5. Geometry of numbers

In this section, we prove the classical finiteness theorems for a number ring R: the Picard group $\mathrm{Pic}(R)$ is a *finite* group, and the unit group R^* is in many cases finitely generated. These are not properties of arbitrary Dedekind domains, and the proofs rely on the special fact that number rings can be embedded in a natural way as lattices in a finite dimensional real vector space. The key ingredient in the proofs is non-algebraic: it is the theorem of Minkowski on the existence of lattice points in symmetric convex bodies given in 5.1.

Let V be a vector space of finite dimension n over the field $\mathbf{R}$ of real numbers, and $\langle\cdot,\cdot\rangle : V \times V \to \mathbf{R}$ a scalar product, i.e. a positive definite bilinear form on $V \times V$. The scalar product induces a notion of volume on V, which is also known as the *Haar measure* on V. For a parallelepiped

$$B = \{r_1x_1 + r_2x_2 + \ldots + r_nx_n : 0 \le r_i < 1\}$$

spanned by $x_1, x_2, \ldots, x_n$, the volume is defined by

$$\mathrm{vol}(B) = |\det(\langle x_i, x_j\rangle)_{i,j=1}^n|^{1/2}.$$

This definition shows that the 'unit cube' spanned by an orthonormal basis for V has volume 1, and that the image of this cube under a linear map T has volume $|\det(T)|$. If the vectors x_i are written with respect to an orthonormal basis for V as $x_i = (x_{ij})_{j=1}^n$, then we have

$$|\det(\langle x_i, x_j\rangle)_{i,j=1}^n|^{1/2} = |\det(M \cdot M^t)|^{1/2} = |\det(M)|$$

for $M = (x_{ij})_{i,j=1}^n$.

The volume function on parallelepipeds can be uniquely extended to a measure on V. Under the identification $V \cong \mathbf{R}^n$ via an orthonormal basis for V, this is the Lebesgue measure on $\mathbf{R}^n$. We usually summarize these properties by saying that V is an n-dimensional *Euclidean space*.

A *lattice* in V is a subgroup of V of the form

$$L = \mathbf{Z}\cdot x_1 + \mathbf{Z}\cdot x_2 + \ldots + \mathbf{Z}\cdot x_k,$$

with $x_1, x_2, \ldots, x_k \in V$ linearly independent. The integer k is the *rank* of L. It cannot exceed $n = \dim V$, and we say that L is *complete* or has *maximal rank* if it is equal to n. For a complete lattice $L \subset V$, the *co-volume* $\mathrm{vol}(V/L)$ of L is defined as the volume of the parallelepiped F spanned by a basis of L. Such a parallelepiped is a *fundamental domain* for L as every $x \in V$ has a unique representation $x = f + l$ with $f \in F$ and $l \in L$. In fact, $\mathrm{vol}(V/L)$ is the volume of V/L under the induced Haar measure on the factor group V/L.

A subset $X \subset V$ is said to be *symmetric* if it satisfies $-X = \{-x : x \in X\} = X$.

5.1. Minkowski's theorem. *Let L be a complete lattice in an n-dimensional Euclidean space V and $X \subset V$ a bounded, convex, symmetric subset satisfying*

$$\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(V/L).$$

Then X contains a non-zero lattice point. If X is closed, the same is true under the weaker assumption $\mathrm{vol}(X) \ge 2^n \cdot \mathrm{vol}(V/L)$.

Proof. By assumption, the set $\frac{1}{2}X = \{\frac{1}{2}x : x \in X\}$ has volume $\mathrm{vol}(\frac{1}{2}X) = 2^{-n}\mathrm{vol}(X) > \mathrm{vol}(V/L)$. This implies that the map $\frac{1}{2}X \to V/L$ cannot be injective, so there are distinct points $x_1, x_2 \in X$ with $\frac{1}{2}x_1 - \frac{1}{2}x_2 = \omega \in L$. As X is symmetric, $-x_2$ is contained in X. By convexity, we find that the convex combination ω of x_1 and $-x_2 \in X$ is in $X \cap L$.

Under the weaker assumption volume $\mathrm{vol}(X) \geq 2^n \mathrm{vol}(V/L)$, each of the sets $X_k = (1+1/k)X$ with $k \in \mathbf{Z}_{\geq 1}$ contains a non-zero lattice point $\omega_k \in L$. As all ω_k are contained in the bounded set $2X$, there are only finitely many different possibilities for ω_k. It follows that there is a lattice element $\omega \in \cap_k X_k$, and for closed X we have $\cap_k X_k = X$. □

Let K be a number field of degree n. Then K is an n-dimensional $\mathbf{Q}$-vector space, and by base extension we can map K into the complex vector space

$$K_{\mathbf{C}} = K \otimes_{\mathbf{Q}} \mathbf{C} \cong \prod_{\sigma : K \to \mathbf{C}} \mathbf{C} = \mathbf{C}^n$$

by the canonical map $\Phi_K : x \mapsto (\sigma(x))_\sigma$. Note that Φ_K is a ring homomorphism, and that the norm and trace on the free $\mathbf{C}$-algebra $K_{\mathbf{C}}$ extend the norm and the trace of the field extension $K/\mathbf{Q}$. The image $\Phi_K[K]$ of K under the embedding lies in the $\mathbf{R}$-algebra

$$K_{\mathbf{R}} = \{(z_\sigma)_\sigma \in K_{\mathbf{C}} : z_{\overline{\sigma}} = \overline{z}_\sigma\}$$

consisting of the elements of $K_{\mathbf{C}}$ invariant under the involution $F : (z_\sigma)_\sigma \longrightarrow (\overline{z}_{\overline{\sigma}})_\sigma$. Here $\overline{\sigma}$ denotes the embedding of K in $\mathbf{C}$ that is obtained by composition of σ with complex conjugation.

On $K_{\mathbf{C}} \cong \mathbf{C}^n$, we have the standard hermitian scalar product $\langle \cdot, \cdot \rangle$. It satisfies $\langle Fz_1, Fz_2 \rangle = \overline{\langle z_1, z_2 \rangle}$, so its restriction to $K_{\mathbf{R}}$ is a real scalar product that equips $K_{\mathbf{R}}$ with a Euclidean structure. In particular, we have a *canonical* volume function on $K_{\mathbf{R}}$. It naturally leads us to the following fundamental observation.

5.2. Lemma. *Let R be an order in a number field K. Then $\Phi_K[R]$ is a lattice of co-volume $|\Delta(R)|^{1/2}$ in $K_{\mathbf{R}}$.*

Proof. Choose a $\mathbf{Z}$-basis $\{x_1, x_2, \ldots, x_n\}$ for R. Then $\Phi_K[R]$ is spanned by the vectors $(\sigma x_i)_\sigma \in K_{\mathbf{R}}$, and using the matrix $X = (\sigma_i(x_j))_{i,j=1}^n$ from the proof of 4.6, we see that the co-volume of $\Phi_K[R]$ equals

$$|\det(\langle(\sigma x_i)_\sigma, (\sigma x_j)_\sigma\rangle)_{i,j=1}^n|^{1/2} = |\det(X^t \cdot \overline{X})|^{1/2} = |\Delta(R)|^{1/2}. \qquad \square$$

If $I \subset R$ is a non-zero ideal of norm $N(I) = [R : I] \in \mathbf{Z}$, then 5.2 implies that $\Phi_K[I]$ is a lattice of co-volume $N(I) \cdot |\Delta(R)|^{1/2}$ in $K_{\mathbf{R}}$. To this lattice in $K_{\mathbf{R}}$ we will apply Minkowski's theorem 5.1, which states that every sufficiently large symmetric box in $K_{\mathbf{R}}$ contains a non-zero element of $\Phi_K[I]$.

In order to compute volumes in $K_{\mathbf{R}}$, we have a closer look at its Euclidean structure. Denote the real embeddings of K in $\mathbf{C}$ by $\sigma_1, \sigma_2, \ldots, \sigma_r$ and the pairs of complex embeddings of K by $\sigma_{r+1}, \overline{\sigma_{r+1}}, \sigma_{r+2}, \overline{\sigma_{r+2}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$. Then we have $r + 2s = n = [K : \mathbf{Q}]$, and an isomorphism of $\mathbf{R}$-algebras

$$\begin{aligned} K_{\mathbf{R}} &\longrightarrow \mathbf{R}^r \times \mathbf{C}^s \\ (z_\sigma)_\sigma &\longmapsto (z_{\sigma_i})_{i=1}^{r+s}. \end{aligned} \tag{5.3}$$