Revision Notes for Infinite Groups 2018

Cornelia Druţu

These notes collect material seen in courses from previous years, and are to be used as a reference only. The material in these notes is not examinable.

CHAPTER 1

General preliminaries

1.1. General metric spaces

A *metric space* is a set X endowed with a function $\mathrm{dist} : X \times X \to \mathbb{R}$ satisfying the following properties:

(M1) $\mathrm{dist}(x, y) \geqslant 0$ for all $x, y \in X$; $\mathrm{dist}(x, y) = 0$ if and only if $x = y$;

(M2) (Symmetry) for all $x, y \in X$, $\mathrm{dist}(y, x) = \mathrm{dist}(x, y)$;

(M3) (Triangle inequality) for all $x, y, z \in X$, $\mathrm{dist}(x, z) \leqslant \mathrm{dist}(x, y)+\mathrm{dist}(y, z)$.

The function dist is called *metric* or *distance function*.

Notation. We will use the notation d or dist to denote the metric on a metric space X. For $x \in X$ and $A \subset X$ we will use the notation $\mathrm{dist}(x, A)$ for the *minimal distance* from x to A, i.e.

$$\mathrm{dist}(x, A) = \inf\{d(x, a) : a \in A\}.$$

Similarly, given two subsets $A, B \subset X$, we define their *minimal distance*

$$\mathrm{dist}(A, B) = \inf\{d(a, b) : a \in A, b \in B\}.$$

We say that two metric spaces (X, dist_X) and (Y, dist_Y) are *isometric* if there exists a bijection $f : X \to Y$ such that for every x, x' in X,

$$\mathrm{dist}_Y\left(f(x), f(x')\right) = \mathrm{dist}_X(x, x').$$

We call such a bijection an *isometry*.

1.2. Zorn's Lemma

This is a set-theoretic principle: it is a form of the Axiom of Choice that is particularly convenient for application in algebra. In order to prove various general existence statements about groups, rings and modules we just have to accept it as an axiom.

Let S be a non-empty *partially ordered* set: a set with a binary relation $\leq$ that is transitive and satisfies $a = b \Longleftrightarrow (a \leq b \text{ and } b \leq a)$.

An element $a \in S$ then a is said to be 'maximal' if

$$a \leq b \Longrightarrow b = a \ (\forall b \in S).$$

An element $c \in S$ is an *upper bound* for a subset T of S if

$$\forall b \in T.\ b \leq c.$$

A subset T of S is a *chain* if T is totally ordered by $\leq$, i.e.

$$\forall x, y \in T\ (x \leq y \text{ or } y \leq x).$$

The partially ordered set $(S, \geq)$ is said to be *inductively ordered* if *every chain in S has an upper bound in S*.

Zorn's Lemma *If S is inductively ordered then S has a maximal element.*

This is often applied to the case where S is a collection of subsets of some set X, and $a \leq b$ means $a \subseteq b$. In this case, we can sometimes verify that S is inductively ordered by checking that the union of a chain in S still belongs to S. This holds, for example, if membership of S can be tested by looking at finite subsets (if S consists of all abelian subgroups of a group, say, we only have to test pairs of elements).

Typical example: S is the set of proper subgroups in a finitely generated group $G = \langle X \rangle$. Thus $H \in S$ iff $X \nsubseteq H$, and (as long as X is *finite*) this holds for the union of a chain if it holds for each term in the chain. It follows that G has maximal proper subgroups.

A group that is not finitely generated may fail to have any maximal subgroups: think of some examples!

CHAPTER 2

Groups and their actions

2.1. Subgroups

Given two subsets A, B in a group G we denote by AB the subset

$$\{ab \ : \ a \in A, \, b \in B\} \subset G.$$

Similarly, we will use the notation

$$A^{-1} = \{a^{-1} : a \in A\}.$$

A *normal subgroup* K in G is a subgroup such that for every $g \in G$, $gKg^{-1} = K$ (equivalently $gK = Kg$). We use the notation $K \lhd G$ to denote that K is a normal subgroup in G. When H and K are subgroups of G and either H or K is a normal subgroup of G, the subset $HK \subset G$ becomes a subgroup of G.

A subgroup K of a group G is called *characteristic* if for every automorphism $\phi : G \to G$, $\phi(K) = K$. Note that every characteristic subgroup is normal (since conjugation is an automorphism). But not every normal subgroup is characteristic:

Example 2.1. Let G be the group $(\mathbb{Z}^2, +)$. Since G is abelian, every subgroup is normal. But, for instance, the subgroup $\mathbb{Z} \times \{0\}$ is not invariant under the automorphism $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$, $\phi(m, n) = (n, m)$.

Definition 2.2. The *center* $Z(G)$ of a group G is defined as the subgroup consisting of elements $h \in G$ so that $[h, g] = 1$ for each $g \in G$.

It is easy to see that the center is a characteristic subgroup of G.

Definition 2.3. A *subnormal descending series* in a group G is a series

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_n \rhd \cdots$$

such that N_{i+1} is a normal subgroup in N_i for every $i \geqslant 0$.

If all N_i's are normal subgroups of G, then the series is called *normal*.

A subnormal series of a group is called a *refinement* of another subnormal series if the terms of the latter series all occur as terms in the former series.

The following is a basic result in group theory:

Lemma 2.4. *If G is a group, $N \lhd G$, and $A \lhd B < G$, then BN/AN is isomorphic to $B/A(B \cap N)$.*

Definition 2.5. Two subnormal series

$$G = A_0 \rhd A_1 \rhd \ldots \rhd A_n = \{1\} \quad \text{and} \quad G = B_0 \rhd B_1 \rhd \ldots \rhd B_m = \{1\}$$

are called *equivalent* if $n = m$ and there exists a bijection between the sets of partial quotients $\{A_i/A_{i+1} \mid i = 1, \ldots, n-1\}$ and $\{B_i/B_{i+1} \mid i = 1, \ldots, n-1\}$ such that the corresponding quotients are isomorphic.

Theorem 2.6 (Jordan-Hölder). *Any two finite subnormal series*

$$G = H_0 \geqslant H_1 \geqslant \ldots \geqslant H_n = \{1\} \quad and \quad G = K_0 \geqslant K_1 \geqslant \ldots \geqslant K_m = \{1\}$$

possess equivalent refinements.

Proof. Define $H_{ij} = (K_j \cap H_i)H_{i+1}$. The following is a subnormal series

$$H_{i0} = H_i \geqslant H_{i1} \geqslant \ldots \geqslant H_{im} = H_{i+1}\,.$$

When inserting all these in the series of H_i one obtains the required refinement.

Likewise, define $K_{rs} = (H_s \cap K_r)K_{r+1}$ and by inserting the series

$$K_{r0} = K_r \geqslant K_{r1} \geqslant \ldots \geqslant K_{rn} = K_r$$

in the series of K_r, we define its refinement.

According to Lemma 2.4

$$H_{ij}/H_{ij+1} = (K_j \cap H_i)H_{i+1}/(K_{j+1} \cap H_i)H_{i+1} \simeq K_j \cap H_i/(K_{j+1} \cap H_i)(K_j \cap H_{i+1})\,.$$

Similarly, one proves that $K_{ji}/K_{ji+1} \simeq K_j \cap H_i/(K_{j+1} \cap H_i)(K_j \cap H_{i+1})$. □

The following properties of finite-index subgroups will be useful.

Lemma 2.7. *If $N \lhd H$ and $H \lhd G$, N of finite index in H and H finitely generated, then N contains a finite-index subgroup K which is normal in G.*

Proof. By hypothesis, the quotient group $F = H/N$ is finite. For an arbitrary $g \in G$ the conjugation by g is an automorphism of H, hence H/gNg^{-1} is isomorphic to F. A homomorphism $H \to F$ is completely determined by the images in F of elements of a finite generating set of H. Therefore there are finitely many such homomorphisms, and finitely many possible kernels of them. Thus, the set of subgroups gNg^{-1}, $g \in G$, forms a finite list $N, N_1, .., N_k$. The subgroup $K = \bigcap_{g \in G} gNg^{-1} = N \cap N_1 \cap \cdots \cap N_k$ is normal in G and has finite index in N, since each of the subgroups $N_1, \ldots, N_k$ has finite index in H. □

Proposition 2.8. *Let G be a finitely generated group. Then:*

(1) *For every $n \in \mathbb{N}$ there exist finitely many subgroups of index n in G.*

(2) *Every finite-index subgroup H in G contains a subgroup K which is finite index and characteristic in G.*

Proof. (1) Let $H \leqslant G$ be a subgroup of index n. We list the left cosets of H:

$$H = g_1 \cdot H, g_2 \cdot H, \ldots, g_n \cdot H,$$

and label these cosets by the numbers $\{1, \ldots, n\}$. The action by left multiplication of G on the set of left cosets of H defines a homomorphism $\phi : G \to S_n$ such that $\phi(G)$ acts transitively on $\{1, 2, \ldots, n\}$ and H is the inverse image under ϕ of the stabilizer of 1 in S_n. Note that there are $(n-1)!$ ways of labeling the left cosets, each defining a different homomorphism with these properties.

Conversely, if $\phi : G \to S_n$ is such that $\phi(G)$ acts transitively on $\{1, 2, \ldots, n\}$, then $G/\phi^{-1}(\mathrm{Stab}\,(1))$ has cardinality n.

Since the group G is finitely generated, a homomorphism $\phi : G \to S_n$ is determined by the image of a generating finite set of G, hence there are finitely many distinct such homomorphisms. The number of subgroups of index n in H is equal to the number η_n of homomorphisms $\phi : G \to S_n$ such that $\phi(G)$ acts transitively on $\{1, 2, \ldots, n\}$, divided by $(n-1)!$.

(2) Let H be a subgroup of index n. For every automorphism $\varphi : G \to G$, $\varphi(H)$ is a subgroup of index n. According to (1) the set $\{\varphi(H) \mid \varphi \in \mathrm{Aut}\,(G)\}$ is finite, equal $\{H, H_1, \ldots, H_k\}$. It follows that

$$K = \bigcap_{\varphi \in \mathrm{Aut}\,(G)} \varphi(H) = H \cap H_1 \cap \ldots \cap H_k .$$

Then K is a characteristic subgroup of finite index in H hence in G. $\square$

Exercise 2.9. Does the conclusion of Proposition 2.8 still hold for groups which are not finitely generated?

Let S be a subset in a group G, and let $H \leqslant G$ be a subgroup. The following are equivalent:

(1) H is the smallest subgroup of G containing S;

(2) $H = \bigcap_{S \subset G_1 \leqslant G} G_1$;

(3) $H = \left\{ s_1 s_2 \cdots s_n \ : \ n \in \mathbb{N}, s_i \in S \text{ or } s_i^{-1} \in S \text{ for every } i \in \{1, 2, \ldots, n\} \right\}$.

The subgroup H satisfying any of the above is denoted $H = \langle S \rangle$ and is said to be *generated by* S. The subset $S \subset H$ is called a *generating set* of H. The elements in S are called *generators* of H.

When S consists of a single element x, $\langle S \rangle$ is usually written as $\langle x \rangle$; it is the cyclic subgroup consisting of powers of x.

We say that a normal subgroup $K \lhd G$ is *normally generated* by a set $R \subset K$ if K is the smallest normal subgroup of G which contains R, i.e.

$$K = \bigcap_{R \subset N \lhd G} N .$$

We will use the notation

$$K = \langle\langle R \rangle\rangle$$

for this subgroup. The subgroup K is also called the *normal closure* or the *conjugate closure* of R in G. Other notations for K which appear in the literature are R^G and $\langle R \rangle^G$.

2.2. Commutators and the commutator subgroup

Recall that the commutator of two elements x, y of a group G is defined as $[x, y] = xyx^{-1}y^{-1}$. Thus:

- two elements x, y commute, i.e. $xy = yx$, if and only if $[x, y] = 1$.
- $xy = [x, y]yx$.

Thus, the commutator $[x, y]$ 'measures the degree of non-commutation' of the elements h and k.

Let H, K be two subgroups of G. We denote by $[H, K]$ the subgroup of G generated by all commutators $[h, k]$ with $h \in H$, $k \in K$.

Definition 2.10. The *commutator subgroup (or* derived subgroup*) of* G is the subgroup $G' = [G, G]$. As above, we may say that the commutator subgroup G' of G 'measures the degree of non-commutativity' of the group G.

A group G is *abelian* if every two elements of G *commute*, i.e. $ab = ba$ for all $a, b \in G$.

EXERCISE 2.11. Suppose that S is a generating set of G. Then G is abelian if and only if $[a, b] = 1$ for all $a, b \in S$.

PROPOSITION 2.12. (1) *G' is a characteristic subgroup of G;*

(2) *G is* abelian *if and only if $G' = \{1\}$;*

(3) *$G_{ab} = G/G'$ is an abelian group (called the* abelianization *of G);*

(4) *if $\varphi : G \to A$ is a homomorphism to an abelian group A, then φ factors through the abelianization: Given the quotient map $p : G \to G_{ab}$, there exists a homomorphism $\overline{\varphi} : G_{ab} \to A$ such that $\varphi = \overline{\varphi} \circ p$.*

PROOF. (1) The set $S = \{[x, y] \mid x, y \in G\}$ is a generating set of G' and for every automorphism $\psi : G \to G$, $\psi(S) = S$.

Part (2) follows from the equivalence $xy = yx \Leftrightarrow [x, y] = 1$, and (3) is an immediate consequence of (2).

Part (4) follows from the fact that $\varphi(S) = \{1\}$. $\square$

Recall that the *finite dihedral group* of order $2n$, denoted by D_{2n} or $I_2(n)$, is the group of symmetries of the regular Euclidean n-gon, i.e. the group of isometries of the unit circle $\mathbb{S}^1 \subset \mathbb{C}$ generated by the rotation $r(z) = e^{\frac{2\pi i}{n}} z$ and the reflection $s(z) = \bar{z}$. Likewise, the *infinite dihedral group* D_∞ is the group of isometries of $\mathbb{Z}$ (with the metric induced from $\mathbb{R}$); the group D_∞ is generated by the translation $t(x) = x + 1$ and the symmetry $s(x) = -x$.

EXERCISE 2.13. Find the commutator subgroup and the abelianization for the finite dihedral group D_{2n} and for the infinite dihedral group D_∞.

EXERCISE 2.14. Let S_n (the symmetric group on n symbols) be the group of permutations of the set $\{1, 2, \ldots, n\}$, and $A_n < S_n$ be the alternating subgroup, consisting of even permutations.

(1) Prove that for every $n \notin \{2, 4\}$ the group A_n is generated by the set of cycles of length 3.

(2) Prove that if $n \geqslant 3$, then for every cycle σ of length 3 there exists $\rho \in S_n$ such that $\sigma^2 = \rho\sigma\rho^{-1}$.

(3) Use (1) and (2) to find the commutator subgroup and the abelianization for A_n and for S_n.

Note that it is not necessarily true that the commutator subgroup G' of G consists entirely of commutators $\{[x, y] : x, y \in G\}$. However, occasionally, every element of the derived subgroup is indeed a single commutator. For instance, every element of the alternating group $A_n < S_n$ is the commutator in S_n, see **[Ore51]**.

2.3. Semidirect products and short exact sequences

Let $G_i, i \in I$, be a collection of groups. The *direct product* of these groups, denoted

$$G = \prod_{i \in I} G_i$$

is the Cartesian product of the sets G_i with the group operation given by

$$(a_i) \cdot (b_i) = (a_i b_i).$$

Note that each group G_i is the quotient of G by the (normal) subgroup

$$\prod_{j \in I \setminus \{i\}} G_j.$$

A group G is said to *split* as a direct product of its normal subgroups $N_i \lhd G, i = 1, \ldots, k$, if one of the following equivalent statements holds:

- $G = N_1 \cdots N_k$ and
$$N_i \cap N_1 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_k = \{1\} \text{ for all } i;$$
- for every element g of G there exists a unique k-tuple
$$(n_1, \ldots, n_k), n_i \in N_i, i = 1, \ldots, k$$
such that $g = n_1 \cdots n_k$.

Then, G is isomorphic to the direct product $N_1 \times \ldots \times N_k$. Thus, finite direct products G can be defined either *extrinsically*, using groups N_i as quotients of G, or *intrinsically*, using normal subgroups N_i of G.

Similarly, one defines *semidirect products* of two groups, by taking the above *intrinsic* definition and relaxing the normality assumption:

Definition 2.15. (1) (*with the ambient group as the given data*) A group G is said to *split as a semidirect product of two subgroups* N and H, which is denoted by $G = N \rtimes H$, if and only if N is a *normal subgroup* of G, H is a *subgroup* of G, and one of the following equivalent statements holds:

- $G = NH$ and $N \cap H = \{1\}$;
- $G = HN$ and $N \cap H = \{1\}$;
- for every element g of G there exists a unique $n \in N$ and $h \in H$ such that $g = nh$;
- for every element g of G there exists a unique $n \in N$ and $h \in H$ such that $g = hn$;
- there exists *a retraction* $G \to H$, i.e. a homomorphism which restricts to the identity on H, and whose kernel is N.

Observe that the map $\varphi : H \to \mathrm{Aut}\,(N)$ defined by $\varphi(h)(n) = hnh^{-1}$, is a group homomorphism.

(2) (*with the quotient groups as the given data*) Given any two groups N and H (not necessarily subgroups of the same group) and a group homomorphism $\varphi : H \to \mathrm{Aut}\,(N)$, one can define a new group $G = N \rtimes_\varphi H$ which is a semidirect product of a copy of N and a copy of H in the above sense, defined as follows. As a set, $N \rtimes_\varphi H$ is defined as the cartesian product $N \times H$. The binary operation $*$ on G is defined by

$$(n_1, h_1) * (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)\,,\ \forall n_1, n_2 \in N \text{ and } h_1, h_2 \in H\,.$$

The group $G = N \rtimes_\varphi H$ is called the *semidirect product of N and H with respect to φ.*

REMARKS 2.16. (1) If a group G is the semidirect product of a normal subgroup N with a subgroup H in the sense of (1), then G is isomorphic to $N \rtimes_\varphi H$ defined as in (2), where

$$\varphi(h)(n) = hnh^{-1}\,.$$

(2) The group $N \rtimes_\varphi H$ defined in (2) is a semidirect product of the normal subgroup $N_1 = N \times \{1\}$ and the subgroup $H = \{1\} \times H$ in the sense of (1).

(3) If both N and H are normal subgroups in (1), then G is a direct product of N and H.

If φ is the trivial homomorphism, sending every element of H to the identity automorphism of N, then $N \rtimes_\phi H$ is the direct product $N \times H$.

Here is yet another way to define semidirect products. An *exact sequence* is a sequence of groups and group homomorphisms

$$\dots G_{n-1} \stackrel{\varphi_{n-1}}{\longrightarrow} G_n \stackrel{\varphi_n}{\longrightarrow} G_{n+1} \dots$$

such that $\operatorname{Im}\varphi_{n-1} = \operatorname{Ker}\varphi_n$ for every n. A *short exact sequence* is an exact sequence of the form:

$$\{1\} \longrightarrow N \stackrel{\varphi}{\longrightarrow} G \stackrel{\psi}{\longrightarrow} H \longrightarrow \{1\}\,. \tag{2.1}$$

In other words, φ is an isomorphism from N to a normal subgroup $N' \lhd G$ and ψ descends to an isomorphism $G/N' \simeq H$.

DEFINITION 2.17. A short exact sequence *splits* if there exists a homomorphism $\sigma : H \to G$ (called a *section*) such that

$$\psi \circ \sigma = \mathrm{Id}\,.$$

When the sequence splits we shall sometimes write it as

$$1 \to N \to G \underset{\curvearrowleft}{\to} H \to 1.$$

Every split exact sequence determines a decomposition of G as the semidirect product $\varphi(N) \rtimes \sigma(H)$. Conversely, every semidirect product decomposition $G = N \rtimes H$ defines a split exact sequence, where φ is the identity embedding and $\psi : G \to H$ is the retraction.

EXAMPLES 2.18. (1) The dihedral group D_{2n} is isomorphic to $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$, where $\varphi(1)(k) = n - k$.

(2) The infinite dihedral group D_∞ is isomorphic to $\mathbb{Z} \rtimes_\varphi \mathbb{Z}_2$, where $\varphi(1)(k) = -k$.

(3) The permutation group S_n is the semidirect product of A_n and $\mathbb{Z}_2 = \{\mathrm{Id}, (12)\}$.

(4) The group $(\mathrm{Aff}(\mathbb{R})\,, \circ)$ of affine maps $f : \mathbb{R} \to \mathbb{R}, f(x) = ax + b\,$, with $a \in \mathbb{R}^*$ and $b \in \mathbb{R}$ is a semidirect product $\mathbb{R} \rtimes_\varphi \mathbb{R}^*$, where $\varphi(a)(x) = ax$.

PROPOSITION 2.19. (1) *Every isometry ϕ of $\mathbb{R}^n$ is of the form $\phi(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$, where $\mathbf{b} \in \mathbb{R}^n$ and $A \in O(n)$.*

(2) *The group* $\mathrm{Isom}(\mathbb{R}^n)$ *splits as the semidirect product* $\mathbb{R}^n \rtimes O(n)$*, with the obvious action of the orthogonal group* $O(n)$ *on* $\mathbb{R}^n$*.*

Sketch of proof of (1). For every vector $\mathbf{a} \in \mathbb{R}^n$ we denote by $T_{\mathbf{a}}$ the translation of vector $\mathbf{a}$, $\mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$.

If $\phi(\mathbf{0}) = \mathbf{b}$, then the isometry $\psi = T_{-\mathbf{b}} \circ \phi$ fixes the origin $\mathbf{0}$. Thus, it suffices to prove that an isometry fixing the origin is an element of $O(n)$. Indeed:

- an isometry of $\mathbb{R}^n$ preserves straight lines, because these are bi-infinite geodesics;
- an isometry is a homogeneous map, i.e. $\psi(\lambda\mathbf{v}) = \lambda\psi(\mathbf{v})$; this is due to the fact that (for $0 < \lambda \leqslant 1$) $\mathbf{w} = \lambda\mathbf{v}$ is the unique point in $\mathbb{R}^n$ satisfying

$$d(\mathbf{0}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v}) = d(\mathbf{0}, \mathbf{v}).$$

- an isometry map is an additive map, i.e. $\psi(\mathbf{a}+\mathbf{b}) = \psi(\mathbf{a}) + \psi(\mathbf{b})$ because an isometry preserves parallelograms.

Thus, ψ is a linear transformation of $\mathbb{R}^n$, $\psi(\mathbf{x}) = A\mathbf{x}$ for some matrix A. The orthogonality of the matrix A follows from the fact that the image of an orthonormal basis under ψ is again an orthonormal basis.

EXERCISE 2.20. 1. Prove the statement (2) of Proposition 2.19. Note that $\mathbb{R}^n$ is identified with the group of translations of the n-dimensional affine space *via* the map $\mathbf{b} \mapsto T_{\mathbf{b}}$.

2. Suppose that G is a subgroup of $\mathrm{Isom}(\mathbb{R}^n)$. Is it true that G is isomorphic to the semidirect product $T \rtimes Q$, where $T = G \cap \mathbb{R}^n$ and Q is the projection of G to $O(n)$?

2.4. Free abelian groups

DEFINITION 2.21. A group G is called *free abelian* on a generating set S if it is isomorphic to the direct sum

$$\bigoplus_{s\in S} \mathbb{Z}.$$

The minimal cardinality of S is called *the rank of* G and denoted $\mathrm{rank}\,(G)$, the set S is called a *basis* of G.

Of course, if $|S| = n$, $G \cong \mathbb{Z}^n$. Given an abelian group G, we define its subgroup

$$2G = \{2x : x \in G\}.$$

Clearly, this subgroup is *characteristic* in G, i.e. is invariant under all automorphisms of G. Then, for the free abelian group $G = \oplus_{s\in S}\mathbb{Z}$, the quotient $G/2G$ is isomorphic to

$$\bigoplus_{s\in S} \mathbb{Z}_2,$$

which has natural structure of a vector space over $\mathbb{Z}_2$ with basis S. Since any two bases of a vector space have the same cardinality, it follows that two bases of a free abelian group have the same cardinality, equal to $\mathrm{rank}\,(G)$.

EXERCISE 2.22. Every free abelian group is torsion-free.

Below is a characterization of free abelian groups by a *universality property*:

THEOREM 2.23. *Let G be an abelian group and X is a subset of G. The group G is free abelian with basis X if and only if it satisfies the following* universality property*: For every abelian group A, every map $f : X \to A$ extends to a unique homomorphism $f : G \to A$.*

PROOF. Suppose that G is free abelian with the basis X. Every element $g \in G$ is uniquely represented as a sum

$$g = \sum_{x \in X} m_x \cdot x, m_x \in \mathbb{Z}$$

with only finitely many non-zero terms. Then, we extend f to G by

$$f(g) = \sum_{x \in X} m_x \cdot f(x).$$

It is clear that this extension is unique.

Conversely, assume that $(G_1, X_1), (G_2, X_2)$ satisfy the universality property and $f : X_1 \to X_2$ is a bijection. Then f and $f^{-1} = \bar{f} : X_2 \to X_1$ admit homomorphic extensions $F : G_1 \to G_2$, $\bar{F} : G_2 \to G_1$ respectively. The compositions $\bar{F} \circ F, F \circ \bar{F}$ are homomorphisms $\phi : G_1 \to G_1, \psi : G_2 \to G_2$, respectively. These homomorphisms extend the identity maps $X_2 \to X_2, X_1 \to X_1$. By the uniqueness part of the universality property, it follows that ϕ and ψ are the identity maps. Therefore, the homomorphism $F : G_1 \to G_2$ is an isomorphism. Applying this to $G_1 = G, X_1 = X$ and G_2 equal to the free abelian group with the basis $X_2 = X_1 = X$, we conclude that G is free abelian with the basis X. □

COROLLARY 2.24. *Let $0 \to A \to B \xrightarrow{r} C \to 0$ be a short exact sequence of abelian groups, where C is free abelian. Then this sequence splits and $B \cong A \oplus C$.*

PROOF. Let $c_i, i \in I$, denote a basis of C. Then, since r is surjective, for every c_i there exists $b_i \in B$ such that $r(b_i) = c_i$. By the universal property of free abelian groups, the map $s : c_i \to b_i$ extends to a homomorphism $s : C \to B$ such that $r \circ s = \mathrm{Id}$. □

EXERCISE 2.25. Show that a group G is free abelian with basis S if and only if G admits the presentation

$$\langle S | [s, s'] = 1, \forall s, s' \in S \rangle .$$

THEOREM 2.26. *1. Subgroups of free abelian groups are again free abelian.*
2. If $G < F$ is a subgroup of a free abelian group F, then $\mathrm{rank}\,(G) \leqslant \mathrm{rank}\,(F)$.

PROOF. Let X be a basis of a free abelian group $F = A_X$. For each subset Y of X let A_Y be the free group with the basis Y, thus A_Y embeds naturally as a free abelian subgroup A_Y in F. We fix a subgroup $G \leqslant F$ once and for all; for each $Y \subset X$ we let G_Y denote the intersection $G \cap A_Y$.

Define the set S consisting of triples (G_Y, B, ϕ), where Y ranges over the set of all subsets of X such that G_Y is free with a basis of cardinality at most the cardinality of X; the sets B are bases of such G_Y, and ϕ is an injective map $\phi : B \to X$.

The set S is non-empty, as we can take $Y = \emptyset$.

We define a partial order $\leqslant$ on S by:

$$(G_Y, B, \phi) \leqslant (G_Z, C, \psi) \iff Y \subset Z, B \subset C, \quad \phi = \psi|_B.$$

Suppose that L is a chain in the above order indexed by an ordered set M:

$$\{(G_{Y_m}, B_m, \phi_m), m \in M\}, (G_{Y_m}, B_m, \phi_m) \leqslant (G_{Y_n}, B_n, \phi_n) \iff m \leqslant n.$$

Then the union

$$\bigcup_{m \in M} G_{Y_m}$$

is again a subgroup in F and the set

$$C = \bigcup_{m \in M} B_m$$

is a basis in the above group. Furthermore, the maps ϕ_m determine an embedding $\psi : C \hookrightarrow X$. Thus,

$$(\bigcup_{m \in M} G_{Y_m}, C, \psi) \in S.$$

Therefore, by Zorn's Lemma, there exists a maximal element (G_Y, B, ϕ) of S. If $Y = X$ then $G_Y = G$ and we are done. Suppose that there exists $x \in X \setminus Y$. Set $Z := Y \cup \{x\}$. We will show that G_Z is still free abelian with a basis C containing B and ϕ extends to an embedding $\psi : Z \to X$. If $G_Z = G_Y$, we take $C = B$, $\psi = \phi$. Otherwise, assume that $G_Z/G_Y \neq 0$. The quotient A_Z/A_Y is isomorphic to $\mathbb{Z}$ and is generated by the image $\bar{x}$ of x. The image of G_Z in this quotient is isomorphic to G_Z/G_Y and is generated by some $n \cdot \bar{x}$, $n \in \mathbb{Z} \setminus 0$. Let $g \in G_Z$ be an element which maps to $n \cdot \bar{x}$. The mapping $G_Z/G_Y \to \langle g \rangle$ splits the sequence

$$0 \to G_Y \to G_Z \to G_Z/G_Y = \mathbb{Z} \to 0$$

and, hence,

$$G_Z \cong G_Y \oplus \langle g \rangle .$$

This means that $C := B \cup \{g\}$ is a basis of G_Z; we extend ϕ to C by $\psi(g) = x$. Thus, $(G_Z, C, \psi) \in S$. This contradicts maximality of (G_Y, B, ϕ).

We conclude that G is free abelian and its basis embeds in a basis of F. □

2.5. Classification of finitely generated abelian groups

THEOREM 2.27. *Every finitely generated abelian group A is isomorphic to a finite direct sum of cyclic groups.*

PROOF. The proof below is taken from [**Mil12**]. The proof is induction on the number of generators of A.

If A is 1-generated, the assertion is clear. Assume that the assertion holds for abelian groups with $\leqslant n-1$ generators and suppose that A is an abelian group generated by n elements. Consider all ordered generating sets $(a_1, ..., a_n)$ of A. Among such generating sets choose one, $S = (a_1, ..., a_n)$, such that the order of a_1 (denoted $|a_1|$) is the least possible. We claim that

$$A \cong \langle a_1 \rangle \oplus A' = \langle a_1 \rangle \oplus \langle a_2, ..., a_n \rangle .$$

(This claim will imply the assertion since, inductively, A' splits as a direct sum of cyclic groups.) Indeed, if A is not the direct sum as above, then we have a non-trivial relation

$$\sum_{i=1}^{n} r_i a_i = 0, r_i \in \mathbb{Z}, r_1 a_1 \neq 0. \tag{2.2}$$

Without loss of generality, $0 < r_1 < |a_1|$ and $r_i \geqslant 0, i = 1, ...n$ (otherwise, we replace a_i's with $-a_i$ whenever $r_i < 0$). Furthermore, let $d = gcd(r_1, ..., r_n)$ be the greatest common divisor of the numbers $r_i, i = 1, ..., n$. Set $q_i := \frac{r_i}{d}$.

LEMMA 2.28. *Suppose that $a_1, ..., a_n$ are generators of A and $q_1, ..., q_n \in \mathbb{Z}_+$ are such that $gcd(q_1, ..., q_n) = 1$. Then there exists a new generating set $b_1, ..., b_n$ of A such that*

$$b_1 = \sum_{i=1}^{n} q_i a_i.$$

PROOF. The proof of this lemma is a form of the Euclid's algorithm for computation of gcd. Note that $q := q_1 + ... + q_n \geqslant 1$. The proof of lemma is induction on q. If $q = 1$ then $b_1 \in \{a_1, ..., a_n\}$ and lemma follows. Suppose the assertion holds for all $q < m$, we will prove the claim for $q = m > 1$. After rearranging the indices, we can assume that $q_1 \geqslant q_2 > 0$.

Clearly, the set $\{a_1, a_1 + a_2, a_3, ..., a_n\}$ generates A. Furthermore,

$$gcd(q_1 - q_2, q_2, q_3, ..., q_n) = 1$$

and

$$q' := (q_1 - q_2) + q_2 + q_3 + ... + q_n < m$$

Thus, by the induction hypothesis, there exists a generating set $b'_1, ..., b'_n$ of A, where

$$b'_1 = (q_1 - q_2)a_1 + q_2(a_1 + a_2) + q_3 a_3 + ... + q_n a_n.$$

However, $b_1 = b'_1$. Lemma follows. $\square$

In view of this lemma, we get a new generating set $b_1, ..., b_n$ of A such that

$$b_1 = \sum_{i=1}^{n} \frac{r_i}{d} a_i.$$

The equation (2.2) implies that $db_1 = 0$ and $d \leqslant r_1 < |a_1|$. Thus, the ordered generating set $(b_1, ..., b_n)$ of A has the property that $|b_1| < |a_1|$, contradicting our choice of S. Theorem follows. $\square$

For a prime p, an abelian group A is called a *p-group* if every element $a \in A$ has the order which is a power of p. Clearly, each subgroup and each quotient of a p-group is again a p-group.

EXERCISE 2.29. A finite abelian group A is a p-group if and only if $|A| = p^\ell$ for some ℓ.

Given an abelian group A, we let $A(p)$ denote the subset of A consisting of elements whose order is a power of p. Since the sum of two elements of the orders p^k, p^m has the order p^n, where $n = \max(k, m)$, the subset $A(p)$ is a subgroup of A. A group T is said to be a *torsion group* if every element of T has finite order. For every abelian group G, the set $\mathrm{Tor}\,(G)$ of finite-order elements is a subgroup T of G, called the *torsion subgroup* $T \leqslant G$. This subgroup of G is characteristic.

EXERCISE 2.30. Every finitely generated abelian torsion group is finite.

THEOREM 2.31 (classification of abelian groups). *Suppose that A is a finitely generated abelian group. Then there exist an integer $r \geqslant 0$, and k-tuples of prime numbers $(p_1, \ldots, p_k)$ and natural numbers $(m_1, \ldots, m_k)$, for which*

$$A \simeq \mathbb{Z}^r \times \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}\,. \tag{2.3}$$

Here $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$, and whenever $p_i = p_{i+1}$, we have $m_i \geqslant m_{i+1}$. Furthermore, the number r, and the k-tuples $(p_1, \ldots, p_k)$ and $(m_1, \ldots, m_k)$ are uniquely determined by A.

PROOF. By Theorem 2.27, A is isomorphic to the direct product of finitely many cyclic groups

$$C_1 \times \ldots C_r \times C_{r+1} \times \ldots \times C_n,$$

where C_i is infinite cyclic for $i \leqslant r$ and finite cyclic for $i > r$.

EXERCISE 2.32. (Chinese remainder theorem) $\mathbb{Z}_s \times \mathbb{Z}_t \cong \mathbb{Z}_{st}$ if and only if the numbers s, t are coprime.

In view of this exercise, we can split every finite cyclic group C_i as a direct product of cyclic groups whose orders are prime powers. This proves existence of the decomposition (2.3).

We now consider the uniqueness part of the theorem. We first note that

$$\mathrm{Tor}\,(A) = C_{r+1} \times \ldots \times C_n,$$

which implies that

$$C_1 \times \ldots \times C_r \simeq \mathbb{Z}^r \simeq A/\mathrm{Tor}\,(A).$$

Since the subgroup $\mathrm{Tor}\,(A)$ is characteristic in A, it follows that the number r is uniquely determined by A.

Thus, in order to prove uniqueness of p_i's and m_i's it suffices to assume that A is finite. Since the primes p_i are the prime divisors of the order of A, the uniqueness question reduces to the case when $|A| = p^\ell$, i.e. when $A = A(p)$ is an abelian p-group. Suppose that A is an abelian p-group and

$$A \cong \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_k}}, \quad m_1 \geqslant \ldots \geqslant m_k.$$

Set $m = m_1$ and let $m_1 = m_2 = \ldots = m_d > m_{d+1}$. Clearly, the number p^m is the largest order of an element of A. The subgroup A_m of A generated by elements of this order is clearly characteristic and equals the d-fold direct product of copies of $\mathbb{Z}_{p^m}$,

$$\mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_d}}$$

in the above factorization of A. Hence, the number m_k and the number d depend only on the group A. We then divide A by A_m and proceed by induction. □

EXERCISE 2.33. The number r equals the rank of a maximal free abelian subgroup of A.

Theorem 2.27 implies that each finitely generated abelian group is isomorphic to a direct sum of finitely many cyclic groups C_i, which are unique up to an isomorphism.

DEFINITION 2.34. Generators of cyclic subgroups C_i such that

$$A = \oplus_{i=1}^{s} C_i$$

will be called *standard generators* of A. (These generators, of course, are not uniquely determined by A.)

Below are several immediate corollaries of Theorem 2.27.

Corollary 2.35. *Each finite abelian group A is isomorphic to the direct product of abelian p-groups:*

$$A \simeq A(p_1) \times \ldots A(p_k),$$

where $p_1, \ldots, p_k$ are the prime divisors of $|A|$.

Corollary 2.36. *Every finitely generated abelian group A is isomorphic to the direct product $F \times \mathrm{Tor}\,(A)$, where F is a free abelian group.*

Corollary 2.37. *A finitely generated abelian group is free abelian if and only if it is torsion-free.*

Exercise 2.38. 1. Show that the torsion-free abelian group $\mathbb{Q}$ is not a free abelian group.

2. Show that the image of the free abelian group F in A is not a characteristic subgroup of A (unless $A \simeq F$ or $A = \mathrm{Tor}\,(A)$).

Corollary 2.39. *Let G be an abelian group generated by n elements. Then every subgroup H of G is finitely generated (with $\leqslant n$ generators).*

Proof. Theorem 2.23 implies that there exists an epimorphism $\phi : \mathbb{Z}^n \to A$. Let $A := \phi^{-1}(H)$. Then, by Theorem 2.26, the subgroup A is free of rank $m \leqslant n$. Therefore, H is also m-generated. □

Exercise 2.40. Construct an example of a finitely generated abelian group G and a subgroup $H \leqslant G$, such that there is no direct product decomposition $G = F \times \mathrm{Tor}\,(G)$ for which $H = (F \cap H) \times (\mathrm{Tor}\,(G) \cap H)$. Hint: Take $G = \mathbb{Z} \times \mathbb{Z}_2$ and H infinite cyclic.

Exercise 2.41. Let F be a free abelian group of rank n and $B = \{x_1, ..., x_n\}$ be a generating set of F. Then B is a basis of F. Conclude that n equals the minimal cardinality of all generating sets of F.

Bibliography

[Mil12] J. S. Milne, *Group theory*, http://www.jmilne.org/math/CourseNotes/GT.pdf, 2012.
[Ore51] O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.