = 2\}$ is the set of roots in $\mathscr{L}$.

Proof. Let $y \in \mathbb{R}^n$ ($n = 8$, 16 or 24). Also, let

$$f_y(x) := (x \cdot y)^2 - \tfrac{(x \cdot x)(y \cdot y)}{n} \text{ for } x \in \mathbb{R}^n.$$

It is easily verified from the definitions that f_y is a spherical polynomial. From the last proposition, $\Theta_{\mathscr{L},f_y}$ is then a cusp form of weight $\frac{n}{2} + 2$ (= 6, 10 or 14). This form is equal to 0 from Theorem 2.6.6. In particular, the coefficient in front of q in the power series for $\Theta_{\mathscr{L},f_y}$ is 0. This coefficient is

$$\sum_{x \in R} f_y(x)$$

and the result follows. ■

Keep assuming that $\mathscr{L} \subseteq \mathbb{R}^n$ is an even unimodular lattice and $n = 8$, 16 or 24. If $\mathscr{L}$ has roots then the root sublattice of $\mathscr{L}$ has rank n since otherwise there would exist a non-zero $y \in \mathbb{R}^n$ orthogonal to every roots of $\mathscr{L}$ and this would contradict the last corollary.

Definition 2.6.14. Let $\mathscr{L} \subseteq \mathbb{R}^n$ be a lattice. If $\mathscr{L}$ has roots and the root sublattice of $\mathscr{L}$ has rank n then we say that $\mathscr{L}$ has a *complete root system*.

For any indecomposable root lattice $\mathscr{L}'$ with set of roots R', it is possible to show that for any $y \in \mathbb{R}\mathscr{L}'$ we have

$$\sum_{x \in R'} (x \cdot y)^2 = 2h(y \cdot y),$$

where $h = \frac{|R'|}{\mathrm{rk}(\mathscr{L}')}$ is the *Coxeter number* of $\mathscr{L}'$ (see [Ebe94], Proposition 1.6). It then follows from Corollary 2.6.13 that all the indecomposable components of the root sublattice of $\mathscr{L}$ have the same Coxeter number h and $h = \frac{1}{n}|R|$. We therefore have the following proposition.

Proposition 2.6.15. *Let $n = 8$, 16 or 24 and let $\mathscr{L} \subseteq \mathbb{R}^n$ be an even unimodular lattice. Then either $\mathscr{L}$ has no roots or has a complete root system. Moreover, if $\mathscr{L}$ has roots then all the indecomposable components of the root sublattice of $\mathscr{L}$ have the same Coxeter number h and $h = \frac{1}{n}|R|$.*

This proposition imposes strong restrictions on the possible root sublattices of an even unimodular lattice in dimension 24. It is then not difficult (see [CS99], chapter 18, Proposition 3) to obtain a list of only 23 possible root sublattices (assuming the lattice indeed has roots). It turn out that each of these 23 possibilities is indeed the root sublattice of an even unimodular lattice of rank 24 and this for a unique lattice up to isomorphism. One can construct them and show their uniqueness using among other things algebraic coding (see [CS99], chapter 18, sections 3 and 4). We can also obtain them from the technique of gluing. They are the following (we won't give the glue vectors, see [CS99], Table 16.1): D_{24}^+, $D_{16}^+ \oplus E_8$, $3E_8$, A_{24}^+, $(2D_{12})^+$, $(A_{17} \oplus E_7)^+$, $(D_{10} \oplus 2E_7)^+$, $(A_{15} \oplus D_9)^+$, $(3D_8)^+$, $(2A_{12})^+$, $(A_{11} \oplus D_7 \oplus E_6)^+$, $(4E_6)^+$, $(2A_9 \oplus D_6)^+$, $(4D_6)^+$, $(3A_8)^+$, $(2A_7 \oplus 2D_5)^+$, $(4A_6)^+$, $(4A_5 \oplus D_4)^+$, $(6D_4)^+$, $(6A_4)^+$, $(8A_3)^+$, $(12A_2)^+$ and $(24A_1)^+$.

In each case, the root sublattice is the orthogonal direct sum of the components of the glue. It remains to talk about the case where an even unimodular lattice of rank 24 has no roots. It can be shown that there is a unique such lattice : the Leech

lattice (see [CS99], chapter 12 and 18). Hence there are exactly 24 even unimodular lattices of rank 24. They are often referred to as the *Niemeier lattices*.

It is possible to verify that the 24 Niemeier lattices are indeed all the even unimodular lattices of rank 24 by using the *Minkowski-Siegel mass formula* (if one knows the cardinality of the automorphism groups of these lattices).

Theorem 2.6.16. *([CS99], Chapter* 16*, Theorem* 2*) Let* Ω *be the set of all inequivalent even unimodular lattices of dimension* n*. Then*

$$\sum_{\mathscr{L}\in\Omega} \frac{1}{|\mathrm{Aut}(\mathscr{L})|} = \frac{|B_k|}{2k} \prod_{j=1}^{k-1} \frac{|B_{2j}|}{4j},$$

if $n = 2k \equiv 0 \ (mod\ 8)$.

For $n = 32$, the right-hand side above is greater than 40 million and since $|\mathrm{Aut}(\mathscr{L})| \geq 2$ for any lattice ($\{Id, -Id\} \subseteq \mathrm{Aut}(\mathscr{L})$), it follows that there are more than 80 million inequivalent even unimodular lattices of rank 32 (In fact, there are more than 1 billion such lattices (see [Kin03])). No general classification of these lattices is known. However, the decomposable even unimodular lattices of rank 32 are easily determined from the classification of even unimodular lattices in dimension 8, 16 and 24 since any indecomposable component is then an even unimodular lattice in dimension 8, 16 or 24. There are 25 of them: $2D_{16}^{+}$ and $E_8 \oplus \mathscr{L}$, where $\mathscr{L}$ is one of the 24 Niemeier lattices. These lattices all have a complete root system with the exclusion of $E_8 \oplus \Lambda$, where Λ is the Leech lattice (note that this example shows that Proposition 2.6.15 is not true for $n = 32$). Maybe quite surprisingly, the even unimodular lattices of rank 32 having a complete root system are all classified ([Ker94]). There are 132 indecomposable even unimodular lattices of rank 32 having a complete root system (and 119 root sublattices are occurring). We can list them according to the *deficiency* of their root sublattice. The deficiency of a root lattice of rank n is the number $n - m$, where m is the maximal cardinality of a set of mutually orthogonal roots in the lattice. The possible deficiencies of an even unimodular

lattices of rank 32 with complete root system are 0, 8, 12, 14, 15 and 16. There are 75 indecomposable even unimodular lattices of rank 32 with complete root system and deficiency 0 (and 62 root sublattices are occurring). The indecomposable even unimodular lattices of rank 32 with complete root system and non-zero deficiencies are unique having their particular root sublattice and the list of these 57 lattices is given in [Ker94]. We shall realize three of these lattices as ideals in cyclotomic fields in chapter 4. But before that, we need to describe how we can see ideals in number fields as lattices and we need to determine their basic properties. We turn to this task in chapter 3.

CHAPTER 3
Lattices from number fields

3.1 Preliminaries and the trace pairing

Let K be a number field with $n = [K : \mathbb{Q}]$. Then K has n embeddings in the complex numbers $\mathbb{C}$, we will denote them by $\{\sigma_1, \ldots, \sigma_n\}$. When $\sigma_i(K) \subseteq \mathbb{R}$, σ_i is said to be a *real* embedding, otherwise it is said to be a *complex* embedding. If σ_i is a complex embedding then the conjugate $\overline{\sigma_i}$ is a distinct embedding. So there is an even number of complex embeddings. Suppose that there exists r_1 real embeddings and $2r_2$ complex embeddings (so $r_1 + 2r_2 = n$). We will assume that $\{\sigma_1, \ldots, \sigma_{r_1}\}$ are the real embeddings and that $\overline{\sigma_{r_1+i}} = \sigma_{r_1+r_2+i}$ for $i = 1, \ldots, r_2$. We use these embeddings to define a map ϕ from K to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by

$$\phi(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

It is clear that ϕ is a ring embedding.

We identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$ by

$$(x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+r_2}) \leftrightarrow$$

$$(x_1, \ldots, x_{r_1}, Re(x_{r_1+1}), Im(x_{r_1+1}), \ldots, Re(x_{r_1+r_2}), Im(x_{r_1+r_2})).$$

We then have the following:

Proposition 3.1.1. *$\phi(K)$ spans $\mathbb{R}^n$ as a vector space over $\mathbb{R}$.*

Proof. Suppose it is not the case. Then there is a non-zero linear functional vanishing on $\phi(K)$. That is, there are $a_1, \ldots, a_{r_1}, b_1, \ldots, b_{r_2}, c_1, \ldots, c_{r_2}$ in $\mathbb{R}$, not all zero, such that for every $x \in K$ we have

$$\sum_{j=1}^{r_1} a_j \sigma_j(x) + \sum_{j=1}^{r_2} b_j Re(\sigma_{r_1+j}(x)) + \sum_{j=1}^{r_2} c_j Im(\sigma_{r_1+j}(x)) = 0.$$

Using that $Re(z) = \frac{z+\overline{z}}{2}$ and $Im(z) = \frac{z-\overline{z}}{2i}$ and regrouping, we get

$$\sum_{j=1}^{r_1} a_j\sigma_j(x) + \sum_{j=1}^{r_2}(\frac{b_j}{2} + \frac{c_j}{2i})\sigma_{r_1+j}(x) + \sum_{j=1}^{r_2}(\frac{b_j}{2} - \frac{c_j}{2i})\overline{\sigma_{r_1+j}}(x) = 0.$$

It now follows from the independence of characters that we must have $a_j = 0$ for $j = 1, \ldots, r_1$, $\frac{b_j}{2} + \frac{c_j}{2i} = 0$ and $\frac{b_j}{2} - \frac{c_j}{2i} = 0$ for $j = 1, \ldots, r_2$. Then also $b_j = 0$ and $c_j = 0$ for $j = 1, \ldots, r_2$. This is a contradiction. ■

The preceding proposition says that there exists linearly independent vectors $\alpha_1, \ldots, \alpha_n$ such that $\phi(K) = Span_{\mathbb{Q}}\{\alpha_1, \ldots, \alpha_n\}$. The map ϕ being a ring embedding, $Span_{\mathbb{Q}}\{\alpha_1, \ldots, \alpha_n\}$ is a field in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The following proposition is a kind of converse to this.

Proposition 3.1.2. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ be linearly independent vectors over $\mathbb{R}$ and suppose that $L = Span_{\mathbb{Q}}\{\alpha_1, \ldots, \alpha_n\}$ is a field as a subring of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (with the same 1). Then the projection maps*

$$\pi_i : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{C},\ (x_1, \ldots, x_{r_1+r_2}) \mapsto x_i,$$

for $i = 1, \ldots, r_1 + r_2$, when restricted to L, give the r_1 real embeddings of L into $\mathbb{C}$ and r_2 complex non-conjugate embeddings of L into $\mathbb{C}$.

Proof. First note that each π_i is a ring homomorphism. Suppose that $\pi_i(x) = 0$ for some $x \in L$. That is, the i^{th} coordinate of x is 0. But then x is not invertible and it belongs to a field, so it must be 0. Therefore, $\pi_i|_L$ is injective. For each $1 \leq i \leq r_1$, $\pi_i|_L$ is a real embedding of L. They are all distinct because $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{R}$. For the same reason, when $r_1+1 \leq i \leq r_1+r_2$, $\pi_i|_L$ is a complex embedding and they are all distinct and non-conjugate. ■

We now use the two last propositions to compute the group of automorphisms of the $\mathbb{R}$-algebra $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Proposition 3.1.3. *Let $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ be the group of continuous ring automorphisms of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}) \cong S_{r_1} \times ((\mathbb{Z}/2\mathbb{Z})^{r_2} \rtimes S_{r_2})$, where S_k is the symmetric group on k elements and S_{r_2} acts on $(\mathbb{Z}/2\mathbb{Z})^{r_2}$ by permuting the components.*

Proof. Given an element of the set $S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2}$, there is a natural automorphism associated to it : the permutation in S_{r_1} acts by permuting the r_1 real components of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, then the element of $(\mathbb{Z}/2\mathbb{Z})^{r_2}$ acts by conjugating the complex components where there is a 1 in the corresponding entry and, after that, the permutation in S_{r_2} acts by permuting the r_2 complex components of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. We will show that these are all the elements of $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$. In particular, since they are linear over $\mathbb{R}$, it will follow that $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ is also the group of automorphisms of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as an $\mathbb{R}$-algebra.

Let K be a finite field extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$ and with r_1 real embeddings and $2r_2$ complex embeddings. By the primitive element theorem, there exists an algebraic element θ of degree n such that $K = \mathbb{Q}(\theta)$. Let f be the minimal polynomial of θ over $\mathbb{Q}$. Let $\zeta = \phi(\theta)$, so that $\phi(K) = \mathbb{Q}(\phi(\theta)) = \mathbb{Q}(\zeta)$. Note that $\mathbb{Q}$ is also seen as the subset $Span_{\mathbb{Q}}\{(1, \ldots, 1)\}$ of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let $\sigma \in \mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$. Then $\sigma(\zeta)$ determines σ on all $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ because $\phi(K)$ is dense in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by Proposition 3.1.1. Also, $\sigma(\mathbb{Q}(\zeta)) = \mathbb{Q}(\sigma(\zeta))$ is dense in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ because σ is continuous and surjective. Any dense subset of $\mathbb{R}^n$ must contain a basis of $\mathbb{R}^n$ and therefore the vectors $1, \sigma(\zeta), \ldots, \sigma(\zeta)^{n-1}$ are linearly independent over $\mathbb{R}$. Then it follows from Proposition 3.1.2 and from

$$f(\sigma(\zeta)) = \sigma(f(\zeta)) = \sigma(0) = 0$$

that the real components of $\sigma(\zeta)$ are the r_1 real roots of f and that the complex components are r_2 non-conjugate complex roots of f. The same is true for ζ and so σ acts on ζ as an element of $S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2}$ would do. We conclude that we can identify $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ with $S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2}$ as sets. The group law on $S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2}$ corresponding to composition of automorphisms in $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ is then

$$(\sigma_2, Y, \tau_2) \circ (\sigma_1, X, \tau_1) = (\sigma_2\sigma_1, X + \tau_1^{-1} \cdot Y, \tau_2\tau_1),$$

where an element of S_{r_2} acts on $(\mathbb{Z}/2\mathbb{Z})^{r_2}$ by permuting the components. Then the map

$$S_{r_1} \times ((\mathbb{Z}/2\mathbb{Z})^{r_2} \rtimes S_{r_2}) \to S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2},\ (\sigma, X, \tau) \mapsto (\sigma, \tau^{-1} \cdot X, \tau)$$

is an isomorphism of groups.■

From now on, we will make no distinction between $\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ and $S_{r_1} \times (\mathbb{Z}/2\mathbb{Z})^{r_2} \times S_{r_2}$ with the group law described in the preceding proof.

Corollary 3.1.4. *An element $(\sigma, X, \tau) \in \mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ has order 2 if and only if it is non-trivial, σ and τ are a product of disjoint transpositions (possibly none) and, if $X = (x_1, \ldots, x_{r_2})$ and (i, j) is a transposition in the decomposition of τ then $x_i = x_j$.*

Definition 3.1.5. An automorphism of order 1 or 2 is called an *involution*.

We now consider the $\mathbb{R}$-algebra $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. It contains an isomorphic copy of the field K in an obvious way: $K \cong \{x \otimes 1 \mid x \in K\} \subseteq K_{\mathbb{R}}$. If $\sigma : K \to \mathbb{C}$ is a field embedding it extends uniquely to an $\mathbb{R}$-algebra homomorphism $\sigma : K_{\mathbb{R}} \to \mathbb{C}$ (we still call it σ). Then also the map $\phi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ extends uniquely to an $\mathbb{R}$-algebra homomorphism $\phi : K_{\mathbb{R}} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (we still call it ϕ). It is in fact an isomorphism because it is surjective by Proposition 3.1.1. This isomorphism and the last proposition give us a concrete description of the group of automorphisms of the $\mathbb{R}$-algebra $K_{\mathbb{R}}$:

$$\mathrm{Aut}(K_{\mathbb{R}}) = \{\phi^{-1} \circ (\sigma, X, \tau) \circ \phi \mid (\sigma, X, \tau) \in \mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})\}.$$

Let $\mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x)$ be the trace of the $\mathbb{R}$-linear map multiplication by x for $x \in K_{\mathbb{R}}$. When $x \in K$, we have $\mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x) = \mathrm{Tr}_{K/\mathbb{Q}}(x)$. From now on, we will write Tr for $\mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}$ or $\mathrm{Tr}_{K/\mathbb{Q}}$. For $x \in K_{\mathbb{R}}$, we have

$$\mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x) = \sum_{i=1}^{r_1} \sigma_i(x) + 2 \sum_{i=r_1+1}^{r_1+r_2} Re(\sigma_i(x)).$$

We use this trace map to define an $\mathbb{R}$-bilinear symmetric non-degenerate pairing on $K_{\mathbb{R}} \times K_{\mathbb{R}}$. Let $- : K_{\mathbb{R}} \to K_{\mathbb{R}}$ be an involution of $K_{\mathbb{R}}$ (the identity is allowed) and let $\alpha \in K_{\mathbb{R}}$ be an invertible element such that $\overline{\alpha} = \alpha$. The pairing

$$K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R},\ (x, y) \mapsto \mathrm{Tr}(\alpha x \overline{y})$$

is $\mathbb{R}$-bilinear because the trace map is linear and it is symmetric because $\mathrm{Tr}(\overline{x}) = \mathrm{Tr}(x)$ for all $x \in K_{\mathbb{R}}$. In fact, for any automorphism f of $K_{\mathbb{R}}$, we have $\mathrm{Tr}(f(x)) = \mathrm{Tr}(x)$ for all $x \in K_{\mathbb{R}}$ (but we won't use that fact). The non-degeneracy of the pairing follows from the independence of characters. We will consider this pairing on ideals of K (fractional ideals). A non-zero ideal is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$ and so the pairing $\mathrm{Tr}(\alpha x \overline{y})$ makes it into a lattice.

Definition 3.1.6. An ideal I with pairing $\mathrm{Tr}(\alpha x \overline{y})$ on $I \times I$ will be called an *ideal lattice.*

3.2 Discriminant

We first compute the discriminant of ideal lattices.

Proposition 3.2.1. *Let I be an ideal of K with pairing $\mathrm{Tr}(\alpha x \overline{y})$ on $I \times I$. Then*

$$\mathrm{disc}(I) = N(I)^2 |N(\alpha)| |D_K|,$$

where $N(I)$ is the norm of the ideal I, $N(\alpha)$ is the norm of α (that is the determinant of the linear map multiplication by α) and D_K is the discriminant of the field K.

Proof. Let O_K be the ring of integers of K. There exists an element $d \in \mathbb{Z}$ such that $dI \subseteq O_K$. Using that, we can easily reduce to the case where $I \subseteq O_K$. Then by using $N(I) = |O_K/I|$ (the index of I in O_K) and the general fact that if $\mathscr{L}' \subseteq \mathscr{L}$ are free $\mathbb{Z}$-module of the same rank (with a pairing on $\mathscr{L}$ restricting to a pairing on $\mathscr{L}'$) then $\mathrm{disc}(\mathscr{L}') = \mathrm{disc}(\mathscr{L})|\mathscr{L}/\mathscr{L}'|^2$, we can reduce to the case where $I = O_K$. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for O_K. Then

$$\begin{aligned}
\mathrm{disc}(O_K) &= |\det(\mathrm{Tr}(\alpha x_i \overline{x_j}))| \\
&= |\det((\sigma_j(x_i))diag(\sigma_i(\alpha))(\sigma_i(\overline{x_j})))| \\
&= |\prod_{i=1}^{n} \sigma_i(\alpha)||\det(\sigma_j(x_i))||\det(\sigma_i(\overline{x_j}))| \\
&= |N(\alpha)||D_K|^{\frac{1}{2}}|D_K|^{\frac{1}{2}} = |N(\alpha)||D_K|,
\end{aligned}$$

because

$$\det((\sigma_j(x_i))(\sigma_i(x_j))) = \det(\mathrm{Tr}(x_i x_j)) = D_K$$

and

$$\det((\sigma_j(\overline{x_i}))(\sigma_i(\overline{x_j}))) = \det(\mathrm{Tr}(\overline{x_i x_j})) = \det(\mathrm{Tr}(x_i x_j)) = D_K. \blacksquare$$

3.3 Signature

We now want to compute the signature of the quadratic form $\mathrm{Tr}(\alpha x \overline{x})$ (or equivalently, the signature of an ideal lattice). Suppose that our chosen involution on $K_{\mathbb{R}}$ is equal to $\phi^{-1} \circ (\tau, X, \omega) \circ \phi$, where (τ, X, ω) is as described in Corollary 2.4. Let $X = (x_1, \ldots, x_{r_2})$ and write $\tau = (i_1, i_2)(i_3, i_4) \cdots (i_{k-1}, i_k)$ and $\omega = (j_1, j_2)(j_3, j_4) \cdots (j_{l-1}, j_l)$ as products of disjoint transpositions. Also let

$$S = \{i \mid \tau(i) = i\},$$

$$E = \{i \in S \mid \sigma_i(\alpha) < 0\},$$

$$S' = \{i \mid \omega(i) = i\},$$

$$A = \{i \in S' \mid x_i = 1\},$$

$$F = \{i \in A \mid Re(\sigma_{r_1+i}(\alpha)) < 0\}.$$

We then have the following result.

Proposition 3.3.1. *Let $(r, n-r)$ be the signature of the real quadratic form $Tr(\alpha x \overline{x})$. Also let $s = |S|$, $e = |E|$, $a = |A|$ and $f = |F|$. Then*

$$r = \tfrac{r_1+s}{2} - e + a - 2f + r_2.$$

Proof. Let $a_i = -1$ when $x_i = 1$ and $a_i = 1$ when $x_i = 0$. Also let $X_i = \sigma_i(x)$ for $1 \leq i \leq r_1$ and $X_{r_1+j} = Re(\sigma_{r_1+\frac{j+1}{2}}(x))$ when j is odd and $X_{r_1+j} = Im(\sigma_{r_1+\frac{j}{2}}(x))$ when j is even, for $1 \leq j \leq 2r_2$. On one hand, we have that $\phi(\overline{x})$ is equal to

$$(\sigma_1(\overline{x}), \ldots, \sigma_{r_1}(\overline{x}), Re(\sigma_{r_1+1}(\overline{x})), Im(\sigma_{r_1+1}(\overline{x})), \ldots, Re(\sigma_{r_1+r_2}(\overline{x})), Im(\sigma_{r_1+r_2}(\overline{x}))).$$

On the other hand, it is equal to $(\tau, X, \omega) \circ \phi(x)$ and $(\tau, X, \omega) \circ \phi(x)$ is equal to

$$(\sigma_{\tau(1)}(x), \ldots, \sigma_{\tau(r_1)}(x), Re(\sigma_{r_1+\omega(1)}(x)), a_1 Im(\sigma_{r_1+\omega(1)}(x)), \ldots, a_{r_2} Im(\sigma_{r_1+\omega(r_2)}(x))).$$

Therefore we have

$$\sigma_i(\overline{x}) = \sigma_{\tau(i)}(x) = X_{\tau(i)} \text{ for } 1 \leq i \leq r_1,$$

$$Re(\sigma_{r_1+i}(\overline{x})) = Re(\sigma_{r_1+\omega(i)}(x)) = X_{r_1+2\omega(i)-1} \text{ for } 1 \leq i \leq r_2$$

and

$$Im(\sigma_{r_1+i}(\overline{x})) = a_i Im(\sigma_{r_1+\omega(i)}(x)) = a_i X_{r_1+2\omega(i)} \text{ for } 1 \leq i \leq r_2.$$

We will use these relations to express the quadratic form $\mathrm{Tr}(\alpha x \overline{x})$ in terms of the X_i's. We have

$$\begin{aligned}
&\sum_{i=1}^{r_1} \sigma_i(\alpha)\sigma_i(x)\sigma_i(\overline{x}) + 2\sum_{i=r_1+1}^{r_1+r_2} Re(\sigma_i(\alpha)\sigma_i(x)\sigma_i(\overline{x})) \\
=&\sum_{i=1}^{r_1} \sigma_i(\alpha)\sigma_i(x)\sigma_i(\overline{x}) + 2\sum_{i=r_1+1}^{r_1+r_2} Re(\sigma_i(\alpha))Re(\sigma_i(x))Re(\sigma_i(\overline{x})) \\
&- 2\sum_{i=r_1+1}^{r_1+r_2} Im(\sigma_i(\alpha))Im(\sigma_i(x))Re(\sigma_i(\overline{x})) - 2\sum_{i=r_1+1}^{r_1+r_2} Im(\sigma_i(\alpha))Re(\sigma_i(x))Im(\sigma_i(\overline{x})) \\
&- 2\sum_{i=r_1+1}^{r_1+r_2} Re(\sigma_i(\alpha))Im(\sigma_i(x))Im(\sigma_i(\overline{x})) \\
=&\sum_{i=1}^{r_1} \sigma_i(\alpha) X_i X_{\tau(i)} + 2\sum_{j=1}^{r_2} Re(\sigma_{j+r_1}(\alpha)) X_{r_1+2j-1} X_{r_1+2\omega(j)-1} \\
&- 2\sum_{j=1}^{r_2} Im(\sigma_{j+r_1}(\alpha)) X_{r_1+2j} X_{r_1+2\omega(j)-1} - 2\sum_{j=1}^{r_2} a_j Im(\sigma_{j+r_1}(\alpha)) X_{r_1+2j-1} X_{r_1+2\omega(j)} \\
&- 2\sum_{j=1}^{r_2} a_j Re(\sigma_{j+r_1}(\alpha)) X_{r_1+2j} X_{r_1+2\omega(j)}
\end{aligned}$$

and the last expression is equal to

$$\sum_{i\in S}\sigma_i(\alpha)X_i^2 + 2\sum_{i\in\{i_2,i_4,\ldots,i_k\}}\sigma_i(\alpha)X_iX_{\tau(i)}$$
$$+ 2\sum_{j\in A} Re(\sigma_{j+r_1}(\alpha))X_{r_1+2j-1}^2 + Re(\sigma_{j+r_1}(\alpha))X_{r_1+2j}^2$$
$$+ 2\sum_{j\in S'\setminus A} Re(\sigma_{j+r_1}(\alpha))X_{r_1+2j-1}^2 - 2Im(\sigma_{j+r_1}(\alpha))X_{r_1+2j-1}X_{r_1+2j} - Re(\sigma_{j+r_1}(\alpha))X_{r_1+2j}^2$$
$$+ 4\sum_{j\in\{j_2,j_4,\ldots,j_l\}} Re(\sigma_{j+r_1}(\alpha))X_{r_1+2j-1}X_{r_1+2\omega(j)-1}$$
$$- Im(\sigma_{j+r_1}(\alpha))X_{r_1+2j}X_{r_1+2\omega(j)-1} - a_jIm(\sigma_{j+r_1}(\alpha))X_{r_1+2j-1}X_{r_1+2\omega(j)}$$
$$- a_jRe(\sigma_{j+r_1}(\alpha))X_{r_1+2j}X_{r_1+2\omega(j)}.$$

For any $\gamma,\beta\in\mathbb{R}$ with γ or β non-zero, the quadratic form $\gamma x_1^2+\beta x_1x_2-\gamma x_2^2$ has signature $(1,1)$ and the quadratic form $\gamma x_1x_2+\beta x_3x_2-\beta x_1x_4+\gamma x_3x_4$ has signature $(2,2)$. It is now easy using the expression for $\mathrm{Tr}(\alpha x\overline{x})$ we have just computed to obtain the formula we wanted to prove. ■

Corollary 3.3.2. *The quadratic form* $\mathrm{Tr}(\alpha x^2)$ *has signature* (r_1+r_2-e, r_2+e).

Definition 3.3.3. The involution $\phi^{-1}\circ(id,(1,1,\ldots,1),id)\circ\phi$ of $K_{\mathbb{R}}$ is called the *canonical involution.*

Corollary 3.3.4. *The quadratic form* $\mathrm{Tr}(\alpha x\overline{x})$ *is positive definite if and only if the involution is the canonical involution and* α *is totally positive (that is,* $\sigma_i(\alpha)$ *is real and* $\sigma_i(\alpha)>0$ *for all* $1\le i\le n$*).*

We end this section with a result on the minimum of ideal lattices in the positive definite case. Let $m(I)=min_{x\in I\setminus\{0\}}\{\mathrm{Tr}(\alpha x\overline{x})\}$ be the minimum squared norm of a non-zero element of the ideal lattice I. We then have the following proposition:

Proposition 3.3.5. *Suppose* $I\subset O_K$ *(the ring of integers of* K*). Then*

$$m(I)\ge nN(\alpha)^{\frac{1}{n}}.$$

Furthermore, when $I = O_K$ and $\alpha = 1$, we have equality and it is attained by $x \in O_K$ if and only if x is a root of unity.

Proof. This is a consequence of the inequality between the arithmetic and the geometric means. For all non-zero $x \in I$, we have

$$\begin{aligned} \mathrm{Tr}(\alpha x\overline{x}) &= \sum_{i=1}^{n} \sigma_i(\alpha)|\sigma_i(x)|^2 \\ &\geq n(\prod_{i=1}^{n} \sigma_i(\alpha)|\sigma_i(x)|^2)^{\frac{1}{n}} \\ &= nN(\alpha x\overline{x})^{\frac{1}{n}} \\ &= nN(\alpha)^{\frac{1}{n}}|N(x)|^{\frac{2}{n}} \\ &\geq nN(\alpha)^{\frac{1}{n}}. \end{aligned}$$

Now, suppose that $I = O_K$ and $\alpha = 1$. If x is a root of unity, it is clear that $\mathrm{Tr}(x\overline{x}) = n$. Therefore $m(I) = n$. Conversely, if $x \in O_K$ satisfies $\mathrm{Tr}(x\overline{x}) = m(I) = n$ we must have equality everywhere above. But the inequality between the arithmetic and the geometric means is an equality if and only if every terms are equal. In our case, this implies that $|\sigma_i(x)| = 1$ for all $1 \leq i \leq n$. Then x is a unit in O_K because $|N(x)| = 1$. Consider the set $E = \{x^k \mid k \text{ is an integer}\}$. If $u \in E$ then $|\sigma_i(u)| = 1$ for all $1 \leq i \leq n$ and so $Tr(u\overline{u}) = n$. Then by the discreteness property of lattices (see Proposition 2.3.2), there can be only a finite number of elements in E. We conclude that x is a root of unity. ■

3.4 Rationality and positive definiteness

We would like to know when an ideal lattice is *rational*, that is, when the pairing is rational valued on $I \times I$. This happens if and only if the pairing is rational valued on $K \times K$ and we therefore have an underlying rational quadratic form.

Proposition 3.4.1. *Let I be an ideal lattice with pairing $\mathrm{Tr}(\alpha x\overline{y})$. Then I is a rational lattice if and only if $\alpha \in K$ and $\overline{K} = K$.*

Proof. If $\alpha \in K$ and $\overline{K} = K$ then it is clear that the pairing is rational valued on $K \times K$ and that I is a rational lattice. Suppose now that I is a rational lattice. Then $\mathrm{Tr}(\alpha x\overline{y}) \in \mathbb{Q}$ for all $x, y \in K$.

The pairing $\mathrm{Tr}(xy)$ on $K \times K$ is rational valued. Let $\{e_1, e_2, \ldots, e_n\} \subseteq K \hookrightarrow K_{\mathbb{R}}$ be an orthogonal basis for K (and so also for $K_{\mathbb{R}}$) with respect to this pairing. Let $a_i = \mathrm{Tr}(e_i^2) \in \mathbb{Q}$ for $1 \leq i \leq n$. Write $\alpha = \sum_{i=1}^n \alpha_i e_i$ with $\alpha_i \in \mathbb{R}$. Then, for all $1 \leq j \leq n$,

$$\begin{aligned} \mathbb{Q} \ni \mathrm{Tr}(\alpha e_j \overline{1}) &= \mathrm{Tr}(\sum_{i=1}^n \alpha_i e_i e_j) \\ &= \sum_{i=1}^n \alpha_i \mathrm{Tr}(e_i e_j) \\ &= a_j \alpha_j. \end{aligned}$$

Thus $\alpha_j \in \mathbb{Q}$ for all $1 \leq j \leq n$. We conclude that $\alpha \in K$. Choose any $y \in K$ and write $\overline{y} = \sum_{i=1}^n y_i e_i$ with $y_i \in \mathbb{R}$. Then, for all $1 \leq j \leq n$,

$$\begin{aligned} \mathbb{Q} \ni \mathrm{Tr}(\alpha(\alpha^{-1} e_j)\overline{y}) &= \mathrm{Tr}(e_j \sum_{i=1}^n y_i e_i) \\ &= \sum_{i=1}^n y_i \mathrm{Tr}(e_i e_j) \\ &= a_j y_j. \end{aligned}$$

Thus $y_j \in \mathbb{Q}$ for all $1 \leq j \leq n$ and $\overline{y} \in K$. We conclude that $\overline{K} = K$. ■

Remark 3.4.2. I is similar to a rational lattice if and only if $\overline{K} = K$ and α is a real multiple of an element of K.

We now turn our attention to the case where $\alpha \in K$ and $\overline{K} = K$. We say a bit more about the signature. Let F be the fixed field of the involution, that is the set of $x \in K$ such that $\overline{x} = x$. Suppose the involution is non-trivial. Then K is a quadratic extension of F and $K = F(\sqrt{\theta})$ for some $\theta \in F^\times$. With the notations of Proposition 3.3.1, for $1 \leq i \leq r_1$, we have

$$\sigma_{\tau(i)}(\sqrt{\theta}) = \sigma_i(\overline{\sqrt{\theta}}) = \sigma_i(-\sqrt{\theta}) = -\sigma_i(\sqrt{\theta}) \neq \sigma_i(\sqrt{\theta}).$$

Thus $\tau(i) \neq i$. Now suppose that $1 \leq i \leq r_2$. If σ_{r_1+i} restricted to F is a complex embedding of F into $\mathbb{C}$ then there exists an $x \in F$ such that $\sigma_{r_1+i}(x) \notin \mathbb{R}$. It follows that

$$\sigma_{r_1+i}(\overline{x}) = \sigma_{r_1+i}(x) \neq \overline{\sigma_{r_1+i}(x)}.$$

Also we have

$$\sigma_{r_1+i}(\overline{\sqrt{\theta}}) = -\sigma_{r_1+i}(\sqrt{\theta}) \neq \sigma_{r_1+i}(\sqrt{\theta}).$$

So $w(i) \neq i$. If σ_{r_1+i} restricted to F is a real embedding of F into $\mathbb{C}$ then

$$\sigma_{r_1+i}(\sqrt{\theta}) = \pm\sqrt{\sigma_{r_1+i}(\theta)} \text{ and } \sigma_{r_1+i}(\theta) < 0.$$

Therefore

$$\sigma_{r_1+i}(\overline{\sqrt{\theta}}) = -\sigma_{r_1+i}(\sqrt{\theta}) = \overline{\sigma_{r_1+i}(\sqrt{\theta})}.$$

Also, for all $x \in F$,

$$\sigma_{r_1+i}(\overline{x}) = \sigma_{r_1+i}(x) = \overline{\sigma_{r_1+i}(x)}.$$

We conclude that $w(i) = i$ and $x_i = -1$. Therefore we have

$$s = 0,$$

$$e = 0,$$

$$a = |\{\text{real embeddings } \sigma \text{ of } F \text{ such that } \sigma(\theta) < 0\}| \text{ and}$$

$$f = |\{\text{real embeddings } \sigma \text{ of } F \text{ such that } \sigma(\theta) < 0 \text{ and } \sigma(\alpha) < 0\}|.$$

By Proposition 3.3.1, if the signature of the quadratic form is $(r, n-r)$ then

$$r = \tfrac{n}{2} + a - 2f.$$

We deduce the following proposition.

Proposition 3.4.3. *Suppose that $\alpha \in K$ and $\overline{K} = K$. Then the quadratic form $\mathrm{Tr}(\alpha x\overline{x})$ is positive definite if and only if α is totally positive and either K is totally real with trivial involution or K is a CM-field with canonical involution.*

Recall that a *CM-field* is a totally imaginary number field that is also a quadratic extension of a totally real number field. An important class of examples of CM-fields

are the cyclotomic fields. This is the topic of the next chapter. But before going into that, we talk about the dual lattice of a rational ideal lattice and we determine a criterion for unimodularity.

For a positive definite rational ideal lattice I, let's consider the dual lattice

$$I^* = \{x \in K_{\mathbb{R}} \mid \mathrm{Tr}(\alpha x\overline{y}) \in \mathbb{Z} \text{ for all } y \in I\}.$$

In fact, we have

$$I^* = \{x \in K \mid \mathrm{Tr}(\alpha x\overline{y}) \in \mathbb{Z} \text{ for all } y \in I\}.$$

Let $a \in O_K$ and $x \in I^*$, then $\mathrm{Tr}(\alpha a x\overline{y}) = \mathrm{Tr}(\alpha x\overline{\overline{a}y}) \in \mathbb{Z}$ for all $y \in I$ and so $ax \in I^*$. Also, if $\{b_1, b_2, \ldots, b_n\} \subseteq K$ is a $\mathbb{Z}$-basis for I^*, then there exists a $\gamma \in \mathbb{Z}$ such that $\gamma b_j \in O_K$ for all $1 \leq j \leq n$. For this γ, we have $\gamma I^* \subseteq O_K$. This shows that I^* is an ideal of K.

Definition 3.4.4. Let $\alpha = 1$. The *different* ideal of the field K over $\mathbb{Q}$ is defined by

$$D_{K/\mathbb{Q}} := (O_K^*)^{-1}.$$

It is easily seen that $N(D_{K/\mathbb{Q}}) = |D_K|$. The different ideal tells us which primes ramify in O_K.

Proposition 3.4.5. *The prime ideal factors of $D_{K/\mathbb{Q}}$ are the primes in K that ramify over $\mathbb{Q}$. More precisely, for any prime ideal $\beta \subseteq O_K$ lying over a prime number p, with ramification index e, the exact power of β in $D_{K/\mathbb{Q}}$ is β^{e-1} if $e \not\equiv 0 \ (mod\ p)$ and $\beta^e | D_{K/\mathbb{Q}}$ if $p|e$.*

Proof. See [Lan94].

Using the different ideal we can get a formula for I^*.

Proposition 3.4.6. *Let I be an ideal lattice in K with pairing $Tr(\alpha x\overline{y})$. Then*

$$I^* = D_{K/\mathbb{Q}}^{-1}\overline{I}^{-1}(\alpha)^{-1}.$$

Proof. Let $x \in I^*$ and $y \in I$. Then, for all $b \in O_K$, $\mathrm{Tr}(\alpha x\overline{y}b) \in \mathbb{Z}$ because $y\overline{b} \in I$ and $x \in I^*$. Thus $\alpha x\overline{y} \in D_{K/\mathbb{Q}}^{-1}$ and so $(\alpha)I^*\overline{I} \subseteq D_{K/\mathbb{Q}}^{-1}$.

Let $z \in D_{K/\mathbb{Q}}^{-1}$. For any $a \in \overline{I}^{-1}$, we have that for all $y \in I$, $\mathrm{Tr}(za\overline{y}) \in \mathbb{Z}$ because $a\overline{y} \in O_K$. Therefore $\alpha^{-1}za \in I^*$ for all $a \in \overline{I}^{-1}$. Now, we can write $1 = \sum_{i=1}^{m} x_i y_i$ for some x_i's in $\overline{I}^{-1}$ and y_i's in $\overline{I}$ because $\overline{I}^{-1}\overline{I} = O_K$. Then $z = \sum_{i=1}^{m} \alpha(\alpha^{-1}zx_i)y_i \in (\alpha)I^*\overline{I}$. This shows $D_{K/\mathbb{Q}}^{-1} \subseteq (\alpha)I^*\overline{I}$. ■

Corollary 3.4.7. *Let I be an ideal lattice in K with pairing $\mathrm{Tr}(\alpha x\overline{y})$. Then*

i) I is integral if and only if

$$\alpha I\overline{I} \subseteq D_{K/\mathbb{Q}}^{-1}.$$

ii) I is unimodular if and only if

$$\alpha I\overline{I} = D_{K/\mathbb{Q}}^{-1}.$$

CHAPTER 4
Lattices from cyclotomic fields

The main references for this chapter are [Bay84] and [Bay99].

4.1 Preliminaries and characterization

A cyclotomic field over the rational numbers is a field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th}-root of unity. If $n = 2m$ with m odd then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$. Therefore, without loss of generality, we may assume that n is not congruent to 2 modulo 4.

Proposition 4.1.1. *Suppose that $n \not\equiv 2 \pmod 4$ and let $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th}-root of unity. Let $\phi(n)$ denote the number of integers k such that $1 \leq k \leq n$ and $(k, n) = 1$. Then*

i) K is a Galois extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = \phi(n)$ and Galois group $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

ii) $O_K = \mathbb{Z}[\zeta_n]$.

iii) $D_K = (-1)^{\frac{\phi(n)}{2}} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}$.

iv) Suppose p is a prime not dividing n and let f be the smallest positive integer such that $p^f \equiv 1 \pmod n$. Then p splits into $g := \frac{\phi(n)}{f}$ distinct prime ideals in K each of which has residue class degree f. The ramification index is $e = 1$.

v) Suppose p is a prime and $p^a || n$ and let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\frac{n}{p^a}}$. Then p splits into $g := \frac{\phi(\frac{n}{p^a})}{f}$ distinct prime ideals in K each of which has residue class degree f. The ramification index is $e = \phi(p^a)$.

Proof. See [Was97].

Remark 4.1.2. Let $K = \mathbb{Q}(\zeta_n)$ and suppose p is a prime and $p^a || n$. The *decomposition group* $D(\beta/p)$ for some prime ideal β over p is defined by

$$D(\beta/p) := \{\sigma \in Gal(K/\mathbb{Q}) \mid \sigma(\beta) = \beta\}.$$

The Galois group $Gal(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/\frac{n}{p^a}\mathbb{Z})^\times$. The decomposition group $D(\beta/p)$ is then isomorphic to the subgroup

$$(\mathbb{Z}/p^a\mathbb{Z})^\times \times < p \ (mod \ \tfrac{n}{p^a}) >$$

of $(\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/\frac{n}{p^a}\mathbb{Z})^\times$. The residue class degree f is then the order of the subgroup $< p \ (mod \ \frac{n}{p^a}) >$ of $(\mathbb{Z}/\frac{n}{p^a}\mathbb{Z})^\times$. The ideal β is fixed by the canonical involution (the automorphism sending ζ_n to ζ_n^{-1}) if and only if

$$(-1 \ (mod \ p^a), -1 \ (mod \ \tfrac{n}{p^a})) \in (\mathbb{Z}/p^a\mathbb{Z})^\times \times < p \ (mod \ \tfrac{n}{p^a}) >$$

and this happens if and only if there exists an integer k such that $p^k \equiv -1 \ (mod \frac{n}{p^a})$.

Before giving examples in the next sections, we show that there is nice characterization of ideal lattices in cyclotomic fields.

Proposition 4.1.3. *Let $\mathscr{L} \subseteq \mathbb{R}^n$ be an euclidean lattice with automorphism group $\mathrm{Aut}(\mathscr{L}) \leq O(n, \mathbb{R})$ (the group of real orthogonal $n \times n$ matrices). Then the following are equivalent:*

i) There exists a cyclotomic field $K = \mathbb{Q}(\zeta_m)$, an invertible element $\alpha \in K_{\mathbb{R}}$ satisfying $\overline{\alpha} = \alpha$ and an ideal I in K such that I with pairing $\mathrm{Tr}_{K_{\mathbb{R}}\backslash\mathbb{R}}(\alpha x \overline{y})$ is isomorphic to $\mathscr{L}$.

ii) $\mathrm{Aut}(\mathscr{L})$ contains a cyclic subgroup of order m acting freely on $\mathscr{L}\backslash\{0\}$ and $\phi(m) = n$.

iii) $\mathrm{Aut}(\mathscr{L})$ contains an automorphism of characteristic polynomial Φ_m (the m^{th}-cyclotomic polynomial).

Proof. *i)* $\Rightarrow$ *ii)*. The element ζ_m acts as an automorphism of the lattice I. It is then immediate that the corresponding automorphism of $\mathscr{L}$ generates a cyclic subgroup of order m acting freely on $\mathscr{L}\backslash\{0\}$.

ii) $\Rightarrow$ *iii)*. The characteristic polynomial is the same for any choice of basis and so by choosing a basis in $\mathbb{Q}\mathscr{L}$, we can assume that the coefficients of every automorphism

is in $\mathbb{Q}$. Let A be a generator for the cyclic subgroup. It is then enough to show that the minimal polynomial of the matrix A (over $\mathbb{Q}$) is Φ_m because the minimal polynomial divides the characteristic polynomial and the degree of the characteristic polynomial is $n = \phi(m)$.

The matrix A satisfies the polynomial $x^m - 1$ and so the minimal polynomial of A divides $x^m - 1$. If an m^{th}-root of unity is not primitive then it is a root of a polynomial $x^d - 1$ for some $d|m$ and $d \neq m$. Then write $x^m - 1 = (x^d - 1)f(x)$. It follows that $(A^d - 1)f(A) = 0$. Now, for any $x \in \mathscr{L}$, we have $A^d f(A)x = f(A)x$ and so $f(A)x = 0$ as the cyclic subgroup generated by A acts freely on $x \in \mathscr{L}\backslash\{0\}$. Hence $f(A) = 0$ because $\mathscr{L}$ contains a basis of $\mathbb{R}^n$. This means that all the roots of the minimal polynomial of A must be primitive m^{th}-roots of unity and we conclude that this minimal polynomial is Φ_m.

iii) $\Rightarrow$ *i)*. Let A be an automorphism of characteristic polynomial Φ_m. We define an action of $K = \mathbb{Q}(\zeta_m)$ on $\mathbb{Q}\mathscr{L}$ by

$$\sum_{i=0}^{n-1} q_i \zeta_m^i \cdot x := \sum_{i=0}^{n-1} q_i A^i x$$

for $q_0, q_1, \ldots, q_{n-1} \in \mathbb{Q}$. It then follows from $\Phi_m(A) = 0$ that this action makes $\mathbb{Q}\mathscr{L}$ into a K-vector space. Fix a non-zero $x \in \mathbb{Q}\mathscr{L}$. Then $x, Ax, \ldots, A^{n-1}x$ are $\mathbb{Q}$-linearly independent and so $\mathbb{Q}\mathscr{L}$ is one dimensional as a K-vector space. We associate $\mathbb{Q}\mathscr{L}$ with K. As $\mathbb{Q}$-vector spaces, the isomorphism between K and $\mathbb{Q}\mathscr{L}$ is the one sending ζ_m^i to $A^i x$.

Now, let $(a_0, a_1, \ldots, a_{n-1})^t \in \mathbb{R}^n$ be the unique solution to the equation

$$(\mathrm{Tr}(\zeta_m^{i+j}))_{0 \leq i,j \leq n-1} y = ((x,x),(x,Ax),\ldots(x,A^{n-1}x))^t,$$

in the variable $y \in \mathbb{R}^n$ (and where $(-,-)$ is the usual inner product on $\mathbb{R}^n$). Let $\alpha = a_0 + a_1\zeta_m + \cdots + a_{n-1}\zeta_m^{n-1} \in K_{\mathbb{R}}$. Then, the pairing $\mathrm{Tr}_{K_{\mathbb{R}}\backslash\mathbb{R}}(\alpha x \overline{y})$ corresponds to the usual inner product on $\mathbb{R}^n$. Also the lattice $\mathscr{L}$ corresponds to an ideal I in K.

■

Corollary 4.1.4. *Let $\mathscr{L}$ be an euclidean lattice similar to an ideal lattice in a cyclotomic field $\mathbb{Q}(\zeta_m)$. Then m divides all the coefficients (except the first one which is 1) of the theta series of $\mathscr{L}$.*

Proof. This follows from *ii*) of the last proposition.■

4.2 Root lattices

For our first examples, we realize the root lattices A_{p-1} (p a prime number) as the unique prime ideal over p in the cyclotomic fields $\mathbb{Q}(\zeta_p)$.

Example 4.2.1. Let $K = \mathbb{Q}(\zeta_p)$, where p is an odd prime. The ideal $\beta = (1-\zeta_p)$ is the only prime ideal containing p. We consider the lattice β with pairing $\mathrm{Tr}(\frac{1}{p}x\overline{y})$, where the involution is the canonical involution. It is a positive definite $(p-1)$-dimensional lattice.

$\{1-\zeta_p, \zeta_p-\zeta_p^2, \ldots, \zeta_p^{p-2}-\zeta_p^{p-1}\}$ is a $\mathbb{Z}$-basis for the ideal β. Using $\mathrm{Tr}(\frac{\zeta_p^a}{p}) = \frac{p-1}{p}$ when $a \equiv 0 \ (mod\ p)$ and $\mathrm{Tr}(\frac{\zeta_p^a}{p}) = \frac{-1}{p}$ when $a \not\equiv 0 \ (mod\ p)$, one can compute that for $x = a_1(1-\zeta_p) + a_2(\zeta_p-\zeta_p^2) + \cdots + a_{p-1}(\zeta_p^{p-2}-\zeta_p^{p-1})$ we have

$$\mathrm{Tr}(\tfrac{1}{p}x\overline{x}) = 2(a_1^2 + a_2^2 + \cdots + a_{p-1}^2 - a_1a_2 - a_2a_3 - \cdots - a_{p-2}a_{p-1}).$$

The matrix corresponding to this quadratic form in $p-1$ variables is the $(p-1)\times(p-1)$ matrix

$$\begin{pmatrix} 2 & -1 & 0 & \ldots & 0 & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 \\ 0 & -1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & -1 & 0 \\ 0 & \vdots & \ddots & -1 & 2 & -1 \\ 0 & 0 & \ldots & 0 & -1 & 2 \end{pmatrix}.$$

This is a Gramm matrix for the root lattice A_{p-1} and thus $\beta \cong A_{p-1}$. The different ideal is $D_{K/\mathbb{Q}} = \beta^{p-2}$ and $(p) = \beta^{p-1}$. Using our formula for the dual, we get

$$\begin{aligned} A_{p-1}^* &\cong (p) D_{K/\mathbb{Q}}^{-1} \overline{\beta}^{-1} \\ &= \beta^{p-1} \beta^{2-p} \beta^{-1} \\ &= O_K. \end{aligned}$$

These lattices are in fact the only A_n lattices that are similar to an ideal lattice in a cyclotomic field.

Proposition 4.2.2. *The root lattice A_n is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ ($m \not\equiv 2 \ (mod\ 4)$) if and only if $m = p$ for some prime number p and $n = p - 1$.*

Proof. The case of the lattice A_1 is trivial. Suppose that A_n (for some $n \geq 2$) is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$. Then also A_n^* is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ and so m divides the kissing number $2(n+1)$ of A_n^* (see Table 2-1 p.19). If m is even (and so divisible by 4 as we assume that $m \not\equiv 2 \ (mod\ 4)$) then both $n = \phi(m)$ and $n+1$ are even, which is a contradiction. Therefore m is odd and then m divides $n + 1$. But then

$$n + 1 = \phi(m) + 1 \leq m \leq n + 1$$

and so $\phi(m) = m - 1$. It follows that m is a prime p and $n = p - 1$. This argument together with the last example concludes the proof. ■

Some orthogonal direct sums of lattices isomorphic to A_{p-1} can be realized as ideal lattices in cyclotomic fields. We give an example of this before answering the question of when an orthogonal direct sum of euclidean lattices is similar to an ideal lattice in a cyclotomic field.

Example 4.2.3. Let $K = \mathbb{Q}(\zeta_{12})$. We consider the lattice O_K with pairing $Tr(\frac{1}{2}x\overline{y})$, where the involution is the canonical involution. It is a positive definite 4-dimensional lattice.

There is a unique prime ideal β above 2 and a unique prime ideal γ above 3. We have $(2) = \beta^2$ and $(3) = \gamma^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^2\gamma$. Our lattice is integral because

$$\tfrac{1}{2}O_K\overline{O_K} = \beta^{-2} \subseteq \beta^{-2}\gamma^{-1} = D_{K/\mathbb{Q}}^{-1}.$$

For any integer a, $\mathrm{Tr}(\frac{1}{2}\zeta_{12}^a\zeta_{12}^{-a}) = \frac{1}{2}\mathrm{Tr}(1) = 2$. This implies that O_K is an even root lattice. The discriminant is 9 and so we conclude from the classification of root lattices that $O_K \cong A_2 \oplus A_2$. The dual is

$$\begin{aligned} A_2^* \oplus A_2^* &\cong (2)D_{K/\mathbb{Q}}^{-1}\overline{O_K}^{-1} \\ &= \beta^2\beta^{-2}\gamma^{-1} \\ &= \gamma^{-1}. \end{aligned}$$

Lemma 4.2.4. *Let $\mathscr{L}$ be an euclidean lattice having an automorphism f with irreducible characteristic polynomial. If $\mathscr{L} = \mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k$ for some indecomposable sublattices $\mathscr{L}_1$, $\mathscr{L}_2$, ..., $\mathscr{L}_k$ then f acts cyclically on $\{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}$ and thus*

$$\mathscr{L}_1 \cong \mathscr{L}_2 \cong \cdots \cong \mathscr{L}_k.$$

Proof. We know from Remark 2.3.5 that f permutes the elements of $\{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}$. Suppose that $f(\mathscr{L}_{i_1} \oplus \mathscr{L}_{i_2} \oplus \cdots \oplus \mathscr{L}_{i_l}) = \mathscr{L}_{i_1} \oplus \mathscr{L}_{i_2} \oplus \cdots \oplus \mathscr{L}_{i_l}$ for some i_j's with $1 \leq i_j \leq k$ for $1 \leq j \leq l$. Then the characteristic polynomial of $f|_{\mathscr{L}_{i_1} \oplus \mathscr{L}_{i_2} \oplus \cdots \oplus \mathscr{L}_{i_l}}$ divides the characteristic polynomial of f and so is equal to it. Hence $\mathrm{rk}(\mathscr{L}) = \mathrm{rk}(\mathscr{L}_{i_1} \oplus \mathscr{L}_{i_2} \oplus \cdots \oplus \mathscr{L}_{i_l})$ and

$$\{\mathscr{L}_{i_1}, \mathscr{L}_{i_2}, \ldots, \mathscr{L}_{i_l}\} = \{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}.$$

We conclude that f acts cyclically on $\{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}$. ■

Proposition 4.2.5. *Let $\mathscr{L}$ be an euclidean lattice and suppose that $\mathscr{L} = \mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \cdots \oplus \mathscr{L}_k$ for some indecomposable sublattices $\mathscr{L}_1$, $\mathscr{L}_2$, ..., $\mathscr{L}_k$. Then $\mathscr{L}$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ if and only if $\mathscr{L} \cong k\mathscr{L}_1$, k divides m, k divides $\phi(m)$, $\frac{\phi(m)}{k} = \phi(\frac{m}{k})$ and $\mathscr{L}_1$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_{\frac{m}{k}})$.*

Proof. $\Rightarrow$): The last lemma implies $\mathscr{L} \cong k\mathscr{L}_1$ (and so k divides $\phi(m)$). Let f be an automorphism of $\mathscr{L}$ of characteristic polynomial Φ_m. Since f acts cyclically on $\{\mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_k\}$ and $f^m = id$, we conclude that k divides m. The automorphism f^k corresponds to $\zeta_m^k \in \mathbb{Q}(\zeta_m)$ and so its minimal polynomial is $\Phi_{\frac{m}{k}}$. Hence the minimal polynomial of the automorphism $f^k|_{\mathscr{L}_1}$ of $\mathscr{L}_1$ is $\Phi_{\frac{m}{k}}$ of degree $\phi(\frac{m}{k})$. But it is always true that $\phi(\frac{m}{k}) \geq \frac{\phi(m)}{k}$ and since $\frac{\phi(m)}{k} = \mathrm{rk}(\mathscr{L}_1)$, the characteristic polynomial of $f^k|_{\mathscr{L}_1}$ is $\Phi_{\frac{m}{k}}$ (and $\frac{\phi(m)}{k} = \phi(\frac{m}{k})$). It then follows from Proposition 4.1.3 that $\mathscr{L}_1$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_{\frac{m}{k}})$.

$\Leftarrow$): Let $l = \mathrm{rk}(\mathscr{L}_1) = \phi(\frac{m}{k})$ and let $A \in O(l, \mathbb{R})$ be an automorphism of $\mathscr{L}_1$ of characteristic polynomial $\Phi_{\frac{m}{k}}$. Then $\mathscr{L}$ has an automorphism f given by the $\phi(m) \times \phi(m)$ matrix

$$\begin{pmatrix} O & O & \cdots & O & A \\ I & O & \ddots & O & O \\ O & I & \ddots & O & \vdots \\ \vdots & \ddots & \ddots & O & O \\ O & \cdots & O & I & O \end{pmatrix}.$$

(in a basis $\{\alpha_1^{(1)}, \ldots, \alpha_l^{(1)}, \alpha_1^{(2)}, \ldots, \alpha_l^{(2)}, \ldots, \alpha_1^{(k)}, \ldots, \alpha_l^{(k)}\}$, where $\{\alpha_1^{(j)}, \ldots, \alpha_l^{(j)}\}$ for $1 \leq j \leq k$ is a basis for one of the copies of $\mathscr{L}_1$ in the orthogonal direct sum decomposition), where O is the $l \times l$ zero matrix, I is the $l \times l$ identity matrix and there are k^2 blocks. The automorphism f^k is then given by the matrix

$$\begin{pmatrix} A & O & \cdots & O & O \\ O & A & O & \cdots & O \\ O & O & \ddots & O & \vdots \\ \vdots & \ddots & \ddots & A & O \\ O & \cdots & O & O & A \end{pmatrix}$$

and so it satisfies $\Phi_{\frac{m}{k}}(f^k) = 0$. But under the assumption $\frac{\phi(m)}{k} = \phi(\frac{m}{k})$ we have $\Phi_{\frac{m}{k}}(x^k) = \Phi_m(x)$ and thus $\Phi_m(f) = 0$. We conclude that the characteristic polynomial of f is Φ_m since $\mathrm{rk}(\mathscr{L}) = \phi(m)$. The result then follows from Proposition 4.1.3.

■

Remark 4.2.6. Let m be an integer with prime decomposition $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ ($r \geq 1$, $a_i \geq 1$ and p_i prime for $1 \leq i \leq r$). An integer k satisfies the conditions k divides m, k divides $\phi(m)$ and $\frac{\phi(m)}{k} = \phi(\frac{m}{k})$ if and only if $k = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ with $0 \leq b_i < a_i$ for $1 \leq i \leq r$.

Corollary 4.2.7. *If m is square free then every positive definite ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ is indecomposable.*

We now continue to give some examples of root lattices as ideals in cyclotomic fields.

Example 4.2.8. Let $r \geq 1$ and $K = \mathbb{Q}(\zeta_{2^{r+1}})$. We first consider the lattice O_K with pairing $\mathrm{Tr}(\frac{1}{2^r} x\overline{y})$, where the involution is the canonical involution. It is a positive definite 2^r-dimensional lattice.

There is a unique prime ideal β above 2 and $(2) = \beta^{2^r}$. The different ideal is $D_{K/\mathbb{Q}} = \beta^{r2^r}$. This lattice is unimodular because

$$\tfrac{1}{2^r} O_K \overline{O_K} = \beta^{-r2^r} = D_{K/\mathbb{Q}}^{-1}.$$

For any integer a, $\mathrm{Tr}(\frac{1}{2^r} \zeta_{2^{r+1}}^a \zeta_{2^{r+1}}^{-a}) = \frac{1}{2^r}\mathrm{Tr}(1) = 1$. This implies that O_K is generated by roots of length 1 and thus $O_K \cong \mathbb{Z}^{2^r}$.

We now consider the ideal β with the same pairing. This lattice is integral because

$$\tfrac{1}{2^r}\beta\overline{\beta} = D_{K/\mathbb{Q}}^{-1}\beta^2 \subseteq D_{K/\mathbb{Q}}^{-1}.$$

For any integer a, $\mathrm{Tr}(\frac{1}{2^r}\zeta_{2^{r+1}}^a(1-\zeta_{2^{r+1}})\zeta_{2^{r+1}}^{-a}(1-\zeta_{2^{r+1}}^{-1})) = 2$. Thus β is an even root lattice. We have $\mathrm{disc}(\beta) = 4$. From the classification of root lattices, β must be isomorphic to one of the following: $E_7 \oplus E_7 \oplus kE_8$, $E_7 \oplus A_1 \oplus kE_8$, $A_3 \oplus kE_8$ or $D_n \oplus kE_8$ (for some $k \geq 0$ in each case). From Proposition 4.2.5 and rank consideration, we get $\beta \cong D_{2^r}$. Using our formula for the dual, we get

$$\begin{aligned} D_{2^r}^* &\cong (2^r) D_{K/\mathbb{Q}}^{-1} \overline{\beta}^{-1} \\ &= \beta^{r2^r} \beta^{-r2^r} \beta^{-1} \\ &= \beta^{-1}. \end{aligned}$$

Proposition 4.2.9. *The lattice $\mathbb{Z}^n$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ if and only if n is a power of 2 and $m = 2n$ (and $m = 1$ if $n = 1$).*

Proof. The case of the lattice $\mathbb{Z}$ is trivial, so let's assume that $n \geq 2$. Suppose that $\mathbb{Z}^n$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$. We do a proof by contradiction. Suppose that m is not a power of 2 and let p be the largest prime dividing m (say $p^a || m$ for some $a \geq 1$). Then $p^{a-1} || \phi(m) = n$. However, since $m | 2n$ (the kissing number of $\mathbb{Z}^n$), we have $p^a | n$ a contradiction. This argument together with the last example concludes the proof. ■

Proposition 4.2.10. *The lattice D_4 is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ if and only if $m = 8$ or $m = 12$. The lattice D_n for $n \geq 5$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ if and only if n is a power of 2 and $m = 2n$.*

Proof. There are 3 values of m with $\phi(m) = 4$: $m = 5$, 8 and 12. The kissing number of D_4 is 24 (see Table 2-1 p.19) and so we can eliminate $m = 5$. We already gave an example of D_4 in $\mathbb{Q}(\zeta_8)$. We show that we can also obtain it as an ideal in the cyclotomic field $\mathbb{Q}(\zeta_{12})$ by exhibiting an automorphism of characteristic polynomial Φ_{12}.

The automorphism group of D_4 is isomorphic to the group $((\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_4) \rtimes S_3$. The subgroup $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_4$ can be seen as the group generated by all permutations of coordinates and all the sign changes of evenly many coordinates. The subgroup S_3 can be seen as the group generated by the matrices

$$B = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } H = \begin{pmatrix} -1/2 & 1/2 & 1/2 & -1/2 \\ -1/2 & 1/2 & -1/2 & 1/2 \\ -1/2 & -1/2 & 1/2 & 1/2 \\ 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}$$

(this group is the graph automorphism group of the Dynkin diagram of D_4, it consists of all the permutations of the 3 basis elements $(-1,-1,0,0)$, $(1,-1,0,0)$ and $(0,0,1,-1)$; if we label them 1, 2 and 3 respectively, B corresponds to the transposition (12) and H to the 3-cycle (123)). Let

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Then one can verify that the automorphism AH of D_4 has characteristic polynomial $x^4 - x^2 + 1 = \Phi_{12}(x)$. For $n \geq 5$, the result follows immediately from the result for $\mathbb{Z}^n$ since in both cases the automorphism group consists of all permutations and sign changes of the coordinates (see [CS99], chapter 4). ■

All the remaining examples of this section will be given in cyclotomic fields $\mathbb{Q}(\zeta_m)$ with m not a power of two. It turns out that, for these fields, any integral ideal lattice is even and we first proceed to prove this fact.

Proposition 4.2.11. *([Bay99], proposition 2.12) Let K be a number field with a non-trivial involution and let F be the fixed field of the involution. Suppose that every prime ideal $\beta \subseteq O_F$ over 2 is unramified in O_K. Then every integral ideal lattice in K is even.*

Proof. The condition of the proposition is equivalent to ask that the extension K/F is tame because $[K : F] = 2$. The extension K/F is tame if and only if the trace

map $\mathrm{Tr}_{K/F} : O_K \to O_F$ is surjective. This is true if and only if there exists a $z \in O_K$ such that $z + \overline{z} = 1$. Suppose now that we have such a $z \in O_K$. Let I be an ideal integral lattice in K with pairing $\mathrm{Tr}(\alpha x\overline{y})$. Then, for all $x \in I$, we have

$$\begin{aligned}\mathrm{Tr}(\alpha x\overline{x}) &= \mathrm{Tr}((z+\overline{z})\alpha x\overline{x}) \\ &= \mathrm{Tr}(z\alpha x\overline{x}) + \mathrm{Tr}(\overline{z}\alpha x\overline{x}) \\ &= 2\mathrm{Tr}(z\alpha x\overline{x}).\end{aligned}$$

This implies that I is even because $\alpha x\overline{x} \in D^{-1}_{K/\mathbb{Q}}$ and so $\mathrm{Tr}(z\alpha x\overline{x}) \in \mathbb{Z}$. ■

Proposition 4.2.12. *Let $\mathbb{Q}(\zeta_n)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_n)$. If $n = p^m$ then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is ramified at the prime ideals above p and unramified at the other prime ideals. If n is not a prime power then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is unramified at every prime ideal.*

Proof. See [Was97].

Corollary 4.2.13. *Let $K = \mathbb{Q}(\zeta_n)$, where n is not a power of 2, and let I be an ideal lattice in K with pairing $\mathrm{Tr}(\alpha x\overline{y})$, where the involution is the canonical involution. If I is integral then it is even.*

Example 4.2.14. Let $K = \mathbb{Q}(\zeta_9)$. There is a unique prime ideal β over 3 and $(3) = \beta^6$. The different ideal is $D_{K/\mathbb{Q}} = \beta^9$. We consider the lattice β^2 with pairing $\mathrm{Tr}(\frac{1}{9}x\overline{y})$, where the involution is the canonical involution. It is a positive definite 6-dimensional lattice. We have

$$\tfrac{1}{9}\beta^2\overline{\beta^2} = \beta^{-12}\beta^4 = \beta^{-8} \subseteq \beta^{-9} = D^{-1}_{K/\mathbb{Q}}$$

and so it is integral. From Corollary 4.2.13, it is even. The discriminant of this lattice is 3. Up to isomorphism, there is only one positive definite 6-dimensional even lattice of discriminant 3 (see Table 15.9 in [CS99]), it is the root lattice E_6. Its dual is easily seen to be isomorphic to the ideal lattice β.

There are two values of n ($n \not\equiv 2 \ (mod\ 4)$) such that $\phi(n) = 6$: $n = 9$ and 7. Since the kissing number of E_6 is 72 (see Table 2-1 p.19) and 7 does not divide 72, we can only obtain E_6 as an ideal in the cyclotomic field $\mathbb{Q}(\zeta_9)$.

We now want to realize the lattice E_8. We know that, up to isomorphism, E_8 is the unique even unimodular lattice of dimension 8 (see Corollary 2.6.7). There are 4 values of n ($n \not\equiv 2 \ (mod\ 4)$) such that $\phi(n) = 8$; $n = 16, 20, 24$ and 15. We can obtain E_8 easily for $n = 20$ and $n = 24$.

Example 4.2.15. Let $K = \mathbb{Q}(\zeta_{20})$. There is a unique prime ideal β above 2 and $(2) = \beta^2$. There are two prime ideals γ and $\overline{\gamma}$ above 5 and $(5) = \gamma^4\overline{\gamma}^4$. The different ideal is $D_{K/\mathbb{Q}} = \beta^2\gamma^3\overline{\gamma}^3$. Then $I = \beta^{-1}\gamma^{-3}$ is an 8-dimensional even unimodular lattice and so $I \cong E_8$.

Example 4.2.16. Let $K = \mathbb{Q}(\zeta_{24})$. There is a unique prime ideal β above 2 and $(2) = \beta^4$. There are two prime ideals γ and $\overline{\gamma}$ above 3 and $(3) = \gamma^2\overline{\gamma}^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^8\gamma\overline{\gamma}$. Then $I = \beta^{-4}\gamma^{-1}$ is an 8-dimensional even unimodular lattice and so $I \cong E_8$.

It is also possible to obtain E_8 in the cyclotomic field $\mathbb{Q}(\zeta_{15})$. This will follow from Theorem 4.3.1 of the next section. However, E_8 is not similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_{16})$. This can be obtained as a consequence of the following result.

Proposition 4.2.17. *([Bay84], Corollary 3.3) Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field, F the fixed field of the involution, C_K the ideal class group of K, C_F the ideal class group of F, $N_{K/F} : C_K \to C_F$ the homomorphism induced by the norm of ideals, C^- the kernel of this homomorphism, h^- the cardinality of C^- (this is equal to the relative class number) and h the cardinality of C^- modulo the Galois group $Gal(K/\mathbb{Q})$. Assume that h^- is odd. Then the number of isometry classes of unimodular lattices having an automorphism of characteristic polynomial Φ_m is at most h.*

The relative class number of the cyclotomic field $\mathbb{Q}(\zeta_{16})$ is 1 (see [Was97], p. 353). Since we know that the lattice $\mathbb{Z}^8$ has an automorphism of characteristic polynomial Φ_{16}, the lattice E_8 cannot have one.

We now have determined all the indecomposable root lattices that can be obtained as an ideal in a cyclotomic field (and also in which cyclotomic fields they can be obtained). We are now in a position to determine all the root lattices that are similar to an ideal in a cyclotomic field (and also to determine all the cyclotomic fields in which they can be obtained).

Theorem 4.2.18. *A root lattice $\mathscr{L}$ is similar to an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ ($m \not\equiv 2 \pmod 4$) if and only if $\mathscr{L}$ is isomorphic to one of the lattices below and m is as specified.*

i) $\mathbb{Z}^{2^r}$ *for* $r \geq 0$ *and then* $m = 2^{r+1}$ *if* $r \geq 1$ *and* $m = 1$ *if* $r = 0$. $2^r A_1$ *for* $r \geq 0$ *and then* $m = 2^{r+1}$ *if* $r \geq 1$ *and* $m = 1$ *if* $r = 0$.

ii) $2^a p^b A_{p-1}$ *for some odd prime number* p *and integers* $a \geq 0$ *and* $b \geq 0$. *Then* $m = 2^{a+1}p^{b+1}$ *if* $a \neq 0$ *and* $m = p^{b+1}$ *if* $a = 0$.

iii) $2^a 3^b D_4$ *for some integers* $a \geq 0$ *and* $b \geq 0$. *Then* $m = 2^{a+3}$ *or* $2^{a+2}3$ *if* $b = 0$ *and* $m = 2^{a+2}3^{b+1}$ *if* $b \neq 0$.

iv) $2^a D_{2^r}$ *for* $r \geq 3$ *and for some integer* $a \geq 0$. *Then* $m = 2^{a+r+1}$.

v) $2^a 3^b E_6$ *for some integers* $a \geq 0$ *and* $b \geq 0$. *Then* $m = 2^{a+1}3^{b+2}$ *if* $a \neq 0$ *and* $m = 3^{b+2}$ *if* $a = 0$.

vi) $2^a 3^b 5^c E_8$ *for some integers* $a \geq 0$, $b \geq 0$ *and* $c \geq 0$. *Then if* $a = b = c = 0$ *we have* $m = 15$, $m = 24$ *or* $m = 20$. *If* $a = b = 0$ *but* $c > 0$ *we have* $m = 5^{c+1}3$ *or* $m = 5^{c+1}4$. *If* $a = c = 0$ *but* $b > 0$ *we have* $m = 3^{b+1}5$ *or* $m = 3^{b+1}8$. *If* $b = c = 0$ *but* $a > 0$ *we have* $m = 2^{a+3}3$, $m = 2^{a+2}5$ *or* $m = 2^{a+1} \cdot 15$. *If* $a = 0$ *but* $b > 0$ *and* $c > 0$ *we have* $m = 3^{b+1}5^{c+1}$. *If* $b = 0$ *but* $a > 0$ *and* $c > 0$ *we have* $m = 2^{a+2}5^{c+1}$ *or* $m = 2^{a+1}5^{c+1}3$. *If* $c = 0$ *but* $a > 0$ *and* $b > 0$ *we have*

$m = 2^{a+3}3^{b+1}$ *or* $m = 2^{a+1}3^{b+1}5$. *Finally, if* $a > 0$, $b > 0$ *and* $c > 0$ *we have* $m = 2^{a+1}3^{b+1}5^{c+1}$.

Proof. This theorem is an easy consequence of Proposition 4.2.5 and of what we already know about the indecomposable root lattices. ■

Remark 4.2.19. This theorem corrects and completes Theorem 3.2 of [Bay99].

4.3 Even unimodular lattices in dimensions ≤ 24

The lattices in *vi*) of the last theorem are all unimodular lattices. It is possible to determine all the cyclotomic fields in which there exists a unimodular ideal lattice.

Theorem 4.3.1. *([Bay99], proposition* 2.8 *and [Bay84], theorem* 1.1*) There exists a unimodular ideal lattice in the cyclotomic field* $\mathbb{Q}(\zeta_m)$ *(*$m \not\equiv 2$ $(mod\ 4)$*) if and only if* m *is a power of* 2 *or* m *is mixed and* $\phi(m) \equiv 0$ $(mod\ 8)$.

When n is not a power of 2, all unimodular ideal lattices are even. We were interested in even unimodular lattices in section 2.6. We now want to determine which of these (in dimensions ≤ 24) can be obtained as ideal lattices in cyclotomic fields (and in which fields they can be obtained). In dimension 8, we already said that we can obtain the unique even unimodular lattice E_8 as an ideal lattice in the cyclotomic field $\mathbb{Q}(\zeta_m)$ ($m \not\equiv 2$ $(mod\ 4)$) if and only if $m = 15$, 20 or 24. This can also be seen as a corollary to the last theorem (assuming the case $m = 16$ has been excluded).

We now turn our attention to even unimodular lattices in dimension 16. There are only 2 such lattices up to isomorphism : $2E_8$ and D_{16}^+ (see section 2.6). If the lattice D_{16}^+ could be realized in a cyclotomic field then also the lattice D_{16} could be realized in the same cyclotomic field since any automorphism of a lattice having roots restricts to an automorphism of its root sublattice. Hence the only possibility for the cyclotomic field would be $\mathbb{Q}(\zeta_{32})$, but the relative class number of this cyclotomic field is 1 (see [Was97], p.353) and we already realized the lattice $\mathbb{Z}^{16}$ in this field. It

therefore follows from Proposition 2.6.21 that D_{16}^+ is not similar to an ideal lattice in a cyclotomic field. The case of the lattice $2E_8$ is covered by the Theorem 4.2.18. We can obtain it in the cyclotomic fields $\mathbb{Q}(\zeta_m)$ for $m = 40$, 48 and 60. In the three cases, we give concrete examples.

Example 4.3.2. Let $K = \mathbb{Q}(\zeta_{40})$. There is a unique prime ideal β above 2 and $(2) = \beta^4$. There are two prime ideals γ and $\overline{\gamma}$ above 5 and $(5) = \gamma^4\overline{\gamma}^4$. The different ideal is $D_{K/\mathbb{Q}} = \beta^8\gamma^3\overline{\gamma}^3$. Then $I = \beta^{-4}\gamma^{-3}$ is a 16-dimensional even unimodular lattice isomorphic to $E_8 \oplus E_8$.

Example 4.3.3. Let $K = \mathbb{Q}(\zeta_{48})$. There is a unique prime ideal β above 2 and $(2) = \beta^8$. There are two prime ideals γ and $\overline{\gamma}$ above 3 and $(3) = \gamma^2\overline{\gamma}^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^{24}\gamma\overline{\gamma}$. Then $I = \beta^{-12}\gamma^{-1}$ is a 16-dimensional even unimodular lattice isomorphic to $E_8 \oplus E_8$.

Example 4.3.4. Let $K = \mathbb{Q}(\zeta_{60})$. There are two prime ideals γ and $\overline{\gamma}$ above 5 and $(5) = \gamma^4\overline{\gamma}^4$. There are two prime ideals β and $\overline{\beta}$ above 2 and $(2) = \beta^2\overline{\beta}^2$. There are two prime ideals α and $\overline{\alpha}$ above 3 and $(3) = \alpha^2\overline{\alpha}^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^2\overline{\beta}^2\gamma^3\overline{\gamma}^3\alpha\overline{\alpha}$. Then $I = \beta^{-2}\gamma^{-3}\alpha^{-1}$ is a 16-dimensional even unimodular lattice isomorphic to $E_8 \oplus E_8$.

We now turn our attention to even unimodular lattices in dimension 24. The values of m ($m \not\equiv 2 \ (mod\ 4)$) such that $\phi(m) = 24$ are 35, 39, 45, 52, 56, 72 and 84. From the list of the Niemeier lattices given in section 2.6 and from Theorem 4.2.18, we obtain the following list of candidates for even unimodular lattices of dimension 24 similar to an ideal lattice in a cyclotomic field: $(12A_2)^+$ ($m = 72$), $(4A_6)^+$ ($m = 56$), $(4E_6)^+$ ($m = 72$), $(6D_4)^+$ ($m = 72$), $(2A_{12})^+$ ($m = 52$), $3E_8$ ($m = 45$ and 72) and the Leech lattice. Hence, when $m = 35$, 39 or 84, the only even unimodular lattice possible is the Leech lattice (and from Theorem 4.3.1 the Leech lattice can indeed be realized in these cyclotomic fields). We give an example for $m = 39$.

Example 4.3.5. Let $K = \mathbb{Q}(\zeta_{39})$. There are two prime ideals β and $\overline{\beta}$ above 13 and $(13) = \beta^{12}\overline{\beta}^{12}$. There are four prime ideals γ, $\overline{\gamma}$, α and $\overline{\alpha}$ above 3 and $(3) = \gamma^2\overline{\gamma}^2\alpha^2\overline{\alpha}^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^{11}\overline{\beta}^{11}\gamma\overline{\gamma}\alpha\overline{\alpha}$. Then $I = \beta^{-11}\gamma^{-1}\alpha^{-1}$ is a 24-dimensional even unimodular lattice isomorphic to the Leech lattice.

For $m = 45$, the relative class number is 1 and we know that we can obtain $3E_8$ from Theorem 4.2.18. Hence the only even unimodular lattice similar to an ideal in the cyclotomic field $\mathbb{Q}(\zeta_{45})$ is $3E_8$.

For $m = 52$, both the lattice $(2A_{12})^+$ and the Leech lattice can be obtained.

Example 4.3.6. Let $K = \mathbb{Q}(\zeta_{52})$. There is one prime ideal β above 2 and $(2) = \beta^2$. There are two prime ideals γ and $\overline{\gamma}$ above 13 and $(13) = \gamma^{12}\overline{\gamma}^{12}$. The different ideal is $D_{K/\mathbb{Q}} = \beta^2\gamma^{11}\overline{\gamma}^{11}$. We consider the ideal lattice γ with pairing $\mathrm{Tr}(\frac{1}{26}x\overline{y})$. This lattice is unimodular because

$$\tfrac{1}{26}\gamma\overline{\gamma} = \beta^{-2}\gamma^{-12}\overline{\gamma}^{-12}\gamma\overline{\gamma} = D_{K/\mathbb{Q}}^{-1}.$$

Let $\zeta_{13} = \zeta_{52}^4$. We have $\gamma \cap \mathbb{Q}(\zeta_{13}) = (1-\zeta_{13})O_{\mathbb{Q}(\zeta_{13})}$ and so in particular γ contains the element $x = 1 - \zeta_{13}$. The squared norm of this element is

$$\mathrm{Tr}_{K/\mathbb{Q}}(\tfrac{1}{26}x\overline{x}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\tfrac{1}{13}x\overline{x}) = 2$$

(see Example 4.2.1). Therefore $\gamma \cong (2A_{12})^+$ since the only other possibility would be the Leech lattice but it has no roots.

One can verify that the Leech lattice indeed has an automorphism of characteristic polynomial Φ_{52} using a software like the MAGMA algebra system.

For $m = 56$, only the Leech lattice can be realized. This follows from the next lemma which implies that the Niemeier lattice $(4A_6)^+$ has no automorphism of characteristic polynomial Φ_{56}.

Lemma 4.3.7. *The Niemeier lattice $(4A_6)^+$ has no automorphism of irreducible characteristic polynomial.*

Proof. Any automorphism of $(4A_6)^+$ restricts to an automorphism of $4A_6$ and acts as a permutation of the components. Let G_2 be the group of all permutations of the components that arise from automorphisms of $(4A_6)^+$. This group has cardinality 12 (see [CS99], Table 16.1) and so is isomorphic to A_4 (the alternating group on 4 elements). The group A_4 contains no 4-cycle and so no automorphism of $(4A_6)^+$ can act cyclically on the components of $4A_6$. ■

For $m = 72$, we already know that we can obtain the lattice $3E_8$. We give a concrete example.

Example 4.3.8. Let $K = \mathbb{Q}(\zeta_{72})$. There is one prime ideal β above 2 and $(2) = \beta^4$. There are two prime ideals γ and $\overline{\gamma}$ above 3 and $(3) = \gamma^6\overline{\gamma}^6$. The different ideal is $D_{K/\mathbb{Q}} = \beta^8\gamma^9\overline{\gamma}^9$. We consider the ideal lattice γ^3 with pairing $\mathrm{Tr}(\frac{1}{36}x\overline{y})$. This lattice is unimodular because

$$\tfrac{1}{36}\gamma^3\overline{\gamma}^3 = \beta^{-8}\gamma^{-12}\overline{\gamma}^{-12}\gamma^3\overline{\gamma}^3 = D_{K/\mathbb{Q}}^{-1}.$$

Using MAGMA, we computed that this lattice has 720 roots. It is therefore isomorphic to $3E_8$.

The relative class number of the cyclotomic field $K = \mathbb{Q}(\zeta_{72})$ is 3 (see [Was97], p.353). One can verify that C^- (in the notation of Proposition 4.2.17) consists of the three elements 1, $[\gamma]$, $[\overline{\gamma}] \in C_K$ (where γ is as in the preceding example). Therefore, from Proposition 4.2.17, there are at most 2 isometry classes of unimodular lattices similar to an ideal lattice in K. It turns out that there is a second one. Indeed, one can verify using MAGMA that the Niemeier lattice $(4E_6)^+$ has an automorphism of characteristic polynomial Φ_{72} (one such automorphism is also constructed in [Bay84]).

We summarize these results about even unimodular lattices of dimension 24 in a table. The table gives all the Niemeier lattices that can be realized as an ideal in a

cyclotomic field and all the cyclotomic fields $\mathbb{Q}(\zeta_m)$ ($m \not\equiv 2 \ (mod\ 4)$) in which they can be realized (see also [Bay84], Proposition 5.1 and [Bay99], Proposition 3.4).

Table 4–1: Niemeier lattices similar to ideals in cyclotomic fields

Lattice	m
Leech	35, 39, 52, 56, 84
$3E_8$	45, 72
$(2A_{12})^+$	52
$(4E_6)^+$	72

4.4 Higher dimensions

We now talk a little bit about higher dimensions. We first give three examples of even unimodular lattices in dimension 32.

Example 4.4.1. Let $K = \mathbb{Q}(\zeta_{68})$. There are two prime ideals β_1 and β_2 above 2 and $(2) = \beta_1^2\beta_2^2$ (both are fixed by the involution). There are two prime ideals γ and $\overline{\gamma}$ above 17 and $(17) = \gamma^{16}\overline{\gamma}^{16}$. The different ideal is $D_{K/\mathbb{Q}} = \beta_1^2\beta_2^2\gamma^{15}\overline{\gamma}^{15}$. We consider the ideal lattice γ with pairing $\mathrm{Tr}(\frac{1}{34}x\overline{y})$. This lattice is unimodular because

$$\tfrac{1}{34}\gamma\overline{\gamma} = \beta_1^{-2}\beta_2^{-2}\gamma^{-16}\overline{\gamma}^{-16}\gamma\overline{\gamma} = D_{K/\mathbb{Q}}^{-1}.$$

Let $\zeta_{17} = \zeta_{68}^4$. We have $\gamma \cap \mathbb{Q}(\zeta_{17}) = (1-\zeta_{17})O_{\mathbb{Q}(\zeta_{17})}$ and so in particular γ contains the element $x = 1 - \zeta_{17}$. The squared norm of this element is

$$\mathrm{Tr}_{K/\mathbb{Q}}(\tfrac{1}{34}x\overline{x}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{17})/\mathbb{Q}}(\tfrac{1}{17}x\overline{x}) = 2$$

(see Example 4.2.1). Any ideal lattice in a cyclotomic field having roots must have a complete root system since the root sublattice is also an ideal in the same cyclotomic field. The only root lattice similar to an ideal lattice in $\mathbb{Q}(\zeta_{68})$ is $2A_{16}$ form Theorem 4.2.18. There exists a unique even unimodular lattice of dimension 32 with root sublattice $2A_{16}$ (see [Ker94]) and so γ is isomorphic to it.

Example 4.4.2. Let $K = \mathbb{Q}(\zeta_{80})$. There is one prime ideal β above 2 and $(2) = \beta^8$. There are two prime ideals γ and $\overline{\gamma}$ above 5 and $(5) = \gamma^4\overline{\gamma}^4$. The different ideal is

$D_{K/\mathbb{Q}} = \beta^{24}\gamma^3\overline{\gamma}^3$. We consider the ideal lattice γ with pairing $\mathrm{Tr}(\frac{1}{40}x\overline{y})$. This lattice is unimodular because

$$\tfrac{1}{40}\gamma\overline{\gamma} = \beta^{-24}\gamma^{-4}\overline{\gamma}^{-4}\gamma\overline{\gamma} = D_{K/\mathbb{Q}}^{-1}.$$

There are only two root lattices similar to an ideal lattice in $\mathbb{Q}(\zeta_{80})$: $8A_4$ and $4E_8$. We computed using MAGMA that our lattice has 160 roots. It follows that γ is an even unimodular lattice of rank 32 and root sublattice $8A_4$. There exists a unique such lattice up to isomorphism (see [Ker94]).

Example 4.4.3. Let $K = \mathbb{Q}(\zeta_{96})$. There is one prime ideal β above 2 and $(2) = \beta^{16}$. There are two prime ideals γ and $\overline{\gamma}$ above 3 and $(3) = \gamma^2\overline{\gamma}^2$. The different ideal is $D_{K/\mathbb{Q}} = \beta^{64}\gamma\overline{\gamma}$. We consider the ideal lattice γ with pairing $\mathrm{Tr}(\frac{1}{48}x\overline{y})$. This lattice is unimodular because

$$\tfrac{1}{48}\gamma\overline{\gamma} = \beta^{-64}\gamma^{-2}\overline{\gamma}^{-2}\gamma\overline{\gamma} = D_{K/\mathbb{Q}}^{-1}.$$

We computed using MAGMA that our lattice has 960 roots. It follows that γ is isomorphic to $4E_8$.

In dimension 48, it is known that there is a unique *extremal* lattice that is similar to an ideal in a cyclotomic field.

Definition 4.4.4. An even unimodular lattice of rank n is *extremal* if its minimum squared norm is $2(1 + \left\lfloor \frac{n}{24} \right\rfloor)$.

In dimension 24, the only extremal lattice is of course the Leech lattice. In dimension 48, only 3 extremal lattices are known: P_{48p}, P_{48q} and P_{48n}. The lattice P_{48n} is constructed in [Neb98]. It is shown in [Neb12] that P_{48n} is the unique extremal lattice in dimension 48 that is similar to an ideal lattice in a cyclotomic field. More precisely, the two following results are obtained.

Proposition 4.4.5. *([Neb12], Corollary* 4.13*) Let $\mathscr{L}$ be an extremal lattice of dimension* 48 *and $\sigma \in \mathrm{Aut}(\mathscr{L})$ of order m. Then Φ_m divides the minimal polynomial of σ.*

Theorem 4.4.6. *([Neb12], Theorem* 5.3*) Let* $\mathscr{L}$ *be an extremal lattice of dimension* 48 *such that* $\mathrm{Aut}(\mathscr{L})$ *contains some element* σ *of order* m *with* $\phi(m) = 48$*. Then* $m = 65$ *or* $m = 104$ *and* $\mathscr{L} \cong P_{48n}$*.*

CHAPTER 5
Conclusion

In this thesis, we studied lattices and a particular way of constructing them in number fields. We first gave some basic definitions about lattices and explained the relationship with quadratic forms. We then introduced the signature of lattices as the signature of the corresponding quadratic forms. We followed by specializing to the particular case of positive definite lattices, or Euclidean lattices. We gave some important results about these lattices that are not true for general lattices. We then introduced some of our main examples of lattices; the root lattices. These lattices are particularly interesting since they are related to geometrical problems. We surveyed the known results about these problems and we concluded our chapter on general facts about lattices by introducing some other of our main examples of lattices; the even unimodular lattices. These lattices are particularly interesting since their theta series are modular forms.

In the following chapter, we presented a way to obtain lattices using ideals in number fields and the trace pairing. These lattices are often referred to as ideal lattices. We determined formulas for the discriminant and the signature of these lattices. Then we considered the properties of positive definiteness, rationality, integrality and unimodularity of ideal lattices.

A logical continuation of our study was then to consider the special case of the cyclotomic fields. Indeed, we know a lot about the ideals in these fields and so we can use this knowledge to build concrete examples of ideal lattices. It turns out that there is an interesting theory of ideal lattices in cyclotomic fields as shown by some papers of E. Bayer. The key fundamental observation to begin with is that a primitive root

of unity acts on our lattices as an automorphism. This automorphism has for characteristic polynomial a cyclotomic polynomial and having such an automorphism characterizes the lattices arising from cyclotomic fields. This characterization allows to determine all the indecomposable root lattices arising from cyclotomic fields and also all the cyclotomic fields in which they can be obtained. Then, with the help of Proposition 4.2.5 telling exactly when an orthogonal direct sum of indecomposable lattices is similar to an ideal lattice in a cyclotomic field, we could obtain Theorem 4.2.18 determining all the root lattices arising from cyclotomic fields and all the cyclotomic fields in which they can be obtained. This is our contribution to this theory. We also presented some of the results of E. Bayer about unimodular ideal lattices in cyclotomic fields. Two of them are given in Proposition 4.2.17 and Theorem 4.3.1. They are very useful tools in determining all the Niemeier lattices arising from cyclotomic fields and all the cyclotomic fields in which they can be obtained. Table $4-1$ summarizes these results about the Niemeier lattices. A question for further investigations could be : Can one obtain more of the Neimeier lattices if one does not restrict to cyclotomic fields? In the same spirit, one might also ask: What are the root lattices that can be obtained in totally real number fields or in arbitrary CM-fields? We also talked a bit about higher dimensions in the last section of chapter 4. Another question that could be investigated is: Is there other interesting examples of lattices that can be obtained in cyclotomic fields in higher dimensions?

REFERENCES

[Bay84] E. Bayer. Definite unimodular lattices having an automorphism of given characteristic polynomial. *Comment. math. Helv.*, 59:509–538, 1984.

[Bay99] E. Bayer. Lattices and number fields. In *Algebraic geometry: Hirzebruch 70*, pages 69–84. Contemporary mathematics 241, American Mathematical Society, Providence, 1999.

[Cha85] G. Chapline. Unification of gravity and elementary particle interactions in 26 dimensions? *Phys. Lett.*, B158:393–396, 1985.

[CS99] J.H. Conway and N.J.A. Sloane. *Sphere packings, lattices and groups*. Third edition, Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York, 1999.

[Ebe94] W. Ebeling. *Lattices and codes, a course partially based on lectures by F.Hirzebruch*. Advanced lectures in Mathematics, Vieweg, Braunschweig/Wiesbaden, 1994.

[Hum72] J.E. Humphreys. *Introduction to Lie algebras and representation theory*. Graduate texts in Mathematics, Springer-Verlag, New York, 1972.

[Ker94] M. Kervaire. Unimodular lattices with a complete root system. *Enseignement mathématique*, 40:59–104, 1994.

[Kin03] O. King. A mass formula for unimodular lattices with no roots. *Mathematics of Computation*, 72:836–863, 2003.

[Lan94] S. Lang. *Algebraic number theory*. Second edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 1994.

[LHF11] J. Lagarias, T. Hales, and S. Ferguson. *The Kepler conjecture : the Hales-Ferguson proof by Thomas Hales, Samuel Ferguson*. Springer, New York, 2011.

[Neb98] G. Nebe. Some cyclo-quaternionic lattices. *Journal of algebra*, 199:472–498, 1998.

[Neb12] G. Nebe. On automorphisms of extremal even unimodular lattices of dimension 48. *arXiv:1212.0865v1 [math.NT]*, 2012.

[OH80] M. O'Keeffe and B.G. Hyde. Plane nets in crystal chemistry. *Phil. Trans. Roy. Soc. London*, A295:553–623, 1980.

[Ser73] J.P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1973.

[Was97] Washington. *Introduction to cyclotomic fields*. Second edition, Graduate texts in Mathematics, Springer-Verlag, New York, 1997.