7.4 Lattices: Basic Definitions and Properties

After seeing the examples in Sects. 7.1 and 7.2 and being reminded of the fundamental properties of vector spaces in Sect. 7.3, the reader will not be surprised by the formal definitions of a lattice and its properties.

Definition. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The *lattice L generated by* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is the set of linear combinations of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ with coefficients in $\mathbb{Z}$,

$$L = \{a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n : a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

A *basis* for L is any set of independent vectors that generates L. Any two such sets have the same number of elements. The *dimension of L* is the number of vectors in a basis for L.

Suppose that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is a basis for a lattice L and that $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in L$ is another collection of vectors in L. Just as we did for vector spaces, we can write each $\boldsymbol{w}_j$ as a linear combination of the basis vectors,

$$\begin{aligned}
\boldsymbol{w}_1 &= a_{11}\boldsymbol{v}_1 + a_{12}\boldsymbol{v}_2 + \cdots + a_{1n}\boldsymbol{v}_n,\\
\boldsymbol{w}_2 &= a_{21}\boldsymbol{v}_1 + a_{22}\boldsymbol{v}_2 + \cdots + a_{2n}\boldsymbol{v}_n,\\
&\vdots \qquad\qquad\qquad \vdots\\
\boldsymbol{w}_n &= a_{n1}\boldsymbol{v}_1 + a_{n2}\boldsymbol{v}_2 + \cdots + a_{nn}\boldsymbol{v}_n,
\end{aligned}$$

but since now we are dealing with lattices, we know that all of the a_{ij} coefficients are integers.

Suppose that we try to express the $\boldsymbol{v}_i$ in terms of the $\boldsymbol{w}_j$. This involves inverting the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Note that we need the $\boldsymbol{v}_i$ to be linear combinations of the $\boldsymbol{w}_j$ using *integer* coefficients, so we need the entries of A^{-1} to have integer entries. Hence

$$1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

where $\det(A)$ and $\det(A^{-1})$ are integers, so we must have $\det(A) = \pm 1$. Conversely, if $\det(A) = \pm 1$, then the theory of the adjoint matrix tells us that A^{-1} does indeed have integer entries. (See Exercise 7.10.) This proves the following useful result.

Proposition 7.14. *Any two bases for a lattice L are related by a matrix having integer coefficients and determinant equal to ± 1.*

For computational purposes, it is often convenient to work with lattices whose vectors have integer coordinates. For example,

$$\mathbb{Z}^n = \big\{(x_1, x_2, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{Z}\big\}$$

is the lattice consisting of all vectors with integer coordinates.

Definition. An *integral* (or *integer*) *lattice* is a lattice all of whose vectors have integer coordinates. Equivalently, an integral lattice is an additive subgroup of $\mathbb{Z}^m$ for some $m \geq 1$.

Example 7.15. Consider the three-dimensional lattice $L \subset \mathbb{R}^3$ generated by the three vectors

$$\boldsymbol{v}_1 = (2, 1, 3), \quad \boldsymbol{v}_2 = (1, 2, 0), \quad \boldsymbol{v}_3 = (2, -3, -5).$$

It is convenient to form a matrix using $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ as the rows of the matrix,

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{pmatrix}.$$

We create three new vectors in L by the formulas

$$\boldsymbol{w}_1 = \boldsymbol{v}_1 + \boldsymbol{v}_3, \qquad \boldsymbol{w}_2 = \boldsymbol{v}_1 - \boldsymbol{v}_2 + 2\boldsymbol{v}_3, \qquad \boldsymbol{w}_3 = \boldsymbol{v}_1 + 2\boldsymbol{v}_2.$$

This is equivalent to multiplying the matrix A on the left by the matrix

$$U = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{pmatrix},$$

and we find that $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3$ are the rows of the matrix

$$B = UA = \begin{pmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{pmatrix}.$$

The matrix U has determinant -1, so the vectors $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3$ are also a basis for L. The inverse of U is

$$U^{-1} = \begin{pmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{pmatrix},$$

and the rows of U^{-1} tell us how to express the $\boldsymbol{v}_i$ as linear combinations of the $\boldsymbol{w}_j$,

$$\boldsymbol{v}_1 = 4\boldsymbol{w}_1 - 2\boldsymbol{w}_2 - \boldsymbol{w}_3, \quad \boldsymbol{v}_2 = -2\boldsymbol{w}_1 + \boldsymbol{w}_2 + \boldsymbol{w}_3, \quad \boldsymbol{v}_3 = -3\boldsymbol{w}_1 + 2\boldsymbol{w}_2 + \boldsymbol{w}_3.$$

Remark 7.16. If $L \subset \mathbb{R}^m$ is a lattice of dimension n, then a basis for L may be written as the rows of an n-by-m matrix A, that is, a matrix with n rows and m columns. A new basis for L may be obtained by multiplying the matrix A on the left by an n-by-n matrix U such that U has integer entries and determinant ± 1. The set of such matrices U is called the *general linear group* (over $\mathbb{Z}$) and is denoted by $\mathrm{GL}_n(\mathbb{Z})$; cf. Example 2.11(g). It is the group of matrices with integer entries whose inverses also have integer entries.

There is an alternative, more abstract, way to define lattices that intertwines geometry and algebra.

Definition. A subset L of $\mathbb{R}^m$ is an *additive subgroup* if it is closed under addition and subtraction. It is called a *discrete additive subgroup* if there is a positive constant $\epsilon > 0$ with the following property: for every $\boldsymbol{v} \in L$,

$$L \cap \bigl\{\boldsymbol{w} \in \mathbb{R}^m : \|\boldsymbol{v} - \boldsymbol{w}\| < \epsilon\bigr\} = \{\boldsymbol{v}\}. \tag{7.8}$$

In other words, if you take any vector $\boldsymbol{v}$ in L and draw a solid ball of radius ϵ around $\boldsymbol{v}$, then there are no other points of L inside the ball.

Theorem 7.17. *A subset of $\mathbb{R}^m$ is a lattice if and only if it is a discrete additive subgroup.*

Proof. We leave the proof for the reader; see Exercise 7.9. □

A lattice is similar to a vector space, except that it is generated by all linear combinations of its basis vectors using integer coefficients, rather than using arbitrary real coefficients. It is often useful to view a lattice as an orderly arrangement of points in $\mathbb{R}^m$, where we put a point at the tip of each vector. An example of a lattice in $\mathbb{R}^2$ is illustrated in Fig. 7.1.

Definition. Let L be a lattice of dimension n and let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ be a basis for L. The *fundamental domain* (or *fundamental parallelepiped*) for L corresponding to this basis is the set

$$\mathcal{F}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \{t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2 + \cdots + t_n\boldsymbol{v}_n \,:\, 0 \le t_i < 1\}. \tag{7.9}$$

The shaded area in Fig. 7.1 illustrates a fundamental domain in dimension 2. The next result indicates one reason why fundamental domains are important in studying lattices.

Proposition 7.18. *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n and let $\mathcal{F}$ be a fundamental domain for L. Then every vector $\boldsymbol{w} \in \mathbb{R}^n$ can be written in the form*

$$\boldsymbol{w} = \boldsymbol{t} + \boldsymbol{v} \quad \text{for a unique } \boldsymbol{t} \in \mathcal{F} \text{ and a unique } \boldsymbol{v} \in L.$$

Equivalently, the union of the translated fundamental domains

$$\mathcal{F} + \boldsymbol{v} = \bigl\{\boldsymbol{t} + \boldsymbol{v} : \boldsymbol{t} \in \mathcal{F}\bigr\}$$

as $\boldsymbol{v}$ ranges over the vectors in the lattice L exactly covers $\mathbb{R}^n$; see Fig. 7.2.

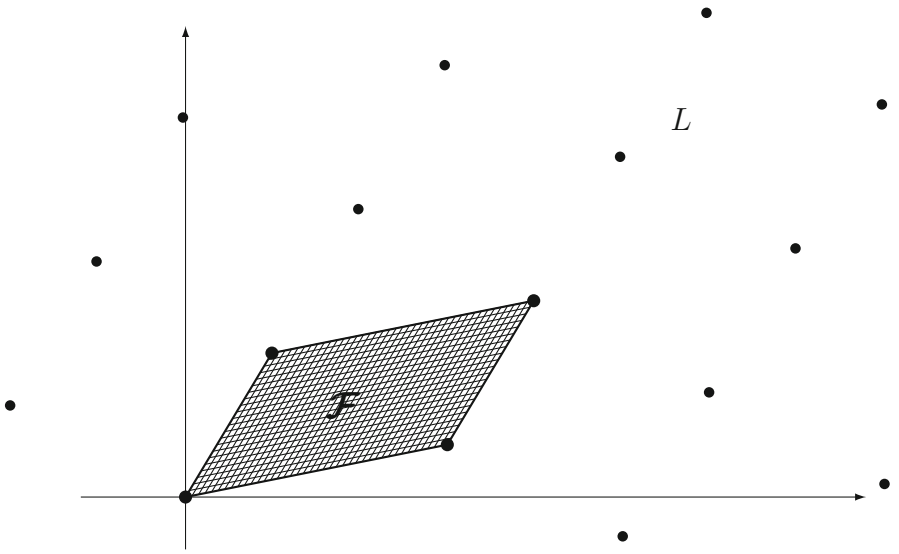

Figure 7.1: A lattice L and a fundamental domain $\mathcal{F}$

Proof. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be a basis of L that gives the fundamental domain $\mathcal{F}$. Then $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are linearly independent in $\mathbb{R}^n$, so they are a basis of $\mathbb{R}^n$. This means that any $\boldsymbol{w} \in \mathbb{R}^n$ can be written in the form

$$\boldsymbol{w} = \alpha_1 \boldsymbol{v}_1 + \alpha_2 \boldsymbol{v}_2 + \cdots + \alpha_n \boldsymbol{v}_n \qquad \text{for some } \alpha_1, \ldots, \alpha_n \in \mathbb{R}.$$

We now write each α_i as

$$\alpha_i = t_i + a_i \qquad \text{with } 0 \le t_i < 1 \text{ and } a_i \in \mathbb{Z}.$$

Then

$$\boldsymbol{w} = \overbrace{t_1 \boldsymbol{v}_1 + t_2 \boldsymbol{v}_2 + \cdots + t_n \boldsymbol{v}_n}^{\text{this is a vector } \boldsymbol{t} \in \mathcal{F}} + \overbrace{a_1 \boldsymbol{v}_1 + a_2 \boldsymbol{v}_2 + \cdots + a_n \boldsymbol{v}_n}^{\text{this is a vector } \boldsymbol{v} \in L}.$$

This shows that $\boldsymbol{w}$ can be written in the desired form.

Next suppose that $\boldsymbol{w} = \boldsymbol{t} + \boldsymbol{v} = \boldsymbol{t}' + \boldsymbol{v}'$ has two representations as a sum of a vector in $\mathcal{F}$ and a vector in L. Then

$$\begin{aligned}(t_1 + a_1)\boldsymbol{v}_1 + (t_2 + a_2)\boldsymbol{v}_2 + \cdots + (t_n + a_n)\boldsymbol{v}_n \\ = (t_1' + a_1')\boldsymbol{v}_1 + (t_2' + a_2')\boldsymbol{v}_2 + \cdots + (t_n' + a_n')\boldsymbol{v}_n.\end{aligned}$$

Since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are independent, it follows that

$$t_i + a_i = t_i' + a_i' \qquad \text{for all } i = 1, 2, \ldots, n.$$

Hence

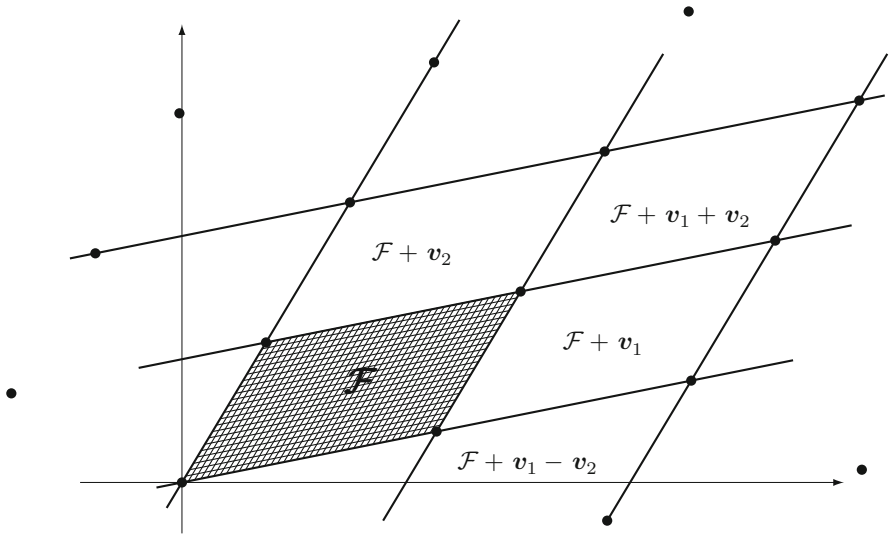

Figure 7.2: Translations of $\mathcal{F}$ by vectors in L exactly covers $\mathbb{R}^n$

$$t_i - t_i' = a_i' - a_i \in \mathbb{Z}$$

is an integer. But we also know that t_i and t_i' are greater than or equal to 0 and strictly smaller than 1, so the only way for $t_i - t_i'$ to be an integer is if $t_i = t_i'$. Therefore $\boldsymbol{t} = \boldsymbol{t}'$, and then also

$$\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{t} = \boldsymbol{w} - \boldsymbol{t}' = \boldsymbol{v}'.$$

This completes the proof that $\boldsymbol{t} \in \mathcal{F}$ and $\boldsymbol{v} \in L$ are uniquely determined by $\boldsymbol{w}$. □

It turns out that all fundamental domains of a lattice L have the same volume. We prove this later (Corollary 7.22) for lattices of dimension n in $\mathbb{R}^n$. The volume of a fundamental domain turns out to be an extremely important invariant of the lattice.

Definition. Let L be a lattice of dimension n and let $\mathcal{F}$ be a fundamental domain for L. Then the n-dimensional volume of $\mathcal{F}$ is called the *determinant of* L (or sometimes the *covolume*[4] of L). It is denoted by $\det(L)$.

If you think of the basis vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ as being vectors of a given length that describe the sides of the parallelepiped $\mathcal{F}$, then for basis vectors

[4]Note that the lattice L itself has no volume, since it is a countable collection of points. If $L \subset \mathbb{R}^n$ has dimension n, then the *covolume of* L is defined to be the volume of the quotient group $\mathbb{R}^n/L$.

of given lengths, the largest volume is obtained when the vectors are pairwise orthogonal to one another. This leads to the following important upper bound for the determinant of a lattice.

Proposition 7.19 (Hadamard's Inequality)**.** *Let L be a lattice, take any basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ for L, and let $\mathcal{F}$ be a fundamental domain for L. Then*

$$\det L = \mathrm{Vol}(\mathcal{F}) \le \|\boldsymbol{v}_1\| \, \|\boldsymbol{v}_2\| \cdots \|\boldsymbol{v}_n\|. \tag{7.10}$$

The closer that the basis is to being orthogonal, the closer that Hadamard's inequality (7.10) comes to being an equality.

It is fairly easy to compute the determinant of a lattice L if its dimension is the same as its ambient space, i.e., if L is contained in $\mathbb{R}^n$ and L has dimension n. This formula, which luckily is the case that is of most interest to us, is described in the next proposition. See Exercise 7.14 to learn how to compute the determinant of a lattice in the general case.

Proposition 7.20. *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n, let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ be a basis for L, and let $\mathcal{F} = \mathcal{F}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be the associated fundamental domain as defined by (7.9). Write the coordinates of the ith basis vector as*

$$\boldsymbol{v}_i = (r_{i1}, r_{i2}, \ldots, r_{in})$$

and use the coordinates of the $\boldsymbol{v}_i$ as the rows of a matrix,

$$F = F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix}. \tag{7.11}$$

Then the volume of $\mathcal{F}$ is given by the formula

$$\mathrm{Vol}\bigl(\mathcal{F}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)\bigr) = \bigl|\det\bigl(F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)\bigr)\bigr|.$$

Proof. The proof uses multivariable calculus. We can compute the volume of $\mathcal{F}$ as the integral of the constant function 1 over the region $\mathcal{F}$,

$$\mathrm{Vol}(\mathcal{F}) = \int_{\mathcal{F}} dx_1 \, dx_2 \cdots dx_n.$$

The fundamental domain $\mathcal{F}$ is the set described by (7.9), so we make a change of variables from $\boldsymbol{x} = (x_1, \ldots, x_n)$ to $\boldsymbol{t} = (t_1, \ldots, t_n)$ according to the formula

$$(x_1, x_2, \ldots, x_n) = t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2 + \cdots + t_n\boldsymbol{v}_n.$$

In terms of the matrix $F = F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ defined by (7.11), the change of variables is given by the matrix equation $\boldsymbol{x} = \boldsymbol{t}F$. The Jacobian matrix of this change of variables is F, and the fundamental domain $\mathcal{F}$ is the image under F of the unit cube $C_n = [0,1]^n$, so the change of variables formula for integrals yields

$$\begin{aligned}\int_{\mathcal{F}} dx_1\, dx_2 \cdots dx_n &= \int_{FC_n} dx_1\, dx_2 \cdots dx_n = \int_{C_n} |\det F|\, dt_1\, dt_2 \cdots dt_n \\ &= |\det F| \operatorname{Vol}(C_n) = |\det F|. \end{aligned}$$ □

Example 7.21. The lattice in Example 7.15 has determinant

$$\det L = |\det A| = \left| \det \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{pmatrix} \right| = |-36| = 36.$$

Corollary 7.22. *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n. Then every fundamental domain for L has the same volume. Hence $\det(L)$ is an invariant of the lattice L, independent of the particular fundamental domain used to compute it.*

Proof. Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ and $\boldsymbol{w}_1, \dots, \boldsymbol{w}_n$ be two fundamental domains for L, and let $F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ and $F(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)$ be the associated matrices (7.11) obtained by using the coordinates of the vectors as the rows of the matrices. Then Proposition 7.14 tells us that

$$F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = AF(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n) \tag{7.12}$$

for some n-by-n matrix with integer entries and $\det(A) = \pm 1$. Now applying Proposition 7.20 twice yields

$$\begin{aligned} &\operatorname{Vol}\bigl(\mathcal{F}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)\bigr) \\ &\quad = \bigl|\det\bigl(F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)\bigr)\bigr| && \text{from Proposition 7.20,} \\ &\quad = \bigl|\det\bigl(AF(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)\bigr)\bigr| && \text{from (7.12),} \\ &\quad = \bigl|\det(A)\bigr|\bigl|\det\bigl(F(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)\bigr)\bigr| && \text{since } \det(AB) = \det(A)\det(B), \\ &\quad = \bigl|\det\bigl(F(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)\bigr)\bigr| && \text{since } \det(A) = \pm 1, \\ &\quad = \operatorname{Vol}\bigl(\mathcal{F}(\boldsymbol{w}_1, \dots, \boldsymbol{w}_n)\bigr) && \text{from Proposition 7.20.} \end{aligned}$$ □