1

Introduction to Lattices

CONTENTS

In this chapter we begin with a review of elementary linear algebra, and in particular the geometry of Euclidean vector space $\mathbb{R}^n$. The main purpose of this first section is to fix our conventions on notation and terminology. We then introduce the concept of a lattice, the main object of study throughout this book, and prove some basic lemmas about these structures. The last section of the chapter recalls some essential facts from the geometry of numbers, by which is meant the interplay between Euclidean geometry and the theory of numbers. Throughout this book we will use the following standard notation:

$\mathbb{Z}$	the domain of integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$\mathbb{F}_p$	the field of congruence classes modulo the prime number p

1.1 Euclidean space $\mathbb{R}^n$

We regard n-tuples of elements from a field $\mathbb{F}$ as either column vectors or as row vectors, and denote them by boldface roman letters:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}^n, \qquad \mathbf{x} = \begin{bmatrix} x_1, x_2, \cdots, x_n \end{bmatrix} \in \mathbb{F}^n.$$

We use the column format when we consider an $n \times n$ matrix acting as a linear operator on $\mathbb{R}^n$ by left multiplication on column vectors. However, we will be primarily concerned with operations on a basis of $\mathbb{R}^n$, and for this reason it is convenient to represent the basis vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ as the rows of an $n \times n$ matrix X. We can then represent operations on the basis as elementary row operations on the matrix. More generally, we can represent a general change of basis as left multiplication of X by an invertible $n \times n$ matrix C.

Definition 1.1. For any field $\mathbb{F}$, and any positive integer n, the **vector space** $\mathbb{F}^n$ consists of all n-tuples of elements from $\mathbb{F}$, with the familiar operations of vector addition and scalar multiplication defined by

$$\mathbf{x} + \mathbf{y} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}, \quad a\mathbf{x} = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix},$$

for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ and any $a \in \mathbb{F}$.

Throughout this book, we will be primarily concerned with the vector space $\mathbb{R}^n$.

Definition 1.2. The **Euclidean space** $\mathbb{R}^n$ consists of all n-tuples of real numbers. We use dot notation for the **scalar product** of vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$:

$$\mathbf{x} \cdot \mathbf{y} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = \sum_{i=1}^{n} x_i y_i.$$

We use single vertical bars for the **length** (or **norm**) of a vector $\mathbf{x} \in \mathbb{R}^n$:

$$|\mathbf{x}| = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} = \left(\sum_{i=1}^{n} x_i^2 \right)^{1/2}.$$

We often use the **square-length** instead of the length of a vector $\mathbf{x} \in \mathbb{R}^n$:

$$|\mathbf{x}|^2 = x_1^2 + x_2^2 + \cdots + x_n^2 = \sum_{i=1}^{n} x_i^2.$$

We usually do computations for which the input consists of vectors in $\mathbb{Q}^n$ or $\mathbb{Z}^n$: the components are rational numbers or integers. We want to store the intermediate results as exact rational numbers, in order to avoid the issue of rounding error with floating-point arithmetic, and so we use the square-length (which is rational) instead of the length (which is usually irrational).

Definition 1.3. The **angle** θ between nonzero vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is given by

$$\mathbf{x} \cdot \mathbf{y} = |\mathbf{x}|\,|\mathbf{y}| \cos\theta, \qquad \cos\theta = \frac{\mathbf{x} \cdot \mathbf{y}}{|\mathbf{x}|\,|\mathbf{y}|}, \qquad \theta = \arccos\left(\frac{\mathbf{x} \cdot \mathbf{y}}{|\mathbf{x}|\,|\mathbf{y}|}\right).$$

Lemma 1.4. *Two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ are orthogonal if and only if $\mathbf{x} \cdot \mathbf{y} = 0$.*

Proof. The cosine is 0 if and only if the angle is an odd multiple of $\pi/2$. □

The angle formulas of Definition 1.3 are closely related to the following famous inequality.

Lemma 1.5. Cauchy-Schwarz inequality. *For any two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,*

$$|\mathbf{x} \cdot \mathbf{y}| \le |\mathbf{x}|\,|\mathbf{y}|.$$

(On the left side, the vertical bars denote the absolute value of the scalar product; on the right side, they denote the lengths of the vectors.)

Given a vector $\mathbf{x} \in \mathbb{R}^n$ and a nonzero vector $\mathbf{y} \in \mathbb{R}^n$, it is often convenient to express $\mathbf{x}$ as a sum of two vectors, $\mathbf{x} = \mathbf{u} + \mathbf{v}$, where $\mathbf{u}$ is parallel to $\mathbf{y}$ (we write $\mathbf{u} \parallel \mathbf{y}$) and $\mathbf{v}$ is orthogonal to $\mathbf{y}$ (we write $\mathbf{v} \perp \mathbf{y}$). If we write $\mathbf{u} = \lambda\mathbf{y}$ where $\lambda \in \mathbb{R}$, then $\mathbf{v} = \mathbf{x} - \mathbf{u} = \mathbf{x} - \lambda\mathbf{y}$ is orthogonal to $\mathbf{y}$, and hence

$$(\mathbf{x} - \lambda\mathbf{y}) \cdot \mathbf{y} = 0.$$

Using the bilinearity of the scalar product we can solve for the scalar λ:

$$\lambda = \frac{\mathbf{x} \cdot \mathbf{y}}{\mathbf{y} \cdot \mathbf{y}} = \frac{\mathbf{x} \cdot \mathbf{y}}{|\mathbf{y}|^2}.$$

It is important for computational reasons to note that if $\mathbf{x}, \mathbf{y} \in \mathbb{Q}^n$ then $\lambda \in \mathbb{Q}$.

Definition 1.6. Given vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ with $\mathbf{y} \neq \mathbf{0}$, we write $\mathbf{u}$ and $\mathbf{v}$ for the **components** (or **projections**) of $\mathbf{x}$ **parallel** and **orthogonal** to $\mathbf{y}$:

$$\mathbf{u} = \left(\frac{\mathbf{x} \cdot \mathbf{y}}{\mathbf{y} \cdot \mathbf{y}}\right)\mathbf{y}, \qquad \mathbf{v} = \mathbf{x} - \left(\frac{\mathbf{x} \cdot \mathbf{y}}{\mathbf{y} \cdot \mathbf{y}}\right)\mathbf{y}.$$

Example 1.7. Consider the triangle in $\mathbb{R}^3$ with these points as its vertices:

$$A = (6, 2, -4), \qquad B = (-8, -6, 6), \qquad C = (1, -3, 9).$$

The two sides of the triangle originating at vertex A are

$$\mathbf{x} = \overrightarrow{AB} = \begin{bmatrix} -14 \\ -8 \\ 10 \end{bmatrix}, \qquad \mathbf{y} = \overrightarrow{AC} = \begin{bmatrix} -5 \\ -5 \\ 13 \end{bmatrix}.$$

The scalar product of these vectors is

$$\mathbf{x} \cdot \mathbf{y} = 240.$$

The lengths of these vectors are

$$|\mathbf{x}| = \sqrt{360}, \qquad |\mathbf{y}| = \sqrt{219}.$$

The cosine of the angle θ at vertex A is

$$\cos\theta = \frac{240}{\sqrt{360}\sqrt{219}} \approx 0.8547476863.$$

Therefore

$$\theta \approx 0.5457317946 \text{ radians} \approx 31.26812857 \text{ degrees}.$$

The projection coefficient for $\mathbf{x}$ in the direction of $\mathbf{y}$ is

$$\lambda = \frac{\mathbf{x}\cdot\mathbf{y}}{\mathbf{y}\cdot\mathbf{y}} = \frac{80}{73}.$$

We obtain the decomposition $\mathbf{x} = \mathbf{u} + \mathbf{v}$ where

$$\mathbf{u} = \frac{80}{73}\begin{bmatrix} -5 \\ -5 \\ 13 \end{bmatrix}, \qquad \mathbf{v} = \frac{2}{73}\begin{bmatrix} -311 \\ -92 \\ -155 \end{bmatrix}.$$

We have $\mathbf{u} \parallel \mathbf{y}$ and $\mathbf{v} \perp \mathbf{y}$, and hence $\mathbf{u}\cdot\mathbf{v} = 0$.

Definition 1.8. The vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in \mathbb{R}^n$ are **linearly dependent** if one of the vectors is a linear combination of the other $k-1$ vectors; equivalently, if there is a non-trivial solution (not all the coefficients are zero) of the equation

$$a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_k\mathbf{x}_k = \mathbf{0} \qquad (a_1, a_2, \ldots, a_k \in \mathbb{R}).$$

The vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\ldots$, $\mathbf{x}_k$ are **linearly independent** if this equation has only the trivial solution $a_i = 0$ for $i = 1, 2, \ldots, k$. This implies that $k \le n$.

The vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in \mathbf{R}^n$ **span** $\mathbb{R}^n$ if every vector $\mathbf{y} \in \mathbb{R}^n$ is a linear combination of the vectors; equivalently, for every $\mathbf{y} \in \mathbb{R}^n$, the equation

$$a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_k\mathbf{x}_k = \mathbf{y},$$

has a solution $a_1, a_2, \ldots, a_k \in \mathbb{R}$. This implies that $k \ge n$.

The vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in \mathbf{R}^n$ form a **basis** of $\mathbb{R}^n$ if they are linearly independent and they span $\mathbb{R}^n$. This implies that $k = n$.

The **standard basis vectors** in $\mathbb{R}^n$ will be denoted $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$; by definition, $\mathbf{e}_i$ has 1 as its i-th component and 0 as its other components.

There are many excellent modern textbooks on elementary linear algebra; we mention in particular those by Anton [11] and Nicholson [112]. At a more advanced level, two standard classical references are Hoffman and Kunze [64] and Jacobson [68]. Computational methods are presented in Golub and van Loan [49] and Trefethen and Bau [137].

1.2 Lattices in $\mathbb{R}^n$

We now introduce the main objects of study in the remainder of this book.

Definition 1.9. Let $n \geq 1$ and let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ be a basis of $\mathbb{R}^n$. The **lattice** with **dimension** n and **basis** $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ is the set L of all linear combinations of the basis vectors with integral coefficients:

$$L = \mathbb{Z}\mathbf{x}_1 + \mathbb{Z}\mathbf{x}_2 + \cdots + \mathbb{Z}\mathbf{x}_n = \Big\{ \sum_{i=1}^{n} a_i \mathbf{x}_i \mid a_1, a_2, \ldots, a_n \in \mathbb{Z} \Big\}.$$

The basis vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ are said to **generate** or **span** the lattice. For $i = 1, 2, \ldots, n$ we write $\mathbf{x}_i = (x_{i1}, \ldots, x_{in})$ and form the $n \times n$ matrix $X = (x_{ij})$. The **determinant** of the lattice L with basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ is

$$\det(L) = |\det(X)|.$$

Note that in this definition we regard the basis vectors as row vectors. We do this so that operations on the basis vectors can be expressed in terms of elementary row operations on the matrix X; equivalently, left multiplication of the matrix X by an integer matrix C with determinant ± 1.

We will prove shortly (Corollary 1.11) that the determinant of the lattice L does not depend on which basis we use. In fact, $\det(L)$ has a natural geometric interpretation: it is the n-dimensional volume of the parallelipiped in $\mathbb{R}^n$ whose edges are the basis vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$.

In the trivial case $n = 1$, the lattice L generated by the nonzero real number $\mathbf{x}$ consists of all integral multiples of $\mathbf{x}$. The lattice $L = \mathbb{Z}\mathbf{x}$ has only two bases, namely $\mathbf{x}$ and $-\mathbf{x}$.

If $n \geq 2$, then every lattice has infinitely many different bases. Let $L \subset \mathbb{R}^n$ be the lattice with basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$. Let $C = (c_{ij})$ be any $n \times n$ matrix with entries in $\mathbb{Z}$ and $\det(C) = \pm 1$; then C^{-1} also has entries in $\mathbb{Z}$ (see Exercise 1.7). Define vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ by

$$\mathbf{y}_i = \sum_{j=1}^{n} c_{ij} \mathbf{x}_j \qquad (i = 1, 2, \ldots, n),$$

and let Y be the $n \times n$ matrix with $\mathbf{y}_i$ in row i. We have the matrix equations

$$Y = CX, \qquad X = C^{-1}Y.$$

It follows that any integral linear combination of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ is also an integral linear combination of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$, and conversely. Hence $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ is another basis for the same lattice L. In fact any two bases for the same lattice are related in this way, as the next lemma shows.

Lemma 1.10. *Let* $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ *and* $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$, *be two bases for the same lattice* $L \subset \mathbb{R}^n$. *Let* X *(respectively* Y*) be the* $n \times n$ *matrix with* $\mathbf{x}_i$ *(respectively* $\mathbf{y}_i$*) in row* i *for* $i = 1, 2, \ldots, n$. *Then* $Y = CX$ *for some* $n \times n$ *matrix* C *with integer entries and determinant* ± 1.

Proof. Every $\mathbf{y}_i$ belongs to the lattice with basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$, and every $\mathbf{x}_i$ belongs to the lattice with basis $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. It follows that

$$\mathbf{x}_i = \sum_{j=1}^{n} b_{ij}\mathbf{y}_j, \qquad \mathbf{y}_i = \sum_{j=1}^{n} c_{ij}\mathbf{x}_j \qquad (i = 1, 2, \ldots, n),$$

where $B = (b_{ij})$ and $C = (c_{ij})$ are $n \times n$ matrices with integer entries. Writing these two equations in matrix form gives $X = BY$ and $Y = CX$, and hence $X = BCX$ and $Y = CBY$. Since both $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ and $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ are bases of $\mathbb{R}^n$, the corresponding matrices X and Y are invertible, and can be canceled from the equations. Therefore $BC = I$ and $CB = I$, and so $\det(B)\det(C) = 1$. Since B and C have integer entries, it follows that either $\det(B) = \det(C) = 1$ or $\det(B) = \det(C) = -1$. □

Corollary 1.11. *The determinant of a lattice does not depend on the basis.*

Proof. Suppose the lattice $L \subset \mathbb{R}^n$ has two bases $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ and $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. Using the notation in the proof of Lemma 1.10, we have

$$|\det(Y)| = |\det(CX)| = |\det(C)\det(X)| = |\pm\det(X)| = |\det(X)|.$$

Since the two bases are arbitrary, this completes the proof. □

Definition 1.12. An $n \times n$ matrix with integer entries and determinant ± 1 will be called **unimodular**.

Definition 1.13. A **unimodular row operation** on a matrix is one of the following elementary row operations:

- multiply any row by -1;
- interchange any two rows;
- add an integral multiple of any row to any other row.

To generate examples of $n \times n$ unimodular matrices, we start with the identity matrix I_n, and then apply any finite sequence of unimodular row operations. The result will be an $n \times n$ unimodular matrix, and in fact any such matrix can be obtained in this way.

If we apply unimodular row operations to the matrix X whose rows contain a basis of the lattice L, then we obtain another basis of the same lattice.

Example 1.14. Start with the 2×2 identity matrix, and apply this sequence of unimodular row operations: add 4 times row 2 to row 1, add 9 times row 1 to row 2, change the sign of row 1, add -4 times row 2 to row 1, change the sign of row 1, change the sign of row 2. We obtain this 2×2 unimodular matrix:

$$C = \begin{bmatrix} 37 & 152 \\ -9 & -37 \end{bmatrix}, \qquad \det(C) = -1.$$

Let L be the lattice in $\mathbb{R}^2$ spanned by the rows of this matrix:

$$X = \begin{bmatrix} 7 & 9 \\ 6 & -5 \end{bmatrix}, \qquad \det(X) = -89.$$

Applying the same sequence of row operations to X gives this matrix Y:

$$Y = CX = \begin{bmatrix} 1171 & -427 \\ -285 & 104 \end{bmatrix}.$$

Writing the the basis vectors as column vectors gives

$$\mathbf{x}_1, \mathbf{x}_2 = \begin{bmatrix} 7 \\ 9 \end{bmatrix}, \begin{bmatrix} 6 \\ -5 \end{bmatrix} \qquad \text{and} \qquad \mathbf{y}_1, \mathbf{y}_2 = \begin{bmatrix} 1171 \\ -427 \end{bmatrix}, \begin{bmatrix} -285 \\ 104 \end{bmatrix}.$$

It is far from obvious that these two bases generate the same lattice in $\mathbb{R}^2$.

We can perform any number of further row operations; a pseudorandom sequence of 100 operations provides this third basis for the same lattice:

$$\mathbf{z}_1, \mathbf{z}_2 = \begin{bmatrix} 91202814184 \\ -26536463447 \end{bmatrix}, \begin{bmatrix} 10682859399 \\ -3108295621 \end{bmatrix}.$$

We can clearly continue this process as long as we want and find bases for the same lattice consisting of arbitrarily long vectors.

The last example shows how easy it is to start with a basis for a lattice consisting of short vectors, and then produce other bases for the same lattice consisting of much longer vectors. Of course, it is much more interesting and important to do exactly the opposite: *Given a basis for a lattice, which in general consists of long vectors, we want to find another "reduced" basis for the same lattice, that is, a basis consisting of short vectors.* This is the problem of lattice basis reduction, the fundamental problem that we will be studying throughout this book.

We now generalize the concept of lattice basis and lattice determinant to any set of m linearly independent vectors in $\mathbb{R}^n$ $(m \leq n)$.

Definition 1.15. Let $n \geq 1$ and let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ $(m \leq n)$ be a set of m linearly independent vectors in $\mathbb{R}^n$. The m-dimensional **lattice** spanned by these vectors in n-dimensional Euclidean space is defined to be

$$L = \mathbb{Z}\mathbf{x}_1 + \mathbb{Z}\mathbf{x}_2 + \cdots + \mathbb{Z}\mathbf{x}_m = \Big\{ \sum_{i=1}^{m} a_i \mathbf{x}_i \mid a_1, a_2, \ldots, a_m \in \mathbb{Z} \Big\}.$$

For $i = 1, \ldots, m$ we write $\mathbf{x}_i = (x_{i1}, \ldots, x_{in})$ and form the $m \times n$ matrix $X = (x_{ij})$. The **Gram matrix** $\Delta(L)$ of the lattice L is the $m \times m$ matrix in which the (i, j) entry is the scalar product of the i-th and j-th basis vectors:

$$\Delta(L) = \big(\mathbf{x}_i \cdot \mathbf{x}_j\big) = XX^t.$$

The determinant of the Gram matrix is always positive (see Exercise 1.11), and we define the **determinant** of the lattice L to be its square root:

$$\det(L) = \sqrt{\det(XX^t)}.$$

If $m = n$ then X is a square matrix, and so

$$\big(\det(L)\big)^2 = \det(XX^t) = \det(X)\det(X^t) = \big(\det(X)\big)^2,$$

which agrees with the previous definition of lattice determinant.

As before, it can easily be shown that the determinant of a lattice does not depend on the choice of basis (see Exercise 1.12). The geometric interpretation is also the same: the determinant is the m-dimensional volume of the parallelipiped in $\mathbb{R}^n$ whose edges are the lattice basis vectors.

Example 1.16. Consider the 3-dimensional lattice L in 5-dimensional Euclidean space spanned by the rows of this matrix:

$$X = \begin{bmatrix} -7 & -7 & 4 & -8 & -8 \\ 1 & 6 & -5 & 8 & -1 \\ -1 & 1 & 4 & -7 & 8 \end{bmatrix}$$

We compute the Gram matrix:

$$\Delta(L) = XX^t = \begin{bmatrix} -7 & -7 & 4 & -8 & -8 \\ 1 & 6 & -5 & 8 & -1 \\ -1 & 1 & 4 & -7 & 8 \end{bmatrix} \begin{bmatrix} -7 & 1 & -1 \\ -7 & 6 & 1 \\ 4 & -5 & 4 \\ -8 & 8 & -7 \\ -8 & -1 & 8 \end{bmatrix}$$

$$= \begin{bmatrix} 242 & -125 & 8 \\ -125 & 127 & -79 \\ 8 & -79 & 131 \end{bmatrix}.$$

The Gram matrix has determinant 618829, and so $\det(L) = \sqrt{618829}$.

In the rest of this section, we consider the problem of extending a linearly independent set of lattice vectors to a basis for the lattice. Our exposition follows Cassels [22], pages 11–14, but we express the results in matrix form as much as possible.

Definition 1.17. Let $L \subset \mathbb{R}^n$ be the lattice with basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$. Suppose that $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n \in L$ are linearly independent, and let $M \subset \mathbb{R}^n$ be the lattice generated by $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. We call M a **sublattice** of L and write $M \subseteq L$.

Each basis vector $\mathbf{y}_i$ for the sublattice M belongs to the lattice L, and so

$$\mathbf{y}_i = \sum_{j=1}^{n} c_{ij}\mathbf{x}_j \qquad (i = 1, 2, \ldots, n),$$

where $c_{ij} \in \mathbb{Z}$ for all i, j. As a matrix equation, this says that

$$Y = CX,$$

where $C = (c_{ij})$ is the non-singular $n \times n$ matrix of integer coefficients, and X (respectively Y) is the $n \times n$ matrix containing $\mathbf{x}_i$ (respectively $\mathbf{y}_i$) in row i. Taking the determinant on both sides of this equation gives

$$\det(Y) = \det(C)\,\det(X), \qquad \det(C) = \frac{\det(Y)}{\det(X)}.$$

Definition 1.18. The **index** ρ of a sublattice M in a lattice L is defined by

$$\rho = |\det(C)| = \frac{|\det(Y)|}{|\det(X)|} = \frac{\det(M)}{\det(L)}.$$

The index is an integer, since the determinant of the sublattice M is an integral multiple of the determinant of the lattice L. (The basis vectors for M span a larger parallelipiped than the basis vectors for L.) It is clear from the above equations that the index depends only on L and M, not on the choice of bases.

Definition 1.19. For any $n \times n$ matrix C, the (i, j) **minor** is the determinant $\det(C_{ij})$ of the $(n-1) \times (n-1)$ matrix C_{ij} obtained by deleting row i and column j, and the (i, j) **cofactor** is $(-1)^{i+j}\det(C_{ij})$. The **adjoint matrix** is the transpose of the matrix of cofactors:

$$\big(\mathrm{adj}(C)\big)_{ij} = (-1)^{i+j}\det(C_{ji}).$$

Lemma 1.20. *The inverse of any non-singular matrix C can be expressed in terms of its adjoint matrix and its determinant:*

$$C^{-1} = \frac{1}{\det(C)}\,\mathrm{adj}(C).$$

Proof. See any textbook on elementary linear algebra. □

Returning to the above discussion of the sublattice M (with matrix Y) of the lattice L (with matrix X), we see that the equation $Y = CX$ implies

$$X = C^{-1}Y = \frac{1}{\det(C)}\,\mathrm{adj}(C)\,Y,$$

and hence

$$\rho\,X = |\det(C)|\,X = \pm\,\mathrm{adj}(C)\,Y.$$

Since the entries of C are integers, so are the entries of $\mathrm{adj}(C)$, and hence every row of the matrix ρX is an integer linear combination of the rows of the matrix Y. We conclude that the lattice ρL, consisting of all multiples by the integer ρ of the vectors in L, is a sublattice of the lattice M.

Lemma 1.21. *If L is a lattice and M is a sublattice of index ρ then*

$$\rho L \subseteq M \subseteq L.$$

We now prove a theorem relating the bases of a lattice L and the bases of a sublattice M. As a corollary we will obtain a necessary and sufficient condition for extending a set of linearly independent lattice vectors to a basis for the lattice.

Theorem 1.22. (Cassels [22], Theorem I, page 11) *Let L be a lattice in $\mathbb{R}^n$ and let M be a sublattice of L. If $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ is a basis of L, then there exists a basis $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ of M such that $Y = CX$ where C is a lower-triangular $n \times n$ integer matrix with nonzero entries on the diagonal. That is, we have*

$$\left.\begin{aligned} \mathbf{y}_1 &= c_{11}\mathbf{x}_1 \\ \mathbf{y}_2 &= c_{21}\mathbf{x}_1 + c_{22}\mathbf{x}_2 \\ &\vdots \\ \mathbf{y}_n &= c_{n1}\mathbf{x}_1 + c_{n2}\mathbf{x}_2 + \cdots + c_{nn}\mathbf{x}_n \end{aligned}\right\} \text{ where } c_{ij} \in \mathbb{Z},\ c_{ii} \neq 0 \text{ for all } i, j.$$

Conversely, if $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ is any basis of M then there exists a basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ of L satisfying the same conditions.

Proof. Lemma 1.21 shows that $\rho L \subseteq M$, and hence $\rho \mathbf{x}_i \in M$ for all i. It follows that there exist vectors $\mathbf{y}_i \in M$ (not necessarily forming a basis for M) and integers c_{ij} satisfying the conditions of the theorem (in fact, we can take $c_{ii} = \rho$ for all i, and $c_{ij} = 0$ for all $i \neq j$). Thus the set of all n-tuples of vectors $\mathbf{y}_i \in M$ satisfying the conditions of the theorem is non-empty, and so for each i we may take $\mathbf{y}_i \in M$ to be the vector for which the coefficient c_{ii} is positive and as small as possible. We will show that the resulting vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ form a basis of the sublattice M. Suppose to the contrary that there is a vector $\mathbf{z} \in M$ which is not an integral linear combination of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. Writing $\mathbf{z}$ as an integral linear combination of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ gives

$$\mathbf{z} = t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_k\mathbf{x}_k, \quad \text{where } k \leq n \text{ and } t_k \neq 0.$$

We choose $\mathbf{z}$ so that the index k is as small as possible. By assumption $c_{kk} \neq 0$, and so we may perform integer division with remainder of t_k by c_{kk}, obtaining

$$t_k = qc_{kk} + r, \qquad 0 \leq r < c_{kk}.$$

We now consider the vector

$$\begin{aligned} \mathbf{z} - q\mathbf{y}_k &= (t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_k\mathbf{x}_k) - q(c_{k1}\mathbf{x}_1 + c_{k2}\mathbf{x}_2 + \cdots + c_{kk}\mathbf{x}_k) \\ &= (t_1 - qc_{k1})\mathbf{x}_1 + (t_2 - qc_{k2})\mathbf{x}_2 + \cdots + (t_k - qc_{kk})\mathbf{x}_k. \end{aligned}$$

Since $\mathbf{z}$ and $\mathbf{y}_k$ are in M and q is an integer, we have $\mathbf{z} - q\mathbf{y}_k \in M$. Since $\mathbf{z}$ is not an integral linear combination of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ neither is $\mathbf{z} - q\mathbf{y}_k$. But the

index k was chosen as small as possible, and so we must have $t_k - qc_{kk} \neq 0$. This implies that the vector $\mathbf{z} - q\mathbf{y}_k \in M$ is an integral linear combination of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k$ whose coefficient of $\mathbf{x}_k$, namely $t_k - qc_{kk} = r$, is nonzero and strictly less than c_{kk}. But this contradicts the choice of $\mathbf{y}_k$. It follows that such a vector $\mathbf{z}$ does not exist, and hence every vector in M must be an integral linear combination of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$.

For the converse, let $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ be a basis of M. By Lemma 1.21 we know that $\rho L \subseteq M$, and so we may apply the first part of the proof to the sublattice ρL of the lattice M. We obtain a basis $\rho\mathbf{x}_1, \rho\mathbf{x}_2, \ldots, \rho\mathbf{x}_n$ of ρL such that

$$\left.\begin{aligned} \rho\mathbf{x}_1 &= d_{11}\mathbf{y}_1 \\ \rho\mathbf{x}_2 &= d_{21}\mathbf{y}_1 + d_{22}\mathbf{y}_2 \\ &\vdots \\ \rho\mathbf{x}_n &= d_{n1}\mathbf{y}_1 + d_{n2}\mathbf{y}_2 + \cdots + d_{nn}\mathbf{y}_n \end{aligned}\right\} \text{ where } d_{ij} \in \mathbb{Z},\ d_{ii} \neq 0 \text{ for all } i, j.$$

We can write these equations in matrix form as $\rho X = DY$ where $D = (d_{ij})$ is a lower-triangular $n \times n$ integer matrix with nonzero entries on the diagonal. Solving for Y we obtain $Y = \rho D^{-1} X$. It is clear that $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ form a basis of L, and since $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n \in M \subseteq L$, we see that the entries of the matrix ρD^{-1} must be integers, by the uniqueness of the representation of each lattice vector as an (integral) linear combination of basis vectors. □

We note an especially interesting and attractive feature of the last proof: it clearly illustrates the principle that reduction of lattice bases can be naturally regarded as a generalization of integer division with remainder.

We now consider a sequence of corollaries of Theorem 1.22. Recall that E_{ij} is the $n \times n$ matrix in which the (i, j) entry is 1 and the other entries are 0.

Corollary 1.23. *In the first part of Theorem 1.22 we may assume that*

$$c_{ii} > 0 \ \ (1 \leq i \leq n) \quad \textit{and} \quad 0 \leq c_{ij} < c_{jj} \ \ (1 \leq j < i \leq n).$$

In the second part of Theorem 1.22 we may assume that

$$c_{ii} > 0 \ \ (1 \leq i \leq n) \quad \textit{and} \quad 0 \leq c_{ij} < c_{ii} \ \ (1 \leq j < i \leq n).$$

Proof. Consider the matrix form of the equations, namely $Y = CX$. If $c_{ii} < 0$ for some i then we left-multiply both sides of the matrix equation by $-E_{ii}$; this corresponds to the unimodular row operation "multiply row i by -1". If $c_{ij} < 0$ or $c_{ij} \geq c_{jj}$ for some i, j then we do integer division with remainder to write $c_{ij} = qc_{jj} + r$ with $0 \leq r < c_{jj}$ (we are now assuming that $c_{jj} > 0$) and then left-multiply both sides of the matrix equation by $I_n - qE_{ij}$; this corresponds to the unimodular row operation "subtract q times row j from row i". We can express the result of all these operations by the matrix equation $UY = UCX$ where U is a unimodular matrix. In fact it is clear that U

is lower-triangular, and hence so is UC. We can therefore replace the basis $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ of M, consisting of the rows of the matrix Y, by the new basis consisting of the rows of the matrix UY. The second part of the proof is left to the reader (see Exercise 1.16). □

Corollary 1.24. *Let L be an n-dimensional lattice in $\mathbb{R}^n$, and let $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ ($m \le n$) be linearly independent vectors in L. There is a basis $\mathbf{x}_1, \mathbf{x}_1, \ldots, \mathbf{x}_n$ of L satisfying the equations*

$$\left.\begin{aligned} \mathbf{y}_1 &= c_{11}\mathbf{x}_1 \\ \mathbf{y}_2 &= c_{21}\mathbf{x}_1 + c_{22}\mathbf{x}_2 \\ &\vdots \\ \mathbf{y}_m &= c_{m1}\mathbf{x}_1 + c_{m2}\mathbf{x}_2 + \cdots + c_{mm}\mathbf{x}_m \end{aligned}\right\} \text{ where } \left\{\begin{array}{l} c_{ij} \in \mathbb{Z} \text{ for all } i,j \\ c_{ii} > 0 \text{ for all } i \\ 0 \le c_{ij} < c_{ii} \text{ for all } i,j \end{array}\right.$$

Proof. We can find another $n-m$ vectors $\mathbf{y}_{m+1}, \ldots, \mathbf{y}_n$ in L such that the vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ are linearly independent. We now apply the second part of Corollary 1.23 to the lattice M with basis $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. □

Corollary 1.25. *Let L be an n-dimensional lattice in $\mathbb{R}^n$ and let $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ ($m < n$) be linearly independent vectors in L. These conditions are equivalent:*

> *(1) There exist another $n-m$ vectors $\mathbf{y}_{m+1}, \ldots, \mathbf{y}_n$ in L such that the vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ form a basis of L.*
>
> *(2) Any vector $\mathbf{z} \in L$ which is a (real) linear combination of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ is in fact an integral linear combination.*

Proof. The implication (1) $\Longrightarrow$ (2) is clear. To prove (2) $\Longrightarrow$ (1), assume that $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ satisfy condition (2). Since $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ are linearly independent vectors in L, we may apply Corollary 1.24 to obtain a basis $\mathbf{x}_1, \mathbf{x}_1, \ldots, \mathbf{x}_n$ of L satisfying the given equations. Considering only the first m basis vectors $\mathbf{x}_1, \mathbf{x}_1, \ldots, \mathbf{x}_m$ we have the matrix equation $Y = CX$ where now the matrix C has size $m \times m$. Hence $X = C^{-1}Y$, and now condition (2) implies that the entries of C^{-1} are integers. But C is lower-triangular with diagonal entries $c_{11}, c_{22}, \ldots, c_{mm}$, and hence C^{-1} is lower-triangular with diagonal entries $c_{11}^{-1}, c_{22}^{-1}, \ldots, c_{mm}^{-1}$. Thus for all $i = 1, 2, \ldots, m$ we see that c_{ii} is an integer for which c_{ii}^{-1} is also an integer, and hence $c_{ii} = \pm 1$. Corollary 1.23 now implies that $c_{ii} = 1$ for $1 \le i \le m$ and $c_{ij} = 0$ for $1 \le j < i \le m$. Thus $C = I_m$, and so $\mathbf{y}_i = \mathbf{x}_i$ for $i = 1, 2, \ldots, m$. To complete the proof we simply set $\mathbf{y}_i = \mathbf{x}_i$ for $i = m{+}1, \ldots, n$. □

Corollary 1.26. *Let L be an n-dimensional lattice in $\mathbb{R}^n$ with basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$. Consider an arbitrary vector $\mathbf{z} \in L$ and write*

$$\mathbf{z} = a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_n\mathbf{x}_n \qquad (a_1, a_2, \ldots, a_n \in \mathbb{Z}).$$

These conditions are equivalent for any integer $m = 1, 2, \ldots, n$:

(1) There are vectors $\mathbf{y}_{m+1}, \ldots, \mathbf{y}_n \in L$ *such that the following* n *vectors form a basis of* L*:*

$$\mathbf{x}_1,\ \mathbf{x}_2,\ \ldots,\ \mathbf{x}_{m-1},\ \mathbf{z},\ \mathbf{y}_{m+1},\ \ldots,\ \mathbf{y}_n.$$

(2) The greatest common divisor of the integers $a_{m+1}, \ldots, a_n$ *is 1.*

Proof. This follows directly from Corollary 1.25 (see Exercise 1.17). □

Up to this point we have been considering "full-rank" sublattices; the dimension of the sublattice M is equal to the dimension of the lattice L. For the next definition and theorem we consider a more general situation.

Definition 1.27. Let L be an n-dimensional lattice in $\mathbb{R}^n$, and let M be an m-dimensional sublattice for some $m < n$: that is, M is the set of all integral linear combinations of m linearly independent vectors in L. We say that M is a **primitive** sublattice if $M = L \cap V$ where V is a subspace of $\mathbb{R}^n$.

Theorem 1.28. (Nguyen [105], Lemma 4, page 28) *The* m*-dimensional sublattice* M *of the* n*-dimensional lattice* $L \subset \mathbb{R}^n$ *is primitive if and only if every basis of* M *can be extended to a basis of* L*; that is, if the vectors* $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ *form a basis of* M*, then there are vectors* $\mathbf{x}_{m+1}, \ldots, \mathbf{x}_n$ *in* L *such that the vectors* $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m, \mathbf{x}_{m+1}, \ldots, \mathbf{x}_n$ *form a basis of* L*.*

Proof. Exercise 1.18. □

1.3 Geometry of numbers

In this final section, we recall some definitions that will be used in the rest of the book, and state some results without proof.

Definition 1.29. Let L be an m-dimensional lattice in n-dimensional Euclidean space $\mathbb{R}^n$. The **first minimum** of the lattice, denoted $\Lambda_1(L)$, is the length of a shortest nonzero vector $\mathbf{x}_1 \in L$. The **second minimum** of the lattice, denoted $\Lambda_2(L)$, is the smallest real number r such that there exist two linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2 \in L$ such that $|\mathbf{x}_1|, |\mathbf{x}_2| \leq r$. In general, for $i = 1, 2, \ldots, m$, the i-th **successive minimum** of the lattice, denoted $\Lambda_i(L)$, is the smallest real number r such that there exist i linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_i \in L$ such that $|\mathbf{x}_1|, |\mathbf{x}_2|, \ldots, |\mathbf{x}_i| \leq r$. This quantity can be expressed more concisely by the equation

$$\Lambda_i(L) = \min_{\mathbf{x}_1, \ldots, \mathbf{x}_i \in L} \max\big(|\mathbf{x}_1|, \ldots, |\mathbf{x}_i|\big),$$

where the minimum is over all sets of i linearly independent vectors in L.

It is easy to see that the successive minima are weakly increasing:

$$\Lambda_1(L) \leq \Lambda_2(L) \leq \cdots \leq \Lambda_m(L).$$

The best possible basis for an m-dimensional lattice L consists of vectors

$$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m \in L \quad \text{such that} \quad |\mathbf{x}_i| = \Lambda_i(L) \quad \text{for} \quad i = 1, 2, \ldots, m.$$

However, such a basis is in general very hard to compute. It is interesting to note that a set of m vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m \in L$ which satisfy the conditions $|\mathbf{x}_i| = \Lambda_i(L)$ for $i = 1, 2, \ldots, m$ do not necessarily form a basis of L; for an example with $m = 4$ see Nguyen [105], page 32.

In order to understand better the size of the first minimum $\Lambda_1(L)$, we scale it by the determinant of the lattice. More precisely, we consider

$$\frac{\Lambda_1(L)}{\sqrt[m]{\det(L)}}.$$

Definition 1.30. Hermite's lattice constant, denoted γ_m, is the supremum of the following quantities as L ranges over all m-dimensional lattices:

$$\frac{\Lambda_1(L)^2}{\big(\det(L)\big)^{2/m}}.$$

The quantities γ_m are very difficult to compute, and are known only for $1 \leq m \leq 8$ and $m = 24$. The following table is from Nguyen [105], page 33:

m	1	2	3	4	5	6	7	8	$\cdots$	24
γ_m	1	$\left(\frac{4}{3}\right)^{1/2}$	$2^{1/3}$	$2^{1/2}$	$8^{1/5}$	$\left(\frac{64}{3}\right)^{1/6}$	$64^{1/7}$	2	$\cdots$	4

Definition 1.31. Let S be an arbitrary subset of n-dimensional Euclidean space $\mathbb{R}^n$. We say that S is **symmetric about the origin** if $\mathbf{x} \in S$ implies $-\mathbf{x} \in S$. We say that S is **convex** if $\mathbf{x}, \mathbf{y} \in S$ implies $\alpha\mathbf{x} + (1-\alpha)\mathbf{y} \in S$ for $0 \leq \alpha \leq 1$; that is, S contains the line segment joining $\mathbf{x}$ and $\mathbf{y}$.

Theorem 1.32. Minkowski's convex body theorem. *Let L be an n-dimensional lattice in n-dimensional Euclidean space $\mathbb{R}^n$ with determinant* $\det(L)$. *Let S be a subset of $\mathbb{R}^n$ which is convex and symmetric about the origin; let* $\mathrm{vol}(S)$ *denote the volume of S. If* $\mathrm{vol}(S) > 2^n \det(L)$ *then S contains a nonzero vector $\mathbf{x} \in L$.*

Proof. Cassels [22], Theorem II, page 71. □

1.4 Projects

Project 1.1. Write a computer program that takes as input three points A, B, C in $\mathbb{R}^n$, verifies that the points are the vertices of a triangle (that is, the points are not collinear), and then calculates:

(*i*) the lengths of the sides of the triangle,

(*ii*) the angles at the vertices of the triangle,

(*iii*) for each ordered pair of sides, the components of the first side parallel and orthogonal to the second side.

Test your program on 10 pseudorandom choices of the points A, B, C having coordinates with 1, 2 or 3 digits in the Euclidean space $\mathbb{R}^n$ for $n = 2, 3, \ldots, 10$.

Project 1.2. Write a computer program that takes as input an operation count k, a range parameter r, and a basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ of $\mathbb{R}^n$ spanning a lattice L, and then applies k unimodular row operations to the corresponding matrix X to obtain another basis of the same lattice. The range parameter is used to limit the scalars: the multiplier m in the third type of row operation ("add an integral multiple of any row to any other row") is a nonzero integer in the range $-r \leq m \leq r$. Test your program for various values of k and r on pseudorandom integral bases of $\mathbb{R}^n$ for $n = 2, 3, \ldots, 10$. (You will also need a parameter to limit the components of the pseudorandom basis vectors.)

Project 1.3. Write a computer program that takes as input a basis $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ of the n-dimensional lattice $L \subset \mathbb{R}^n$ together with m vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ in L $(1 \leq m < n)$, and determines whether there exist vectors $\mathbf{y}_{m+1}, \ldots, \mathbf{y}_n$ in L such that $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ form a basis of L. Extend your program to find vectors $\mathbf{y}_{m+1}, \ldots, \mathbf{y}_n$ satisfying this condition (if they exist).

Project 1.4. Write a survey report on algorithmic aspects of the geometry of numbers and its applications, and give a seminar presentation based on your report. The following survey papers will be useful references: Kannan [72], Vallée [138], and Aardal [1].

1.5 Exercises

Exercise 1.1. Consider the triangle in $\mathbb{R}^2$ with these points as its vertices:

$$A = (-5, -4), \qquad B = (-5, -1), \qquad C = (5, -8).$$

Find the lengths of the sides of this triangle. Calculate the angles at the vertices and verify that their sum is 180 degrees. For each ordered pair of

sides, find the components of the first side parallel and orthogonal to the second side.

Exercise 1.2. Same as Exercise 1.1 for these points in $\mathbb{R}^2$:

$$A = (45, -81), \qquad B = (-50, -22), \qquad C = (-16, -9).$$

Exercise 1.3. Same as Exercise 1.1 for these points in $\mathbb{R}^3$:

$$A = (2, -9, 0), \qquad B = (-8, 2, -5), \qquad C = (-9, 7, 7).$$

Exercise 1.4. Same as Exercise 1.1 for these points in $\mathbb{R}^3$:

$$A = (77, 9, 31), \qquad B = (20, -61, -48), \qquad C = (24, 65, 86).$$

Exercise 1.5. Same as Exercise 1.1 for these points in $\mathbb{R}^4$:

$$A = (4, -9, -2, -5), \qquad B = (1, 7, 8, -1), \qquad C = (-6, -8, -2, -2).$$

Exercise 1.6. Same as Exercise 1.1 for these points in $\mathbb{R}^4$:

$$A = (-62, -33, -68, -67), \quad B = (42, 18, -59, 12), \quad C = (52, -13, 82, 72).$$

Exercise 1.7. Let C be an $n \times n$ matrix with integer entries and determinant ± 1. Prove that C^{-1} also has integer entries.

Exercise 1.8. Show that these three bases of $\mathbb{R}^2$ generate the same lattice. For each ordered pair of bases, find a sequence of unimodular row operations which converts from the first basis to the second:

$$\{ \mathbf{x}_1, \mathbf{x}_2 \} = \left\{ \begin{bmatrix} -41 \\ -82 \end{bmatrix}, \begin{bmatrix} 1 \\ -99 \end{bmatrix} \right\},$$
$$\{ \mathbf{y}_1, \mathbf{y}_2 \} = \left\{ \begin{bmatrix} -79 \\ -461 \end{bmatrix}, \begin{bmatrix} -198 \\ -1103 \end{bmatrix} \right\},$$
$$\{ \mathbf{z}_1, \mathbf{z}_2 \} = \left\{ \begin{bmatrix} 26080957 \\ 43756088 \end{bmatrix}, \begin{bmatrix} 3875510 \\ 6501953 \end{bmatrix} \right\}.$$

Exercise 1.9. Same as Exercise 1.8 for these three bases of $\mathbb{R}^3$:

$$\{ \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \} = \left\{ \begin{bmatrix} 4 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ -3 \\ -3 \end{bmatrix}, \begin{bmatrix} -1 \\ -6 \\ -1 \end{bmatrix} \right\},$$
$$\{ \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \} = \left\{ \begin{bmatrix} 143 \\ -20 \\ 19 \end{bmatrix}, \begin{bmatrix} -241 \\ -64 \\ -45 \end{bmatrix}, \begin{bmatrix} 110 \\ -5 \\ 16 \end{bmatrix} \right\},$$
$$\{ \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3 \} = \left\{ \begin{bmatrix} -26357 \\ 13270 \\ 2307 \end{bmatrix}, \begin{bmatrix} 4836 \\ -2438 \\ -424 \end{bmatrix}, \begin{bmatrix} -105971 \\ 53351 \\ 9275 \end{bmatrix} \right\}.$$

Exercise 1.10. Same as Exercise 1.8 for these three bases of $\mathbb{R}^4$:

$$\left\{ \begin{bmatrix} 5 \\ 0 \\ -5 \\ -1 \end{bmatrix}, \begin{bmatrix} -7 \\ 0 \\ -6 \\ 7 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \\ -7 \\ 4 \end{bmatrix}, \begin{bmatrix} -1 \\ 7 \\ -3 \\ 1 \end{bmatrix} \right\},$$

$$\left\{ \begin{bmatrix} 82 \\ -371 \\ 271 \\ -129 \end{bmatrix}, \begin{bmatrix} -101 \\ 425 \\ -303 \\ 149 \end{bmatrix}, \begin{bmatrix} -705 \\ 2915 \\ -2090 \\ 1039 \end{bmatrix}, \begin{bmatrix} -2100 \\ 8689 \\ -6240 \\ 3102 \end{bmatrix} \right\},$$

$$\left\{ \begin{bmatrix} 21463771 \\ 1248392 \\ -30241207 \\ -775616 \end{bmatrix}, \begin{bmatrix} 79458521 \\ 4621448 \\ -111952377 \\ -2871329 \end{bmatrix}, \begin{bmatrix} -2726297 \\ -158475 \\ 3841129 \\ 98526 \end{bmatrix}, \begin{bmatrix} 7377273 \\ 428791 \\ -10393946 \\ -266612 \end{bmatrix} \right\}.$$

Exercise 1.11. Let X be any $m \times n$ matrix ($m \leq n$) with real entries. Prove that the determinant of the matrix XX^t is always non-negative, and equals 0 if and only if the rows of X are linearly dependent.

Exercise 1.12. Let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ be m linearly independent vectors in $\mathbb{R}^n$ spanning the lattice L, and let X be the $m \times n$ matrix with $\mathbf{x}_i$ as row i. Let $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$ be another basis for L with corresponding matrix Y. Prove that there exists a unimodular matrix C such that $Y = CX$ and $X = C^{-1}Y$. Deduce that $\det(XX^t) = \det(YY^t)$, and hence the determinant of L does not depend on the choice of basis.

Exercise 1.13. In each case, find the Gram matrix and the determinant of the m-dimensional lattice L in n-dimensional Euclidean space $\mathbb{R}^n$ spanned by the rows $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ of the $m \times n$ matrix X:

$$\text{(a)} \quad X = \begin{bmatrix} -5 & -4 & 6 \\ -1 & 1 & -5 \end{bmatrix},$$

$$\text{(b)} \quad X = \begin{bmatrix} 25 & 62 & 58 \\ 53 & 17 & -37 \end{bmatrix},$$

$$\text{(c)} \quad X = \begin{bmatrix} -156 & -142 & 27 \\ 901 & 560 & -733 \end{bmatrix},$$

$$\text{(d)} \quad X = \begin{bmatrix} 5166 & 3296 & -1487 \\ -7461 & 7833 & -5023 \end{bmatrix}.$$

Exercise 1.14. Same as Exercise 2.6 for these matrices:

$$\text{(a)} \quad X = \begin{bmatrix} 7 & 0 & 6 & 3 & 7 \\ 8 & -1 & -2 & -9 & -2 \\ 9 & 6 & 1 & -8 & -6 \end{bmatrix},$$

$$\text{(b)} \quad X = \begin{bmatrix} -59 & -23 & -2 & -31 & 29 \\ 99 & -73 & -83 & 38 & 17 \\ 58 & 30 & -84 & -77 & -63 \end{bmatrix},$$

$$\text{(c)} \quad X = \begin{bmatrix} -932 & -95 & -672 & -139 & 784 \\ 989 & -504 & 193 & -489 & 334 \\ -978 & -312 & -712 & -39 & -19 \end{bmatrix}.$$

Exercise 1.15. Same as Exercise 2.6 for these matrices:

$$\text{(a)} \quad X = \begin{bmatrix} -9 & -6 & 7 & 4 & 2 & 3 & -8 \\ -6 & 2 & -4 & 9 & -2 & 1 & -8 \\ -8 & -2 & 7 & -8 & 7 & 2 & 5 \\ 7 & -7 & -3 & 6 & -9 & 1 & 9 \end{bmatrix},$$

$$\text{(b)} \quad X = \begin{bmatrix} -46 & -42 & 12 & 76 & -51 & -97 & 37 \\ -77 & -84 & 85 & 92 & -34 & 88 & 92 \\ -51 & 65 & 41 & -59 & -4 & 88 & 23 \\ -77 & 54 & -78 & -89 & 0 & -63 & 47 \end{bmatrix},$$

$$\text{(c)} \quad X = \begin{bmatrix} 323 & 209 & -629 & 480 & 889 & 91 & -104 \\ -894 & 205 & 691 & 768 & 281 & -242 & 63 \\ -842 & 137 & -399 & 730 & 353 & 586 & 56 \\ -227 & -605 & 130 & 89 & -769 & -409 & -236 \end{bmatrix}.$$

Exercise 1.16. Complete the proof of Corollary 1.23.

Exercise 1.17. Complete the proof of Corollary 1.26.

Exercise 1.18. Prove Theorem 1.28.

Exercise 1.19. (Cassels [22], Lemma 2, page 15). Let $\mathbf{x}_1, \mathbf{x}_1, \ldots, \mathbf{x}_n$ be a basis for the n-dimensional lattice $L \subset \mathbb{R}^n$. Consider m lattice vectors,

$$\mathbf{y}_i = \sum_{j=1}^{n} a_{ij}\mathbf{x}_j, \qquad a_{ij} \in \mathbb{Z}, \qquad i = 1, 2, \ldots, m.$$

Let $A = (a_{ij})$ be the $m \times n$ matrix of coefficients. Prove that the vectors $\mathbf{y}_1$, $\mathbf{y}_2, \ldots, \mathbf{y}_m$ can be extended to a basis of L if and only if the $\binom{n}{m}$ determinants of size $m \times m$ obtained by taking m columns of A have no common factor.

Exercise 1.20. Let C be an $n \times n$ matrix with integer entries, and suppose that only the first m rows of C are known for some $m = 1, 2, \ldots, n-1$. Find necessary and sufficient conditions on the first m rows in order that the remaining $n-m$ rows can be filled in (with integers) to give a unimodular matrix.

Exercise 1.21. Consider the lattice $L \subset \mathbb{R}^2$ with basis $\mathbf{x}_1, \mathbf{x}_2$ and the vector $\mathbf{y}_1 \in L$. Determine whether there exists a vector $\mathbf{y}_2 \in L$ such that $\mathbf{y}_1, \mathbf{y}_2$ is a basis of L, and find such a vector if it exists:

$$\mathbf{x}_1, \mathbf{x}_2 = \begin{bmatrix} 4 \\ -7 \end{bmatrix}, \begin{bmatrix} -7 \\ -8 \end{bmatrix}; \qquad \mathbf{y}_1 = \begin{bmatrix} -79 \\ -44 \end{bmatrix}.$$

Exercise 1.22. Same as Exercise 1.21 for

$$\mathbf{x}_1, \mathbf{x}_2 = \begin{bmatrix} -72 \\ -32 \end{bmatrix}, \begin{bmatrix} -2 \\ -74 \end{bmatrix}; \qquad \mathbf{y}_1 = \begin{bmatrix} -632 \\ 304 \end{bmatrix}.$$

Exercise 1.23. Consider the lattice $L \subset \mathbb{R}^3$ with basis $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$ and the vectors $\mathbf{y}_1, \mathbf{y}_2 \in L$. Determine whether there exists a vector $\mathbf{y}_3 \in L$ such that $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ is a basis of L, and find such a vector if it exists:

$$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 = \begin{bmatrix} -6 \\ -5 \\ -4 \end{bmatrix}, \begin{bmatrix} 5 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} -8 \\ -5 \\ -3 \end{bmatrix}; \quad \mathbf{y}_1, \mathbf{y}_2 = \begin{bmatrix} 33 \\ 33 \\ 15 \end{bmatrix}, \begin{bmatrix} -54 \\ -16 \\ -15 \end{bmatrix}.$$

Exercise 1.24. Same as Exercise 1.23 for

$$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 = \begin{bmatrix} 31 \\ 43 \\ 12 \end{bmatrix}, \begin{bmatrix} -50 \\ 25 \\ -2 \end{bmatrix}, \begin{bmatrix} -80 \\ 94 \\ 50 \end{bmatrix}; \quad \mathbf{y}_1, \mathbf{y}_2 = \begin{bmatrix} -795 \\ 267 \\ 74 \end{bmatrix}, \begin{bmatrix} 317 \\ -712 \\ -392 \end{bmatrix}.$$

Exercise 1.25. Consider the lattice $L \subset \mathbb{R}^3$ with basis $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$ and the vector $\mathbf{y}_1 \in L$. Determine whether there exist vectors $\mathbf{y}_2, \mathbf{y}_3 \in L$ such that $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ is a basis of L, and find such vectors if they exist:

$$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 = \begin{bmatrix} 7 \\ 4 \\ -5 \end{bmatrix}, \begin{bmatrix} 8 \\ -9 \\ 5 \end{bmatrix}, \begin{bmatrix} -1 \\ -2 \\ -4 \end{bmatrix}; \qquad \mathbf{y}_1 = \begin{bmatrix} -31 \\ 8 \\ -4 \end{bmatrix}.$$

Exercise 1.26. Same as Exercise 1.25 for

$$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 = \begin{bmatrix} 18 \\ -62 \\ -67 \end{bmatrix}, \begin{bmatrix} -59 \\ -33 \\ 22 \end{bmatrix}, \begin{bmatrix} 12 \\ -68 \\ 14 \end{bmatrix}; \qquad \mathbf{y}_1 = \begin{bmatrix} 178 \\ 46 \\ -678 \end{bmatrix}.$$