On the Construction and Uniqueness of the E_8 Lattice

Mathematics Bachelor Thesis

Casper Jeukendrup

Supervisor: Dr. J.M. Commelin
Department of Mathematics

Universiteit Utrecht

January 17th, 2025

Abstract

In this thesis, we set out the basic theory of lattices, and study the E_8 lattice in particular. Lattices are finitely generated free abelian groups equipped with a symmetric bilinear form, and have many applications in mathematics and computer science. We define the most important properties of lattices, and construct the E_8 lattice based on the construction shown by Jean-Pierre Serre. We then study an article by Noam Elkies, in which he introduces the characteristic vectors and theta series of a lattice. The latter, after the necessary complex analysis, leads to a characterisation of the $\mathbb{Z}^n$ lattices by their shortest characteristic vectors. It turns out that E_8 and $\mathbb{Z}^8$ have a common sublattice D_8, and that both are contained in the dual lattice D_8^*. After studying the lattices between D_8 and D_8^*, we conclude that E_8 is, up to isomorphism, the unique even, positive-definite, unimodular lattice in dimension 8.

Contents

Introduction

A *lattice* is a finitely generated free abelian group equipped with a symmetric bilinear form. In this thesis, we discuss the basic theory of lattices, and study the E_8 lattice in particular.

Lattices have many applications in mathematics and computer science. They play a big role in the study of quadratic forms and of sphere packings, but also find applications in cryptography and coding theory. And even in themselves, lattices form an interesting subject of study. Much work has been done on the classification and enumeration of lattices based on their properties, for example by Conway and Sloane in [2]. Particularly interesting and important are the 24-dimensional Leech lattice, and the eight-dimensional E_8 lattice to which this thesis is dedicated.

In Chapter 1, we introduce the most important properties of lattices. In particular, we define *integral*, *unimodular* and *even* lattices. In Chapter 2, we construct the E_8 lattice, based on the construction shown by Jean-Pierre Serre in [6], and show that it satisfies all of the mentioned properties. In Chapter 3, we study an article by Noam Elkies [4], in which he introduces the *characteristic vectors* and theta series of a lattice. After the necessary complex analysis, this results in a characterisation of the $\mathbb{Z}^n$ lattice by its shortest characteristic vectors. This finally enables us to prove in Chapter 4, following another article by Elkies, that the E_8 lattice is, up to isomorphism, the unique lattice with its properties in dimension 8.

1.

Basic theory of lattices

In this chapter, we discuss the definition of a lattice, as well as some basic properties and general results. After that, we will show some examples of lattices.

1.1 Preliminaries

Below, we will write all groups additively, unless otherwise specified. Multiplication of group elements with integers is defined as repeated addition.

Definition 1.1.1. A *free abelian group* V is an abelian group that has a *basis*; that is, a set $B \in V$ such that for every element $x \in V$, there exist unique non-zero elements $a_1, \ldots, a_k \in \mathbb{Z}$ and unique $b_1, \ldots, b_k \in B$ such that $x = a_1 b_1 + \cdots + a_k b_k$ for some integer $k \geq 0$.

The cardinality of B is called the *rank* of V. We say that V is *generated* by B; if B has finite cardinality, we say that V is *finitely generated*.

We note that a free abelian group of rank n is exactly a free $\mathbb{Z}$-module of rank n.

As an example, for $n \in \mathbb{N}$, the group $\mathbb{Z}^n$ is a free abelian group of rank n; a possible basis is the standard basis $e_1, \ldots, e_n$.

Definition 1.1.2. Let V be a finitely generated free abelian group. A *bilinear form* on V is a function $(\cdot, \cdot) : V \times V \to \mathbb{R}$ that is linear in both its arguments. A bilinear form is called *symmetric* if $(x, y) = (y, x)$ for all $x, y \in G$.

Suppose V has a basis $B = \{b_1, \ldots, b_n\}$. Symmetric bilinear forms on V can be identified with symmetric $n \times n$ matrices in the following way. Let $(\cdot, \cdot)$ be a bilinear form, and let x, y be elements of V. Because V is a free abelian group, we can write these elements as $x = \sum_{i=1}^{n} x_i b_i$ and $y = \sum_{j=1}^{n} y_j b_j$. Now, using bilinearity, we can rewrite the expression (x, y) as follows:

$$\begin{aligned}(x, y) &= \left(\sum_{i=1}^{n} x_i b_i, \quad \sum_{j=1}^{n} y_j b_j \right) \\ &= \sum_{i=1}^{n} x_i \sum_{j=1}^{n} y_j (b_i, b_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j (b_i, b_j)\end{aligned}$$

This means that the values of $(\cdot,\cdot)$ are fully determined by its values on $B \times B$. Thus, $(\cdot,\cdot)$ is determined by the following symmetric matrix:

$$M = \begin{pmatrix} (b_1,b_1) & \dots & (b_1,b_n) \\ \vdots & \ddots & \vdots \\ (b_n,b_1) & \dots & (b_n,b_n) \end{pmatrix}$$

(The symmetry of this matrix follows from the fact that $(\cdot,\cdot)$ is symmetric.)

Note that we can write $(x,x) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j (b_i,b_j) = x^T M x$ for all $x \in V$.

Next, we introduce the concept of a *quadratic form*. Usually, a quadratic form is defined as a polynomial where all terms have degree 2, but in this case we opt for the following definition:

Definition 1.1.3. Let V be finitely generated free abelian group. A *quadratic form* on V is a function $q : V \to \mathbb{R}$ that satisfies the following:

- For all $a \in \mathbb{R}$ and $x \in V$, we have $q(ax) = a^2 q(x)$.
- The function $(x,y) \mapsto q(x+y) - q(x) - q(y)$ is a bilinear form.

Like for symmetric matrices, there is also a correspondence between symmetric bilinear forms and quadratic forms. Given a quadratic form q, the function

$$(x,y) \mapsto \frac{1}{2}[q(x+y) - q(x) - q(y)]$$

is a symmetric bilinear form; the fact that it is a bilinear form, follows from the second requirement of definition 1.1.3, while the symmetry follows from the fact that both V and $\mathbb{R}$ are abelian groups.

Conversely, given a symmetric bilinear form $(\cdot,\cdot)$, the function $q : x \mapsto (x,x)$ is a quadratic form. The first requirement of definition 1.1.3 follows from the bilinearity of b; for the second, we note that

$$\begin{aligned} q(x+y) - q(x) - q(y) &= (x+y, x+y) - (x,x) - (y,y) \\ &= (x,x) + (x,y) + (y,x) + (y,y) - (x,x) - (y,y) \\ &= 2(x,y) \end{aligned}$$

which is indeed a bilinear form.

In summary, this establishes a correspondence between quadratic forms and symmetric bilinear forms, via the mapping

$$\left\{ q \text{ quadratic form} \right\} \quad \mapsto \quad \left\{ (x,y) \mapsto \frac{1}{2}[q(x+y) - q(x) - q(y)] \right\}$$

with inverse

$$\left\{ (\cdot,\cdot) \text{ symmetric bilinear form} \right\} \quad \mapsto \quad \left\{ q : x \mapsto (x,x) \right\}.$$

That these are inverses follows from the calculations above.

To close the circle, we show a correspondence between quadratic forms and symmetric

matrices. Suppose we have a quadratic form q, with corresponding symmetric bilinear form $(\cdot, \cdot)$, and that this symmetric bilinear form corresponds to the symmetric matrix M. Then, for all $x \in V$, we have

$$\begin{aligned} q(x) &= (x, x) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j (b_i, b_j) \\ &= x^T M x \end{aligned}$$

where $b_i, 1 \leq i \leq n$, form a basis of V.

Incidentally, from the second line, we can see that each quadratic form according to the above definition is also a quadratic form in the usual sense, of a polynomial with all terms of degree 2.

1.2 Lattices

We are now ready to give a definition of a lattice and related concepts.

Definition 1.2.1. A *lattice* is a finitely generated free abelian group L of rank n, together with a symmetric bilinear form $(\cdot, \cdot)$ on it, or equivalently, with a quadratic form q on it.

We call a lattice *integral* if $(\cdot, \cdot)$ produces integer values.

Remark 1.2.2. We note that every lattice can be identified with a lattice that is contained in $\mathbb{R}^n$ with the same bilinear form, by choosing a basis for the lattice and identifying each lattice point with its coordinates with respect to the chosen basis. The lattice is then a *discrete subgroup* of $\mathbb{R}^n$ as an additive group, which means that every lattice point has a neighbourhood that contains no other lattice points.[1] Some authors define a lattice as a discrete subgroup of $\mathbb{R}^n$, and always use the standard inner product as the bilinear form. $\Diamond$

Definition 1.2.3. With a *sublattice* of a lattice L, we mean a subgroup of L, which is a lattice with the same bilinear form.

Definition 1.2.4. The *Gram matrix* M of a lattice L with respect to a basis B of L, is the symmetric matrix corresponding to the symmetric bilinear form with respect to B. The *determinant*, or *discriminant*, of a lattice is the determinant of the Gram matrix.

Whereas the Gram matrix depends on the choice of basis, the determinant of a lattice does not. Changing to a different basis B' comes down to multiplying all elements of L with an invertible matrix X with integer entries; the Gram matrix with respect to B' is given by $M' = XMX^T$. Because of the properties of determinants, we have

$$\det(M') = \det(X) \det(M) \det(X^T) = \det(M) \det(X)^2.$$

Since X is an invertible matrix with integer entries, its determinant must be a multiplicatively invertible integer, i.e. ± 1. Its square is then 1, so it follows that $\det(M') = \det(M)$. From now on, we can thus speak of *the* determinant of a lattice.

For a lattice L contained in $\mathbb{R}^n$ with the standard inner product, the Gram matrix can also

[1] Source: `https://en.wikipedia.org/wiki/Discrete_group`

be written as B^TB, where B is the matrix with the basis vectors as columns. It follows that $\det(L) = \det(B)^2$. This leads to a geometrical interpretation of the determinant of a lattice: the determinant of matrix B is the volume of the parallelepiped spanned by the basis vectors, so the determinant of the lattice is the square of this volume. Thus, this volume appears to be invariant under basis transformations. This parallelepiped is sometimes called the *fundamental region* of the lattice.

Definition 1.2.5. When an integral lattice has determinant ± 1, we call the lattice *unimodular*.

To illustrate the usefulness of unimodularity, we prove the following lemma:

Lemma 1.2.6. *Let L be a unimodular lattice with bilinear form $(\cdot, \cdot)$. Then for every element $v \in L$, $v \notin 2L$, there exists an element $w \in L$ such that $(v, w) \equiv 1 \pmod 2$.*

Proof. We will prove the contrapositive. Suppose that there is an element $v \in L$, $v \notin 2L$, such that for all $w \in L$, $(v, w) \equiv 0 \pmod 2$. We choose a basis for L that contains v as one of the basis vectors, and calculate the Gram matrix M with respect to this basis. The column corresponding to v will contain only even entries. It follows that the determinant of M is even, so the lattice is not unimodular. □

Definition 1.2.7. The *dual lattice* of a lattice $L \subset \mathbb{R}^n$, commonly notated as L^*, is defined as follows:

$$L^* = \{x \in \text{span}(L) : (x, y) \in \mathbb{Z} \text{ for all } y \in L\}.$$

It is clear that L^* is also a lattice. If L is integral, then $L \subseteq L^*$. Furthermore, we have the following lemma:

Lemma 1.2.8. *Let L be a unimodular lattice. Then $L = L^*$.*

In order to prove this, we need the following theorem from module theory and a corollary of it:

Theorem 1.2.9 ([3, Ch.12, Theorem 4])**.** *Let R be a Principal Ideal Domain, let M be a free R-module of finite rank n and let N be a submodule of M. Then*

1. *N is free of rank m, $m \leq n$ and*
2. *there exists a basis $y_1, \ldots, y_m$ of M so that $a_1y_1, \ldots, a_my_m$ is a basis of N where $a_1, \ldots, a_m$ are nonzero elements of R with the divisibility relations*

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

For the proof, we refer to [3].

This theorem applies to lattices too, since free abelian groups are free $\mathbb{Z}$-modules and $\mathbb{Z}$ is a principal ideal domain.

Corollary 1.2.10. *Let $M \subset \mathbb{R}^n$ be a lattice of dimension n, and let N be a sublattice of M of equal dimension. Then $\det(N) = [M : N]^2 \cdot \det(M)$, where $[M : N]$ denotes the index of N in M.*

Proof. This proof was partly inspired by [1], replacing the dependency on the Smith normal form by the theorem above.

Let $b_1, \ldots, b_n$ be the basis of M as provided by the theorem above, and let $a_1 b_1, \ldots, a_n b_n$ be the corresponding basis of N, where $a_1, \ldots, a_n$ are positive integers. If we let B and C denote the matrices consisting of respectively $b_1, \ldots, b_n$ and $a_1 b_1, \ldots, a_n b_n$ as columns, then $C = XB$ holds for the diagonal matrix

$$X := \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}.$$

We observe that $\det(X) = a_1 \cdots a_n$.

Furthermore, we see that $[M : N]$ also equals $a_1 \cdots a_n$: from the relations between the basis vectors of M and N, we deduce that

$$M/N \cong Z_{a_1} \oplus \cdots \oplus Z_{a_n},$$

where Z_m denotes the cyclic group of order m.

We conclude that $[M : N] = a_1 \cdots a_n = \det(X)$ and thus

$$\det(C) = \det(X) \det(B) = [M : N] \cdot \det(B).$$

Since $\det(M) = \det(B)^2$ and $\det(N) = \det(C)^2$, it follows that

$$\det(N) = [M : N]^2 \cdot \det(M). \qquad \square$$

This corollary enables us to prove Lemma 1.2.8:

Proof of Lemma 1.2.8. We will show this by contrapositive. Suppose $L \neq L^*$. Since it was already clear that $L \subseteq L^*$, that means there must exist an element $w \in L^*$ such that $w \notin L$. Then $L + \mathbb{Z}w = \{v + kw : v \in L, k \in \mathbb{Z}\}$ is also an integral lattice of the same dimension as L, that contains L as a sublattice. As $L + \mathbb{Z}w$ is not equal to L, it follows that $[L + \mathbb{Z}w : L] > 1$. From corollary 1.2.10, we know that

$$\det(L) = [L + \mathbb{Z}w : L]^2 \cdot \det(L + \mathbb{Z}w).$$

Since $\det(L + \mathbb{Z}w)$ is an integer, it follows that $\det(L)$ cannot be equal to 1, so L is not unimodular. $\square$

The converse can also be shown; because of this, the terms *unimodular* and *self-dual* are sometimes used interchangeably.

We end this section with a few more definitions.

Definition 1.2.11. We define the *norm* of a lattice element x to be (x, x), i.e. the quadratic form associated with $(\cdot, \cdot)$.

A lattice is *positive definite* if the norm of all non-zero elements is positive.

An integral lattice is called *even*, or *of type II*, if the norm on it only takes even values. Otherwise, it is called *odd*, or *of type I*.

Definition 1.2.12. Two lattices L, L' are called *isomorphic* if there exists an isomorphism $f : L \to L'$ of abelian groups between them, and this isomorphism preserves the bilinear form, i.e. $(f(x), f(y)) = (x, y)$ for all x, y in L.

1.3 Examples

Example 1.3.1. For $n \in \mathbb{N}$, the free abelian group $\mathbb{Z}^n$ with the standard inner product $(\cdot, \cdot)$ forms a lattice. The corresponding quadratic form is $(x, x) = x_1^2 + \cdots + x_n^2$. Since the standard inner product clearly takes integer values on $\mathbb{Z}^n \times \mathbb{Z}^n$, this lattice is integral.

The Gram matrix of this lattice, with respect to the standard basis of $\mathbb{Z}^n$, is the identity matrix $\mathbf{I}_n$. It has determinant 1, which makes the lattice unimodular. Furthermore, since it is known that the standard inner product is positive definite, the lattice is positive-definite too. However, not all elements have an even norm: for example, the basis vector e_1 has norm $(e_1, e_1) = 1$. Therefore, this lattice is odd, or of type I. ◊

Example 1.3.2. Let U denote the lattice given by $\mathbb{Z}^2$ with the quadratic form $q(x) = 2x_1x_2$. The corresponding matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (with respect to the standard basis). From the fact that this Gram matrix has integer entries, it follows that the corresponding bilinear form takes integer values on $U \times U$, so U is an integral lattice. The determinant of the Gram matrix is -1, so U is unimodular.

From the definition of the quadratic form, which is also the norm on U, it is clear that this norm takes even values, so U is even, or of type II.

The lattice U is called the *hyperbolic lattice*. ◊

Example 1.3.3. Let L_1 and L_2 be lattices with bilinear forms $B_1(\cdot, \cdot)$ and $B_2(\cdot, \cdot)$. Recall that the *direct sum* $L_1 \oplus L_2$ of abelian groups is the abelian group that consists of all elements $x_1 \oplus x_2$ for $x_1 \in L_1, x_2 \in L_2$, with "coordinate-wise" group operation. This direct sum $L_1 \oplus L_2$ can also be made a lattice, with bilinear form $(x_1 \oplus x_2, y_1 \oplus y_2) := B_1(x_1, y_1) + B_2(x_2, y_2)$. ◊

Example 1.3.4. The lattice E_8 is the unique even, positive-definite, unimodular lattice of rank 8. It is studied in the rest of this paper. ◊

2.

An algebraic construction of the E_8 lattice

In this chapter, we will show a construction of the E_8 lattice as described by J.P. Serre in [6, Ch.V, 1.4.3].

Let k be an integer ≥ 0, and let $n = 4k$. Let V be the vector space $\mathbb{R}^n$, with the standard inner product $(x, y) = \sum_{i=1}^{n} x_i y_i$. With respect to the standard basis $e_1, \ldots, e_n$, the matrix corresponding to this inner product (viewed as a symmetric bilinear form) is the identity matrix $\mathbf{I}_n$.

Let E_0 be the subgroup of V formed by the points with integer coordinates; that is, $E_0 = \mathbb{Z}^n$. As seen in Example 1.3.1, this is a positive-definite, unimodular integral lattice.

Let E_1 be the sublattice of E_0 formed by the points with even norm, i.e. the points x such that

$$(x, x) \equiv 0 \pmod 2 \quad \Leftrightarrow \quad \sum_{i=1}^{n} x_i^2 \equiv 0 \pmod 2 \quad \Leftrightarrow \quad \sum_{i=1}^{n} x_i \equiv 0 \pmod 2. \tag{2.1}$$

We observe that $[E_0 : E_1] = 2$.

Let E be the subgroup of V generated by E_1 and the element $e = (\frac{1}{2}, \ldots, \frac{1}{2})$. We note that $2e \in E_1$: it has integer coordinates, and $(2e, 2e) = n$, which was chosen to be a multiple of 4, thus even. On the other hand, we note that $e \notin E_1$, since it does not have integer coordinates. This leads to the conclusion that $[E : E_1] = 2$.

We will now give a characterisation of the elements of E:

Lemma 2.0.1. *An element $x = (x_i)$ of V is contained in E if and only if*

$$2x_i \in \mathbb{Z} \quad (1 \leq i \leq n) \qquad x_i - x_j \in \mathbb{Z} \quad (1 \leq i, j \leq n) \qquad \textit{and} \qquad \sum_{i=1}^{n} x_i \in 2\mathbb{Z}.$$

Proof. ($\Rightarrow$) Suppose $x \in E$. Then either $x \in E_1$ or $x \in E_1 + e$.

In the case that $x \in E_1$, it has integer coordinates, so the first two conditions are satisfied; the third follows from (2.1).

In the case that $x \in E_1 + e$, it can be written as $x = y + e$ for some $y = (y_1, \ldots, y_n) \in E_1$.

We have:

$$\begin{aligned} 2x_i &= 2y_i + 2 \cdot \frac{1}{2} \in \mathbb{Z} \qquad (1 \leq i \leq n) \\ x_i - x_j &= y_i - y_j \in \mathbb{Z} \qquad (1 \leq i, j \leq n) \\ \sum_{i=1}^{n} x_i &= \sum_{i=1}^{n} (y_i + \frac{1}{2}) = \sum_{i=1}^{n} y_i + \frac{n}{2} \in 2\mathbb{Z}. \end{aligned}$$

($\Leftarrow$) Suppose x satisfies the three conditions. From the first condition, it follows that every coordinate of x is either an integer or an integer plus $\frac{1}{2}$. The second condition implies that if any coordinate is an integer plus $\frac{1}{2}$, then all coordinates are. It follows that either $x \in E_0$ or $x \in E_0 + e$.

In the first case, the third condition immediately implies $x \in E_1$. In the second case, we have $x = y + e$ for some $y \in E_0$; so, the third condition implies $\sum_{i=1}^{n} y_i + \frac{n}{2} \in 2\mathbb{Z}$, thus $\sum_{i=1}^{n} y_i \in 2\mathbb{Z}$, so $y \in E_1$ and $x \in E_1 + e$. We conclude that in either case, $x \in E$. □

We will now show that E is a unimodular lattice. We observe that $(x, e) = \frac{1}{2} \sum_{i=1}^{n} x_i \in \mathbb{Z}$ for all $x \in E$, and that $(e, e) = k$. By bilinearity and symmetry of $(\cdot, \cdot)$, it follows that $(\cdot, \cdot)$ takes integer values on E, which makes E an integral lattice. To show that E is unimodular, we recall Corollary 1.2.10, which says that if L is a lattice in $\mathbb{R}^n$ with the standard inner product and L' is a sublattice of L of equal dimension, then

$$\det(L') = [L : L']^2 \cdot \det(L).$$

Applying this to the lattices E_0, E_1, and E, for which we have $[E_0 : E_1] = [E : E_1] = 2$, we find that $\det(E)$ must be equal to $\det(E_0) = 1$. This makes E a unimodular lattice.

Because $(\cdot, \cdot)$ is positive definite, E is also positive definite.

From now on, we will focus on the case that k is even, so that n is a multiple of 8. In this situation, we see that $(e, e) = k$ is even. Furthermore, we can show that (x, x) is even for all $x \in E$: again, either $x \in E_1$ or $x \in E_1 + e$; in the first case, (x, x) is even by definition of E_1, and in the second case, $(x, x) = (y + e, y + e) = (y, y) + 2(y, e) + (e, e)$, which is also even. We conclude that E is an even lattice.

The construction above leads to a family of unimodular, positive definite, even lattices Γ_{8m}, $m \in \mathbb{N}$. In the continuation of this paper, we will study the lattice $E_8 = \Gamma_8$ in more detail.

A possible basis for the E_8 lattice is given by Serre in [6, Ch.V, 1.4.3]:

$$\begin{gathered} \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + \cdots + e_7), \\ e_1 + e_2, \\ e_i - e_{i-1} \quad (2 \leq i \leq 7). \end{gathered}$$

The corresponding Gram matrix is given by

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

When identifying E_8 with $\mathbb{Z}^8$ by identifying every lattice point with its coordinates with respect to a basis, a corresponding quadratic form is given in [2, Chap.2, §2.2]:

$$\xi_1^2 - \xi_1\xi_2 + \xi_2^2 - \xi_2\xi_3 + \xi_3^2 - \xi_3\xi_4 + \xi_4^2 - \xi_4\xi_5 + \xi_5^2 - \xi_5\xi_6 + \xi_6^2 - \xi_6\xi_7 + \xi_7^2 - \xi_5\xi_8 + \xi_8^2.$$

The following chapters will be dedicated to proving that E_8 is, up to isomorphism, the unique even positive-definite unimodular integral lattice of rank 8.

3.

Characteristic vectors

In this chapter, we will study an article by Noam Elkies [4], in which he defines *characteristic vectors* of a lattice and then gives a characterisation of the $\mathbb{Z}^n$ lattice using this concept. We will first discuss some background material, and then introduce characteristic vectors and the theta series of a lattice; we will then follow Elkies's path towards the following result:

Theorem. *Let L be a unimodular integral lattice in $\mathbb{R}^n$, with no characteristic vectors of norm smaller than n. Then L is isomorphic to $\mathbb{Z}^n$.*

3.1 The modular group

To start, we will introduce the modular group and take a glance at the concept of modular forms. Although we will not use this theory directly, it is useful to discuss it at this point, as it provides some insight into the background of the ideas from the next sections.

Let $H := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the upper half-plane of the complex plane, and let $\mathrm{SL}_2(\mathbb{Z})$ denote the group of matrices $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with integer coefficients and determinant $\det(g) = ad - bc = 1$.

We define the following group action of $\mathrm{SL}_2(\mathbb{Z})$ on H: for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in H$,

$$gz := \frac{az + b}{cz + d}.$$

To see that the image lies indeed in H for all g and z, we can write z as $x + iy$ to obtain

$$\begin{aligned} gz &= \frac{a(x + iy) + b}{c(x + iy) + d} \\ &= \frac{(ax + b)(cx + d) + acy^2 + iy(ad - bc)}{|cz + d|^2}; \end{aligned}$$

because of the assumption about g that $ad - bc = 1$, it follows that

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz + d|^2} > 0.$$

We observe that the element $-I := \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially on H, as $-Iz = \frac{-z}{-1} = z$. Therefore, we can consider the quotient group $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, and let it act

on H by the action naturally induced by the action of $\mathrm{SL}_2(\mathbb{Z})$. One could show that this action is *faithful*.

Definition 3.1.1. We call the group $G := \mathrm{PSL}_2(\mathbb{Z})$ the *modular group*.

Consider the elements S and T of G represented respectively by the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The following identities hold:

$$Sz = -\frac{1}{z}, \qquad Tz = z + 1$$
$$S^2 = I, \qquad (ST)^3 = I.$$

As shown in [6, Ch. VII, Thm. 2], the group G is generated by S and T; since we will not use this fact here, we will not discuss the proof.

Definition 3.1.2. A *fundamental domain* for a group action on a set X is a subset $D \subseteq X$ that contains exactly one representative of each orbit under the group action.[1]

Consider the set $D := \{z \in H : |z| \geq 1, |\mathrm{Re}(z)| \leq \frac{1}{2}\}$. There is a set $D^\circ \in D$ such that $D = \overline{D^\circ}$ and D° is a fundamental domain for the action of G on H, as shown in [6, Ch. VII, Thm. 1]. In other words, D minus (part of) its border is a fundamental domain for this action. (D itself is not: for example, the points $z_1 = -\frac{1}{2} + i$ and $z_2 = \frac{1}{2} + i$ are both in D but are in the same orbit under the action, since $Tz_1 = z_2$.)

Figure 3.1 shows the fundamental domain D, as well as a few points of the orbit under G of an arbitrarily chosen point $z \in D$.

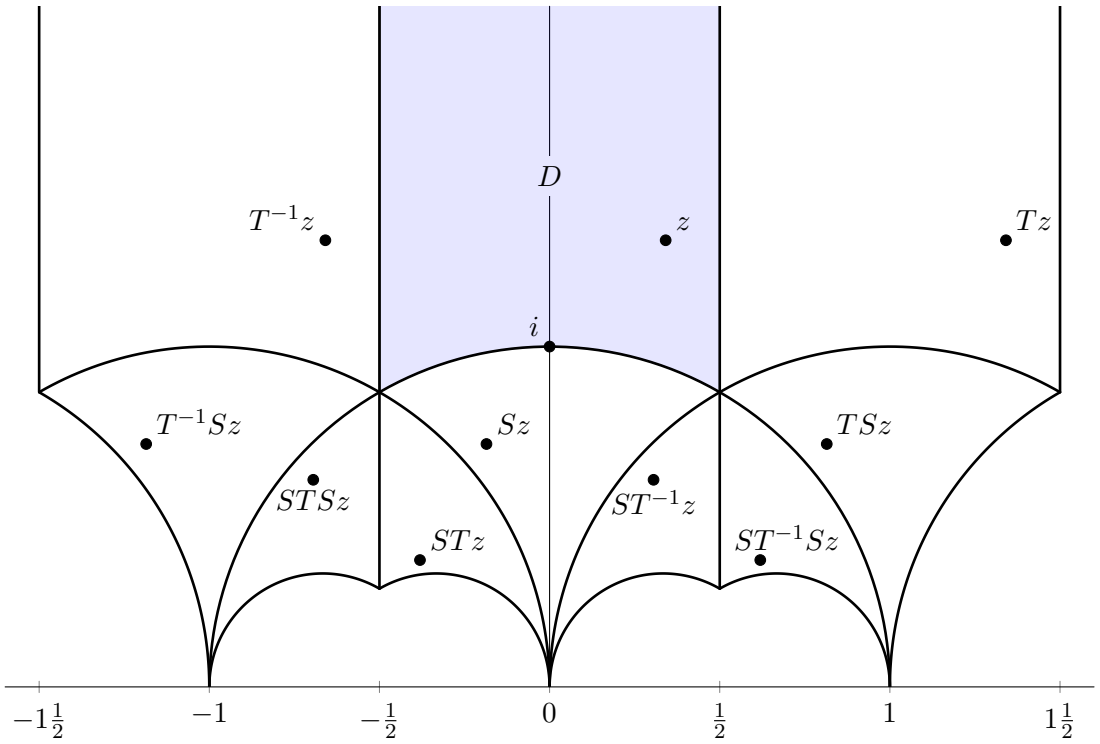

Figure 3.1: The fundamental domain of the modular group

[1] Source: `https://en.wikipedia.org/wiki/Fundamental_domain`

To give an application of the theory discussed above: one can now define the notion of "weakly modular functions" on H, which are meromorphic functions f that satisfy

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$$

for all $z \in H$ and all $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, for some integer k. Because of the fact that G is generated by S and T, it suffices to check that $f(Tz) = f(z+1)$ and $f(Sz) = z^2 k f(z)$.

Based on that information, one can introduce a finer class of functions, the *modular forms*, that satisfy the above conditions and are also holomorphic among other things. In [6, Ch. VII], the theory of modular forms is developed further, and then utilised to prove facts about lattices, among other things. In particular, for even lattices, Serre shows that the *theta series*, which we will introduce in one of the next sections, is a modular form, which leads to certain results. We too will investigate the behaviour of the theta series in relation to the action of the modular group, but in a more direct way.

3.2 Characteristic vectors

But first, we give a definition of the *characteristic vectors* of a lattice, because we will encounter them in the next section. This definition and the motivation for it stems from [4].

Let L be a unimodular integral lattice in $\mathbb{R}^n$ with the standard inner product.

In this section, we will use the term *character* to refer to a group homomorphism from L to $\{\pm 1\}$. (Usually, this term is used for a slightly wider definition, but this one suits our needs.)

First, we claim that the map $h : L \to \{\pm 1\}, v \mapsto (-1)^{|v|^2}$ is a character: for $v_1, v_2 \in L$, we have

$$h(v_1+v_2) = (-1)^{|v_1+v_2|^2} = (-1)^{|v_1|^2+2(v_1,v_2)+|v_2|^2} = (-1)^{|v_1|^2}(-1)^{|v_2|^2} = h(v_1)h(v_2),$$

where we used that (v_1, v_2) is an integer and thus $(-1)^{2(v_1,v_2)} = 1$.

Similarly, for every $w \in L$, the map $h_w : L \to \{\pm 1\}, v \mapsto (-1)^{(v,w)}$ is also a character: for $v_1, v_2 \in L$, we have

$$h_w(v_1+v_2) = (-1)^{(v_1+v_2,w)} = (-1)^{(v_1,w)+(v_2,w)} = (-1)^{(v_1,w)}(-1)^{(v_2,w)} = h_w(v_1)h_w(v_2)$$

(which, in contrast, only depends on bilinearity of the inner product).

We might wonder, given $w_1, w_2 \in L$, under what circumstance $h_{w_1} = h_{w_2}$ holds. This is the case if and only if $(w_1, v) \equiv (w_2, v) \pmod 2$ for all $v \in L$. A sufficient condition for that is that $w_1 = w_2 + 2u$ for some $u \in L$: then $(w_1, v) = (w_2, v) + 2(u, v) \equiv (w_2, v) \pmod 2$. In other words, if w_1 and w_2 are in the same coset of $2L$ in L, then $h_{w_1} = h_{w_2}$. This motivates the following proposition.

Proposition 3.2.1. *The map $(w + 2L) \mapsto h_w$ defines a bijection between cosets of $2L$ in L and characters.*

Proof. That this map is well-defined, follows from the above.

It is clear that there are 2^n different cosets of $2L$ in L. We observe that there are also 2^n different characters: from the homomorphism property, it follows that a character is fully determined by its values on a basis of L. A basis consists of n elements, and for each of them, the value can be either 1 or -1; that gives 2^n different possibilities.

Because we are working with finite sets, it suffices to show that the map is injective.

We note that the set of characters forms a group under pointwise multiplication, where every character is its own inverse. Furthermore, the map $(w + 2L) \mapsto h_w$ is a group homomorphism from $L/2L$ to the group of characters: if w_1, w_2 are representatives of elements of $L/2L$, we have for all $v \in L$

$$h_{(w_1+w_2)}(v) = (-1)^{(v,w_1+w_2)} = (-1)^{(v,w_1)}(-1)^{(v,w_2)} = h_{w_1}(v)h_{w_2}(v),$$

so $h_{(w_1+w_2)} = h_{w_1}h_{w_2}$.

To show that a group homomorphism is injective, it suffices to show that the kernel is trivial, i.e. that only the trivial coset $\in L/2L$ is mapped to the trivial character. Suppose that w is a representative of a nontrivial coset. As L is unimodular, Lemma 1.2.6 tells us that there is a vector $v \in L$ such that (v, w) is odd. Then $h_w(v) = -1$, so h_w is not the trivial character.

We conclude that the map is a bijection as claimed. □

So, for all characters k, there is a coset $w + 2L$ such that $h_w = k$. In particular, there must be one for the character h defined at the beginning of this section. Vectors w in this coset satisfy the following property:

$$(-1)^{|v|^2} = (-1)^{(v,w)} \quad \text{for all } v \in L$$

and thus

$$|v|^2 \equiv (v, w) \pmod 2 \quad \text{for all } v \in L. \tag{3.1}$$

That leads to the main definition of this section:

Definition 3.2.2. Vectors $w \in L$ that satisfy (3.1) are called *characteristic vectors* of L.

Proposition 3.2.1 assures us that every lattice has characteristic vectors.

Example 3.2.3. For the lattice $\mathbb{Z}^2$ (with the standard inner product), the quotient group $\mathbb{Z}^2/2\mathbb{Z}^2$ consists of four cosets: $2\mathbb{Z}^2$, $2\mathbb{Z}^2 + \binom{1}{0}$, $2\mathbb{Z}^2 + \binom{0}{1}$, and $2\mathbb{Z}^2 + \binom{1}{1}$. We observe:

$$\begin{aligned}
\left|\tbinom{1}{0}\right|^2 &\not\equiv \left(\tbinom{1}{0}, \tbinom{0}{0}\right) \pmod 2 \\
\left|\tbinom{1}{1}\right|^2 &\not\equiv \left(\tbinom{1}{1}, \tbinom{1}{0}\right) \pmod 2 \\
\left|\tbinom{1}{1}\right|^2 &\not\equiv \left(\tbinom{1}{1}, \tbinom{0}{1}\right) \pmod 2
\end{aligned}$$

so the first three of the mentioned cosets are not the one containing characteristic vectors. Thus, that must be $2\mathbb{Z}^2 + \binom{1}{1}$: all vectors with both coordinates odd are characteristic vectors of $\mathbb{Z}^2$. ◊

3.3 Theta series

For certain types of problems, it may be useful to know how many vectors of a certain norm there are in a lattice [2, Ch. 2, §2.3]. A tool to facilitate such calculations is the *theta series* of a lattice, which encodes the norms of the vectors of the lattice in the following way:

Definition 3.3.1. Let L be a lattice. The *theta series* of L is the function $\theta_L : H \to \mathbb{C}$ defined by

$$\theta_L(z) := \sum_{v \in L} e^{\pi i (v,v) z}.$$

If L is a lattice in $\mathbb{R}^n$ with the standard inner product, we can also write

$$\theta_L(z) = \sum_{v \in L} e^{\pi i |v|^2 z}.$$

For integral lattices L, the theta series can be written as the power series

$$\theta_L(z) = \sum_{m=0}^{\infty} N_{L,m} q(z)^m, \tag{3.2}$$

where $N_{L,m}$ is the number of vectors of norm m in L and $q(z) = e^{\pi i z}$.

It can be shown that this series converges for all $z \in H$: by comparing the volume of the unit sphere in $\mathbb{R}^n$ with the volume of the fundamental region of L, one can conclude that for $k \in \mathbb{N}$, the sum $\sum_{m=0}^{k} N_m$ is $O(k^{n/2})$ [6, Ch.VII, §6.5]; this means that the power series above converges for $|q(z)| < 1$, and $|q(z)| = |e^{\pi i z}| = e^{-\pi \operatorname{Im}(z)} < 1$ for all $z \in H$. It follows that θ_L is a holomorphic function on H.

Example 3.3.2. For the lattice $\mathbb{Z}$ (with multiplication as the bilinear form), we have

$$\begin{aligned} \theta_{\mathbb{Z}}(z) &= \sum_{n \in \mathbb{Z}} e^{\pi i n^2 z} \\ &= 1 + 2 \sum_{m=1}^{\infty} e^{\pi i m^2 z} \\ &= 1 + 2 \left(e^{\pi i z} + e^{4 \pi i z} + e^{9 \pi i z} + \dots \right). \end{aligned}$$

The power series $\sum_{n=1}^{\infty} q(z)^{(n^2)}$ converges if $|q(z)| < 1$, which, as said, is the case for all $z \in H$. This confirms that $\theta_{\mathbb{Z}}$ is a holomorphic function on H. ◊

We show the following property of the theta series:

Proposition 3.3.3. *Let $L = L_1 \oplus L_2$ be a direct sum of lattices as in Example 1.3.3. Then $\theta_L(z) = \theta_{L_1}(z) \cdot \theta_{L_2}(z)$ for all $z \in H$.*

Proof. For every element $v = v_1 \oplus v_2 \in L$, we have $(v, v) = (v_1, v_1) + (v_2, v_2)$; therefore,

$$\begin{aligned}\theta_L(z) = \sum_{v\in L} e^{\pi i(v,v)z} &= \sum_{\substack{v_1\in L_1\\ v_2\in L_2}} e^{\pi i((v_1,v_1)+(v_2,v_2))z} \\ &= \sum_{v_1\in L_1}\sum_{v_2\in L_2} e^{\pi i(v_1,v_1)z} e^{\pi i(v_2,v_2)z} \\ &= \sum_{v_1\in L_1}\left(e^{\pi i(v_1,v_1)z}\sum_{v_2\in L_2} e^{\pi i(v_2,v_2)z}\right) \\ &= \sum_{v_1\in L_1} e^{\pi i(v_1,v_1)z}\sum_{v_2\in L_2} e^{\pi i(v_2,v_2)z} = \theta_{L_1}(z)\cdot\theta_{L_2}(z). \qquad \square\end{aligned}$$

A consequence of this property is that $\theta_{\mathbb{Z}^n}(z) = \theta_{\mathbb{Z}}(z)^n$ for all $z \in H$, which confirms that $\theta_{\mathbb{Z}^n}$, too, is a holomorphic function on H.

In the rest of this section, we will assume that L is a unimodular integral lattice in $\mathbb{R}^n$ with the standard inner product. We will investigate the behaviour of θ_L in relation to the action of the modular group, but not with the goal to achieve a concise conclusion; we will only uncover just enough information to be able to prove the theorem that is the goal of this chapter.

Before considering the modular group, we will first investigate the behaviour of θ_L in relation to the action of the subgroup $G_+ \leq G$ generated by the matrices S and T^2, with S and T as defined in the previous section. The action of this subgroup on the upper half-plane has a different fundamental domain than that of the modular group; for example, $D_+ := \{z \in H : |z| \geq 1, |\mathrm{Re}(z)| \leq 1\}$ (minus parts of its border) is a fundamental domain for this subgroup, depicted in Figure 3.3.

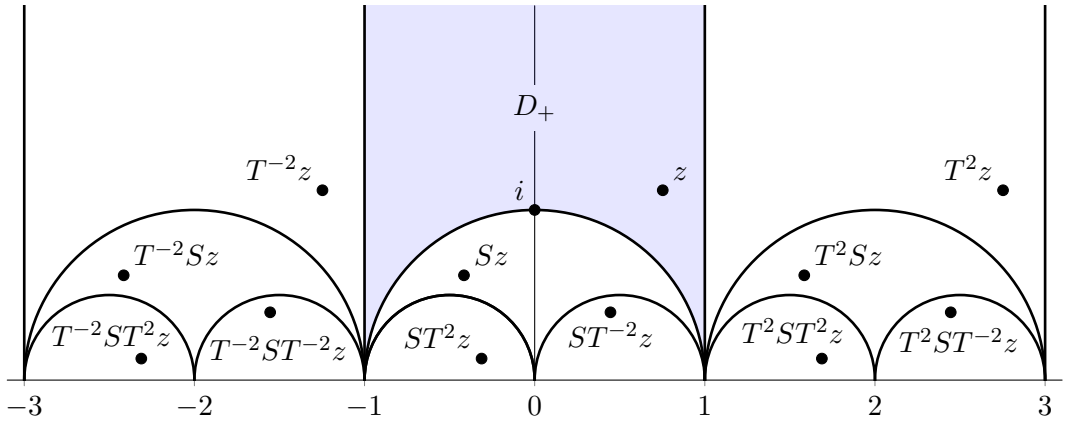

Figure 3.2: The fundamental domain of the group generated by S and T^2

For T^2, we have:

$$\theta_L(T^2z) = \theta_L(z+2) = \theta_L(z), \tag{3.3}$$

where the latter equality follows from the fact that for all $v \in L$, the norm $|v|^2$ is an integer, and thus the map $z \mapsto e^{\pi i|v|^2 z}$ is periodic with period 2.

Remark 3.3.4. Note that if we had assumed that L is even, then the same equality would also hold with T instead of T^2, because $|v|^2$ would be even. But we do not make that assumption here. $\Diamond$

For S, we need to do a bit more work. We will need the following result from complex analysis, which we take, without proof, from [6, Ch.VII, §6.1]:

Proposition 3.3.5. *Let f be a so-called "rapidly decreasing" function $\mathbb{R}^n \to \mathbb{C}$. The* Fourier transform *of f is the function $\hat{f} : \mathbb{R}^n \to \mathbb{C}$ defined by*

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i(x,y)}\, dx.$$

If L is a lattice in $\mathbb{R}^n$ with the standard inner product, and L^* denotes its dual lattice, we have:

$$\sum_{v \in L} f(v) = \frac{1}{\sqrt{\det(L)}} \sum_{v \in L^*} \hat{f}(v).$$

Now let $f(x) = e^{-\pi |x|^2}$. We claim that $\hat{f} = f$:

$$\begin{aligned}
\hat{f}(y) &= \int_{\mathbb{R}^n} e^{-\pi|x|^2} e^{-2\pi i(x,y)}\, dx \\
&= \int_{\mathbb{R}^n} e^{-\pi(x_1^2 + \cdots + x_n^2)} e^{-2\pi i(x,y)}\, dx \\
&= \prod_{j=1}^{n} \int_{-\infty}^{\infty} e^{-\pi x_j^2} e^{-2\pi i x_j y_j}\, dx_j.
\end{aligned}$$

This last integral evaluates to $e^{-\pi y_j^2}$, so the product evaluates to $e^{-\pi(y_1^2 + \cdots + y_n^2)} = e^{-\pi|y|^2} = f(y)$.

Back to our unimodular integral lattice L; by Lemma 1.2.8, $L^* = L$. Now let $t \in \mathbb{R}_{>0}$. If we apply Proposition 3.3.5 to f and the lattice $\sqrt{t}L$, which has determinant t^n and dual lattice $\frac{1}{\sqrt{t}} L^* = \frac{1}{\sqrt{t}} L$, we find:

$$\begin{aligned}
\sum_{v \in \sqrt{t}L} e^{-\pi|v|^2} &= \frac{1}{\sqrt{t^n}} \sum_{v \in \frac{1}{\sqrt{t}}L} e^{-\pi|v|^2} \\
\sum_{v \in L} e^{-\pi|v|^2 t} &= \frac{1}{\sqrt{t^n}} \sum_{v \in L} e^{-\pi|v|^2/t} \\
\theta_L(it) &= \frac{1}{(\sqrt{t})^n} \theta_L(-1/it).
\end{aligned}$$

Since θ_L is a holomorphic and thus analytic function, it is determined by its values on a set that contains an accumulation point, such as the set $i\mathbb{R}_{>0}$. Therefore, this equation holds not only for it, but for all $z \in H$. Substituting z for it, we find:

$$\theta_L(z) = \frac{1}{(\sqrt{z/i})^n} \theta_L(-1/z)$$

and thus:

$$\theta_L(Sz) = \theta_L(-1/z) = (\sqrt{z/i})^n \theta_L(z) = (\sqrt{-i} \cdot \sqrt{z})^n \theta_L(z), \tag{3.4}$$

where $\sqrt{}$ denotes the principal branch of the square root.

(What "principal branch" refers to, is best understood from the perspective of polar coordinates: taking the square root of a complex number corresponds to taking the (real)

square root of its modulus and halving its argument. This is a continuous operation, except at a half-line starting at the origin, the so-called *branch cut*. Which half-line is the branch cut, depends on how we choose to normalise the argument. If we say that the argument is in the range $[0, 2\pi)$, then there is a discontinuity at the positive real axis. If we choose the range $(-\pi, \pi]$, then the discontinuity is at the negative real axis. Every choice results in a *branch* of the square root. The last-mentioned choice is called the *principal branch* of the square root.)

By combining the results (3.3) and (3.4), we find the following for general $g \in G_+$:

Proposition 3.3.6. *For all $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_+$, there exists an eighth root of unity $\epsilon(g)$, not dependent on the lattice L, such that*

$$\theta_L(gz) = \left(\epsilon(g) \cdot \sqrt{cz+d}\right)^n \theta_L(z)$$

holds for all $z \in H$, where, again, $\sqrt{}$ denotes the principal branch of the square root.

Proof. Since G_+ is generated by S and T^2, each element g of G_+ can be written as a product of copies of S and T^2 and their inverses. We will use induction on the "length" of this product.

For the base case $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we have

$$\theta_L(Iz) = \theta_L(z) = \left(\epsilon(I) \cdot \sqrt{0z+1}\right)^n \theta_L(z),$$

where we choose $\epsilon(I)$ to be 1.

For the inductive step, assume that the statement holds for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$; we will show that it also holds for T^2g, $T^{-2}g$, and $Sg = S^{-1}g$:

- For $T^2g = \begin{pmatrix} a+2c & b+2d \\ c & d \end{pmatrix}$, result (3.3) combined with the induction hypothesis gives
$$\theta_L(T^2gz) = \theta_L(gz) = \left(\epsilon(g) \cdot \sqrt{cz+d}\right)^n \theta_L(z),$$
so the statement holds for T^2g too, with $\epsilon(T^2g)$ chosen to be $\epsilon(g)$.
- For $T^{-2}g$, the situation is analogous to that for T^2g.
- For $Sg = S^{-1}g = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$, result (3.4) combined with the induction hypothesis gives
$$\begin{aligned} \theta_L(Sgz) &= (\sqrt{-i} \cdot \sqrt{gz})^n \theta_L(gz) \\ &= \left(\sqrt{-i} \cdot \sqrt{\frac{az+b}{cz+d}}\right)^n \left(\epsilon(g) \cdot \sqrt{cz+d}\right)^n \theta_L(z) \\ &= \left(\epsilon(Sg) \cdot \sqrt{az+b}\right)^n \theta_L(z), \end{aligned}$$
where we choose $\epsilon(Sg)$ to be $\sqrt{-i} \cdot \epsilon(g)$, which is indeed an eighth root of unity.

By induction, the statement holds for all $g \in G_+$. □

It can be shown that $\epsilon(g)$ is *uniquely* determined by g, or even by only the lower two

coefficients of g, but we will not need that fact here.

Remark 3.3.7. In connection to remark 3.3.4, note that for even lattices, the proposition would hold for all $g \in G$ rather than just G_+. ◊

We continue our investigation by looking at the behaviour of θ_L in relation other elements of G. It turns out that G/G_+ consists of three cosets: G_+ itself, TG_+, and TSG_+. So, for the latter two, we only need to consider one representative of each, for instance $g = T$ and $g = TS$.

For $g = T$, the situation is relatively simple:

$$\theta_L(Tz) = \theta_L(z+1) = \sum_{v \in L} e^{\pi i |v|^2 (z+1)} = \sum_{v \in L} (-1)^{|v|^2} e^{\pi i |v|^2 z},$$

as $e^{\pi i} = -1$.

Or, if we choose any characteristic vector w of L, we can write this as

$$\theta_L(Tz) = \sum_{v \in L} e^{\pi i (|v|^2 z + (v,w))},$$

because of (3.1).

For $g = TS$, we will build on this last result: by performing a calculation similar to how we found (3.4), we find

$$(\sqrt{z/i})^n \theta_L(z+1) = \sum_{v \in L} e^{\pi i |v + \frac{w}{2}|^2 (\frac{-1}{z})} = \theta'_L(Sz) \tag{3.5}$$

where

$$\theta'_L(z) := \sum_{v \in L + \frac{w}{2}} e^{\pi i |v|^2 z}.$$

By replacing z by $Sz = -\frac{1}{z}$ in (3.5), we find

$$\begin{aligned} \left(\sqrt{-\frac{1}{zi}}\right)^n \theta_L\left(\frac{-1}{z} + 1\right) &= \theta'_L(S^2 z); \\ (\sqrt{i/z})^n \theta_L(TSz) &= \theta'_L(z); \\ \theta_L(TSz) &= (\sqrt{z/i})^n \theta'_L(z). \end{aligned} \tag{3.6}$$

We could use that to express $\theta_L(z)$ in terms of $\theta'_L(z)$:

$$\theta_L(z) = (\sqrt{ST^{-1}z/i})^n \theta'_L(ST^{-1}z). \tag{3.7}$$

This might be a good moment to make a slight digression, and prove the following proposition; we will need it in the next chapter.

Proposition 3.3.8. *For characteristic vectors w of an unimodular integral lattice L in $\mathbb{R}^n$, we have*

$$|w|^2 \equiv n \pmod 8.$$

Proof. By replacing z with $z+1$ in (3.6), we find:

$$\begin{aligned}\left(\sqrt{\frac{z+1}{i}}\right)^n \theta'_L(z+1) &= \theta_L(TSTz) \\ &= \theta_L(ST^{-1}Sz) && \text{(since } S^2=(ST)^3=1\text{)} \\ &= (\sqrt{T^{-1}Sz/i})^n \theta_L(T^{-1}Sz) && \text{(by (3.4))} \\ &= \left(\sqrt{\frac{i(z+1)}{z}}\right)^n \theta_L(TSz) && \text{(by (3.3))} \end{aligned} \tag{3.8}$$

Combining (3.6) and (3.8) gives

$$\left(\sqrt{\frac{z+1}{i}}\right)^n \theta'_L(z+1) = \left(\sqrt{\frac{i(z+1)}{z}}\right)^n (\sqrt{z/i})^n \theta'_L(z)$$

which can be simplified to

$$(\sqrt{1/i})^n \theta'_L(z+1) = \theta'_L(z).$$

Since $(\sqrt{i})^n = e^{\pi i n/4}$, we have

$$\theta'_L(z+1) = e^{\pi i n/4} \theta'_L(z). \tag{3.9}$$

Furthermore, we have

$$\begin{aligned}\theta'_L(z+1) &= \sum_{v\in L} e^{\pi i|v+\frac{w}{2}|^2(z+1)} \\ &= \sum_{v\in L} e^{\pi i|v+\frac{w}{2}|^2 z} e^{\pi i|v+\frac{w}{2}|^2} \\ &= \sum_{v\in L} e^{\pi i|v+\frac{w}{2}|^2 z} e^{\pi i(|v|^2+(v,w))} e^{\pi i|w|^2/4} && \text{(since } |v+\frac{w}{2}|^2 = |v|^2+(v,w)+\frac{1}{4}|w|^2 \\ &&& \text{for all } v\in L\text{)} \\ &= \sum_{v\in L} e^{\pi i|v+\frac{w}{2}|^2 z} e^{\pi i|w|^2/4} && \text{(since } |v|^2 \equiv (v,w) \pmod 2 \\ &&& \text{for all } v\in L\text{)} \\ &= e^{\pi i|w|^2/4}\theta'_L(z). \end{aligned} \tag{3.10}$$

From the combination of (3.9) and (3.10), we find

$$e^{\pi i n/4} = e^{\pi i|w|^2/4},$$

which implies that $n = |w|^2 + 8k$ for some integer k. Because n and $|w|^2$ are integers, the desired result $n \equiv |w|^2 \pmod 8$ follows. □

This concludes our investigation of the theta series in relation to the action of the modular group. We will now consider $\theta_{\mathbb{Z}}$. It is easy to check, for example as in Example 3.2.3, that

the characteristic vectors of $\mathbb{Z}$ are the odd integers. Thus, choosing $w = 1$ gives:

$$\begin{aligned}\theta'_{\mathbb{Z}}(z) &= \sum_{m\in\mathbb{Z}+\frac{1}{2}} e^{\pi i m^2 z} = \sum_{m\in\mathbb{Z}} e^{\pi i (m+\frac{1}{2})^2 z} = \sum_{m\in\mathbb{Z}} e^{\pi i (m^2+m+\frac{1}{4})z} \\ &= \sum_{m=0}^{\infty} e^{\pi i (m^2+m+\frac{1}{4})z} + \sum_{m=1}^{\infty} e^{\pi i (m^2-m+\frac{1}{4})z} \\ &= \sum_{m=0}^{\infty} e^{\pi i (m^2+m+\frac{1}{4})z} + \sum_{m=0}^{\infty} e^{\pi i (m^2+m+\frac{1}{4})z} \quad (\text{since } (m+1)^2-(m+1) = m^2+m) \\ &= 2e^{\pi i z/4} \sum_{m=0}^{\infty} e^{\pi i (m^2+m)z} = 2e^{\pi i z/4}(1 + e^{2\pi i z} + e^{6\pi i z} + e^{12\pi i z} + \dots). \end{aligned} \tag{3.11}$$

When z approaches $i\infty$, all terms $e^{2\pi i z}, e^{6\pi i z}$, etc. go to 0, so $\theta'_{\mathbb{Z}} \sim 2e^{\pi i z/4} \cdot 1$ as $z \to i\infty$; the right-hand side goes to zero as $z \to i\infty$, thus so does $\theta'_{\mathbb{Z}}$.

Furthermore, when z approaches 1 from D_+, then ST^{-1} approaches $i\infty$; thus, by (3.7), $\theta_{\mathbb{Z}}(z) \to 0$ as $z \to 1$. Because of invariance of $\theta_{\mathbb{Z}}$ under T^{-2}, the same goes for $z \to -1$.

The last thing we will check in this section is that $\theta_{\mathbb{Z}}$ is never zero on H. Elkies mentions the following product formula for $\theta'_{\mathbb{Z}}$:

$$\sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2} = q^{1/4} \prod_{j=1}^{\infty} (1+q^{2j})(1-q^{4j}).$$

That this expression holds, can be made plausible by writing out the first few partial sums and products; both sides become equal to $q^{1/4} + q^{9/4} + q^{25/4} + q^{49/4} + \dots$. Elkies remarks that this is a special case of the Jacobi triple product identity.

From this expression, combined with (3.7), it follows that the only zeros of $\theta'_{\mathbb{Z}}$ are at $e^{2\pi i (ST^{-1}z)} = -1$ and $e^{4\pi i (ST^{-1}z)} = 1$; in D_+, that is only the case when $z = \pm 1$.

Furthermore, as can be seen from example 3.3.2, $\theta_{\mathbb{Z}}(z)$ approaches 1 as $z \to i\infty$, so in particular it is bounded away from 0 as $z \to i\infty$.

3.4 The shortest characteristic vector

The results from the previous sections enable us to prove the main theorem from [4]:

Theorem 3.4.1. *Let L be a unimodular integral lattice in $\mathbb{R}^n$, with no characteristic vector w such that $|w|^2 < n$. Then L is isomorphic to $\mathbb{Z}^n$.*

Proof. We will show that L and $\mathbb{Z}^n$ have the same theta series, by showing that their quotient is constantly 1 on H: consider the function

$$R(z) := \theta_L(z)/\theta_{\mathbb{Z}^n}(z) = \theta_L(z)/\theta_{\mathbb{Z}}(z)^n.$$

Proposition 3.3.6 gives the following: for $g \in G_+$ there exists an eighth root of unity $\epsilon(g)$ such that

$$R(gz) = \frac{\theta_L(gz)}{\theta_{\mathbb{Z}^n}(gz)} = \frac{\left(\epsilon(g)\cdot\sqrt{cz+d}\right)^n \theta_L(z)}{\left(\epsilon(g)\cdot\sqrt{cz+d}\right)^n \theta_{\mathbb{Z}^n}(z)} = R(z),$$

so R is invariant under G_+.

By the hypothesis on L, all characteristic vectors w have $|w|^2 \geq n$. For all $v \in L$ the element $2v + w$ is in the same coset of $2L$ in L as w and thus is also a characteristic vector of L, so $|2v + w|^2 \geq n$ and $|v + \frac{w}{2}|^2 \geq \frac{1}{4}n$. In other words, $|v + \frac{w}{2}|^2 = \frac{1}{4}n + r$ for some real number $r_v \geq 0$. That allows us to rewrite θ'_L as

$$\theta'_L(z) = \sum_{v \in L} e^{\pi i |v + \frac{w}{2}|^2 z} = e^{\pi i n z/4} \sum_{v \in L} e^{\pi i r_v z}.$$

As z approaches $i\infty$, the sum $\sum_{v \in L} e^{\pi i r_v z}$ decreases towards 0, so $\sum_{v \in L} e^{\pi i r_v z} \ll 1$ and thus $\theta'_L(z) \ll e^{\pi i n z/4}$ as $z \to i\infty$.

The combination of (3.6) with Proposition 3.3.3 gives $\theta'_{\mathbb{Z}^n} = {\theta'_{\mathbb{Z}}}^n$; based on our conclusions about $\theta'_{\mathbb{Z}}$ in (3.11), we find that $\theta'_{\mathbb{Z}^n} \sim 2^n e^{\pi i n z/4}$ we find that $\theta'_L(z)/\theta'_{\mathbb{Z}^n}(z)$ is bounded as $z \to i\infty$. By (3.7), it follows that $R(z)$ is bounded as $z \in D_+$ approaches ± 1.

Finally, we show that both $\theta_L(z)$ and $\theta_{\mathbb{Z}^n}(z)$ approach 1 as $z \to i\infty$. Since L and $\mathbb{Z}^n$ are positive-definite, there is exactly one vector with norm 0, namely the zero vector. Viewing θ_L as a power series like in (3.2), we see that it can be written as

$$\theta_L(z) = 1 + \sum_{m=1}^{\infty} N_{L,m} e^{\pi i m z},$$

where all terms of the sum go to zero when $z \to i\infty$. The same applies to $\theta_{\mathbb{Z}^n}$. So, both approach 1 as $z \to i\infty$, and thus R does too.

As R is thus bounded towards all cusps of D_+, we conclude that R is bounded on D_+.

The *maximum modulus principle* is a result from complex analysis, that states that if f is a holomorphic function on a connected open subset U of $\mathbb{C}$, then $|f|$ cannot have a strict maximum on U; i.e. f is either constant on U, or for every $z \in U$, there is a z' arbitrarily close to z such that $|f(z')| > |f(z)|$. Thus, if f is bounded on U, then f must be constant on U.

Applying this principle to R, we find that R is constant on D_+, and thus, because of its invariance under G_+, on H. It follows that $\theta_L = \theta_{\mathbb{Z}^n}$.

For power series, we know that their coefficients are uniquely determined by the function they define; it follows thus that for all $m \in \mathbb{Z}$, the lattices L and $\mathbb{Z}^n$ have the same number of vectors of norm m.

If we take $m = 1$ in particular, we see that L has n pairs of unit vectors (two opposite ones for each direction), just like $\mathbb{Z}^n$. We choose one per pair, so that we have n unit vectors left, say $u_1, \ldots, u_n$. That these are orthogonal to each other, i.e. for $i \neq j$, $(u_i, u_j) = 0$, can be seen using a geometrical argument. Geometrically, the inner product of two unit vectors is the cosine of the angle between them; this has a maximum of 1, and only reaches that maximum for two unit vectors with an angle of 0 between them. So, for non-identical u_i and u_j, the inner product must be less than 1. Because L is integral, this means that (u_i, u_j) must be 0, so they are orthogonal.

So, these unit vectors generate a copy of $\mathbb{Z}^n$ inside L. It turns out that this copy is all of L: since L is integral, all elements of L will be seen when looking at the set of elements with norm m for every $m \in \mathbb{Z}$; and, as we have seen, for every $m \in \mathbb{Z}$, L has the same number of vectors of norm m as $\mathbb{Z}^n$, and in particular not *more* than $\mathbb{Z}^n$. We conclude that L is isomorphic to $\mathbb{Z}^n$. □

4.

Uniqueness of the E_8 lattice

In this final section, we will show that the E_8 lattice is, up to isomorphism, the unique even unimodular positive-definite lattice of rank 8. This was first shown by L.J. Mordell in 1938; we will follow the proof given by Elkies in [5].

Theorem 4.0.1. *Let L be an even unimodular positive-definite lattice of rank 8. Then $L \cong E_8$.*

Proof. First, we will construct an odd so-called 2-*neighbour* L' of L; this is a unimodular lattice $L' \subset L \otimes \mathbb{Q}$ such that $L_0 := L \cap L'$ is a sublattice of index 2 in both L and L'. In a way, this construction will look as if we are reverse-engineering the construction of the E_8 lattice from Chapter 2. We will then identify this L' with $\mathbb{Z}^8$.

(The notation $L \otimes \mathbb{Q}$ denotes the *tensor product* of L with $\mathbb{Q}$; in this case, this is a $\mathbb{Q}$-module created from the $\mathbb{Z}$-module L, by "extending the scalars" to $\mathbb{Q}$. If L is a lattice in $\mathbb{R}^8$, this has a very natural meaning, but otherwise, it consists of formal elements $v \otimes q$ for $v \in L$ and $q \in \mathbb{Q}$, which are equivalence classes under a certain equivalence relation of ordered pairs (v, q). More about this can be read in [3, Sec. 10.4].)

To start, we fix a vector $v_0 \notin 2L$ such that $(v_0, v_0) \equiv 0 \pmod 4$; for example, choosing a basis for L, the sum of three distinct basis vectors e_1, e_2, e_3 would work:

$$\begin{aligned}(e_1 + e_2 + e_3, e_1 + e_2 + e_3)& \\ &= (e_1, e_1) + 2(e_1, e_2) + (e_2, e_2) + 2(e_2, e_3) + (e_3, e_3) + 2(e_1, e_3).\end{aligned}$$

Since L is an even lattice, all six terms on the right-hand side are even, so the sum is divisible by 4.

We can assume that $(v_0, v_0) \equiv 4 \pmod 8$; if not, i.e. if $(v_0, v_0) \equiv 0 \pmod 8$, we can replace v_0 by $v_0 + 2w$ for some vector $w \in L$ such that (v_0, w) is odd (such a vector w exists because of Lemma 1.2.6). Then $(v_0 + 2w, v_0 + 2w) = (v_0, v_0) + 4(v_0, w) + 4(w, w) \equiv 0 + 4 + 0 \pmod 8$.

We now define L_0 and L' as follows:

$$L_0 := \{v \in L : (v, v_0) \equiv 0 \pmod 2\}, \qquad L' := L_0 \cup (L_0 + \frac{v_0}{2}).$$

The element $\frac{v_0}{2} \in L \otimes \mathbb{Q}$ plays a similar role to the element $e = (\frac{1}{2}, \ldots, \frac{1}{2})$ in Chapter 2. We note that it is not an element of L, and thus not in L_0: even if L was in $\mathbb{R}^8$, so

that multiplying by $\frac{1}{2}$ would have a natural meaning, the element $\frac{v_0}{2}$ would not be in L, because of the assumption that $v_0 \notin 2L$.

On the other hand, $2 \cdot \frac{v_0}{2} = v_0$ *is* in L_0. This makes L' closed under addition, and thus a lattice $\subset L \otimes \mathbb{Q}$.

We will show that the lattice L' is unimodular and odd. We observe that $[L' : L_0] = [L : L_0] = 2$; by Lemma 1.2.10, it follows that $\det(L') = \det(L) = 1$, so L' is unimodular. To show that L' is odd, we observe that the element $\frac{v_0}{2} \in L'$ has odd norm: from the assumption that $(v_0, v_0) \equiv 4 \pmod 8$, or in other words, $(v_0, v_0) = 8k+4$ for some integer k, it follows that $(\frac{v_0}{2}, \frac{v_0}{2}) = (v_0, v_0)/4 = 2k + 1$.

In chapter 3, we saw that every unimodular lattice M has characteristic vectors: vectors $w \in M$ such that $(v, w) \equiv (v, v) \pmod 2$ for all $v \in M$. In Proposition 3.3.8, we saw that if M is positive-definite and of rank n, then all these characteristic vectors have norm $(w, w) \equiv n \pmod 8$.

For L', that means that all characteristic vectors w of L' have norm $(w, w) \equiv 0 \pmod 8$. We observe that the element $0 \in L'$ is *not* a characteristic vector: since L' is odd, there is some vector $v \in L'$ which has odd norm, but $(v, 0) = 0$, which is even. Because L' is positive-definite, it follows that all characteristic vectors w have norm $(w, w) > 0$; combined with $(w, w) \equiv 0 \pmod 8$, that means $(w, w) \geq 8$. By Theorem 3.4.1, we conclude that $L' \cong \mathbb{Z}^8$.

We take another look at the lattice L_0. Being a sublattice of L, it is even; and being an even lattice with index 2 in $\mathbb{Z}^8$, we claim that it is exactly the lattice $D_8 := \{(x_1, \ldots, x_8) \in \mathbb{Z}^8 : \sum_{i=1}^8 x_i \text{ even}\}$. We note that D_8 also has index 2 in $\mathbb{Z}^8$, and that $L_8 \subseteq D_8$, since the sum of the coordinates of a vector in $\mathbb{Z}_8$ is even if and only if the norm, i.e. the sum of the squares of the coordinates, is even. The combination of these facts gives that $L_0 = D_8$.

Let $D_8^* := \{y \in \mathbb{R}^8 : (x, y) \in \mathbb{Z} \text{ for all } x \in D_8\}$ denote the dual lattice of D_8. It is clear that $D_8 \subseteq \mathbb{Z}^8 \subseteq D_8^*$. Furthermore, from this definition, it follows that any lattice Λ is (equivalent to) a lattice between D_8 and D_8^* if and only if Λ contains D_8 and all elements of Λ have integer-valued inner products with all elements of D_8. The lattice L that we started with, satisfies these criteria, and is thus one of the lattices between D_8 and D_8^*. On the way to the desired conclusion about L, we will study the lattices between D_8 and D_8^*.

If we let $y = (y_1, \ldots, y_8)$ be an element of D_8^*, and apply the definition of D_8^* specifically with $x = (1, 1, 0, \ldots, 0)$ and with $x = (2, 0, \ldots, 0)$ and permutations of those (i.e. with all vectors consisting of either two ones or one two and for the rest zeros), we find that either all y_i must be integers, or all y_i must be half-integers. It follows that $D_8^* = \mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8$, and thus that $[D_8^* : \mathbb{Z}^8] = 2$ and $[D_8^* : D_8] = 4$.

So there must be three lattices between D_8 and D_8^*, of the form $L_0 \cup S$ where S denotes a nontrivial coset in D_8^*/D_8. One such lattice $L' = \mathbb{Z}^8$. Thus, for the other two, the cosets S must together form $(\mathbb{Z} + \frac{1}{2})^8$. The set $(\mathbb{Z} + \frac{1}{2})^8$ can be split into

$$S_+ := \{(y_1, \ldots, y_8) \in (\mathbb{Z} + \frac{1}{2})^8 : \sum_{i=1}^8 y_i \text{ even}\},$$

$$S_- := \{(y_1, \ldots, y_8) \in (\mathbb{Z} + \frac{1}{2})^8 : \sum_{i=1}^8 y_i \text{ odd}\}.$$

$L_0 \cup S_+$ is an even unimodular integral lattice: it corresponds exactly to the construction we followed in Chapter 2, and thus is isomorphic to E_8.

We claim that $L_0 \cup S_-$ is also an even unimodular integral lattice. That it is an integral unimodular lattice follows in the same way as for $L_0 \cup S_+$. To see that it is even, we check that elements of S_- have even norm: for $y = (y_1, \ldots, y_8) \in S_-$, write y as $y_1' + \frac{1}{2}, \ldots, y_8' + \frac{1}{2}$; then $\sum_{i=1}^8 y_i' = \sum_{i=1}^8 y_i - 4$ is even, so

$$(y, y) = \sum_{i=1}^{8} (y_i' + \frac{1}{2})^2 = \underbrace{\sum_{i=1}^{8} y_i'^2}_{\text{odd}} + \underbrace{\sum_{i=1}^{8} y_i'}_{\text{odd}} + 2 \equiv 0 \pmod 2.$$

Furthermore, $L_0 \cup S_-$ is isomorphic to E_8: consider the linear map that flips the sign of the first coordinate of each vector in $L_0 \cup S_-$; it sends vectors from L_0 to L_0 and vectors from S_- to S_+, and respects the inner product, so it is an isomorphism between $L_0 \cup S_-$ and $L_0 \cup S_+$ and thus to E_8.

To summarise, we have found that there are three lattices between D_8 and D_8^*, of which one is $\mathbb{Z}^8$ and the other two are isomorphic to E_8. We found L is one of these three lattices, and obviously not isomorphic to $\mathbb{Z}^8$. Thus, $L \cong E_8$. $\square$

Acknowledgements

I would like to express my gratefulness to my supervisor Johan Commelin, for his valuable advice and support during the process of writing this thesis.

Bibliography

[1] Jyrki Lahtonen (https://math.stackexchange.com/users/11619/jyrki-lahtonen). *Explain why the determinant of A is the index of the subring?* Mathematics Stack Exchange. URL: https://math.stackexchange.com/q/925015.

[2] John Conway and N. Sloane. *Sphere Packings, Lattices and Groups*. Vol. 290. Jan. 1988. ISBN: 978-1-4757-2018-1. DOI: 10.1007/978-1-4757-2016-7.

[3] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003. ISBN: 9780471433347.

[4] Noam D. Elkies. *A characterization of the $\mathbb{Z}^n$ lattice*. 1999. arXiv: math/9906019 [math.NT]. URL: https://arxiv.org/abs/math/9906019.

[5] Noam D. Elkies. *Yet another proof of the uniqueness of the E_8 lattice*. 2004. URL: https://people.math.harvard.edu/~elkies/Misc/E8.pdf.

[6] Jean-Pierre Serre. *Cours d'arithmétique*. Paris: Presses Universitaires de France, 1970.