6

Lattices

At this stage we take a radical new view of the theory, turning from purely algebraic methods to techniques inspired by geometry. This approach requires a different attitude of mind from the reader, in which formal ideas are built on a visual foundation. We begin with basic properties of lattices: subsets of $\mathbf{R}^n$ which in some sense generalize the way $\mathbf{Z}$ is embedded in $\mathbf{R}$. We characterize lattices topologically as the discrete subgroups of $\mathbf{R}^n$. We introduce the fundamental domain and quotient torus corresponding to a lattice and relate the two concepts. Finally we define a concept of volume for subsets of the quotient torus.

6.1 Lattices

Let $e_1, \ldots, e_m$ be a linearly independent set of vectors in $\mathbf{R}^n$ (so that $m \leq n$). The additive subgroup of $(\mathbf{R}^n, +)$ generated by $e_1, \ldots, e_m$ is called a *lattice* of *dimension* m, *generated* by $e_1, \ldots, e_m$. Figure 6.1 shows a lattice of dimension 2 in $\mathbf{R}^2$, generated by $(1, 2)$ and $(2, -1)$. (Do not confuse this with any other uses of the word 'lattice' in algebra.) Obviously, as regards the group-theoretic structure, a lattice of dimension m is a free abelian group of rank m, so we can apply the terminology and theory of free abelian groups to lattices.

We shall give a topological characterization of lattices. Let $\mathbf{R}^n$ be equipped with the usual metric (à la Pythagoras), where $\|x - y\|$ denotes the distance between x and y, and denote the (closed) ball centre x radius r by $B_r[x]$. Recall that a subset $X \subseteq \mathbf{R}^n$ is *bounded* if $X \subseteq B_r[0]$ for some

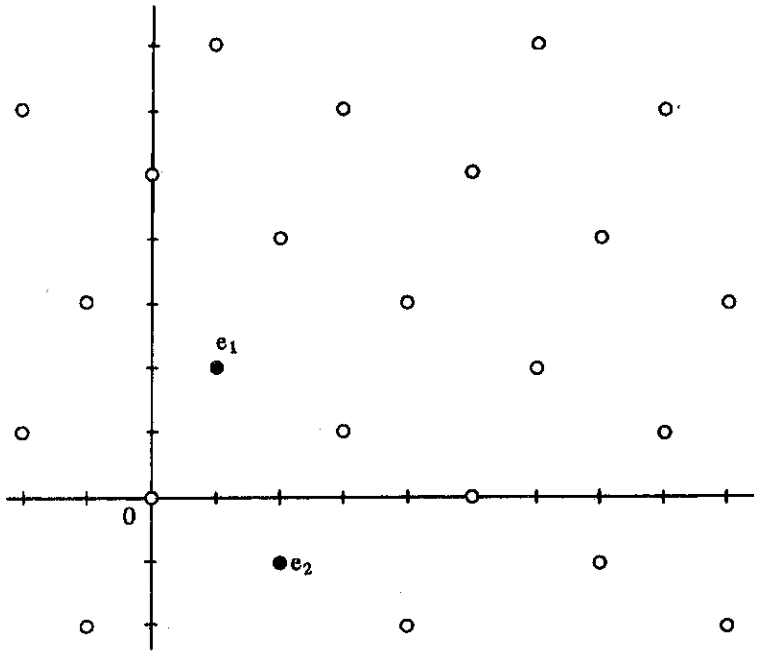

Figure 6.1. The lattice in $\mathbf{R}^2$ generated by $e_1 = (1,2)$ and $e_2 = (2,-1)$.

r. We say that a subset of $\mathbf{R}^n$ is *discrete* if and only if it intersects every $B_r[0]$ in a finite set.

Theorem 6.1. *An additive subgroup of $\mathbf{R}^n$ is a lattice if and only if it is discrete.*

Proof: Suppose L is a lattice. By passing to the subspace spanned by L we may assume L has dimension n. Let L be generated by $e_1, \ldots, e_n$; then these vectors form a basis for the space $\mathbf{R}^n$. Every $v \in \mathbf{R}^n$ has a unique representation

$$v = \lambda_1 e_1 + \ldots + \lambda_n e_n \quad (\lambda_i \in \mathbf{R}).$$

Define $f : \mathbf{R}^n \to \mathbf{R}^n$ by

$$f(\lambda_1 e_1 + \ldots + \lambda_n e_n) = (\lambda_1, \ldots, \lambda_n).$$

Then $f(B_r[0])$ is bounded, say

$$||f(v)|| \leq k \text{ for } v \in B_r[0].$$

If $\sum a_i e_i \in B_r[0]$ $(a_i \in \mathbf{Z})$, then certainly $||(a_1, \ldots, a_n)|| \leq k$. This implies

$$|a_i| \leq ||(a_1, \ldots, a_n)|| \leq k. \tag{6.1}$$

The number of integer solutions of (6.1) is finite and so $L \cap B_r[0]$, being a subset of the solutions of (6.1), is also finite, and L is discrete.

Conversely, let G be a discrete subgroup of $\mathbf{R}^n$. We prove by induction on n that G is a lattice. Let $\{g_1, \ldots, g_m\}$ be a maximal linearly independent subset of G, let V be the subspace spanned by $\{g_1, \ldots, g_{m-1}\}$, and let $G_0 = G \cap V$. Then G_0 is discrete so, by induction, is a lattice. Hence there exist linearly independent elements $h_1, \ldots, h_{m'}$ generating G_0. Since the elements $g_1, \ldots, g_{m-1} \in G_0$ we have $m' = m - 1$, and we can replace $\{g_1, \ldots, g_{m-1}\}$ by $\{h_1, \ldots, h_{m-1}\}$, or equivalently assume that every element of G_0 is a $\mathbf{Z}$-linear combination of $g_1, \ldots, g_{m-1}$. Let T be the subset of all $x \in G$ of the form

$$x = a_1 g_1 + \ldots + a_m g_m$$

with $a_i \in \mathbf{R}$, such that

$$0 \leq a_i < 1 \quad (i = 1, \ldots, m-1)$$
$$0 \leq a_m \leq 1.$$

Then T is bounded, hence finite since G is discrete, and we may therefore choose $x' \in T$ with smallest non-zero coefficient a_m, say

$$x' = b_1 g_1 + \ldots + b_m g_m.$$

Certainly $\{g_1, \ldots, g_{m-1}, x'\}$ is linearly independent. Now starting with any vector $g \in G$ we can select integer coefficients c_i so that

$$g' = g - c_m x' - c_1 g_1 - \ldots - c_{m-1} g_{m-1}$$

lies in T, and the coefficient of g_m in g' is less than b_m, but non-negative. By choice of x' this coefficient must be zero, so $g' \in G_0$. Hence $\{x', g_1, \ldots, g_{m-1}\}$ generates G, and G is a lattice. □

If L is a lattice generated by $\{e_1, \ldots, e_n\}$ we define the *fundamental domain* T to consist of all elements $\sum a_i e_i$ $(a_i \in \mathbf{R})$ for which

$$0 \leq a_i < 1.$$

Note that this depends on the choice of generators.

Lemma 6.2. *Each element of $\mathbf{R}^n$ lies in exactly one of the sets $T + l$ for $l \in L$.*

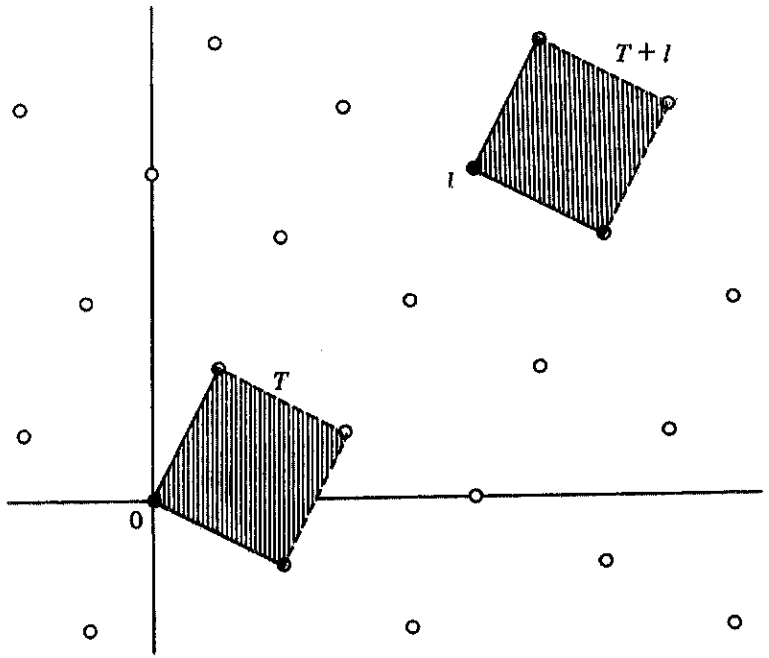

Figure 6.2. A fundamental domain T for the lattice of Figure 1, and a translate $T + l$. Dotted lines indicate omission of boundaries.

Proof: Chop off the integer parts of the coefficients. □

Figure 6.2 illustrates the concept of a fundamental domain, and the result of Lemma 6.2, for the lattice of Figure 6.1.

6.2 The Quotient Torus

Let L be a lattice in $\mathbf{R}^n$, and assume to start that L has dimension n. We shall study the quotient group $\mathbf{R}^n/L$.

Let $\mathbf{S}$ denote the set of all complex numbers of modulus 1. Under multiplication $\mathbf{S}$ is a group, called for obvious reasons the *circle group*.

Lemma 6.3. *The quotient group* $\mathbf{R}/\mathbf{Z}$ *is isomorphic to the circle group* $\mathbf{S}$.

Proof: Define a map $\phi : \mathbf{R} \to \mathbf{S}$ by

$$\phi(x) = e^{2\pi i x}.$$

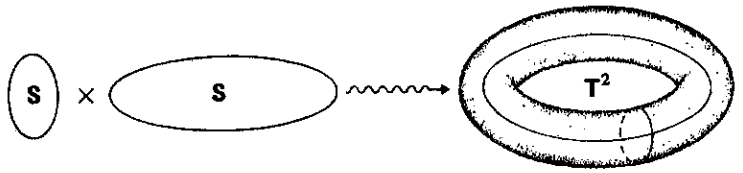

Figure 6.3. The Cartesian product of two circles is a torus.

Then ϕ is a surjective homomorphism with kernel $\mathbf{Z}$, and the lemma follows. □

Next let $\mathbf{T}^n$ denote the direct product of n copies of $\mathbf{S}$, and call this the *n-dimensional torus*. For instance, $\mathbf{T}^2 = \mathbf{S} \times \mathbf{S}$ is the usual torus (with a group structure) as sketched in Figure 6.3.

Theorem 6.4. *If L is an n-dimensional lattice in $\mathbf{R}^n$ then $\mathbf{R}^n/L$ is isomorphic to the n-dimensional torus $\mathbf{T}^n$.*

Proof: Let $\{e_1, \ldots, e_n\}$ be generators for L. Then $\{e_1, \ldots, e_n\}$ is a basis for $\mathbf{R}^n$. Define $\phi : \mathbf{R}^n \to \mathbf{T}^n$ by

$$\phi(a_1 e_1 + \ldots + a_n e_n) = (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n}).$$

Then ϕ is a surjective homorphism, and the kernel of ϕ is L. □

Lemma 6.5. *The map ϕ defined above, when restricted to the fundamental domain T, yields a bijection $T \to \mathbf{T}^n$.* □

Geometrically, $\mathbf{T}^n$ is obtained by 'glueing' (i.e. identifying) opposite faces of the closure of the fundamental domain, as in Figure 6.4.

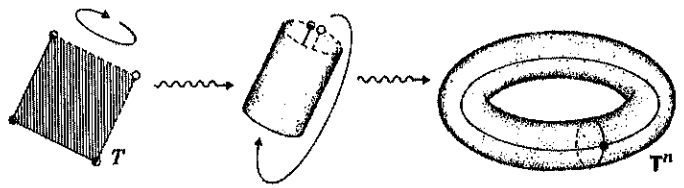

Figure 6.4. The quotient of Euclidean space by a lattice of the same dimension is a torus, obtained by identifying opposite edges of a fundamental domain.

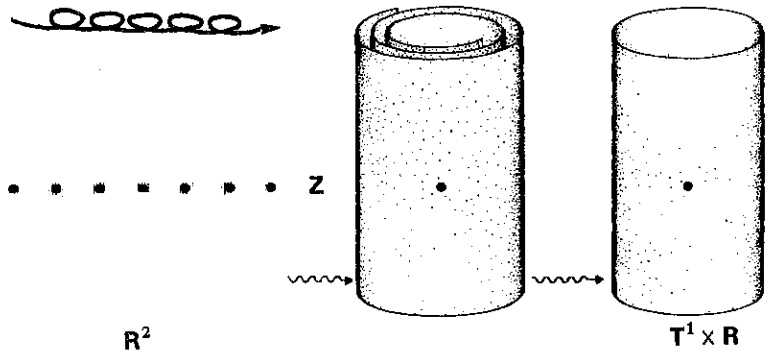

Figure 6.5. The quotient of Euclidean space by a lattice of smaller dimension is a cylinder.

If the dimension of L is less than n, we have a similar result:

Theorem 6.6. *Let L be an m-dimensional lattice in $\mathbf{R}^n$. Then $\mathbf{R}^n/L$ is isomorphic to $\mathbf{T}^m \times \mathbf{R}^{n-m}$.*

Proof: Let V be the subspace spanned by L, and choose a complement W so that $\mathbf{R}^n = V \oplus W$. Then $L \subseteq V$, $V/L \cong \mathbf{T}^m$ by Theorem 6.4, $W \cong \mathbf{R}^{n-m}$, and the result follows. □

For example, $\mathbf{R}^2/\mathbf{Z} \cong \mathbf{T}^1 \times \mathbf{R}$, which geometrically is a cylinder as in Figure 6.5.

The *volume* $v(X)$ of a subset $X \subseteq \mathbf{R}^n$ is defined in the usual way: for precision we take it to be the value of the multiple integral

$$\int_X \mathrm{d}x_1 \ldots \mathrm{d}x_n$$

where $(x_1, \ldots, x_n)$ are coordinates. Of course the volume exists only when the integral does.

Let $L \subseteq \mathbf{R}^n$ be a lattice of dimension n, so that $\mathbf{R}^n/L \cong \mathbf{T}^n$. Let T be a fundamental domain of L. We have noted the existence of a bijection

$$\phi : T \to \mathbf{T}^n.$$

For any subset X of $\mathbf{T}^n$ we define the *volume* $v(X)$ by

$$v(X) = v(\phi^{-1}(X))$$

which exists if and only if $\phi^{-1}(X)$ has a volume in $\mathbf{R}^n$.

Let $\nu : \mathbf{R}^n \to \mathbf{T}^n$ be the natural homomorphism with kernel L. It is intuitively clear that ν is 'locally volume-preserving', that is, for each $x \in \mathbf{R}^n$ there exists a ball $B_\epsilon[x]$ such that for all subsets $X \subseteq B_\epsilon[x]$ for which $v(X)$ exists we have

$$v(X) = v(\nu(X))$$

It is also intuitively clear that if an injective map is locally volume-preserving then it is volume-preserving. We prove a result which combines these two intuitive ideas:

Theorem 6.7. *If X is a bounded subset of $\mathbf{R}^n$ and $v(X)$ exists, and if $v(\nu(X)) \neq v(X)$, then $\nu|_X$ is not injective.*

Proof: Assume $\nu|_X$ is injective. Now X, being bounded, intersects only a finite number of the sets $T + l$, for T a fundamental domain and $l \in L$. Put

$$X_l = X \cap (T + l).$$

Then we have

$$X = X_{l_1} \cup \ldots \cup X_{l_n}.$$

For each l_i define

$$Y_{l_i} = X_{l_i} - l_i,$$

so that $Y_{l_i} \subseteq T$. We claim that the Y_{l_i} are disjoint. Since $\nu(x - l_i) = \nu(x)$ for all $x \in \mathbf{R}^n$ this follows from the assumed injectivity of ν. Now

$$v(X_{l_i}) = v(Y_{l_i})$$

for all i. Also

$$\nu(X_{l_i}) = \phi(Y_{l_i})$$

where ϕ is the bijection $T \to \mathbf{T}^n$. Now we compute:

$$\begin{aligned} v(\nu(X)) &= v(\nu(\cup X_{l_i})) \\ &= v(\cup Y_{l_i}) \\ &= \sum v(Y_{l_i}) \text{ by disjointness} \\ &= \sum v(X_{l_i}) \\ &= v(X), \end{aligned}$$

which is a contradiction. □

The idea of the proof can be summed up pictorially by Figure 6.6.

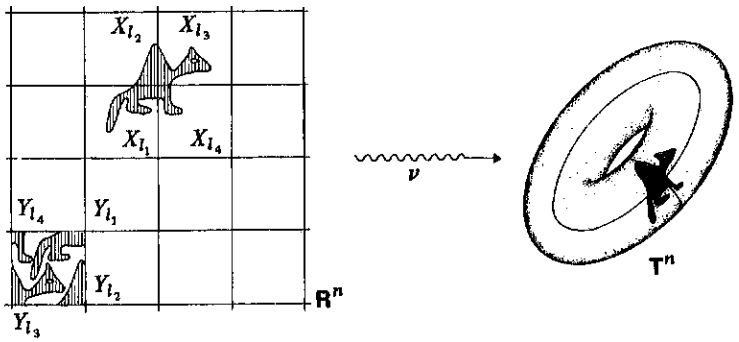

Figure 6.6. Proof of Theorem 6.7: if a locally volume-preserving map does not preserve volume globally, then it cannot be injective.

6.3 Exercises

1. Let L be a lattice in $\mathbf{R}^2$ with $L \subseteq \mathbf{Z}^2$. Prove that the volume of a fundamental domain T is equal to the number of points of $\mathbf{Z}^2$ lying in T.

2. Generalize the previous exercise to $\mathbf{R}^n$ and link this to Lemma 9.3 by using Theorem 1.17.

3. Sketch the lattices in $\mathbf{R}^2$ generated by:

   (a) $(0,1)$ and $(1,0)$.

   (b) $(-1,2)$ and $(2,2)$.

   (c) $(1,1)$ and $(2,3)$.

   (d) $(-2,-7)$ and $(4,-3)$.

   (e) $(1,20)$ and $(1,-20)$.

   (f) $(1,\pi)$ and $(\pi,1)$.

4. Sketch fundamental domains for these lattices.

5. Hence show that the fundamental domain of a lattice is not uniquely determined until we specify a set of generators.

6. Verify that nonetheless the volume of a fundamental domain of a given lattice is independent of the set of generators chosen.

7. Find two different fundamental domains for the lattice in $\mathbf{R}^3$ generated by $(0,0,1)$, $(0,2,0)$, $(1,1,1)$. Show by direct calculation that they have the same volume. Can you prove this geometrically by dissecting the fundamental domains into mutually congruent pieces?

7

Minkowski's Theorem

The aim of this chapter is to prove a marvellous theorem, due to Minkowski in 1896. This asserts the existence within a suitable set X of a non-zero point of a lattice L, provided the volume of X is sufficiently large relative to that of a fundamental domain of L. The idea behind the proof is deceptive in its simplicity: it is that X cannot be squashed into a space whose volume is less than that of X, unless X is allowed to overlap itself. Minkowski discovered that this essentially trivial observation has many non-trivial and important consequences, and used it as a foundation for an extensive theory of the 'geometry of numbers'. As immediate and accessible instances of its application we prove the two- and four-squares theorems of classical number theory.

7.1 Minkowski's Theorem

A subset $X \subseteq \mathbf{R}^n$ is *convex* if whenever x, $y \in X$ then all points on the straight line segment joining x to y also lie in X. In algebraic terms, X is convex if, whenever x, $y \in X$, the point

$$\lambda x + (1 - \lambda)y$$

belongs to X for all real λ, $0 \leq \lambda \leq 1$.

For example a circle, a square, an ellipse, or a triangle is convex in $\mathbf{R}^2$, but an annulus or crescent is not (Figure 7.1). A subset $X \subseteq \mathbf{R}^n$ is (*centrally*) *symmetric* if $x \in X$ implies $-x \in X$. Geometrically this means that X is invariant under reflection in the origin. Of the sets in Figure 7.1,

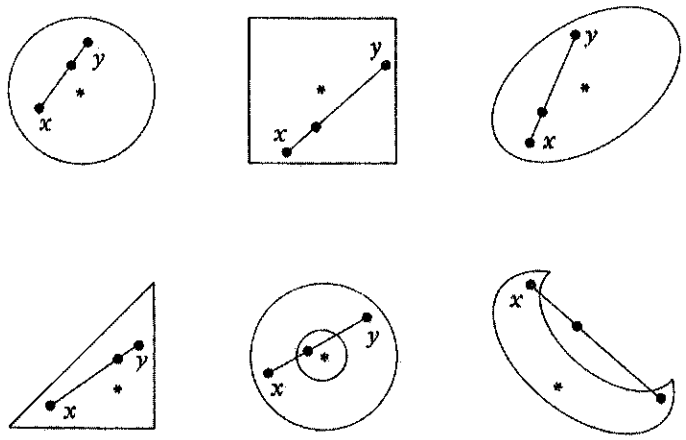

Figure 7.1. Convex and non-convex sets. The circular disc, square, ellipse, and triangle are convex; the annulus and crescent are not. The circle, square, ellipse, and annulus are centrally symmetric about *; the triangle and crescent are not.

assuming the origin to be at the positions marked with an asterisk, the circle, square, ellipse, and annulus are symmetric, but the triangle and crescent are not.

We may now state Minkowski's theorem.

Theorem 7.1. (Minkowski's Theorem.) *Let L be an n-dimensional lattice in $\mathbf{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex subset of $\mathbf{R}^n$. If*

$$v(X) > 2^n v(T)$$

then X contains a non-zero point of L.

Proof: Double the size of L to obtain a lattice $2L$ with fundamental domain $2T$ of volume $2^n v(T)$. Consider the torus

$$\mathbf{T}^n = \mathbf{R}^n / 2L.$$

By definition,

$$v(\mathbf{T}^n) = v(2T) = 2^n v(T).$$

Now the natural map $\nu : \mathbf{R}^n \to \mathbf{T}^n$ cannot preserve the volume of X, since this is strictly larger than $v(\mathbf{T}^n)$: since $\nu(X) \subseteq \mathbf{T}^n$ we have

$$v(\nu(X)) \leq v(\mathbf{T}^n) = 2^n v(T) < v(X).$$

It follows by Theorem 6.7 that $\nu|_X$ is not injective. Hence there exist $x_1 \neq x_2$, $x_1, x_2 \in X$, such that

$$\nu(x_1) = \nu(x_2),$$

or equivalently

$$x_1 - x_2 \in 2L. \tag{7.1}$$

But $x_2 \in X$, so $-x_2 \in X$ by symmetry; and now by convexity

$$\tfrac{1}{2}(x_1) + \tfrac{1}{2}12(-x_2) \in X,$$

that is,

$$\tfrac{1}{2}(x_1 - x_2) \in X.$$

But by Equation (7.1),

$$\tfrac{1}{2}(x_1 - x_2) \in L.$$

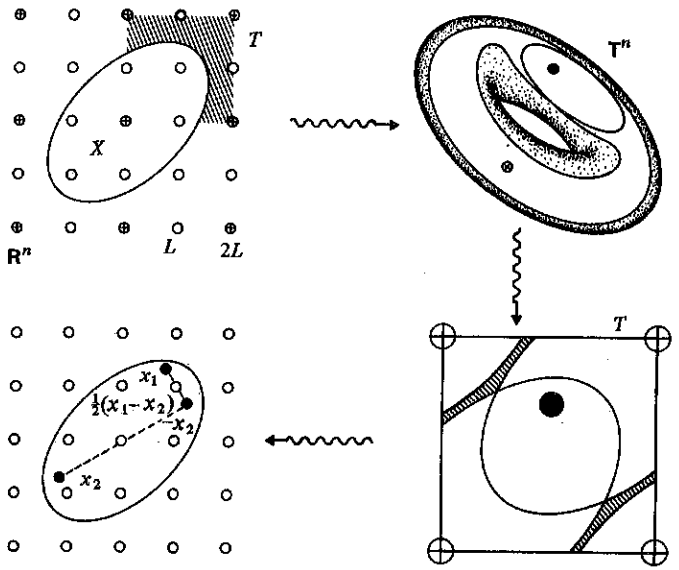

Figure 7.2. Proof of Minkowski's theorem. Expand the original lattice (○) to double the size (⊕) and form the quotient torus. By computing volumes, the natural quotient map is not injective when restricted to the given convex set. From point x_1 and x_2 with the same image we may construct a non-zero lattice point $\frac{1}{2}(x_1 - x_2)$.

Hence

$$0 \neq \tfrac{1}{2}(x_1 - x_2) \in X \cap L,$$

as required. □

The geometrical reasoning is illustrated in Figure 7.2. The decisive step in the proof is that since $\mathbf{T}^n$ has smaller volume than X it is impossible to squash X into $\mathbf{T}^n$ without overlap: the ancient platitude of quarts and pint pots. That such olde-worlde wisdom becomes, in the hands of Minkowski, a weapon of devastating power, was the wonder of the 19th century and a lesson for the 20th. We will unleash this power at several crucial stages in the forthcoming battle. (Note that our original Thespian metaphor has been abandoned in favour of a military one, reinforcing the change of viewpoint from that of the algebraic *voyeur* to that of the geometric participant.) As a more immediate affirmation, we now give two traditional applications to number theory: the 'two-squares' and 'four-squares' theorems.

7.2 The Two-Squares Theorem

We start by proving:

Theorem 7.2. *If p is prime of the form $4k+1$ then p is a sum of two integer squares.*

Proof: The multiplicative group G of the field $\mathbf{Z}_p$ is cyclic (Garling [28] Corollary 1 to Theorem 12.3, p. 105; Stewart [71], p. 171) and has order $p-1 = 4k$. It therefore contains an element u of order 4. Then $u^2 \equiv -1 \pmod{p}$ since -1 is the only element of order 2 in G.

Let $L \subseteq \mathbf{Z}^2$ be the lattice in $\mathbf{R}^2$ consisting of all pairs (a, b) $(a, b \in \mathbf{Z})$ such that

$$b \equiv ua \pmod{p}.$$

This is a subgroup of $\mathbf{Z}^2$ of index p (an easy verification left to the reader) so the volume of a fundamental domain for L is p. By Minkowski's theorem any circle, centre the origin, of radius r, which has area

$$\pi r^2 > 4p$$

contains a non-zero point of L. This is the case for $r^2 = 3p/2$. So there exists a point $(a, b) \in L$, not the origin, for which

$$0 \neq a^2 + b^2 \leq r^2 = 3p/2 < 2p.$$

But modulo p we have

$$a^2 + b^2 \equiv a^2 + u^2 a^2 \equiv 0.$$

Hence $a^2 + b^2$, being a multiple of p strictly between 0 and $2p$, must equal p. □

The reader should draw the lattice L and the relevant circle in a few cases $(p = 5, 13, 17)$ and check that the relevant lattice point exists and provides suitable a, b.

Theorem 7.2 goes back to Fermat, who stated it in a letter to Mersenne in 1640. He sent a sketch proof to Pierre de Carcavi in 1659. Euler gave a complete proof in 1754.

7.3 The Four-Squares Theorem

Refining this argument leads to another famous theorem:

Theorem 7.3. *Every positive integer is a sum of four integer squares.*

Proof: We prove the theorem for primes p, and then extend the result to all integers. Now

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

so we may suppose p is odd. We claim that the congruence

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

has a solution $u, v \in \mathbf{Z}$. This is because u^2 takes exactly $(p+1)/2$ distinct values as u runs through $0, \ldots, p-1$; and $-1 - v^2$ also takes on $(p+1)/2$ values: for the congruence to have no solution all these values, $p+1$ in total, will be distinct: then we have $p + 1 \leq p$ which is absurd.

For such a choice of u, v consider the lattice $L \subseteq \mathbf{Z}^4$ consisting of (a, b, c, d) such that

$$c \equiv ua + vb, \quad d \equiv ub - va \pmod{p}.$$

Then L has index p^2 in $\mathbf{Z}^4$ (another easy computation) so the volume of a fundamental domain is p^2. Now a 4-dimensional sphere, centre the origin, radius r, has volume

$$\pi^2 r^4/2$$

and we choose r to make this greater than $16p^2$; say $r^2 = 1.9p$.

Then there exists a lattice point $0 \neq (a, b, c, d)$ in this 4-sphere, and so

$$0 \neq a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p.$$

Modulo p, it is easy to verify that $a^2 + b^2 + c^2 + d^2 \equiv 0$, hence as before must equal p.

To deal with an arbitrary integer n, it suffices to factorize n into primes and then use the identity

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)$$

$$= (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2$$

$$+(aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2.$$

□

Theorem 7.3 also goes back to Fermat. Euler spent 40 years trying to prove it, and Lagrange succeeded in 1770.

7.4 Exercises

1. Which of the following solids are convex? Sphere, pyramid, icosahedron, cube, torus, ellipsoid, parallelepiped.
2. How many different convex solids can be made by joining n unit cubes face to face, so that their vertices coincide, for $n = 1, 2, 3, 4, 5, 6$; counting two solids as different if and only if they cannot be mapped to each other by rigid motions? What is the result for general n?
3. Verify the two-squares theorem on all primes less than 200.
4. Verify the four-squares theorem on all integers less than 100.
5. Prove that not every integer is a sum of three squares.
6. Prove that the number $\mu(n)$ of pairs of integers (x, y) with $x^2+y^2 < n$ satisfies $\mu(n)/n \to \pi$ as $n \to \infty$.

8

Geometric Representation of Algebraic Numbers

The purpose of this chapter is to develop a method of embedding a number field K in a real vector space of dimension equal to the degree of K, in such a way that ideals in K map to lattices in this vector space. This opens the way to applications of Minkowski's theorem. The embedding is defined in terms of the monomorphisms $K \to \mathbf{C}$, and we have to distinguish between those which map K into $\mathbf{R}$ and those which do not.

8.1 The Space $\mathbf{L}^{st}$

Let $K = \mathbf{Q}(\theta)$ be a number field of degree n, where θ is an algebraic integer. Let $\sigma_1, \ldots, \sigma_n$ be the set of all monomorphisms $K \to \mathbf{C}$ (see Theorem 2.4). If $\sigma_i(K) \subseteq \mathbf{R}$, which happens if and only if $\sigma_i(\theta) \in \mathbf{R}$, we say that σ_i, is *real*; otherwise σ_i is *complex*. As usual denote complex conjugation by bars and define

$$\bar{\sigma}_i(\alpha) = \overline{\sigma_i(\alpha)}.$$

Since complex conjugation is an automorphism of $\mathbf{C}$ it follows that $\bar{\sigma}_i$ is a monomorphism $K \to \mathbf{C}$, so equals σ_j for some j. Now $\sigma_i = \bar{\sigma}_i$ if and only if σ_i is real, and $\overline{\bar{\sigma}}_i = \sigma_i$, so the complex monomorphisms come in conjugate pairs. Hence

$$n = s + 2t$$