6. Finitely generated abelian groups and lattices.

The contents of this section are not of a number theoretical nature. The results are used in the next sections. Our first subject is the structure of finitely generated abelian groups. We expain the relation between indices of finitely generated free groups and determinants.

The second part of this section concerns *lattices.* Lattices are finitely generated groups with additional structure. We explain the relations between indices of free groups and certain volumes.

An abelian group is said to be *free of rank* n, if it is isomorphic to $\mathbf{Z}^n$. A subgroup B of a free group $A \cong \mathbf{Z}^n$ is said to have rank m if the $\mathbf{Q}$-vector space generated by B in $\mathbf{Q}^n$ has dimension m.

For any two integers a and b, the notation $a|b$ means that a divides b.

Theorem 6.1. *Let $A \cong \mathbf{Z}^n$ be a free group of rank n and let $B \subset A$ be a subgroup. Then*

(a) The group B is free of rank $m \leq n$.

(b) There exists a $\mathbf{Z}$-basis $e_1, \ldots, e_n$ of A and integers $a_1, \ldots, a_m \in \mathbf{Z}_{\geq 0}$ such that $a_1|a_2|\ldots|a_m$ and such that the elements $a_1e_1, \ldots, a_me_m$ form a $\mathbf{Z}$-basis for B. The integers $a_1, \ldots, a_m$ are unique.

Proof. Let B be a non-zero subgroup of A. Consider the group $\mathrm{Hom}(A, \mathbf{Z})$ of functionals $f : A \longrightarrow \mathbf{Z}$. For every $f : A \longrightarrow \mathbf{Z}$ the image $f(B)$ is an ideal in $\mathbf{Z}$. Since $\mathbf{Z}$ is Noetherian, there is a maximal element in the collection of ideals $\{f(B) : f : A \longrightarrow \mathbf{Z}\}$. Since $B \neq 0$, the maximal element $f(B)$ is not the zero ideal. Let a denote a positive generator and let $\mathbf{v} \in B$ be an element for which $f(\mathbf{v}) = a$.

We claim that a divides $g(b)$ for every $g : A \longrightarrow \mathbf{Z}$. Indeed, let $d = \gcd(g(\mathbf{v}), a)$ and let $u, v \in \mathbf{Z}$ such that $ua + vg(\mathbf{v}) = d$. Then d is the value of the functional $uf + vg$ at $\mathbf{v}$. Since d divides a, it follows from the maximality of a that d is equal to a. Therefore a divides $g(\mathbf{v})$.

In particular, a divides all coordinates of $\mathbf{v}$. We let $\mathbf{w} = \frac{1}{a}\mathbf{v}$. Then we have $f(\mathbf{w}) = 1$ and in addition

$$A = \mathbf{w}\mathbf{Z} \oplus \ker(f),$$
$$B = \mathbf{v}\mathbf{Z} \oplus (\ker(f) \cap B).$$

This follows easily from the fact that for every $\mathbf{x} \in A$ one has that $\mathbf{x} = f(\mathbf{x})\cdot\mathbf{w} + \mathbf{x} - f(\mathbf{x})\cdot\mathbf{w}$. If, moreover, $\mathbf{x}$ is in B, then $f(\mathbf{x})$ is in $a\mathbf{Z}$ by definition of a. We leave the easy verifications to the reader.

Now we prove part (a) by induction with respect to the rank m of A. If $m = 0$ the group B is zero and the statement is trivially true. If $m > 0$, we can split A and B as we did in the discussion above. The group $\ker(f) \cap B$ obviously has rank at most m. Since $B = \mathbf{v}\mathbf{Z} \oplus (\ker(f) \cap B)$ has clearly strictly larger rank, we conclude that the rank of $\ker(f) \cap B$ is at most $m - 1$. By induction we see that this is a free group and consequently B is free as well. This proves *(a)*

Part *(b)* is proved by induction with respect to n. If $n = 0$ the statement is trivially true. If $n > 0$, either $B = 0$, in which case the result is clear, or $B > 0$. In the latter case

we can split A and B as explained above:

$$A = \mathbf{w}\mathbf{Z} \oplus \ker(f),$$
$$B = \mathbf{v}\mathbf{Z} \oplus (\ker(f) \cap B).$$

The group $\ker(f)$ has rank at most $n-1$. By *(a)* it is *free* of rank at most $n-1$. By induction there exists a basis $\mathbf{e}_2, \ldots, \mathbf{e}_n$ of $\ker(f)$ and integers $a_2, \ldots, a_m$ such that $a_2e_2, \ldots, a_me_m$ is a basis for $\ker(f) \cap B$. We now take $e_1 = \mathbf{w}$ and $a_1 = a$. To complete the proof it suffices to verify that a divides a_2. If there is no $\mathbf{e}_2$, there is nothing to prove. If there is, we define a functional g by $g(\mathbf{e}_1) = g(\mathbf{e}_2) = 1$ and $g(\mathbf{e}_i) = 0$ for $i > 2$. We see that a is in $g(B)$ and therefore, by maximality of a, that $g(B) = (a)$. Since $a_2 \in g(B)$ the result follows.

Corollary 6.2.

(a) For any finitely generated abelian group G there exist unique integers $r \geq 0$ and $a_1, a_2, \ldots, a_t \in \mathbf{Z}_{>1}$ satisfying $a_1|a_2|\ldots|a_t$ and such that

$$A \cong \mathbf{Z}^r \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \mathbf{Z}/a_t\mathbf{Z}.$$

The abelian group G is finite if and onbly if $r = 0$.

(b) Let $A \cong \mathbf{Z}^n$ be a free group of rank n and let $B \subset A$ be a subgroup. Then B has finite index in A if and only if $\mathrm{rk}(B) = \mathrm{rk}(A)$.

Proof. *(a)* Let G be a finitely generated group and let n be an integer such that there is a surjective map

$$\theta : \mathbf{Z}^n \longrightarrow G.$$

By Theorem 6.1 there is a basis $e_1, \ldots, e_n$ of $\mathbf{Z}^n$ and there exist positive integers $a_1, a_2, \ldots, a_m$ such that $a_1|a_2|\ldots|a_m$ and $a_1e_1 \ldots, a_me_m$ is a basis for $B = \ker(\theta)$. It follows at once that

$$A \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_m\mathbf{Z}$$

as required. The uniqueness of the a_i's follows easily by considering A modulo a_iA for various i.

(b) Choose a $\mathbf{Q}$-basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of A such that the subgroup B has $a_1\mathbf{e}_1, \ldots, a_m\mathbf{e}_m$ as a basis. We have that

$$A/B \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_m\mathbf{Z}$$

and clearly $\mathrm{rk}(B) = \mathrm{rk}(A)$ if and only if $n = m$ if and only if $[A : B] = \#(A/B)$ is finite. This proves *(b)*.

Corollary 6.3. *Let M be a $n \times n$-matrix with integral coefficients. Let $A = \mathbf{Z}^n$ and B its subgroup $MA = \{Ma : a \in A\}$. Then*

(a) The index of B in A is finite if and only if $\det(M) \neq 0$.

(b) If $\det(M) \neq 0$ *then* $[A : B] = |\det(M)|$.

Proof. According to Theorem 6.1 we can choose a $\mathbf{Z}$-basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ of A such that $B = a_1\mathbf{e}_1\mathbf{Z} \oplus \ldots \oplus a_m\mathbf{e}_m\mathbf{Z}$. The matrix M is therefore conjugate to

$$M' = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix}.$$

We see that A/B is infinite if and only if one of the a_i is zero. This proves *(a)*. Part *(b)* follows from the fact that $\det(M) = \det(M') = \prod_i a_i$.

Next we apply the results on finitely generated abelian groups to number theory.

Corollary 6.4. *Let $f \in \mathbf{Z}[T]$ be a monic irreducible polynomial. Let α denote a zero and let $F = \mathbf{Q}(\alpha)$. Then the index $[O_F : \mathbf{Z}[\alpha]]$ is finite and we have*

$$\mathrm{Disc}(f) = [O_F : \mathbf{Z}[\alpha]]^2 \cdot \Delta_F.$$

Proof. Let $\omega_1, \ldots, \omega_n$ denote a $\mathbf{Z}$-basis for the ring of integers of F. There is then a matrix M with integral coefficients such that

$$M \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}.$$

Therefore we have

$$(\det(M))^2 \Delta_F = \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

and hence, by Cor. 6.3 and Prop. 3.8, we have

$$[O_F : \mathbf{Z}[\alpha]]^2 \Delta_F = \mathrm{Disc}(f)$$

as required.

Corollary 6.5. *Let F be a number field and let $x \in O_F$. Then the norm of the O_F-ideal generated by x is equal to the absolute value of the norm of x. In other words, we have*

$$N((x)) = |N(x)|.$$

Proof. Let M denote the matrix which expresses the multiplication by x with respect to a $\mathbf{Q}$-basis of F. We have

$$\begin{aligned} |N(x)| &= |\det(M)| && \text{by definition,} \\ &= [O_F : \mathrm{im}(M)] && \text{by Cor. 6.3,} \\ &= \#O_F/(x) = N((x)). \end{aligned}$$

as required.

Many of the finitely generated groups that arise in algebraic number theory are equipped with extra structure. Very often they are, in natural way, *lattices*. In the rest of this section we study lattices. We show that the ring of integers O_F of an algebraic number field F admits a natural lattice structure. In section 9 we will see that, in a certain sense, the unit group O_F^* admits a lattice structure as well.

Definition. *Let V be a Euclidean space, i.e. a finite dimensional real vector space equipped with a scalar product. A subset $L \subset V$ is called a lattice if it is of the form $L = \sum_i \mathbf{Z}\mathbf{e}_i$ for some basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of the vector space V.*

An easy example of a lattice is the group $\mathbf{Z}^n$ contained in the vector space $\mathbf{R}^n$ equipped with the usual scalar product.

Proposition 6.6. *Let V be a real vector space equipped with scalar product and let $L \subset V$ be a subgroup. Then*
(a) L is a lattice.
(b) L is discrete and cocompact.
(c) L generates V over $\mathbf{R}$ and for every bounded set $B \subset V$ one has that $B \cap L < \infty$.

Proof. *(a) $\Rightarrow$ (b)* The subgroup L is clearly discrete. We have that $V = \sum_i e_i \mathbf{R}$ and therefore V/F, being a continuous image of the compact space $\sum_i e_i[0,1]$ is compact.
(b) $\Rightarrow$ (c) Suppose L is discrete and cocompact. Let $W \subset V$ be the subspace generated by L. Then there is a continuous surjection $V/L \longrightarrow V/W$. It follows that the vector space V/W is compact. Therefore it is zero. If there were a bounded set B with $B \cap L$ infinite, then there would be an accumulation point of elements in L, so that L is not discrete.
(c) $\Rightarrow$ (a) Since L generates V over $\mathbf{R}$, there is an $\mathbf{R}$-basis $e_1, \ldots, e_n \in L$ of V. The set $B = \sum_i e_i[0,1]$ is bounded and therefore the following union is finite:

$$L = \bigcup_{x \in B \cap L} (x + \sum_i e_i \mathbf{Z}).$$

We conclude that the index $m = [L : \sum_i e_i \mathbf{Z}]$ is finite and that $mL \subset \sum_i e_i \mathbf{Z}$. By Theorem 6.1 the group mL is free and by Cor. 6.2 it is of rank n. We conclude that L is free of rank m as well. This concludes the proof of the proposition.

Definition. *Let V be a Euclidean space. Let $L \subset V$ be a lattice. The covolume of L is defined by*

$$\mathrm{covol}(L) = \mathrm{vol}(V/L).$$

Equivalently, the covolume of L is the volume of the fundamental domain of L in V. In other words, if $v_1, \ldots, v_n$ is a $\mathbf{Z}$-basis for L, then

$$\mathrm{covol}(L) = \mathrm{vol}(\{\sum_i \lambda_i v_i : 0 \leq \lambda_i < 1 \text{ for } 1 \leq i \leq n\}).$$

For example, the $\mathbf{Z}$-span of the columns of an invertible $n \times n$ matrix A with real coefficients is a lattice in $\mathbf{R}^n$. Its covolume is equal to $|\det(A)|$.

Proposition 6.7. *Let V be an n-dimensional Euclidean space. Let $L \subset V$ be a lattice. Then*
(a) If $L' \subset L$ is a sublattice of L, then $\mathrm{covol}(L') = [L' : L]\mathrm{covol}(L)$.
(b) If $f : V \longrightarrow V$ is an invertible linear map, then $f(L)$ is also a lattice. If M is a representative matrix of f with respect to an orthonomal basis of V, then $\mathrm{covol}(f(L))$ is equal to $\det(M)\mathrm{covol}(L)$.

Proof. (a) A fundamental domain of L' is the union of $[L' : L]$ translates of a fundamental domain of L. To see (b), we choose an orthonormal basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of V and let A be an $n \times n$-matrix whose columns generate L. Then $f(L)$ is the $\mathbf{Z}$-span of the columns of the matrix MA. Therefore the covolume of $f(L)$ is equal to $\det(MA) = \det(M)\mathrm{covol}(L)$ as required.

The following example is very important.

Example 6.8. *Let F be a number field of degree n. The complex vector space $F_{\mathbf{C}} = \prod_{i=1}^{n} \mathbf{C}$ admits a natural Hermitian product with respect to which its canonical basis is orthonormal. This Hermitian product on $F_{\mathbf{C}}$ restricts to a scalar product on $F_{\mathbf{R}}$. The image of the ring homomorphism*

$$\Phi : O_F \longrightarrow F_{\mathbf{C}} \cong \prod_{i=1}^{n} \mathbf{C}$$

given by $\Phi(x) = (\phi_1(x)), \ldots, \phi_n(x))$ is contained in $F_{\mathbf{R}}$ and is a lattice in $F_{\mathbf{R}}$.

Proof. Let e_i denote the canonical basis of $F_{\mathbf{C}} = \prod_{i=1}^{n} \mathbf{C}$. We equip $F_{\mathbf{C}}$ with the Hermitain product given by

$$\langle e_i, e_j \rangle = \begin{cases} 0; & \text{when } i \neq j, \\ 1. & \text{when } i = j. \end{cases}$$

Since the same identities hold for for the trace of $e_i e_j$, the Hermitian product on $F_{\mathbf{C}}$ is given by $\langle z, w \rangle = \mathrm{Tr}(z\overline{w})$ for $z, w \in \mathbf{C}^n$. To see that it induces a scalar product on $F_{\mathbf{R}}$, it suffices to see that it is positive definite. Since the trace of $z\overline{z}$ of an element in $F_{\mathbf{R}}$ of the form

$$z = (x_1, \ldots, x_{r_1}, z_1, \overline{z}_1, \ldots, z_{r_2}, \overline{z}_{r_2})$$

is equal to $\sum_{i=1}^{r_1} x_i^2 + 2\sum_{i=1}^{r_2} |z_i|^2$, which is ≥ 0 and only vanishes when $z = 0$, this is indeed the case.

By Lemma 2.5 the map Φ maps $\mathbf{Q}$-bases of F to $\mathbf{R}$-bases of $F_{\mathbf{R}}$. In particular, every $\mathbf{Z}$-base of O_F is mapped to an $\mathbf{R}$-base of $F_{\mathbf{R}}$. This implies that $\Phi(O_F)$ is a lattice in $F_{\mathbf{R}}$.

Corollary 6.9. *Let F be a number field. The image of a fractional ideal I under $\Phi : F \longrightarrow F_{\mathbf{R}}$ is a also lattice.*

Proof. First suppose that I is an ideal of O_F. Then it contains a non-zero integer m. We have inclusions

$$mO_F \ \subset \ I \ \subset \ O_F.$$

Since $\Phi(mO_F)$ is a lattice, the first inclusion shows that I contains a basis of $F_{\mathbf{R}}$. Since $\Phi(O_F)$ is a lattice, the second inclusion shows that $\Phi(I) \cap B$ is finite for every bounded subset $B \subset F_{\mathbf{R}}$. Therefore $\Phi(I)$ is a lattice.

In general, let $\alpha \in F^*$ an element for which that $J = \alpha I$ is a non-zero ideal. Then J is a lattice and hence is the $\mathbf{Z}$-span of an $\mathbf{R}$-basis $\omega_1, \ldots, \omega_n$ of $F_{\mathbf{R}}$. Since $\alpha\omega_1, \ldots, \alpha\omega_n$ is also an $\mathbf{R}$-basis of $\mathbf{R}$, the fractional ideal I is also a lattice, as required.

Proposition 6.10. *Let F be a number field of degree n.*
(a) The covolume of the lattice O_F or rather $\Phi(O_F)$ in $F_{\mathbf{R}}$ is given by

$$\mathrm{covol}(O_F) = \sqrt{|\Delta_F|}.$$

(b) Let I be a fractional ideal, the covolume of I in $F_{\mathbf{R}}$ is given by

$$\mathrm{covol}(I) = N(I)\sqrt{|\Delta_F|}.$$

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbf{Z}$-basis of O_F. Then a $\mathbf{Z}$-basis for the image of O_F in $F_{\mathbf{R}}$ is given by the vectors $(\phi_k(\omega_j))$ for $1 \leq j \leq n$. The covolume of $\Phi(O_F)$ is equal to the absolute value of the determinant of the matrix whose colums are the coordinates of the vectors $(\phi_k(\omega_j))$ with respect to some ortonormal basis of $F_{\mathbf{R}}$. Since any orthonormal basis of $\mathbf{F_R}$ is also an orthonormal basis of $F_{\mathbf{C}}$, the covolume is also simply the absolute value of the determinant of the matrix $(\phi_k(\omega_j))$, which is $\sqrt{|\Delta_F|}$.
(b) If I is an ideal, then $I \subset O_F$ are lattices and the result follows from Prop. 6.7. In general, let I be fractional ideal and let $\alpha \in F^*$ be such that $J = \alpha I$ is an ideal of O_F. Then I is the image of J under the multiplication by α map. Therefore we have $\text{covol}(I) = N(\alpha)^{-1}\text{covol}(J) = N(\alpha)^{-1}N(J)\sqrt{|\Delta_F|} = N(I)\sqrt{|\Delta_F|}$ as required.

6.1. Let $A = \binom{3}{0}\mathbf{Z} + \binom{0}{5}\mathbf{Z} \subset \mathbf{Z}^2$. Find a basis of $\mathbf{Z}^2$ as in Theorem 6.1.

6.2 Let H in $\mathbf{Z}^3$ be the subgroup generated by $(1,1,2)$, $(5,1,1)$ abd $(-1,-5,-3)$. What is the structure of the finite abelian group $\mathbf{Z}^3/H$?

6.3 Let $L = \{(x,y,z) \in \mathbf{Z}^3 : 2x + 3y + 4z \equiv 0 \pmod 7\}$. Show that $L \subset \mathbf{R}^3$ is a lattice. Find a $\mathbf{Z}$-basis and calculate its covolume.

6.4 Let $H \subset \mathbf{Z}^3$ be the subgroup generated by $(1,1,1)$, $(0,1,1)$ and $(-1,2,3)$ and let A be the matrix $\begin{pmatrix} 1 & 0 & -2 \\ 0 & 2 & 1 \\ 3 & 1 & 1 \end{pmatrix}$. Show that $A(H)$ is a lattice in $\mathbf{R}^3$ and compute its covolume.

6.5 For a quaternion $z = a + bi + cj + dk$ (with $a,b,c,d \in \mathbf{R}$), the reduced trace is given by $\text{Tr}(z) = z + \overline{z} = 2a$.
- (a) Show that $\langle z, w\rangle = \frac{1}{2}\text{Tr}(z\overline{w}\rangle$ for $z, w \in \mathbf{H}$, defines a scalar product on the underlying 4-dimensional real vector space $\mathbf{H}$.
- (b) Show that $\mathbf{Z} + i\mathbf{Z} + j\mathbf{Z} + k\mathbf{Z}$ is a lattice in $\mathbf{H}$ and compute its covolume.
- (c) Compute the covolume of the subring of Hurwitz quaternions.

6.6 Let F be a number field. Suppose $R \subset F$ is a subring with the property that its image in $F_{\mathbf{R}}$ is a lattice. Show that $R \subset O_F$.

6.7 *(Euclidean imaginary quadratic rings.)* Let F be an imaginary quadratic number field. We identify O_F with its Φ-image in $F_{\mathbf{R}} = \mathbf{C}$.
- (a) Show that O_F is Euclidean for the norm if and only if the closed circles with radius 1 and centers in O_F cover $\mathbf{C}$.
- (b) Show that O_F is Euclidean for the norm if and only if $\Delta_F = -3, -4, -7$ or -11.
- (c) Show that the rings of integers of the real quadratic fields F with $\Delta_F = 5, 8$ and 12 are Euclidean for the norm.

6.8*Let L be a free abelian group of rank r. Let $Q(x)$ be a positive definite quadratic form on L. Supppose that for every $B \in \mathbf{R}$ there are only finitely many $x \in L$ with $Q(x) < B$. Show that there is an injective map $I : L \hookrightarrow \mathbf{R}^r$ such that $i(L)$ is a lattice and $\|i(x)\| = Q(x)$. Here $\|v\|$ denotes the usual length of a vector $v \in \mathbf{R}^r$.

6.9 Let $L \subset \mathbf{R}^n$ be a lattice. Show that

$$\lim_{t\to\infty} \frac{1}{t^n} \#\{(v_1, \ldots, v_n) \in L : |a_i| \leq t \quad \text{for all } 1 \leq i \leq n\} = \frac{2^n}{\text{covol}(L)}.$$