Infinite Groups

Cornelia Druţu

November 29, 2019

Abstract

These notes are, for the main part, based on chapters of the book [DK], with additional text from the lecture notes of Dan Segal, whom I would like to thank for kindly sharing his notes with me.

1 Notation and terminology

With very few exceptions, in a group G we use the multiplication sign $\cdot$ to denote its binary operation. We denote its identity element either by e or by 1. We denote the inverse of an element $g \in G$ by g^{-1}.

For abelian groups the neutral element may also be denoted by 0, the inverse of x by $-x$ and the binary operation by $+$. We will also frequently use the notation mg or $m \cdot g$ for the m-fold sum

$$\underbrace{g + \ldots + g}_{m \text{ times}},$$

with $m \in \mathbb{N}$. This extends to $m \in \mathbb{Z}$ by declaring that

$$0 \cdot g = 0 \in G$$

and that

$$-(m \cdot g) = (-m) \cdot g.$$

We use the notation

$$[x, y] = xyx^{-1}y^{-1}$$

for the *commutator* of elements x, y of a group G.

A surjective homomorphism is called an *epimorphism*, while an injective homomorphism is called a *monomorphism*. If two groups G and G' are isomorphic we write $G \simeq G'$. An isomorphism of groups $\varphi : G \to G$ is also called an *automorphism*. In what follows, we denote by $\mathrm{Aut}(G)$ the group of automorphisms of G.

We use the notation $H < G$ or $H \leqslant G$ to denote that H is a subgroup in G. Given a subgroup H in G:

- the *order* $|H|$ of H is its cardinality;
- the *index* of H in G, denoted $|G : H|$, is the common cardinality of the quotients G/H and $H\backslash G$.

We use the notation $H \lhd G$ to denote that H is a normal subgroup of G.

For every positive integer m we denote by $\mathbb{Z}_m$ *the cyclic group of order* m, $\mathbb{Z}/m\mathbb{Z}$. Given $x, y \in G$ we let x^y denote the conjugation of x by y, i.e. yxy^{-1}.

We say that two elements a and b in a group G are *conjugate* if there exists $c \in G$ with $b = a^c$.

If G is a group and Y is a subset of G then the *subgroup generated by* Y, denoted by $\langle Y \rangle$, is the smallest subgroup of G that contains Y, namely the set composed of the identity and of all products $y_1^{\pm 1} \dots y_n^{\pm 1}$ with $y_i \in Y$, $n \geq 1$. For homogeneity of notation, we make the convention that the identity corresponds to the case of a product (or word) as above with $n = 0$, that is, an *empty product* (or *word*). We say that Y *generates* G if $\langle Y \rangle = G$. See Revision notes for further details.

The *order* of an element g in a group $(G, \cdot)$ is the order of the subgroup $\langle g \rangle$ of G generated by g. In other words, the order of g is the minimal positive integer n such that $g^n = 1$. If no such integer exists, then g is said to be *of infinite order*. In this case, $\langle g \rangle$ is isomorphic to $\mathbb{Z}$.

Definition 1.1. A group G is a *torsion group* if all its elements have finite order.

A group G is said to be *without torsion* (or *torsion-free*) if all its non-trivial elements have infinite order.

Note that the subset $\operatorname{Tor} G = \{g \in G \mid g \text{ of finite order}\}$ of the group G, sometimes called the *torsion* of G, is in general not a subgroup.

Definition 1.2. A group G is said to have property * *virtually* if some finite-index subgroup H of G has the property *.

For instance, a group is *virtually torsion-free* if it contains a torsion-free subgroup of finite index, a group is *virtually abelian* if it contains an abelian subgroup of finite index and a *virtually free group* is a group that contains a free subgroup of finite index.

2 Direct sums and wreath products

When providing examples, the following two constructions of groups will be very useful.

Let X be a non-empty set, and let $\mathcal{G} = \{G_x \mid x \in X\}$ be a collection of groups indexed by X. Consider the set of maps $Map_f(X, \mathcal{G})$ with finite support, i.e.

$$Map_f(X, \mathcal{G}) := \{f : X \to \bigsqcup_{x \in X} G_x \mid f(x) \in G_x\,,\ f(x) \neq 1_{G_x}$$

$$\text{for only finitely many } x \in X\}\,.$$

Definition 2.1. The *direct sum* $\bigoplus_{x\in X} G_x$ is defined as $Map_f(X, \mathcal{G})$, endowed with the pointwise multiplication of functions:

$$(f \cdot g)(x) = f(x) \cdot g(x)\,,\ \forall x \in X.$$

Clearly, if A_x are abelian groups, then $\bigoplus_{x\in X} A_x$ is abelian.

When $G_x = G$ is the same group for all $x \in X$, the direct sum is the set of maps

$$Map_f(X, G) := \{f : X \to G \mid f(x) \neq 1_G \text{ for only finitely many } x \in X\}\,,$$

and we denote it either by $\bigoplus_{x\in X} G$ or by $G^{\oplus X}$.

If, in this latter case, the set X is itself a group H, then there is a natural action of H on the direct sum, defined by

$$\varphi : H \to \text{Aut}\left(\bigoplus_{h\in H} G\right)\,,\ \varphi(h)f(x) = f(h^{-1}x)\,,\ \forall x \in H\,.$$

Thus, we define the semidirect product

$$\left(\bigoplus_{h\in H} G\right) \rtimes_\varphi H\,. \tag{1}$$

Definition 2.2. The semidirect product (1) is called *the wreath product of G with H*, and it is denoted by $G \wr H$. The wreath product $G = \mathbb{Z}_2 \wr \mathbb{Z}$ is called the *lamplighter group*.

3 Finitely generated and finitely presented groups

3.1 Finitely generated groups

A group that has a finite generating set is called *finitely generated*.

Definition 3.1. The *rank* of a finitely generated group G, denoted $\text{rank}\,(G)$, is the minimal number o generators of G.

Exercise 3.2. Show that every finitely generated group is countable.

Examples 3.3.
1. The group $(\mathbb{Z}, +)$ is finitely generated by both $\{1\}$ and $\{-1\}$. Also, any set $\{p, q\}$ of coprime integers generates $\mathbb{Z}$.
2. The group $(\mathbb{Q}, +)$ is not finitely generated.

Exercise 3.4. Prove that the transposition (12) and the cycle $(12\ldots n)$ generate the permutation group S_n.

Remarks 3.5. Every quotient $\bar{G}$ of a finitely generated group G is finitely generated; we can take as generators of $\bar{G}$ the images of the generators of G.

The converse of the above statement is clearly not true, the fact that a quotient G/N is finitely generated does not imply anything on the group, one needs to add an extra assumption: if N is a normal subgroup of G, and both N and G/N are finitely generated, then G is finitely generated. In terms of short exact sequences, this can be reformulated as follows

Lemma 3.6. *Suppose that we have a short exact sequence of groups*

$$\{1\} \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{\pi} G_3 \longrightarrow \{1\}\,, \tag{2}$$

such that the groups G_1, G_3 are finitely generated. Then G_2 is also finitely generated.

Proof. See Ex. Sheet 1. □

We will see in examples below that if N is a normal subgroup in a group G and G is finitely generated, it *does not* necessarily follow that N is finitely generated (not even if G is a semidirect product of N and G/N).

Example 3.7. Let G be the wreath product $\mathbb{Z} \wr \mathbb{Z} \cong N \ltimes \mathbb{Z}$, where N is the (countably) infinite direct sum of copies of $\mathbb{Z}$. Then G is 2-generated. On the other hand, the subgroup N is not finitely generated (see Ex. Sheet 1).

Example 3.8. Let H be the group of permutations of $\mathbb{Z}$ generated by the transposition $t = (01)$ and the translation map $s(i) = i + 1$. Let H_i be the group of permutations of $\mathbb{Z}$ supported on $[-i, i] = \{-i, -i+1, \ldots, 0, 1, \ldots, i-1, i\}$, and let H_ω be the group of finitely supported permutations of $\mathbb{Z}$ (i.e. the group of bijections $f : \mathbb{Z} \to \mathbb{Z}$ such that f is the identity outside a finite subset of $\mathbb{Z}$),

$$H_\omega = \bigcup_{i=0}^{\infty} H_i\,.$$

Then H_ω is a normal subgroup in H and $H/H_\omega \simeq \mathbb{Z}$, while H_ω is not finitely generated. (Ex. Sheet 1).

We will see later that a *finite index* subgroup of a finitely generated group is always finitely generated (Lemma 3.32).

Below we describe a finite generating set for the group $GL(n, \mathbb{Z})$. In the proof we use the *elementary matrices* $N_{i,j} = I_n + E_{i,j}$ $(i \neq j)$; here I_n is the identity $n \times n$ matrix and the matrix $E_{i,j}$ has a unique non-zero entry 1 in the intersection of the i–th row and the j–th column.

Proposition 3.9. *The group $GL(n, \mathbb{Z})$ is generated by*

$$s_1 = \begin{pmatrix} 0 & \ldots & & \ldots & 0 & 1 \\ 1 & \ddots & & & \vdots & 0 \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & 0 \end{pmatrix}, s_2 = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix},$$

$$s_3 = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, s_4 = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Proof. Step 1. The permutation group S_n acts (effectively) on $\mathbb{Z}^n$ by permuting the basis vectors; we thus obtain a monomorphism $\varphi : S_n \to GL(n, \mathbb{Z})$, so that $\varphi(12\dots n) = s_1$, $\varphi(12) = s_2$. Consider now the corresponding action of S_n on $n \times n$ matrices. Multiplication of a matrix by s_1 on the left permutes rows cyclically, multiplication to the right does the same with columns. Multiplication by s_2 on the left swaps the first two rows, multiplication to the right does the same with columns. Therefore, by multiplying an elementary matrix A by appropriate products of s_1, s_1^{-1} and s_2 on the left and on the right, we obtain the matrix s_3. In view of Exercise 3.4, the permutation $(12\dots n)$ and the transposition (12) generate the permutation group S_n. Thus, every elementary matrix N_{ij} is a product of s_1, s_1^{-1}, s_2 and s_3.

Let d_j denote the diagonal matrix with diagonal entries

$$(1, \dots, 1, -1, 1, \dots 1),$$

where -1 occurs in j-th place. Thus, $d_1 = s_4$. The same argument as above shows that for every d_j and $s = (1j) \in S_n$, $sd_js = d_1$. Thus, all diagonal matrices d_j belong to the subgroup generated by s_1, s_2 and s_4.

Step 2. Now, let g be an arbitrary element in $GL(n, \mathbb{Z})$. Let $a_1, \dots, a_n$ be the entries of the first column of g. We will prove that there exists an element p in $\langle s_1, s_2, s_3, s_4\rangle \subset GL(n, \mathbb{Z})$, such that pg has the entries $1, 0, \dots, 0$ in its first column. We argue by induction on $k = C_1(g) = |a_1| + \dots + |a_n|$. Note that $k \geqslant 1$. If $k = 1$, then $(a_1, \dots, a_n)$ is a permutation of $(\pm 1, 0, \dots, 0)$; hence, it suffices to take p in $\langle s_1\,, s_2, s_4\rangle$ permuting the rows so as to obtain $1, 0, \dots, 0$ in the first column.

Assume that the statement is true for all integers $1 \leqslant i < k$; we will prove it for k. After to permuting rows and multiplying by $d_1 = s_4$ and d_2, we may assume that $a_1 > a_2 > 0$. Then $N_{1,2}d_2g$ has the following entries in the first column: $a_1 - a_2, -a_2, a_3, \dots a_n$. Therefore, $C_1\left(N_{1,2}d_2g\right) < C_1(g)$. By the induction assumption, there exists an element p of $\langle s_1, s_2, s_3, s_4\rangle$ such that $pN_{1,2}d_2g$ has the entries of its first column equal to $1, 0, \dots, 0$. This proves the claim.

Step 3. We leave it to the reader to check that for every pair of matrices $A, B \in GL(n-1, \mathbb{R})$ and row vectors $L = (l_1, \dots, l_{n-1})$ and $M = (m_1, \dots, m_{n-1})$

$$\begin{pmatrix} 1 & L \\ 0 & A \end{pmatrix} \cdot \begin{pmatrix} 1 & M \\ 0 & B \end{pmatrix} = \begin{pmatrix} 1 & M + LB \\ 0 & AB \end{pmatrix}.$$

Therefore, the set of matrices

$$\left\{ \begin{pmatrix} 1 & L \\ 0 & A \end{pmatrix} \; ; \; A \in GL(n-1,\mathbb{Z}) \, , \, L \in \mathbb{Z}^{n-1} \right\}$$

is a subgroup of $GL(n,\mathbb{Z})$ isomorphic to $\mathbb{Z}^{n-1} \rtimes GL(n-1,\mathbb{Z})$.

Using this, an induction on n and Step 2, one shows that there exists an element p in $\langle s_1, s_2, s_3, s_4 \rangle$ such that pg is upper triangular and with entries on the diagonal equal to 1. It therefore suffices to prove that every integer upper triangular matrix as above is in $\langle s_1, s_2, s_3, s_4 \rangle$. This can be done for instance by multiplying such a matrix to the right with matrices of the form $d_1 N_{1i}^{a_{1i}} d_1$, until all the entries on the first row become zero, except the diagonal one which remains 1; then by multiplying with $d_2 N_{2i}^{a_{2i}} d_2$ to perform the same operation on the second row etc. In the end we obtain the identity matrix, and can therefore deduce that every integer upper triangular matrix with entries on the diagonal equal to 1 is a product of matrices $d_i, i \in \{1, 2, \ldots, n\}$, and $N_{jk}, j, k \in \{1, 2, \ldots, n\}$, and is therefore in $\langle s_1, s_2, s_3, s_4 \rangle$. □

3.2 Free groups

What is the 'largest' group that can be generated by a set with n elements (more generally, a set of a given cardinality) ? Such a group G, generated by a set of n elements X, should have the following property: given any group H, generated by a set of at most n elements Y, any surjection $X \to Y$ has an extension $G \to H$ that is an epimorphism. Clearly, this extension must be unique, and clearly this property implies that given any group K, every map $X \to K$ extends to a homomorphism $G \to K$ (also unique). Does such a group exist ? In what follows we describe a way to construct it.

Let X be a set. Its elements are called *letters* or *symbols*. We define the set of *inverse letters* (or *inverse symbols*) $X^{-1} = \{a^{-1} \mid a \in X\}$. We will think of $X \cup X^{-1}$ as an *alphabet*.

A *word* in $X \cup X^{-1}$ is a finite (possibly empty) string of letters in $X \cup X^{-1}$, i.e. an expression of the form

$$a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_k}^{\epsilon_k},$$

where $a_i \in X, \epsilon_i = \pm 1$; here $x^1 = x$ for every $x \in X$. We will use the notation 1 for the *empty word* (the one that has no letters).

Convention 3.10. Sometimes, by abusing the terminology, we will refer to words in $X \cup X^{-1}$ as *words in* X.

Denote by X^* the set of words in the alphabet $X \cup X^{-1}$, where the empty word, denoted by 1, is included. For instance,

$$a_1 a_2 a_1^{-1} a_2 a_2 a_1 \in X^*.$$

The *length* of a word w is the number of letters in this word. The length of the empty word is 0.

A word $w \in X^*$ is *reduced* if it contains no pair of consecutive letters of the form aa^{-1} or $a^{-1}a$. The *reduction* of a word $w \in X^*$ is the deletion of all pairs of consecutive letters of the form aa^{-1} or $a^{-1}a$.

For instance, the words

$$1, a_2a_1, a_1a_2a_1^{-1}$$

are reduced, while

$$a_2a_1a_1^{-1}a_3$$

is not reduced.

More generally, a word w is *cyclically reduced* if it is reduced and, in addition, the first and the last letters of w are not inverses of each other. Equivalently, conjugating w by an element of $X \cup X^{-1}$:

$$w' = awa^{-1}, \quad a \in X \cup X^{-1}$$

results in a word w' whose reduction has length $\gg$ the length of w.

We define an equivalence relation on X^* by $w \sim w'$ if w can be obtained from w' by a finite sequence of reductions and their inverses, i.e. the relation $\sim$ on X^* is generated by

$$ua_ia_i^{-1}v \sim uv, \quad ua_i^{-1}a_iv \sim uv$$

where $u, v \in X^*$.

Proposition 3.11. *Any word $w \in X^*$ is equivalent to a unique reduced word.*

Proof. Existence. We prove the statement by induction on the length of a word. For words of length 0 and 1 the statement is clearly true. Assume that it is true for words of length n and consider a word of length $n+1$, $w = a_1 \cdots a_n a_{n+1}$, where $a_i \in X \cup X^{-1}$. According to the induction hypothesis, there exists a reduced word $u = b_1 \cdots b_k$ with $b_j \in X \cup X^{-1}$ such that $a_2 \cdots a_{n+1} \sim u$. Then $w \sim a_1u$. If $a_1 \neq b_1^{-1}$ then a_1u is reduced. If $a_1 = b_1^{-1}$ then $a_1u \sim b_2 \cdots b_k$ and the latter word is reduced.

Uniqueness. Let $F(X)$ be the set of reduced words in $X \cup X^{-1}$. For every $a \in X \cup X^{-1}$ we define a map $L_a : F(X) \to F(X)$ by

$$L_a(b_1 \cdots b_k) = \begin{cases} ab_1 \cdots b_k & \text{if} \quad a \neq b_1^{-1}, \\ b_2 \cdots b_k & \text{if} \quad a = b_1^{-1}. \end{cases}$$

For every word $w = a_1 \cdots a_n$ define $L_w = L_{a_1} \circ \cdots \circ L_{a_n}$. For the empty word 1 define $L_1 = \mathrm{id}$. It is easy to check that $L_a \circ L_{a^{-1}} = \mathrm{id}$ for every $a \in X \cup X^{-1}$, and to deduce from it that $v \sim w$ implies $L_v = L_w$.

We prove by induction on the length that if w is reduced then $w = L_w(1)$. The statement clearly holds for w of length 0 and 1. Assume that it is true for reduced words of length n and let w be a reduced word of length $n+1$. Then $w = au$, where $a \in X \cup X^{-1}$ and u is a reduced word that does not begin with a^{-1}, i.e. such that $L_a(u) = au$. Then $L_w(1) = L_a \circ L_u(1) = L_a(u) = au = w$.

In order to prove uniqueness it suffices to prove that if $v \sim w$ and v, w are reduced then $v = w$. Since $v \sim w$ it follows that $L_v = L_w$, hence $L_v(1) = L_w(1)$, that is $v = w$. □

Let $F(X)$ be the set of reduced words in $X \cup X^{-1}$. Proposition 3.11 implies that $X^*/\sim$ can be identified with $F(X)$.

Definition 3.12. The *free group over* X is the set $F(X)$ endowed with the product $*$ defined by: $w * w'$ is the unique reduced word equivalent to the word ww'. The unit is the empty word.

The cardinality of X is called the *rank* of the free group $F(X)$.

We note that, at the moment, we have two, *a priori* distinct, notions of rank for (finitely generated) free groups: one is the least number of generators and the second is the cardinality of the set X. We will see, however, that the two numbers are the same.

The set $F = F(X)$ with the product defined in Definition 3.12 is indeed a group. The inverse of a reduced word

$$w = a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_k}^{\epsilon_k}$$

is given by

$$w^{-1} = a_{i_k}^{-\epsilon_k} a_{i_{k-1}}^{-\epsilon_{k-1}} \cdots a_{i_1}^{-\epsilon_1}.$$

It is clear that the product ww^{-1} projects to the empty word 1 in F.

Exercise 3.13. A free group of rank at least 2 is not abelian. Thus, *free non-abelian* means 'free of rank at least 2.'

We sometimes say that X *freely generates* $F(X)$ or that X is a basis of $F(X)$. Given an isomorphism $\varphi : F(X) \to G$, the same terminology applies to G and $\varphi(X)$.

Proposition 3.14 (Universal property of free groups)**.** *A map $\varphi : X \to G$ from the set X to a group G can be extended to a homomorphism $\Phi : F(X) \to G$ and this extension is unique.*

Proof. Existence. The map φ can be extended to a map on $X \cup X^{-1}$ (which we denote also φ) by $\varphi(a^{-1}) = \varphi(a)^{-1}$.

For every reduced word $w = a_1 \cdots a_n$ in $F = F(X)$ define

$$\Phi(a_1 \cdots a_n) = \varphi(a_1) \cdots \varphi(a_n).$$

Set $\Phi(1_F) := 1_G$, the identity element of G. We leave it to the reader to check that Φ is a homomorphism.

Uniqueness. Let $\Psi : F(X) \to G$ be a homomorphism such that $\Psi(x) = \varphi(x)$ for every $x \in X$. Then for every reduced word $w = a_1 \cdots a_n$ in $F(X)$,

$$\Psi(w) = \Psi(a_1) \cdots \Psi(a_n) = \varphi(a_1) \cdots \varphi(a_n) = \Phi(w).$$

□

Corollary 3.15. *Every group is the quotient of a free group.*

Proof. Apply Proposition 3.14 to the group G and a generating set X of G (e.g., $X = G$). □

Lemma 3.16. *Every short exact sequence* $1 \to N \to G \xrightarrow{r} F(X) \to 1$ *splits. In particular,* G *contains a subgroup isomorphic to* $F(X)$.

Proof. See Ex. Sheet 1. □

Corollary 3.17. *Every short exact sequence* $1 \to N \to G \to \mathbb{Z} \to 1$ *splits.*

3.3 Ping-pong lemma. Examples of free groups

The ping-pong lemma is a simple, yet powerful, tool for constructing free groups acting on sets.

The setup for the ping-pong lemma is a pair of bijections $g_1, g_2 \in Bij(X)$ ("ping-pong partners") and a quadruple of non-empty subsets

$$B_i^{\pm} \subset X, \quad i = 1, 2.$$

Define

$$C_i^+ := B_i^+ \cup B_j^- \cup B_j^+, C_i^- := B_i^- \cup B_j^- \cup B_j^+ \quad \{i, j\} = \{1, 2\}.$$

We require that:
$C_i^{\pm} \not\subset B_j^{\pm}$ and $C_i^{\pm} \not\subset B_j^{\mp}$ for all choices of i, j and $+, -$.

Typically, this is achieved by assuming that all the four sets $B_1^{\pm}, B_2^{\pm}$ are pairwise disjoint and non-empty.

Lemma 3.18 (Ping–pong, or table–tennis, lemma)**.** *Let* X, $B_i^{\pm}, C_i^{\pm}$ *be as above, and suppose that*

$$g_i^{\pm 1}(C_i^{\pm}) \subset B_i^{\pm}, \quad i = 1, 2.$$

Then the bijections g_1, g_2 *generate a rank 2 free subgroup of* $Bij(X)$.

Proof. Let w be a non-empty reduced word in $\{g, g^{-1}, h, h^{-1}\}$. In order to prove that w corresponds to a non-identity element of $Bij(X)$, it suffices to check that $w(C_j^{\pm}) \subset B_i^{\pm}$ for some i, j and for some choice of $+$ or $-$. We claim that whenever w has the form

$$w = g_i^{\pm 1} u g_j^{\pm 1},$$

we have

$$w(C_j^{\pm}) \subset B_i^{\pm}.$$

This would immediately imply that w does not represent the identity map $X \to X$. The claim is proven by induction on the length $\ell(w)$ of w. The statement is clear if $\ell(w) = 1$. Suppose it holds for all words w' of length n, we will prove it for words w or length $n + 1$. Such w has the form

$$w = g_i^{\pm 1} w', \quad \ell(w') = n.$$

Since the prefix of w' cannot equal $g_i^{\mp 1}$ (as w is a reduced word), it follows from the induction hypothesis that (for some j and a choice of $+, -$)

$$w'(C_j^{\pm}) \subset C_i^{\pm}.$$

Since

$$g_i^{\pm 1} w'(C_j^{\pm}) \subset g_i^{\pm 1}(C_i^{\pm}) \subset B_i^{\pm},$$

the claim follows. □

Exercise 3.19. Suppose that $g \in Bij(X)$ is a bijection such that for some $A \subset X$,

$$g(A) \subsetneq A.$$

Then g has infinite order.

Example 3.20. For any real number $r \geqslant 2$ the matrices

$$g_1 = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

generate a free subgroup of $SL(2, \mathbb{R})$.

First proof. The group $SL(2, \mathbb{R})$ acts (with the kernel $\pm I$) on the upper half plane $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by linear fractional transformations

$$z \mapsto \frac{az + b}{cz + d}.$$

Define quater-planes

$$B_1^+ = \{z \in \mathbb{H}^2 : \Re(z) > r/2, \quad B_1^- = \{z \in \mathbb{H}^2 : \Re(z) < -r/2\}$$

and open disks

$$B_2^+ := \{z \in \mathbb{H}^2 : |z - \frac{1}{r}| < \frac{1}{r}\}, \quad B_2^- := \{z \in \mathbb{H}^2 : |z + \frac{1}{r}| < \frac{1}{r}\}.$$

The reader will verify that $g_k, B_k^{\pm}, k = 1, 2$ satisfy the assumptions of Lemma 3.18. It follows that the group $\langle g_1, g_2 \rangle$ is free of rank 2.

Second proof. The group $SL(2, \mathbb{R})$ also acts linearly on $\mathbb{R}^2$. Consider the infinite cyclic subgroups $G_k = \langle g_k \rangle$, $i = 1, 2$ of $SL(2, \mathbb{R})$. Define the following subsets of $\mathbb{R}^2$

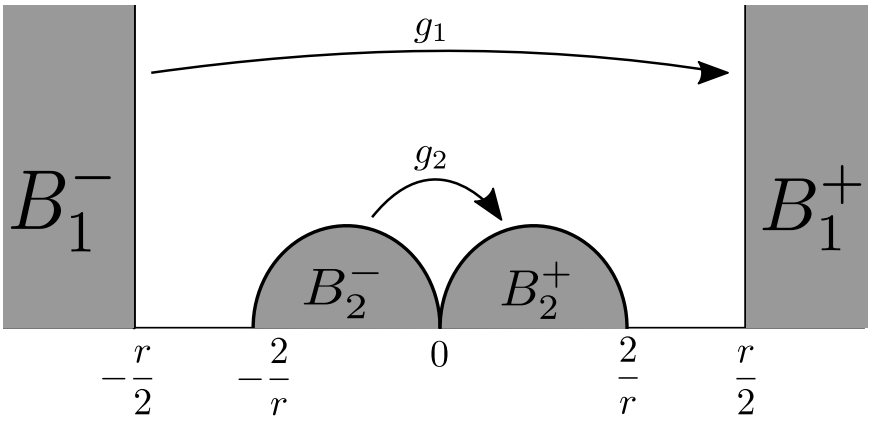
$$A_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : |x| > |y| \right\} \text{ and } A_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : |x| < |y| \right\}.$$

Then for each $g \in G_1 \setminus \{1\}$, $g(A_2) \subset A_1$ and for each $g \in G_2 \setminus \{1\}$, $g(A_1) \subset A_2$. Therefore, the subgroup of $SL(2, \mathbb{R})$ generated by g_1, g_2 is free of rank 2 according to Lemma **??**. □

Remark 3.21. The statement in the Example 3.20 no longer holds for $r = 1$. Indeed, in this case we have

$$g_1^{-1} g_2 g_1^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus, $(g_1^{-1} g_2 g_1^{-1})^2 = I$, and, hence, the group generated by g_1, g_2 is not free.



fig

Figure 1: Example of ping-pong.

3.4 Cayley graphs

A key method for studying groups is by treating them as geometric objects. The oldest, and most common, way to 'geometrize' groups, is by their *Cayley graphs*.

Every group may be turned into a geometric object (a graph) as follows. Given a group G and its generating set S, one defines the *Cayley graph* of G with respect to S. This is a directed graph $\mathrm{Cayley}_{\mathrm{dir}}(G, S)$ such that

- its set of vertices is G;
- its set of oriented edges is (g, gs), with $s \in S$.

Usually, the underlying non-oriented graph $\mathrm{Cayley}(G, S)$ of $\mathrm{Cayley}_{\mathrm{dir}}(G, S)$, i.e. the graph such that:

- its set of vertices is G;
- its set of edges consists of all pairs of elements in G, $\{g, h\}$, such that $h = gs$, with $s \in S$,

is also called the *Cayley graph of G with respect to S*.

We will also use the notation $\overline{gh}$ and $[g, h]$ for the edge $\{g, h\}$. In order to avoid the confusion with the notation for the commutator of the elements g and h we will always add the word *edge* in this situation.

Exercise 3.22. Show that the graph $\mathrm{Cayley}(G, S)$ is connected.

One can attach a *color* (*label*) from S to each oriented edge in $\mathrm{Cayley}_{\mathrm{dir}}(G, S)$: the edge (g, gs) is labeled by s.

We endow the graph $\mathrm{Cayley}(G, S)$ with the standard length metric (where every edge has unit length). The restriction of this metric to G is called *the word metric associated to S* and it is denoted by dist_S or d_S.

Notation 3.23. For an element $g \in G$ and a generating set S we denote $\mathrm{dist}_S(1, g)$ by $|g|_S$, the *word norm* of g. With this notation, $\mathrm{dist}_S(g, h) = |g^{-1}h|_S = |h^{-1}g|_S$.

Convention 3.24. In this course, unless stated otherwise, all Cayley graphs are defined for finite generating sets S.

Much of the discussion in this section, though, remains valid for arbitrary generating sets, including infinite ones.

Remark 3.25. 1. Every group acts on itself, on the left, by the left multiplication:

$$G \times G \to G\,,\ (g, h) \mapsto gh\,.$$

This action extends to any Cayley graph: if $[x, xs]$ is an edge of $\mathrm{Cayley}(G, S)$ with the vertices x, xs, we extend g to the isometry

$$g : [x, xs] \to [gx, gxs]$$

between the unit intervals. Both actions $G \curvearrowright G$ and $G \curvearrowright \mathrm{Cayley}(G, S)$ are by isometries. It is also clear that the action on G is free, while the action on $\mathrm{Cayley}(G, S)$ is free if and only if none of the generators is of order two. Both actions are properly discontinuous and cocompact (provided that S is finite): the quotient $\mathrm{Cayley}(G, S)/G$ is homeomorphic to the bouquet of n circles, where n is the cardinality of S, if no $s \in S$ satisfies $s^2 = 1$; while in the opposite case, for each generator of order two the corresponding circle must be replaced by an interval of length $\frac{1}{2}$ with one endpoint the basepoint of the bouquet.

2. The action of the group on itself by right multiplication defines maps

$$R_g : G \to G\,,\ R_g(h) = hg$$

that are, in general, not isometries with respect to a word metric, but are at finite distance from the identity map:

$$\mathrm{dist}(\mathrm{id}(h), R_g(h)) = |g|_S\,.$$

Exercise 3.26. Prove that the word metric on a group G associated to a generating set S may also be defined

1. either as the unique maximal left-invariant metric on G such that

$$\mathrm{dist}(1, s) = \mathrm{dist}(1, s^{-1}) = 1\,,\ \forall s \in S\,;$$

2. or by the following formula: $\mathrm{dist}(g, h)$ is the length of the shortest word w in the alphabet $S \cup S^{-1}$ such that $w = g^{-1}h$ in G.

Below are two simple examples of Cayley graphs.

Example 3.27. Consider the group $\mathbb{Z}^2$ with the set of generators

$$S = \{a = (1, 0), b = (0, 1)\}.$$

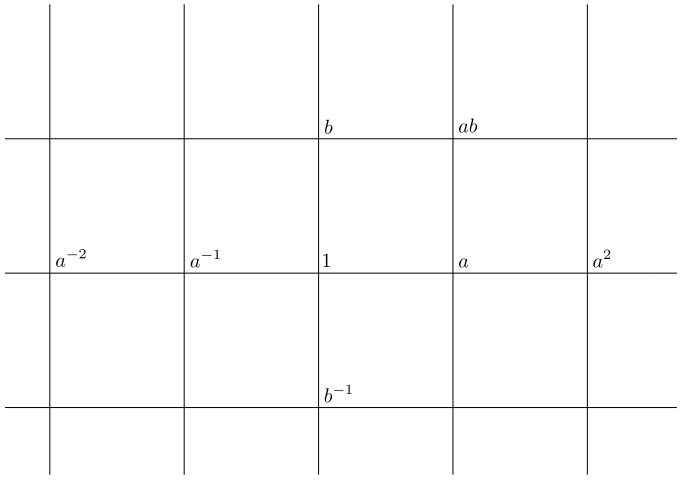


Figure 2: The Cayley graph of $\mathbb{Z}^2$.

The Cayley graph Cayley(G, S) is the square grid in the Euclidean plane: the vertices are points with integer coordinates, two vertices are connected by an edge if and only if either their first or their second coordinates differ by ± 1. See Figure 2.

The Cayley graph of $\mathbb{Z}^2$ with respect to the generating set$\{(1, 0), (1, 1)\}$ has the same set of vertices as the above, but the vertical lines are replaced by diagonal lines.

Example 3.28. Let G be the free group on two generators a, b. Take $S = \{a, b\}$. The Cayley graph Cayley(G, S) is the 4-valent tree (there are four edges incident to each vertex). See Figure 3.

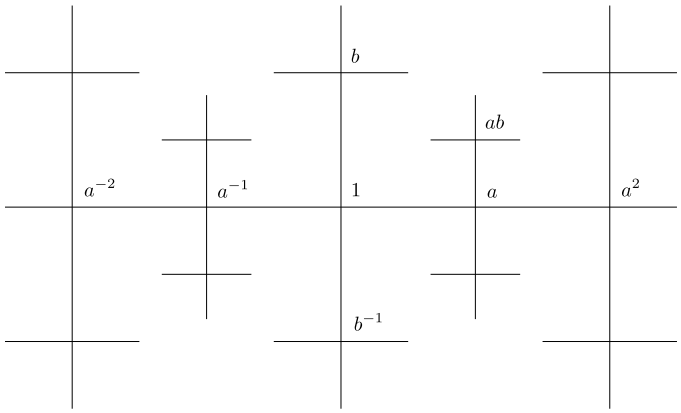


Figure 3: The Cayley graph of the free group F_2.

Thus, we succeeded in assigning to every finitely generated group G a metric space $\mathrm{Cayley}(G,S)$. The problem, however, is that this assignment

$$G \to \mathrm{Cayley}(G,S)$$

is far from canonical: different generating sets could yield completely different Cayley graphs.

Exercise 3.29. 1. Prove that if S and $\bar{S}$ are two finite generating sets of G, then the word metrics dist_S and $\mathrm{dist}_{\bar{S}}$ on G are bi-Lipschitz equivalent, i.e. there exists $L>0$ such that

$$\frac{1}{L}\mathrm{dist}_S(g,g') \leqslant \mathrm{dist}_{\bar{S}}(g,g') \leqslant L\mathrm{dist}_S(g,g')\,, \forall g,g' \in G\,. \tag{3}$$

Hint: Verify the inequality (14) first for $g'=1_G$ and $g \in S$; then verify the inequality for arbitrary $g \in G$ and $g'=1_G$. Lastly, verify the inequality for all g,g' using left-invariance of word-metrics.

2. Prove that an isomorphism between two finitely generated groups is a bi-Lipschitz map when the two groups are endowed with word metrics.

Convention 3.30. From now on, unless otherwise stated, by a metric on a finitely generated group we mean a word metric coming from a finite generating set.

Exercise 3.31. Show that the Cayley graph of a finitely generated infinite group contains an isometric copy of $\mathbb{R}$, i.e. a bi-infinite geodesic. Hint: Apply Arzela-Ascoli theorem to a sequence of geodesic segments in the Cayley graph.

Lemma 3.32. *A* finite index *subgroup of a finitely generated group is finitely generated.*

Proof. Let G be a group and S a finite generating set of G, and let H be a finite-index subgroup in G. Then

$$G = H \sqcup \bigsqcup_{i=1}^{k} Hg_i$$

for some elements $g_i \in G$. Consider

$$R = \max_{1 \leqslant i \leqslant k} |g_i|_S\,.$$

Then $G = HB(1,R)$. We now prove that $X = H \cap B(1,2R+1)$ is a generating set of H.

Let h be an arbitrary element in H and let $g_0 = 1, g_1, \ldots, g_n = h$ be the consecutive vertices on a geodesic in $\mathrm{Cayley}(G,S)$ joining 1 and h. In particular, this implies that $\mathrm{dist}_S(1,h) = n$.

For every $1 \leqslant i \leqslant n-1$ there exist $h_i \in H$ such that $\mathrm{dist}_S(g_i,h_i) \leqslant R$. Set $h_0 = 1$ and $h_n = h$. Then $\mathrm{dist}_S(h_i,h_{i+1}) \leqslant 2R+1$, hence $h_{i+1} = h_i x_i$ for some $x_i \in X$, for every $0 \leqslant i \leqslant n-1$. It follows that $h = h_n = x_1 x_2 \cdots x_n$, whence X generates H and $|h|_X \leqslant |h|_S = n$. □

3.5 Geometry and rank of free groups

The results in this section will be proved and generalized in the Hilary Term part C course C3.2 "Geometric Group Theory". Here we simply list the results, in order to give a complete picture. To begin with, one can easily check the following

Proposition 3.33. *The group G is a free group generated by Y if and only if* Cayley$(G; Y)$ *is a tree.*

This has the following strengthened version.

Theorem 3.34. *A group is free if and only if it acts freely on a tree.*

The 'only if' part of Theorem 3.34 is an obvious consequence of Proposition 3.33. The 'if' part on the other hand is more subtle.

The usefulness of this characterization is illustrated by its immediate corollary, the 'Nielsen-Schreier Theorem':

Theorem 3.35. *Every subgroup of a free group is free.*

Other interesting considerations concern the notion of rank for free groups.

Proposition 3.36. *Two free groups $F(X)$ and $F(Y)$ are isomorphic if and only if X and Y have the same cardinality.*

Proposition 3.36 implies that for every cardinal number n there exists, up to isomorphism, exactly one free group of rank n. We denote this group by F_n. Recall that the *rank* of a finitely generated group G is the least number of generators of G. In other words,

$$\text{rank}(G) = \min\{r \mid \exists \text{ an epimorphism } F_r \to G\}.$$

Proposition 3.37. *For each finite n, the number n is the least cardinality of a generating set of F_n. In other words, rank $(F_n) = n$.*

3.6 Presentations of groups

How does one define a group, other than a free group? For finite groups the table of multiplications could be provided, but not for infinite groups. One approach is to exploit the fact that every group is a homomorphic image of a free group. A free group is given by a generating set that satisfies no relations. More generally, we can specify a group 'by generators and relations', also called 'a presentation of the group.'

Thus, let G be a group and S a generating set of G. According to Proposition 3.14, the inclusion map $i : S \to G$ extends uniquely to an epimorphism $\pi_S : F(S) \to G$. The elements of $\text{Ker}(\pi_S)$ are called *relators* (or *relations*) of the group G with the generating set S.

N.B. In the above, by an abuse of language we used the symbol s to designate two different objects: s is a letter in $F(S)$, as well as an element in the group G.

If $R = \{r_i \mid i \in I\} \subset F(S)$ is such that $\mathrm{Ker}(\pi_S)$ is normally generated by R (i.e. $\langle\langle R\rangle\rangle = \mathrm{Ker}(\pi_S)$) then we say that the ordered pair (S, R), usually denoted $\langle S|R\rangle$, is *a presentation of* G. The elements $r \in R$ are called *defining relators* (or *defining relations*) of the presentation $\langle S|R\rangle$.

A group G is said to be *finitely presented* if it admits a finite presentation, i.e. a presentation with finitely many generators and relators.

By abuse of language we also say that the generators $s \in S$ and the *relations* $r = 1$, $r \in R$, constitute a presentation of the group G. Sometimes we will write presentations in the form

$$\langle s_i, i \in I | r_j = 1, j \in J\rangle$$

where

$$S = \{x_i\}_{i\in I}, \quad R = \{r_j\}_{j\in J}.$$

If both S and R are finite, then the pair S, R is called *a finite presentation of* G. A group G is called *finitely presented* if it admits a finite presentation. Sometimes it is difficult, and even algorithmically impossible, to find a finite presentation of a finitely presented group, see [BW11].

Conversely, given an alphabet S and a set R of (reduced) words in the alphabet S, we can form the quotient

$$G := F(S)/\langle\langle R\rangle\rangle .$$

Then $\langle S|R\rangle$ is a presentation of G. By abusing notation, we will often write

$$G = \langle S|R\rangle ,$$

if G is a group with the presentation $\langle S|R\rangle$. If w is a word in the generating set S, we will use $[w]$ to denote its projection to the group G. An alternative notation for the equality

$$[v] = [w]$$

is

$$v \equiv_G w.$$

Note that the significance of a presentation of a group is the following:

- every element in G can be written as a finite product $x_1 \cdots x_n$ with

$$x_i \in S \cup S^{-1} = \{s^{\pm 1} : s \in S\}$$

  i.e. as a word in the alphabet $S \cup S^{-1}$;

- a word $w = x_1 \cdots x_n$ in the alphabet $S \cup S^{-1}$ is *equal to the identity in* G, $w \equiv_G 1$, *if and only if* in $F(S)$ the word w is the product of finitely many conjugates of words $r_i \in R$, i.e.

$$w = \prod_{i=1}^{m} r_i^{u_i}$$

for some $m \in \mathbb{N}$, $u_i \in F(S)$ and $r_i \in R$.

Below are a few examples of group presentations:

Examples 3.38.

1. $\langle a_1, \ldots, a_n \mid [a_i, a_j], 1 \leqslant i, j \leqslant n \rangle$ is a finite presentation of $\mathbb{Z}^n$;

2. $\langle x, y \mid x^n, y^2, yxyx \rangle$ is a presentation of the finite dihedral group D_{2n} ;

3. $\langle x, y \mid x^2, y^3, [x, y] \rangle$ is a presentation of the cyclic group $\mathbb{Z}_6$.

4. *Integer Heisenberg group:*

$$H_{2n+1}(\mathbb{Z}) := \langle x_1, \ldots, x_n, y_1, \ldots, y_n, z \mid$$

$$[x_i, z] = 1, [y_j, z] = 1, [x_i, x_j] = 1, [y_i, y_j] = 1, [x_i, y_j] = z^{\delta_{ij}}, 1 \leqslant i, j \leqslant n \rangle .$$

Let $\langle S|R \rangle$ be a presentation of a group G. Let H be a group and $\psi : S \to H$ be a map which "preserves the relators", i.e. $\psi(r) = 1$ for every $r \in R$. Then:

Lemma 3.39. *The map ψ extends to a group homomorphism $\psi : G \to H$.*

Proof. By the universal property of free groups, the map ψ extends to a homomorphism $\tilde{\psi} : F(S) \to H$. We need to show that $\langle\langle R \rangle\rangle$ is contained in $\mathrm{Ker}(\tilde{\psi})$. However, $\langle\langle R \rangle\rangle$ consists of products of elements of the form grg^{-1}, where $g \in F, r \in R$. Since $\tilde{\psi}(grg^{-1}) = 1$, the claim follows. □

Exercise 3.40. The group $\bigoplus_{x \in X} \mathbb{Z}_2$ has the presentation

$$\langle x \in X | x^2, [x, y], \forall x, y \in X \rangle .$$

Proposition 3.41 (Finite presentability is independent of the generating set)**.** *Assume that a group G has finite presentation $\langle S \mid R \rangle$, and let $\langle X \mid T \rangle$ be an arbitrary presentation of G, such that X is finite. Then there exists a finite subset $T_0 \subset T$ such that $\langle X \mid T_0 \rangle$ is a presentation of G.*

Proof. Every element $s \in S$ can be written as a word $a_s(X)$ in X. The map $i_{SX} : S \to F(X)$, $i_{SX}(s) = a_s(X)$ extends to a unique homomorphism $p : F(S) \to F(X)$. Moreover, since $\pi_X \circ i_{SX}$ is an inclusion map of S into G, and both π_S and $\pi_X \circ p$ are homomorphisms from $F(S)$ to G extending the inclusion map $S \to G$, by the uniqueness of the extension we have that

$$\pi_S = \pi_X \circ p.$$

This implies that $\operatorname{Ker}(\pi_X)$ contains $p(r)$ for every $r \in R$.

Likewise, every $x \in X$ can be written as a word $b_x(S)$ in S, and this defines a map $i_{XS} : X \to F(S)$, $i_{XS}(x) = b_x(S)$, which extends to a homomorphism $q : F(X) \to F(S)$. A similar argument shows that $\pi_S \circ q = \pi_X$.

For every $x \in X$,

$$\pi_X(p(q(x))) = \pi_S(q(x)) = \pi_X(x).$$

This implies that for every $x \in X$, $x^{-1}p(q(x))$ is in $\operatorname{Ker}(\pi_X)$. Let N be the normal subgroup of $F(X)$ normally generated by

$$\{p(r) \mid r \in R\} \cup \{x^{-1}p(q(x)) \mid x \in X\}.$$

We have that $N \leqslant \operatorname{Ker}(\pi_X)$. Therefore, there is a natural projection

$$\operatorname{proj} : F(X)/N \to F(X)/\operatorname{Ker}(\pi_X).$$

Let $\bar{p} : F(S) \to F(X)/N$ be the homomorphism induced by p. Since $\bar{p}(r) = 1$ for all $r \in R$, it follows that $\bar{p}(\operatorname{Ker}\pi_S) = 1$, hence, $\bar{p}$ induces a homomorphism

$$\varphi : F(S)/\operatorname{Ker}(\pi_S) \to F(X)/N.$$

We next observe that the homomorphism φ is onto. Indeed, $F(X)/N$ is generated by elements of the form $xN = p(q(x))N$, and the latter is the image under φ of $q(x)\operatorname{Ker}(\pi_S)$.

Consider the homomorphism

$$\operatorname{proj} \circ \varphi : F(S)/\operatorname{Ker}(\pi_S) \to F(X)/\operatorname{Ker}(\pi_X)$$

Both the domain and the target groups are isomorphic to G. Each element x of the generating set X is sent by the isomorphism $G \to F(S)/\operatorname{Ker}(\pi_S)$ to $q(x)\operatorname{Ker}(\pi_S)$. The same element x is sent by the isomorphism $G \to F(X)/\operatorname{Ker}(\pi_X)$ to $x\operatorname{Ker}(\pi_X)$. Note that

$$\operatorname{proj} \circ \varphi\,(q(x)\operatorname{Ker}(\pi_S)) = \operatorname{proj}(xN) = x\operatorname{Ker}(\pi_X).$$

This means that, modulo the two isomorphisms mentioned above, the map $\operatorname{proj} \circ \varphi$ is id_G. This implies that φ is injective, hence, a bijection. Therefore, proj is also a bijection. This happens if and only if $N = \operatorname{Ker}(\pi_X)$. In particular, $\operatorname{Ker}(\pi_X)$ is normally generated by the finite set of relators

$$\Re = \{p(r) \mid r \in R\} \cup \{x^{-1}p(q(x)) \mid x \in X\}.$$

Since $\Re = \langle\langle T \rangle\rangle$, every relator $\rho \in \Re$ can be written as a product

$$\prod_{i \in I_\rho} t_i^{v_i}$$

with $v_i \in F(X), t_i \in T$ and I_ρ finite. It follows that $\mathrm{Ker}(\pi_X)$ is normally generated by the finite subset

$$T_0 = \bigcup_{\rho \in \Re} \{t_i \mid i \in I_\rho\}$$

of T. □

Proposition 3.41 can be reformulated as follows: If G is finitely presented, X is finite and

$$1 \to N \to F(X) \to G \to 1$$

is a short exact sequence, then N is normally generated by finitely many elements $n_1, \ldots, n_k$. This can be generalized to an arbitrary short exact sequence:

Lemma 3.42. *Consider a short exact sequence*

$$1 \to N \to K \xrightarrow{\pi} G \to 1\,, \quad \textit{with } K \textit{ finitely generated.} \tag{4}$$

If G is finitely presented, then N is normally generated by finitely many elements $n_1, \ldots, n_k \in N$.

Proof. Let S be a finite generating set of K; then $\overline{S} = \pi(S)$ is a finite generating set of G. Since G is finitely presented, by Proposition 3.41 there exist finitely many words $r_1, \ldots, r_k$ in S such that

$$\left\langle \overline{S} \mid r_1(\overline{S}), \ldots, r_k(\overline{S}) \right\rangle$$

is a presentation of G.

Define $n_j = r_j(S)$, an element of N by the assumption.

Let n be an arbitrary element in N and $w(S)$ a word in S such that $n = w(S)$ in K. Then $w(\overline{S}) = \pi(n) = 1$, whence in $F(S)$ the word $w(S)$ is a product of finitely many conjugates of $r_1, \ldots, r_k$. When projecting such a relation *via* $F(S) \to K$ we obtain that n is a product of finitely many conjugates of $n_1, \ldots, n_k$. □

Proposition 3.43. *Suppose that N a normal subgroup of a group G. If both N and G/N are finitely presented then G is also finitely presented.*

Proof. Let X be a finite generating set of N and let Y be a finite subset of G such that $\overline{Y} = \{yN \mid y \in Y\}$ is a generating set of G/N. Let $\langle X \mid r_1, \ldots, r_k \rangle$ be a finite presentation of N and let $\left\langle \overline{Y} \mid \rho_1, \ldots, \rho_m \right\rangle$ be a finite presentation

of G/N. The group G is generated by $S = X \cup Y$ and this set of generators satisfies a list of relations of the following form:

$$r_i(X) = 1\,,\ 1 \leqslant i \leqslant k\,,\ \rho_j(Y) = u_j(X)\,,\ 1 \leqslant j \leqslant m\,, \tag{5}$$

$$x^y = v_{xy}(X)\,,\ x^{y^{-1}} = w_{xy}(X) \tag{6}$$

for some words u_j, v_{xy}, w_{xy} in S.

We claim that this is a complete set of defining relators of G.

All the relations above can be rewritten as $t(X, Y) = 1$ for a finite set T of words t in S. Let K be the normal subgroup of $F(S)$ normally generated by T.

The epimorphism $\pi_S : F(S) \to G$ defines an epimorphism $\varphi : F(S)/K \to G$. Let wK be an element in $\mathrm{Ker}(\varphi)$, where w is a word in S. Due to the set of relations (6), there exist a word $w_1(X)$ in X and a word $w_2(Y)$ in Y, such that $wK = w_1(X)w_2(Y)K$.

Applying the projection $\pi : G \to G/N$, we see that $\pi(\varphi(wK)) = 1$, i.e. $\pi(\varphi(w_2(Y)K)) = 1$. This implies that $w_2(Y)$ is a product of finitely many conjugates of $\rho_i(Y)$, hence $w_2(Y)K$ is a product of finitely many conjugates of $u_j(X)K$, by the second set of relations in (5). This and the relations (6) imply that $w_1(X)w_2(Y)K = v(X)K$ for some word $v(X)$ in X. Then the image $\varphi(wK) = \varphi(v(X)K)$ is in N; therefore, $v(X)$ is a product of finitely many conjugates of relators $r_i(X)$. This implies that $v(X)K = K$.

We have thus obtained that $\mathrm{Ker}(\varphi)$ is trivial, hence φ is an isomorphism, equivalently that $K = \mathrm{Ker}(\pi_S)$. This implies that $\mathrm{Ker}(\pi_S)$ is normally generated by the finite set of relators listed in (5) and (6). □

Proposition 3.44. *Let G be a group, and $H \leq G$ such that $|G : H|$ is finite. Then G is FP if and only if H is FP.*

Proof. Suppose that $G = \langle X; R\rangle$ with X and R finite. We have an epimorphism $\pi : F = F(X) \to G$ with $K = \mathrm{Ker}\,\pi = \langle\langle R\rangle\rangle$. Put $E = \pi^{-1}(H)$. Then $|F : E| = |G : H|$ is finite, so E is free on some finite basis Y. Since $K \leq E$, each $r \in R$ satisfies $r = s_r(Y)$ for some word s_r on Y. Put $S = \{s_r(Y) \mid r \in R\}$. Then $\pi_1 = \pi_{|E} : E \to H$ is an epimorphism and

$$\mathrm{Ker}\,\pi_1 = K = \left\langle\left\langle S^F\right\rangle\right\rangle = \left\langle S^F\right\rangle.$$

Say $F = a_1E \cup \ldots \cup a_nE$. Then $S^F = (S^{a_1} \cup \ldots \cup S^{a_n})^E$. Thus $\langle Y; S^{a_1} \cup \ldots \cup S^{a_n}\rangle$ is a presentation for H.

Suppose conversely that H is FP. Let $N \leq H$ be a normal subgroup of finite index in G (see Revision notes). Then $|H : N|$ is finite, so N is FP by the first part. Also G/N is FP (Ex. Sheet 2). Therefore G is FP by Proposition 3.43. □

4 Residual finiteness

Even though studying infinite groups is our primary focus, questions in group theory can be, sometimes, reduced to questions about finite groups. *Residual finiteness* is the concept that (sometimes) allows such a reduction.

Definition 4.1. A group G is said to be *residually finite* if

$$\bigcap_{i\in I} G_i = \{1\},$$

where $\{G_i : i \in I\}$ is the set of all finite-index subgroups in G.

Clearly, subgroups of residually finite groups are also residually finite. In contrast, if G is an infinite simple group, then G cannot be residually-finite.

Lemma 4.2. *A finitely generated group G is residually finite if and only if for every $g \in G\setminus\{1\}$, there exists a finite group Φ and a homomorphism $\varphi : G \to \Phi$, such that $\varphi(g) \neq 1$.*

Proof. Suppose that G is residually finite. Then, for every $g \in G \setminus \{1\}$ there exists a finite-index subgroup $G_i \leqslant G$ so that $g \notin G_i$. It follows that G contains a normal subgroup of finite index $N_i \lhd G$, such that $N_i \leqslant G_i$. Clearly, $g \notin N_i$ and $|G : N_i| < \infty$. Now, setting $\Phi := G/N_i$, we obtain the required homomorphism $\varphi : G \to \Phi$.

Conversely, suppose that for every $g \neq 1$ we have a homomorphism $\varphi_g : G \to \Phi_g$, where Φ_g is a finite group, so that $\varphi_g(g) \neq 1$. Setting $N_g := \mathrm{Ker}(\varphi_g)$, we get

$$\bigcap_{g\in G} N_g = \{1\}.$$

The above intersection, of course, contains the intersection of all finite-index subgroups in G. □

Exercise 4.3. Direct products of residually finite groups are again residually finite.

Lemma 4.4. *If a group G contains a residually finite subgroup of finite index, then G itself is residually finite.*

Proof. Let $H \leqslant G$ be a finite index residually finite subgroup. The intersection of all finite-index subgroups

$$\bigcap_{i\in I} H_i \tag{7}$$

of H is $\{1\}$. Since H has finite index in G and each $H_i \leqslant H$ as above has finite index in G, the intersection of all finite-index subgroups of G is contained in (7) and, hence, is trivial. □

Proposition 4.5. *A semidirect product of a finitely generated residually finite group with a (not necessarily finitely generated) residually finite group is also residually finite.*

Proof. Let G be a group that splits as a semidirect product $H \rtimes Q$, where H and Q are residually finite, and H is moreover finitely generated. Let p denote the projection homomorphism $G \to Q$.

Consider $g \in G \setminus \{1\}$. If g does not belong to H, then $p(g) \neq 1$ and the residual finiteness of Q implies that there exists a homomorphism of Q to a finite group which sends sends $p(g)$ to a non-trivial element. By composing the homomorphisms, we obtain a homomorphism of G to a finite group which sends g to a non-trivial element.

Suppose, therefore, that g is in H. Let $F < H$ be a finite-index subgroup which does not contain g. Since H is finitely generated, Proposition **??**, (2), implies that there exists a finite-index subgroup $A \leqslant F$ which is a characteristic subgroup of H. The subgroup $A \rtimes Q$ is a finite index subgroup in $G = H \rtimes Q$ that does not contain g. □

Remark 4.6. Proposition 4.5 cannot extend to short exact sequences that do not split. In other words, it is not true that if H and Q are residually finite, H is finitely generated, and there is a short exact sequence

$$1 \to H \to G \to Q \to 1,$$

then G is residually finite. Indeed, there exist coextensions

$$1 \to \mathbb{Z}_2 \to G \to Q \to 1$$

where Q is finitely generated residually finite, while G is not residually finite; see [Mil79].

Corollary 4.7. *Suppose that H is a finitely generated residually finite group and we have a cyclic extension of H, i.e. a group G which appears in a short exact sequence*

$$1 \to H \to G \xrightarrow{p} C \to 1,$$

where C is a cyclic group. Then G is also residually finite.

Proof. When C is finite, the statement follows from Lemma 4.4. When C is infinite, that is $C \simeq \mathbb{Z}$, the short exact sequence splits and $G \simeq H \rtimes \mathbb{Z}$, by Corollary 3.17. The result now follows from Proposition 4.5. □

A special case of this corollary is residual finiteness of groups virtually isomorphic to cyclic groups.

Corollary 4.8. *Each group G virtually isomorphic to $\mathbb{Z}$ is residually finite and contains an infinite cyclic subgroup of finite index.*

Proof. In view of Lemma 4.4, it suffices to show that if G is a finite coextension of the infinite cyclic group C,

$$1 \to F \to G \xrightarrow{p} C \to 1$$

(where F is finite), then G contains an infinite cyclic subgroup of finite index. This is an immediate consequence of Corollary 4.7. □

Remark 4.9. The first part of Corollary 4.8 can be generalized, by replacing $\mathbb{Z}$ with "a polycyclic group"; see Theorem 5.42.

Example 4.10. The group $\Gamma = GL(n, \mathbb{Z})$ is residually finite. Indeed, we take subgroups $\Gamma(p) \leqslant \Gamma$, $\Gamma(p) = \mathrm{Ker}(\varphi_p)$, where $\varphi_p : \Gamma \to GL(n, \mathbb{Z}_p)$ is the reduction modulo p.

Assume $g \in \Gamma$ is a non-trivial element. If g has a non-zero off-diagonal entry $g_{ij} \neq 0$, then $g_{ij} \neq 0 \bmod p$, whenever $p > |g_{ij}|$. Thus, $\varphi_p(g) \neq 1$.

If $g \in \Gamma$ has only zero entries off-diagonal then it is a diagonal matrix with only ± 1 on the diagonal, and at least one entry -1. Then $\varphi_3(g)$ has at least one 2 on the diagonal, hence $\varphi_3(g) \neq 1$.

Thus Γ is residually finite.

Corollary 4.11. *The free group F_2 of rank 2 is residually finite. Every free group of (at most) countable rank is residually finite.*

Proof. As we saw in the Example 3.20 the group F_2 embeds in $SL(2, \mathbb{Z})$. Furthermore, every free group of (at most) countable rank embeds in F_2 (see Ex. Sheet 2). Now, the assertion follows from the Example 4.10. □

Exercise 4.12. For an arbitrary cardinality r, the free group F_r of rank r is residually finite.

The simple argument for $GL(n, \mathbb{Z})$ is a model for a proof of a harder theorem:

Theorem 4.13 (A. I. Mal'cev [Mal40])**.** *Let Γ be a finitely generated subgroup of $GL(n, R)$, where R is a commutative ring with unity. Then Γ is residually finite.*

Mal'cev's theorem is complemented by the following result proven by A. Selberg and known as *Selberg's Lemma* [Sel60]:

Theorem 4.14 (Selberg's Lemma)**.** *Let Γ be a finitely generated subgroup of $GL(n, F)$, where F is a field of characteristic zero. Then Γ contains a torsion-free subgroup of finite index.*

5 Solvable groups

This section covers basic properties of general solvable groups and some special classes of solvable groups: abelian, nilpotent and polycyclic groups. Solvable and polycyclic groups appear naturally in the framework of *poly-X-groups*, where X is a certain class of groups: A group G is said to be poly-X if it admits a subnormal descending series:

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_k \triangleright G_{k+1} = \{1\},$$

such that each successive quotient G_i/G_{i+1} belongs to the class X. Solvable groups will be obtained by taking X to be the class of abelian groups, while polycyclic groups will use the class of cyclic groups (a further refinement of the definition uses X consisting of infinite cyclic groups, all isomorphic to each other, of course).

5.1 Nilpotent groups

Recall that $[x,y] = xyx^{-1}y^{-1}$ is the commutator of the elements x, y in a group G and that $x^g := gxg^{-1}$ is the g-conjugate of x in G. We begin the discussion of nilpotent groups with some useful commutator identities:

Lemma 5.1. *Let $(G,\cdot)$ be a group and x,y,z elements in G. The following identities hold:*

1. $[x,y]^{-1} = [y,x]$;
2. $[x^{-1},y] = [x^{-1},[y,x]]\,[y,x]$;
3. $[x,yz] = [x,y]\,[y,[x,z]]\,[x,z]$;
4. $[xy,z] = [x,[y,z]]\,[y,z]\,[x,z] = [y,z]^x[x,z]$.
5. $[x,y]^g = [x^g,y^g]$.

Proof. (1) and (2) are immediate, (4) follows from (3) and (1). It remains to prove (3). Since $[y,[x,z]]\,[x,z] = y[x,z]y^{-1}$ we have that

$$[x,y]\,[y,[x,z]]\,[x,z] = xyx^{-1}[x,z]y^{-1} = xyzx^{-1}z^{-1}y^{-1} = [x,yz]\,.$$

We leave the last identity as an exercise to the reader. □

Notation 5.2. For every $x_1,\ldots,x_n$ in a group G we denote by $[x_1,\ldots,x_n]$ the *n-fold left-commutator*

$$[[[x_1,x_2],\ldots,x_{n-1}],x_n].$$

We declare that the 1-fold left commutator $[x]$ is simply x.

Exercise 5.3. $[x_1,\ldots,x_n]^g = [x_1^g,\ldots,x_n^g]$.

Recall that for subsets A,B in a group G, $[A,B]$ denotes the subgroup of G generated by all the commutators $[a,b], a\in A, b\in B$. In what follows we also use:

Notation 5.4. Given n subgroups $H_1,H_2,\ldots,H_n$ in a group G we denote by $[H_1,\ldots,H_n]$ the subgroup $[\ldots[H_1,H_2],\ldots,H_n] \leqslant G$.

We define *the lower central series* of a group G,

$$C^1G \trianglerighteq C^2G \trianglerighteq \ldots \trianglerighteq C^nG \trianglerighteq \ldots,$$

inductively by:

$$C^1G = G\,,\ C^{n+1}G = [C^nG,G]\,.$$

In particular, each C^kG is a *characteristic subgroup* of G. We will see later on (Proposition 5.27) that

$$[C^iG,C^kG] \leqslant C^{i+k}G.$$

Note that $C^2G = [G,G] = G'$ is the commutator subgroup, or the *derived subgroup*, of G.

Exercise 5.5. 1. The subgroup $C^kG \leqslant G$ is normal in G.

2. $C^{n+1}G = [G, C^nG]$.

Definition 5.6. A group G is called *k-step nilpotent* if $C^{k+1}G = \{1\}$. The minimal k for which G is k-step nilpotent is called the (nilpotency) *class* of G.

Examples 5.7. 1. Every non-trivial abelian group is nilpotent of class 1.

2. The group $\mathcal{U}_n(\mathbb{K})$ of upper triangular $n \times n$ matrices with 1 on the diagonal and entries in a ring $\mathbb{K}$, is nilpotent of class $n-1$ (see Exercise 5.9).

3. The *Heisenberg group*

$$H_{2n+1}(\mathbb{K}) = \left\{ \begin{pmatrix} 1 & x_1 & x_2 & \dots & \dots & x_n & z \\ 0 & 1 & 0 & \dots & \dots & 0 & y_n \\ 0 & 0 & 1 & \dots & \dots & 0 & y_{n-1} \\ \vdots & \vdots & \ddots & \ddots & & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 & y_2 \\ 0 & 0 & \dots & \dots & 0 & 1 & y_1 \\ 0 & 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix} ; x_1, \dots, x_n, y_1, \dots, y_n, z \in \mathbb{K} \right\}$$

is nilpotent of class 2.

Taking $\mathbb{K} = \mathbb{Z}$, we obtain the *integer Heisenberg group*

$$H_{2n+1}(\mathbb{Z}).$$

The group $H_{2n+1}(\mathbb{Z})$ is finitely generated; we can take as generators the elementary matrices $N_{ij} = I + E_{ij}$ with

$$(i,j) \in \{(1,2), \dots, (1,n+1), (2,n), \dots, (n+1,n)\}.$$

All the groups $H_{2n+1}(\mathbb{K})$ are nilpotent of class 2. Indeed $C^2H_{2n+1}(\mathbb{K})$ is the subgroup $x_i = y_i = 0, i = 1, \dots, n$.

Exercise 5.8. Which of the permutation groups S_n are nilpotent? Which of these groups are solvable?

Exercise 5.9. The goal of this exercise is to prove that the group $\mathcal{U}_n(\mathbb{K})$ is nilpotent of class $n-1$.

Let $\mathcal{U}_{n,k}(\mathbb{K})$ be the subset of $\mathcal{U}_n(\mathbb{K})$ formed by matrices (a_{ij}) such that $a_{ij} = \delta_{ij}$ for $j < i + k$. Note that $\mathcal{U}_{n,1}(\mathbb{K}) = \mathcal{U}_n(\mathbb{K})$.

1. Prove that for every $k \geqslant 1$ the map

$$\begin{array}{rcc} \varphi_k : \mathcal{U}_{n,k}(\mathbb{K}) & \to & \left(\mathbb{K}^{n-k}, +\right) \\ A = (a_{i,j}) & \mapsto & (a_{1,k+1}, a_{2,k+2}, \dots, a_{n-k,n}) \end{array}$$

is a homomorphism. Deduce that $(\mathcal{U}_{n,k}(\mathbb{K}))' \subset \mathcal{U}_{n,k+1}(\mathbb{K})$ and that $\mathcal{U}_{n,k+1}(\mathbb{K}) \lhd \mathcal{U}_{n,k}(\mathbb{K})$ for every $k \geqslant 1$.

2. Let E_{ij} be the matrix with all entries 0 except the (i,j)–entry, which is equal to 1. Consider the triangular matrix $T_{ij}(a) = I + aE_{ij}$.

   Deduce from (1), using induction, that $\mathcal{U}_{n,k}$ is generated by the set

$$\{T_{ij}(a) \mid j \geqslant i+k, a \in \mathbb{R}\}\,.$$

3. Prove that for every three distinct numbers i, j, k in $\{1, 2, \ldots, n\}$

$$[T_{ij}(a), T_{jk}(b)] = T_{ik}(ab)\,,\ [T_{ij}(a), T_{ki}(b)] = T_{kj}(-ab)\,,$$

   and that for all quadruples of distinct numbers i, j, k, ℓ,

$$[T_{ij}(a), T_{k\ell}(b)] = I\,.$$

4. Prove that $C^k\mathcal{U}_n(\mathbb{K}) \leqslant \mathcal{U}_{n,k+1}(\mathbb{K})$ for every $k \geqslant 0$. Deduce that $\mathcal{U}_n(\mathbb{K})$ is nilpotent.

Remark. All the arguments above work also when all matrices have integer entries. In this case (2) implies that $\mathcal{U}_n(\mathbb{Z})$ is generated by $\{T_{ij}(1) \mid j \geqslant i+1\}$.

Exercise 5.10. The group $\mathcal{U}_n(\mathbb{K})$ is torsion-free provided that $\mathbb{K}$ has zero characteristic.

We now proceed with establishing some basic properties of lower central series and nilpotent groups.

Lemma 5.11. *If S is a generating set of a group G (not necessarily nilpotent), then for every k the subgroup C^kG is generated by the k-fold left commutators in S and their inverses, together with $C^{k+1}G$.*

Proof. We prove the assertion by induction on k. For $k = 1$ the statement is clear, since 1-fold commutators of elements of S are just elements of S. Assume that the assertion holds for some $k \geqslant 1$ and consider $C^{k+1}G$.

By definition, $C^{k+1}G$ is generated by all commutators $[c_k, g]$ with $c_k \in C^kG$ and $g \in G$. The induction hypothesis and normality of $C^{k+1}G$ in G imply that $c_k = \ell_1^{\pm 1} \cdots \ell_m^{\pm 1} x$, where $m \in \mathbb{N}$, ℓ_i are k-fold left commutators in S and $x \in C^{k+1}G$.

According to Lemma 5.1, (4),

$$[c_k, g] = [\ell_1^{\pm 1} \cdots \ell_m^{\pm 1} x, g] = [\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, [x, g]][x, g][\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, g]\,.$$

The first two factors are in $C^{k+2}G$, so it remains to deal with the third.

We write $g = s_1 \cdots s_r$, where $s_i \in S$, and we prove that $[\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_1 \cdots s_r]$ is a product of $(k+1)$–fold left commutators in S and their inverses, and of elements in $C^{k+2}G$; our proof is another induction, this time on $m + r \geqslant 2$.

For the case $m + r = 2$ it suffices to note that $[\ell^{-1}, s] = [\ell^{-1}, [s, \ell]][s, \ell]$. The first factor is in $C^{k+2}G$, the second is the inverse of a $(k+1)$–fold left commutator.

Assume that the statement is true for $m + r = n \geqslant 2$. We now prove it for $m + r = n + 1$.

Suppose that $m \geqslant 2$. We apply Lemma 5.1, (4), and obtain that

$$[\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_1 \dots s_r] = [\ell_1^{\pm 1} \cdots \ell_{m-1}^{\pm 1}, [\ell_m^{\pm 1}, g]]\, [\ell_m^{\pm 1}, s_1 \cdots s_r]\, [\ell_1^{\pm 1} \cdots \ell_{m-1}^{\pm 1}, s_1 \dots s_r]\,.$$

The first factor is in $C^{k+2}G$, and for the second and the third the induction hypothesis applies.

Likewise, if $r \geqslant 2$ then we apply Part 3 of Lemma 5.1, and write

$$[\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_1 \cdots s_r] =$$

$$[\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_1 \cdots s_{r-1}]\, [s_1 \cdots s_{r-1}, [\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_r]]\, [\ell_1^{\pm 1} \cdots \ell_m^{\pm 1}, s_r]\,. \quad \square$$

Corollary 5.12. *If G is nilpotent, then $C^n G$ is generated by k-fold left commutators in S and their inverses, where $k \geqslant n$. In particular, if G is finitely generated, so is each group $C^n G$.*

Proof. Suppose that $C^{m+1}G = \{1\}$. Then $C^m G$ is generated by the m-fold left commutators in S and their inverses. By applying the reverse induction in n, each $C^n G$ is generated by the set of all k-fold left commutators of elements of S and their inverses, $k \geqslant n$. $\square$

Thus, if G is finitely generated, each quotient $C^i G / C^{i+1} G$ is a finitely generated abelian group and, hence, we define two important invariants of finitely generated nilpotent groups:

Definition 5.13. Let G be a finitely generated nilpotent group of class k. Let m_i denote the free rank of the abelian group $C^i G / C^{i+1} G$; define the *Hirsch length* (or the *Hirsch number*) of G

$$h(G) = \sum_{i=1}^{k} m_i.$$

So far, we were describing nilpotent groups "from the top–down", starting from the group G and then looking at the chain of decreasing subgroups. It is also useful to have a "bottom-up" description of nilpotent groups, which we present below.

Recall that the center of a group H is denoted $Z(H)$. Given a group G, consider the sequence of normal subgroups $Z_i(G) \lhd G$ defined inductively by:

- $Z_0(G) = \{1\}$.
- If $Z_i(G) \lhd G$ is defined and $\pi_i : G \to G/Z_i(G)$ is the quotient map, then

$$Z_{i+1}(G) = \pi_i^{-1}\left(Z(G/Z_i(G))\right).$$

Note that $Z_{i+1}(G)$ is normal in G, as the preimage of a normal subgroup of a quotient of G. In particular,

$$Z_{i+1}(G)/Z_i(G) \cong Z(G/Z_i(G)).$$

Proposition 5.14. *The group G is k-step nilpotent if and only if $Z_k(G) = G$.*

Proof. Assume that G is nilpotent of class k. We prove by induction on $i \geqslant 0$ that $C^{k+1-i}G \leqslant Z_i(G)$. For $i = 0$ we have equality. Assume that

$$C^{k+1-i}G \leqslant Z_i(G).$$

For every $g \in C^{k-i}G$ and every $x \in G$, $[g, x] \in C^{k+1-i}G \leqslant Z_i(G)$, whence $gZ_i(G)$ is in the center of $G/Z_i(G)$, i.e. $g \in Z_{i+1}(G)$. Thence, the inclusion follows by induction. For $i = k$ the inclusion becomes $C^1G = G \leqslant Z_k(G)$, hence, $Z_k(G) = G$.

Conversely, assume that there exists k such that $Z_k(G) = G$. We prove by induction on $j \geqslant 1$ that $C^jG \leqslant Z_{k+1-j}(G)$. For $j = 1$ the two are equal. Assume that the inclusion is true for j. The subgroup $C^{j+1}G$ is generated by commutators $[c, g]$ with $c \in C^jG$ and $g \in G$. Since $c \in C^jG \leqslant Z_{k+1-j}(G)$, by the definition of $Z_{k+1-j}(G)$, the element c commutes with g modulo $Z_{k-j}(G)$, equivalently $[c, g] \in Z_{k-j}(G)$. This implies that $[c, g] \in Z_{k-j}(G)$. It follows that $C^{j+1}G \leqslant Z_{k-j}(G)$.

For $j = k + 1$ this gives $C^{k+1}G \leqslant Z_0(G) = \{1\}$, hence G is k-step nilpotent. □

Definition 5.15. The ascending series

$$Z_0(G) = \{1\} \lhd Z_1(G) \lhd \ldots \lhd Z_i(G) \lhd Z_{i+1}(G) \lhd \ldots$$

of normal subgroups of G is called the *upper central series* of G.

In view of Proposition 5.14, a group G is nilpotent if and only if its upper central series is finite, and its nilpotency class is the minimal k such that $Z_k(G) = G$.

Exercise 5.16. Any central coextension of a nilpotent group is again nilpotent.

Remark 5.17. Yet another equivalent definition of a nilpotent group is to require that the group admits a finite normal series

$$\{1\} = \Gamma_0 \lhd \ldots \Gamma_i \lhd \Gamma_{i+1} \lhd \ldots \Gamma_{n-1} \lhd \Gamma_n = G,$$

such that $\Gamma_{i+1}/\Gamma_i \leqslant Z(G/\Gamma_i)$, or, equivalently, $[G, \Gamma_{i+1}] \leqslant \Gamma_i$. In particular, the quotients Γ_{i+1}/Γ_i are abelian for each i. We will need only the fact that the existence of such a normal series implies that G is n-step nilpotent. Indeed, the condition $\Gamma_{i+1}/\Gamma_i \leqslant Z(G/\Gamma_i)$ implies that $\Gamma_i \leqslant Z_i(G)$ for every i. In particular, $G = Z_n(G)$. Now, the assertion follows from Proposition 5.14. We refer to [Hal76, Theorem 10.2.2] for further details.

The following example shows that the difference between lower and upper central series of groups can be quite substantial, in particular, $C^{k+1-i}G \leqslant Z_i(G)$ could be of infinite index:

Example 5.18. We start with the integer Heisenberg group H; it is 2-step nilpotent, $C^2H = H' = Z(H) \cong \mathbb{Z}$. Next, take $G = H \times \mathbb{Z}$. Then G is still 2-step nilpotent, but now $C^2G = C^2H \cong \mathbb{Z}$, while $Z(G) \cong \mathbb{Z}^2$.

Exercise 5.19. Construct an example of a 2-step nilpotent group G with torsion-free center, such that G/C^2G is not torsion-free.

The following useful lemma is a converse to Corollary 5.12:

Lemma 5.20. *Let S be a generating set of a group G. Suppose that all $N+1$-fold commutators $[s_1, \dots, s_{N+1}]$ of elements of S are trivial. Then G is N-step nilpotent.*

Proof. Let G_n be the subgroup of Γ generated by the n-fold commutators $y_n = [s_1, \dots, s_n]$ of generators $s_i \in S$ of the group G. For every generator x of G and every generator y_n of G_n we have:

$$[y_n, x] = y_n x y_n^{-1} x^{-1} \in G_{n+1} \leqslant G_n.$$

Since $y_n \in G_n$, it follows that $xy_n^{-1}x^{-1} \in G_n$ which implies that G_n is a normal subgroup of G.

We claim that for every n, G_{n-1}/G_n embeds (under the map induced by inclusion $G_{n-1} \hookrightarrow G$) in the center of G/G_n. To simplify the notation, we will regard G_{n-1}/G_n as a subgroup of G/G_n. The proof of this statement is the reverse induction on n.

The subgroup G_{N+1} is trivial, hence it is contained in the center of G. Suppose that the assertion holds for $n = k+1$, we will now prove it for $n = k$. To show that G_{k-1}/G_k is in the center of G/G_k it is enough to verify that for all elements $\bar{z}$ and $\bar{w}$ of generating sets of G_{n-1}/G_n and G/G_n, respectively, the commutator $[\bar{z}, \bar{w}]$ is trivial.

The group G is generated by the set S, the group G_{n-1} is generated by the $n-1$-fold commutators y_{n-1} of elements $x \in S$. Thus, the groups G_{n-1}/G_n and G/G_n are generated by the projections $\bar{x}, \bar{y}_{n-1}$ of the elements x, y_{n-1}. By definition of G_n we have: $[y_{n-1}, x] \in G_n$, thus, dividing by G_n, we obtain $[\bar{y}_{n-1}, \bar{x}] = 1$. Thus, $G_{n-1}/G_n \leqslant Z(G/G_n)$ for every n and Lemma follows from Remark 5.17. □

Lemma 5.21. *1. Every subgroup of a nilpotent group is nilpotent.*

2. If G is nilpotent and $N \lhd G$ then G/N is nilpotent.

3. The direct product of a family of nilpotent groups is again nilpotent.

Proof. (1) Let H be a subgroup in a nilpotent group G. Then $C^iH \leqslant C^iG$. Hence, if G is k-step nilpotent then $C^{k+1}H = \{1\}$.

(2) If $\pi : G \to G/N$ is the quotient map, $\pi(C^iG) = C^i(G/N)$.

(3) The assertion follows from the equality

$$C^j(\prod_{i\in I} G_i) = \prod_{i\in I} C^j G_i \ . \quad \square$$

Theorem 5.22. *Every subgroup of a finitely generated nilpotent group is finitely generated, i.e. finitely generated nilpotent groups are* noetherian.

Proof. We argue by induction on the class of nilpotency k. For $k = 1$ the group is abelian and the statement is already proven in Corollary **??**. Assume that the assertion holds for k, let G be a nilpotent group of class $k+1$ and let $H \leqslant G$ be a subgroup. By the induction hypothesis $H_1 = H \cap C^2G$ and $H_2 = H/(H \cap C^2G)$ are both finitely generated. Thus, H fits in the short exact sequence

$$1 \to H_1 \to H \stackrel{\pi}{\to} H_2 \to 1,$$

where H_1, H_2 are finitely generated. Lemma **??** then shows that H is also finitely generated. $\square$

Our next goal is to prove some structural results for nilpotent groups. We begin the "calculus of commutators."

Lemma 5.23. *If A, B, C are normal subgroups in a group G, then the subgroup $[A, B, C] \leqslant G$ is generated by the commutators $[a, b, c]$ with $a \in A, b \in B, c \in C$.*

Proof. By the definition, $[A, B, C]$ is generated by the commutators $[k, c]$ with $k \in [A, B]$ and $c \in C$. The element k is a product $t_1 \cdots t_n$, where each t_i is equal either to a commutator $[a, b]$ or to a commutator $[b, a]$, $a \in A, b \in B$.

We prove, by the induction on n, that $[k, c]$ is a product of finitely many commutators $[a, b, c]$ and their inverses. For $n = 1$ we only need to consider the case $[t^{-1}, c]$, where $t = [a, b]$. By Lemma 5.1, (2),

$$[t^{-1}, c] = [c, t]^{t^{-1}} = [c^{t^{-1}}, t] = [c', t] = [a, b, c']^{-1} .$$

In the second equality above we applied the identity $\phi([x, y]) = [\phi(x), \phi(y)]$ for the inner automorphism $\phi(x) = x^{t^{-1}}$.

Assume that the statement is true when k is a product of n commutators t_i and consider $k = k_1 t$, where t is equal to either a commutator $[a, b]$ or a commutator $[b, a]$, and k_1 is a product of n such commutators. According to Lemma 5.1, (4),

$$[k_1 t, c] = [t, c]^{k_1} [k_1, c] .$$

Both factors are products of finitely many commutators $[a, b, c]$ and their inverses, by the induction hypothesis and the fact that A, B, C are normal subgroups and, thus, are invariant under conjugation. $\square$

Exercise 5.24. Prove the same result for $[H_1, \ldots, H_n]$, where all H_i are normal subgroups of G.

Lemma 5.25 (The Hall identity)**.** *Given a group G and three arbitrary elements x, y, z in G, the following identity holds:*

$$\left[x^{-1}, y, z\right]^x \left[z^{-1}, x, y\right]^z \left[y^{-1}, z, x\right]^y = 1\,. \tag{8}$$

Proof. The factor $\left[x^{-1}, y, z\right]^x$ equals $yxy^{-1}zyx^{-1}y^{-1}xz^{-1}x^{-1}$. The other two factors can be obtained by proper cyclic permutation and a direct calculation shows that all the terms cancel and the product is 1. □

Corollary 5.26. *Assume that A, B, C are normal subgroups in G. Then*

$$[A, B, C] \leqslant [B, C, A][C, A, B]\,. \tag{9}$$

The next proposition shows that the lower central series of G is *graded* with respect to commutators:

Proposition 5.27. *Let C^kG be the k-th group in the lower central series of a group G. Then for every $i, j \geqslant 1$*

$$\left[C^iG, C^jG\right] \leqslant C^{i+j}G\,. \tag{10}$$

Proof. We prove by induction on $i \geqslant 1$ that for every $j \geqslant 1$, the inclusion (10) holds.

For $i = 1$ this follows from the definition of C^kG. Assume that the statement is true for i. Consider $j \geqslant 1$ arbitrary.

$$[C^{i+1}G, C^jG] = [C^iG, G, C^jG] \leqslant [G, C^jG, C^iG][C^jG, C^iG, G] \leqslant$$

$$[C^{j+1}G, C^iG][C^{j+i}G, G] = [C^iG, C^{j+1}G][C^{j+i}G, G] \leqslant C^{j+i+1}G\,,$$

since $[C^iG, C^{j+1}G] \leqslant C^{j+i+1}G$ by the induction hypothesis. □

We now prove that, as for abelian groups, all elements of finite order in a finitely generated nilpotent group form a finite subgroup. We will need the following lemma:

Lemma 5.28. *Let G be a nilpotent group of class k. For every $x \in G$ the subgroup H generated by x and C^2G is a normal subgroup, which is nilpotent of class $\leqslant k - 1$.*

Proof. By normality of C^2G in G, the subgroup H can be described as

$$H = \{x^m c \mid m \in \mathbb{Z},\, c \in C^2G\}.$$

For every $g \in G$, and $h \in H$, $h = x^m c$, $ghg^{-1} = x^m[x^{-m}, g]gcg^{-1}$, and, since the last two factors are in C^2G, the whole product is in H. Hence, H is normal in G.

We now prove that $C^2H \leqslant C^3G$, which will imply that H is of class $\leqslant k-1$ and, thereby conclude the proof of lemma.

Let h, h' be two elements in H, $h = x^m c_1$, $h' = x^n c_2$ with $c_i \in C^2G$. Then, according to Lemma 5.1, (3),

$$[h, h'] = [h, x^n c_2] = [h, x^n]\,[x^n, [h, c_2]]\,[h, c_2].$$

The last term is in C^3G, hence the middle term is in C^4G.

For $[h, x^n] = [x^m c_1, x^n]$ we apply Lemma 5.1, (4), and obtain

$$[h, h'] = [x^m, [c_1, x^n]][c_1, x^n].$$

Since the last term is in C^3G and the first in C^4G, lemma follows. □

Theorem 5.29. *Let G be a nilpotent group. The set of all finite order elements forms a characteristic subgroup of G, called the torsion subgroup of G and denoted by* $\operatorname{Tor} G$.

Proof. We argue by induction on the class of nilpotency k of G. For $k = 1$ the G group is abelian and the assertion is clear. Assume that the statement is true for all nilpotent groups of class $\leqslant k$, and consider a $(k+1)$–step nilpotent group G.

It suffices to prove that for two arbitrary elements a, b of finite order in G, the product ab is likewise of finite order. The subgroup $B = \langle b, C^2G \rangle$ is nilpotent of class $\leqslant k$, according to Lemma 5.28. By the induction hypothesis, the set of finite order elements of B is a subgroup $\operatorname{Tor} B \leqslant B$, which is necessarily characteristic in B. Since B is normal in G it follows that $\operatorname{Tor} B$ is normal in G.

Assume that a is of order m. Then

$$(ab)^m = aba^{-1}a^2ba^{-2}a^3b \cdots a^{-m+1}a^m ba^{-m}\,,$$

and right-hand side is a product of conjugates of b, hence it is in $\operatorname{Tor} B$. We conclude that $(ab)^m$ is of finite order. □

Proposition 5.30. *A finitely generated nilpotent torsion group is finite.*

Proof. We again argue by induction on the nilpotency class n of the group G. For $n = 1$ we apply known results for abelian groups (see Revision notes). Assume that the property holds for all nilpotent groups of class at most n and consider G, a finitely generated torsion group that is $(n+1)$–step nilpotent. Then C^2G and G/C^2G are finite, by the induction hypothesis, whence G is finite as well. □

Corollary 5.31. *Let G be a finitely generated nilpotent group. Then the torsion subgroup* $\operatorname{Tor} G$ *is finite.*

Proposition 5.32. *If G is nilpotent then $\bar{G} := G/\operatorname{Tor} G$ is torsion-free.*

Proof. Each element $\bar{x} \in \bar{G}$, is the image of $x = ty \in G$ under the quotient map $\pi : G \to \bar{G}$, where $t \in \operatorname{Tor} G$. Then $1 = (\bar{x})^k$ would imply that

$$1 = (\bar{x})^k = \pi(y^k),$$

$y^k \in \operatorname{Tor} G$ and, hence, $y \in \operatorname{Tor} G$. It follows that $\bar{x} = 1$. □

Exercise 5.33. Let D_∞ be the infinite dihedral group.

1. Give an example of two elements a, b of finite order in D_∞ such that their product ab is of infinite order.

2. Is D_∞ a nilpotent group ?

3. Are any of the finite dihedral groups D_{2n} nilpotent?

Proposition 5.34 (A. I. Mal'cev, [Mal49])**.** *Let G be a nilpotent group. The following are equivalent:*
(a) Z(G)is torsion free;
(b) Each quotient $Z_{i+1}(G)/Z_i(G)$ is torsion-free;
(c) G is torsion-free.

Proof. Clearly (c) ⇒ (a).

(a)⇒ (b). We argue by induction on the nilpotency class n of G. The assertion is clear for $n = 1$; assume it holds for all nilpotent groups of class $< n$. We first prove that the group $Z_2(G)/Z_1(G)$ is torsion-free.

We will show that for each non-trivial element $\bar{x} \in Z_2(G)/Z_1(G)$, there exists a homomorphism $\varphi \in \operatorname{Hom}(Z_2(G)/Z_1(G), Z_1(G))$ such that $\varphi(\bar{x}) \neq 1$. Since $Z_1(G)$ is torsion-free this would imply that $Z_2(G)/Z_1(G)$ is torsion-free as well. Let $x \in Z_2(G)$ be the element which projects to $\bar{x} \in Z_2(G)/Z_1(G)$. Thus $x \notin Z_1(G)$, therefore there exists an element $g \in G$ such that $[g, x] \in Z_1(G) \setminus \{1\}$. Define the map $\tilde{\varphi} : Z_2(G) \to Z_1(G)$ by:

$$\tilde{\varphi}(y) := [y, g],$$

where $g \in G$ is the element above (such that $[g, x] \neq 1$). Clearly, $\tilde{\varphi}(x) \neq 1$; since $Z_1(G)$ is the center of G, the map $\tilde{\varphi}$ descends to a map $\varphi : Z_2(G)/Z_1(G) \to Z_1(G)$. It follows from Part 3 of Lemma 5.1 that $\tilde{\varphi}$ is a homomorphism. Hence, φ is a homomorphism as well. Since $Z_1(G)$ is torsion-free, it follows that $Z_2(G)/Z_1(G)$ is torsion-free too. Now, we replace G by the group $\bar{G} = G/Z_1(G)$.

Since $Z_2(G)/Z_1(G)$ is torsion-free, the group $\bar{G}$ has torsion-free center. Hence, by the induction hypothesis, $Z_i(\bar{G})/Z_{i-1}(\bar{G})$ is torsion-free for every $i \geq 1$. However,

$$Z_i(\bar{G})/Z_{i-1}(\bar{G}) \cong Z_{i+1}(G)/Z_i(G),$$

for every $i \geqslant 1$. Thus, every group $Z_{i+1}(G)/Z_i(G)$ is torsion-free, proving (b).

(b)⇒ (c). In view of (b), for each i, $m \neq 0$ and each $x \in Z_i(G) \setminus Z_{i-1}(G)$ we have that $x^m \notin Z_{i-1}(G)$. Thus $x^m \neq 1$. Therefore, G is torsion-free. □

Remark 5.35. Proposition 5.34 *does not imply* that for torsion-free nilpotent groups the quotients $C^iG/C^{i+1}G$ are torsion-free. This is, in general, false. Indeed, given an integer $p \geqslant 2$, consider the following subgroup G of the integer Heisenberg group $H_3(\mathbb{Z})$:

$$G = \left\{ \begin{pmatrix} 1 & k & n \\ 0 & 1 & pm \\ 0 & 0 & 1 \end{pmatrix} \; ; \; k, m, n \in \mathbb{Z} \right\} .$$

Since $H_3(\mathbb{Z})$ is poly-C_∞, so is G. On the other hand, the commutator subgroup in G is:

$$G' = \left\{ \begin{pmatrix} 1 & 0 & pn \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \; ; \; n \in \mathbb{Z} \right\} .$$

The quotient G/G' is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}_p$.

5.2 Polycyclic groups

Definition 5.36. A group G is *polycyclic* if it admits a subnormal descending series

$$G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_n \triangleright N_{n+1} = \{1\} \tag{11}$$

such that N_i/N_{i+1} is cyclic for all $i \geqslant 0$.

A series as in (11) is called a *cyclic series*, and its *length* is the number of non-trivial groups in this sequence, this number is $\leqslant n+1$ in (11). The *length* $\ell(G)$ of a polycyclic group is the least length of a cyclic series of G.

If, moreover, N_i/N_{i+1} is infinite cyclic for all $i \geqslant 0$, then the group G is called *poly-C_∞* and the series is called a *C_∞–series*.

We declare the trivial group to be poly-C_∞ as well.

Remark 5.37. If G is poly-C_∞ then Corollary 3.17 implies that $N_i \simeq N_{i+1} \rtimes \mathbb{Z}$ for every $i \geqslant 0$; thus, the group G is obtained from $N_n \simeq \mathbb{Z}$ by *successive semidirect products with $\mathbb{Z}$*.

For general polycyclic groups G the above is no longer true, for instance, G could be a finite group. However, the above property is *almost true* for G: *every polycyclic group contains a normal subgroup of finite index which is poly-C_∞* (see Proposition 5.45).

Proposition 5.38. *1. A polycyclic group has the bounded generation property. More precisely, let G be a group with a cyclic series* (11) *of length n and let t_i be such that t_iN_{i+1} is a generator of N_i/N_{i+1}. Then every $g \in G$ can be written as $g = t_1^{k_1} \cdots t_n^{k_n}$, with $k_1, \ldots, k_n$ in $\mathbb{Z}$.*

2. A polycyclic torsion group is finite.

3. Any subgroup of a polycyclic group is polycyclic, and, hence, finitely generated.

4. *If N is a normal subgroup in a polycyclic group G, then G/N is polycyclic.*

5. *If $N \lhd G$ and both N and G/N are polycyclic then G is polycyclic.*

6. *Properties (3) and (5) hold with 'polycyclic' replaced by 'poly-C_∞', but not (4).*

Proof. Part (1) follows by an easy induction on n.

Part (2) follows immediately from (1).

(3). Let H be a subgroup in G. Given a cyclic series for G as above, the intersections $H \cap N_i$ define a cyclic series for H.

(4). The proof is by induction on the length $\ell(G) = n$. For $n = 1$, G is cyclic and any quotient of G is also cyclic.

Assume that the statement is true for all $k \leqslant n$, and consider a group G with $\ell(G) = n + 1$. Let N_1 be the first term distinct from G in this cyclic series. By the induction hypothesis, $N_1/(N_1 \cap N) \simeq N_1N/N$ is polycyclic. The subgroup N_1N/N is normal in G/N and $(G/N)/(N_1N/N) \simeq G/N_1N$ is cyclic, as it is a quotient of G/N_1. It follows that G/N is polycyclic.

(5) Consider the cyclic series

$$G/N = Q_0 \geqslant Q_1 \geqslant \cdots \geqslant Q_n = \{\overline{1}\}$$

and

$$N = N_0 \geqslant N_1 \geqslant \cdots \geqslant N_k = \{1\}\,.$$

Given the quotient map $\pi : G \to G/N$ and $H_i := \pi^{-1}(Q_i)$, the following is a cyclic series for G:

$$G \geqslant H_1 \geqslant \ldots \geqslant H_n = N = N_0 \geqslant N_1 \geqslant \ldots \geqslant N_k = \{1\}\,.$$

(6) The proofs of properties (3) and (5) with 'polycyclic' replaced by 'poly-C_∞' are identical. A counter-example for (4) with 'polycyclic' replaced by 'poly-C_∞' is $G = \mathbb{Z}$, $N = 2\mathbb{Z}$. □

Remarks 5.39. 1. If G is polycyclic then, in general, the subset $\operatorname{Tor} G \subset G$ of finite order elements in G is neither a subgroup nor a finite set.

Consider for instance the infinite dihedral group D_∞. This group can be realized as the group of isometries of $\mathbb{R}$ generated by the symmetry $s : \mathbb{R} \to \mathbb{R}$, $s(x) = -x$ and the translation $t : \mathbb{R} \to \mathbb{R}$, $t(x) = x + 1$, and as noted before (see Section **??**) $D_\infty = \langle t \rangle \rtimes \langle s \rangle$. Therefore D_∞ is polycyclic by Proposition 5.38, (5), but $\operatorname{Tor} D_\infty$ is the union of a left coset and the trivial subgroup:

$$\operatorname{Tor} G = s\,\langle t \rangle \cup \{1\}.$$

2. Every polycyclic group is virtually torsion-free (see Proposition 5.45).

Proposition 5.40. *Every finitely generated nilpotent group is polycyclic.*

Proof. This may be proved using Proposition 5.38, Part (5), and an induction on the nilpotency class or directly, by constructing a series as in (11) as follows: Consider the finite descending series with terms $C^k G$. For every $k \geqslant 1$, $C^k G / C^{k+1} G$ is finitely generated abelian (see Corollary 5.12). According to the classification of finitely generated abelian groups, there exists a finite subnormal descending series

$$C^k G = A_0 \geqslant A_1 \geqslant \cdots \geqslant A_n \geqslant A_{n+1} = C^{k+1} G$$

such that every quotient A_i / A_{i+1} is cyclic. By inserting all these finite descending series into the one defined by $C^k G$'s, we obtain a finite subnormal cyclic series for G. □

Theorem 5.41 (K. A. Hirsch, [Hir38])**.** *All polycyclic groups are residually finite.*

We will prove a slightly stronger statement, generalizing Corollary 4.8.

Theorem 5.42. *If a group G is virtually isomorphic to a polycyclic group, then G is residually finite.*

Proof. Since for a subgroup $G_0 \leqslant G$ of finite index, G_0 is residually finite if and only if G is, the problem reduces to the following: If $F \lhd G$ is a finite subgroup and $G_1 \cong G/F$ is polycyclic, then G is residually finite. The proof is by induction on the cyclic length $\ell(G_1)$ of G_1. For $\ell(G_1) = 1$ the statement follows from Corollary 4.7.

Assuming that the claim holds for all groups G_1 of cyclic length n, consider the case when $\ell(G_1) = n + 1$. Then G_1 contains a normal subgroup G_2 such that $C = G_1/G_2$ is cyclic. Let H denote the preimage of G_2 under the quotient homomorphism $G \to G_1$. We thus have the short exact sequence

$$1 \to H \to G \to C \to 1.$$

By the induction hypothesis, the group H is residually finite. The subgroup G_2 of G_1 is finitely generated according to Proposition 5.38. Hence, H is finitely generated as well. Corollary 4.7 implies that G is residually finite. This concludes the proof of the theorem. □

An edifying example of a polycyclic group is the following.

Proposition 5.43. *Let $m, n \geqslant 1$ be two integers, and let $\varphi : \mathbb{Z}^n \to \mathrm{Aut}(\mathbb{Z}^m)$ be a homomorphism.*

The semidirect product $G = \mathbb{Z}^m \rtimes_\varphi \mathbb{Z}^n$ is a poly-C_∞ group.

Proof. The quotient $G/\mathbb{Z}^m$ is isomorphic to $\mathbb{Z}^n$. Therefore by Proposition 5.38, (6), the group G is poly-C_∞. □

Exercise 5.44. Let $\mathcal{T}_n(\mathbb{K})$ be the group of invertible upper-triangular $n \times n$ matrices with entries in a field $\mathbb{K}$.

1. Prove that $\mathcal{T}_n(\mathbb{K})$ is a semidirect product of its nilpotent subgroup $\mathcal{U}_n(\mathbb{K})$ introduced in Exercise 5.9, and the subgroup of diagonal matrices.

2. Prove that, if $\mathbb{K}$ hsa zero characteristic, the subgroup of $\mathcal{T}_n(\mathbb{K})$ generated by $I + E_{12}$ and by the diagonal matrix with $(-1, 1, \ldots, 1)$ on the diagonal is isomorphic to the infinite dihedral group D_∞. Deduce that $\mathcal{T}_n(\mathbb{K})$ is not nilpotent.

Proposition 5.45. *A polycyclic group G contains a normal subgroup of finite index which is poly-C_∞.*

Proof. We argue by induction on the length $\ell(G) = n$. For $n = 1$ the group G is cyclic and the statement obviously true. Assume that the assertion is true for n and consider a polycyclic group G having a cyclic series (11).

The induction hypothesis implies that N_1 contains a normal subgroup S of finite index which is poly-C_∞. Known results in group theory imply that S has a finite-index subgroup S_1 which is normal in G. Proposition 5.38, Part (6), implies that S_1 is poly-C_∞ as well.

If G/N_1 is finite then S_1 has finite index in G.

Assume that G/N_1 is infinite cyclic. Then the group $K = G/S_1$ contains the finite normal subgroup $F = N_1/S_1$ such that K/F is isomorphic to $\mathbb{Z}$. Corollary 3.17 implies that K is a semidirect product of F and an infinite cyclic subgroup $\langle x \rangle$. The conjugation by x defines an automorphism of F and since $\mathrm{Aut}(F)$ is finite, there exists r such that the conjugation by x^r is the identity on F. Hence $F \langle x^r \rangle$ is a finite-index subgroup in K and it is a direct product of F and $\langle x^r \rangle$. We conclude that $\langle x^r \rangle$ is a finite index normal subgroup of K. We have that $\langle x^r \rangle = G_1/S_1$, where G_1 is a finite index normal subgroup in G, and G_1 is poly-C_∞ since S_1 is poly-C_∞. □

Corollary 5.46. *(a) A poly-C_∞ group is torsion-free.*

(b) A polycyclic group is virtually torsion-free.

Proof. In view of Proposition 5.45, it suffices to prove (a). Consider a poly-C_∞ group G. We argue by induction on the cyclic length $\ell(G) = n$. For $n = 1$, the group G is infinite cyclic and the statement obviously holds. Assume that the statement is true for all groups of cyclic length at most n and consider a group G with $\ell(G) = n + 1$ and the cyclic series (11). Let g be an element of finite order in G. Then its image in the infinite cyclic quotient G/N_1 is the identity, hence $g \in N_1$. The induction hypothesis implies that $g = 1$. □

Proposition 5.47. *Let G be a finitely generated nilpotent group. The following are equivalent:*

1. *G is poly-C_∞;*
2. *G is torsion-free;*
3. *the center of G is torsion-free.*

Proof. Implication (1)⇒ (2) is Corollary 5.46, (a), while the implication (2)⇒ (3) is obvious. The implication (3)⇒ (1) follows from Proposition 5.34. □

Proposition 5.48. *Every polycyclic group is finitely presented.*

Proof. The proof is an easy induction on the minimal length of a cyclic series, combined with Proposition 3.43. □

One parameter measuring the complexity of the "poly-C_∞ part" of any polycyclic group is the *Hirsch number* (generalizing the Hirsch length for nilpotent groups), defined as follows:

Proposition 5.49. *The number of infinite factors in a cyclic series of a polycyclic group G is the same for all series. This number is called the* Hirsch number *(or* Hirsch length*) of G.*

Proof. The proof will follow from the following observation on cyclic series:

Lemma 5.50. *Any refinement of a cyclic series is also cyclic. Moreover, the number of quotients isomorphic to $\mathbb{Z}$ is the same for both series.*

Proof. Consider a cyclic series

$$H_0 = G \geqslant H_1 \geqslant \ldots \geqslant H_n = \{1\}\,.$$

A refinement of this series is composed of the following sub-series

$$H_i = R_k \geqslant R_{k+1} \geqslant \ldots \geqslant R_{k+m} = H_{i+1}\,.$$

Each quotient R_j/R_{j+1} embeds naturally as a subgroup in H_i/R_{j+1}, and the latter is a quotient of the cyclic group H_i/H_{i+1}; hence all quotients are cyclic. If H_i/H_{i+1} is finite then all quotients R_j/R_{j+1} are finite.

Assume now that $H_i/H_{i+1} \simeq \mathbb{Z}$. We prove by induction on $m \geqslant 1$ that exactly one among the quotients R_j/R_{j+1} is isomorphic to $\mathbb{Z}$, and the other quotients are finite. For $m = 1$ the statement is clear. Assume that it is true for m and consider the case of $m + 1$.

If H_i/R_{k+m} is finite then all R_j/R_{j+1} with $j \leqslant k+m-1$ are finite. On the other, under this assumption, hand R_{k+m}/R_{k+m+1} cannot be finite, otherwise H_i/H_{i+1} would be finite.

Assume that $H_i/R_{k+m} \simeq \mathbb{Z}$. The induction hypothesis implies that exactly one quotient R_j/R_{j+1} with $j \leqslant k+m-1$ is isomorphic to $\mathbb{Z}$ and the others are finite. The quotient R_{k+m}/R_{k+m+1} is a subgroup of $H_i/R_{k+m} \simeq \mathbb{Z}$ such that the quotient by this subgroup is also isomorphic to $\mathbb{Z}$. This can only happen when R_{k+m}/R_{k+m+1} is trivial. □

Proposition 5.49 now follows from Lemma 5.50 and the Jordan-Hölder Theorem. □

Exercise 5.51. Show that for each finitely generated nilpotent group the Hirsch number equals the *Hirsch length* $h(G)$, defined earlier.

In view of this exercise, the Hirsch number for a polycyclic group G will be again denoted $h(G)$.

A natural question to ask is the following.

Question 5.52. Since poly-C_∞ groups are constructed by successive semidirect products with $\mathbb{Z}$, is there a way to detect during this construction whether the group is nilpotent or not?

The answer to this question has some interesting relation to the geometry of groups (more precisely, their rate of growth).

Remark 5.53. We conclude the section on polycyclic groups by noting that one is able to list three types of induction arguments that can be used when proving results about polycyclic groups:

1. induction on the length;
2. induction on the Hirsch length;
3. noetherian induction. The third type of induction will be explained later on (see Remark 5.64).

5.3 Solvable groups: Definition and basic properties

Recall that G' denotes the *derived subgroup* $[G, G]$ of the group G. Given a group G, we define its *iterated commutator subgroups* $G^{(k)}$ inductively by:

$$G^{(0)} = G, G^{(1)} = G', \ldots, G^{(k+1)} = \left(G^{(k)}\right)', \ldots$$

The descending series

$$G \trianglerighteq G' \trianglerighteq \ldots \trianglerighteq G^{(k)} \trianglerighteq G^{(k+1)} \trianglerighteq \ldots$$

is called the *derived series* of the group G.

Note that all subgroups $G^{(k)}$ are *characteristic* in G.

Definition 5.54. A group G is *solvable* if there exists k such that $G^{(k)} = \{1\}$. The minimal k such that $G^{(k)} = \{1\}$ is called the *derived length* of G and the group G itself is called *k-step solvable*. A solvable group of derived length at most two is called *metabelian*.

We will use the notation $\ell_{\mathrm{der}}(G)$ for the derived length.

Proposition 5.55. *1. If N is a normal subgroup in G and both N and G/N are solvable, then G is solvable. If the derived lengths of G/N and N are at most d, d' respectively, then the derived length of G is at most $d + d'$. In other words, the derived length is subadditive:*

$$\ell_{\mathrm{der}}(G) \leqslant \ell_{\mathrm{der}}(N) + \ell_{\mathrm{der}}(G/N).$$

2. Every subgroup H of a solvable group G is solvable and

$$\ell_{\mathrm{der}}(H) \leqslant \ell_{\mathrm{der}}(G).$$

3. If G is solvable and $N \lhd G$, then G/N is solvable and

$$\ell_{\mathrm{der}}(G/N) \leqslant \ell_{\mathrm{der}}(G).$$

Note that the statement (1) is not true when 'solvable' is replaced by 'nilpotent', consider, for instance, the infinite dihedral group D_∞.

Proof. (1) We are assuming that G/N is solvable of derived length d and N is solvable of derived length d'. Since $(G/N)^{(d)} = \{\bar{1}\}$ it follows that $G^{(d)} \leqslant N$. Then, as $G^{(d+i)} \leqslant N^{(i)}$, we obtain $G^{(d+d')} = \{1\}$.

(2) Note that for every subgroup H of a group G, $H' \leqslant G'$. Thus, by induction,

$$H^{(i)} \leqslant G^{(i)}.$$

If G is solvable of derived length k then $G^{(k)} = \{1\}$; thus $H^{(k)} = \{1\}$ as well and, hence, H is also solvable.

(3) Consider the quotient map $\pi : G \to G/N$. It is immediate that $\pi\left(G^{(i)}\right) = (G/N)^{(i)}$, in particular if G is solvable then G/N is solvable. □

For the next exercise, we will need the following definition: A finite sequence of vector subspaces

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_k$$

in a vector space V is called a *flag* in V. If the number of the subspaces in such a sequence is maximal possible (equal $\dim(V) + 1$), the flag is called *full* or *complete*. In other words, $\dim(V_i) = i$ for all members of this sequence.

Exercise 5.56. 1. Prove that the subgroup $\mathcal{T}_n(\mathbb{K})$ of upper-triangular matrices in $GL(n, \mathbb{K})$, where $\mathbb{K}$ is a field, is solvable. [Hint: you may use Exercise 5.9.]

2. Use Part (1) to show that for a finite-dimensional vector space V, the subgroup G of $GL(V)$ consisting of elements g preserving a complete flag in V (i.e. $gV_i = V_i$, for every $g \in G$ and every i) is solvable.

3. Let V be a $\mathbb{K}$-vector space of dimension n, and let

$$V_0 = 0 \subset V_1 \subset \cdots \subset V_{k-1} \subset V_k = V$$

be a flag, not necessarily complete. Let G be a subgroup of $GL(V)$ preserving this flag. For every $i \in \{1, 2, \ldots, k-1\}$ let ρ_i be the projection $G \to GL(V_{i+1}/V_i)$. Prove that if every $\rho_i(G)$ is solvable, then G is also solvable.

Exercise 5.57. 1. Let $\mathbb{F}_k$ denote the field with k elements. Use the 1-dimensional vector subspaces in $\mathbb{F}_k^2$ to construct a homomorphism $GL(2, \mathbb{F}_k) \to S_n$ for an appropriate n.

2. Prove that $GL(2, \mathbb{F}_2)$ and $GL(2, \mathbb{F}_3)$ are solvable.

5.4 Solvable versus polycyclic

Proposition 5.58. *Every polycyclic group G is solvable.*

Proof. This follows immediately by an induction argument on the cyclic length of G and Part (1) of Proposition 5.55. □

Definition 5.59. A group is said to be *noetherian*, or to satisfy the *maximal condition* if for every increasing sequence of subgroups

$$H_1 \leqslant H_2 \leqslant \cdots \leqslant H_n \leqslant \cdots \tag{12}$$

there exists N such that $H_n = H_N$ for every $n \geqslant N$.

Proposition 5.60. *A group G is noetherian if and only if every subgroup of G is finitely generated.*

Proof. Assume that G is a noetherian group, and let $H \leqslant G$ be a subgroup which is not finitely generated. Pick $h_1 = H \setminus \{1\}$ and let $H_1 = \langle h_1 \rangle$. Inductively, assume that

$$H_1 < H_2 < ... < H_n$$

is a strictly increasing sequence of finitely generated subgroups of H, pick $h_{n+1} \in H \setminus H_n$, and set $H_{n+1} = \langle H_n, h_{n+1} \rangle$. We thus have a strictly increasing infinite sequence of subgroups of G, contradicting the assumption that G is noetherian.

Conversely, assume that all subgroups of G are finitely generated, and consider an increasing sequence of subgroups as in (12). Then $H = \bigcup_{n \geqslant 1} H_n$ is a subgroup, hence generated by a finite set S. There exists N such that $S \subseteq H_N$, hence $H_N = H = H_n$ for every $n \geqslant N$. □

Exercise 5.61. If G_1 is noetherian and G_2 is virtually isomorphic to G_1, then G_2 is also noetherian.

Proposition 5.62. *A solvable group is polycyclic if and only if it is noetherian.*

Proof. The 'only if' part follows immediately from Parts (1) and (3) of Proposition 5.38. Let G be a noetherian solvable group. We prove by induction on the derived length k that G is polycyclic.

For $k = 1$ the group is abelian, and since, by hypothesis, G is finitely generated, it is polycyclic.

Assume that the statement is true for k and consider a solvable group G of derived length $k + 1$. The commutator subgroup $G' \leqslant G$ is also noetherian and solvable of derived length k. Hence, by the induction hypothesis, G' is polycyclic. The abelianization $G_{ab} = G/G'$ is finitely generated (because G is, by hypothesis), hence it is polycyclic. It follows that G is polycyclic by Proposition 5.38 (5). □

Remark 5.63. There are noetherian groups that are not virtually polycyclic, e.g. *Tarski monsters*: finitely generated groups such that every proper subgroup is cyclic, see [Ol′91].

Remark 5.64.

1. Proposition 5.62 implies that, given any property $(*)$ satisfied by the trivial group $\{1\}$, a polycyclic group contains a maximal subgroup with property $(*)$.

2. With the above result, we can introduce a third type of inductive argument that can be used in polycyclic groups, besides those appearing in Remark 5.53: the noetherian induction. Thus, assume that we have to prove that every polycyclic group has a certain property P. Then it suffices to check that the trivial group $\{1\}$ has property P (initial case), and that a group G such that all its proper quotients G/N have P must in its turn have property P (inductive step).

   Indeed, assume that, once all the above was checked, one finds a group G that does not have property P. Let $(*)$ be the property of being a normal subgroup K such that the quotient G/K does not have property P, and let N be a maximal subgroup satisfying $(*)$. Then G/N is a polycyclic subgroup without property P such that all its proper quotients have property P, contradicting the inductive step.

3. The noetherian induction can be used not only for polycyclic groups, but for any class of noetherian groups that is closed with respect to the operation of taking quotients.

By Proposition 5.58 every nilpotent group is solvable. A natural question to ask is to find a relationship between nilpotency class and derived length.

Proposition 5.65. *1. For every group G and every $i \geqslant 0$,*

$$G^{(i)} \leqslant C^{2^i} G.$$

2. If G is a k-step nilpotent group then its derived length is at most

$$[\log_2 k] + 1\,.$$

Proof. (1) The statement is obviously true for $i = 0$. Assume that it is true for i. Then

$$G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] \leqslant \left[C^{2^i} G, C^{2^i} G\right] \leqslant C^{2^{i+1}} G.$$

In the last inclusion we applied Proposition 5.27.

(2) follows immediately from (1). □

Remark 5.66. The derived length can be much smaller than the nilpotency class: the dihedral subgroup D_{2n} with $n = 2^k$ is k-step nilpotent and metabelian.

An instructive example of solvable group is the *lamplighter group*. This group is the wreath product $G = \mathbb{Z}_2 \wr \mathbb{Z}$ in the sense of Definition 2.2.

Exercise 5.67. Prove that if K, H are solvable groups then $K \wr H$ is solvable. In particular, the lamplighter group G is solvable (even metabelian).

In view of Ex. Sheet 1, since wreath products of finitely generated groups are finitely generated as well, the lamplighter group is finitely generated. On the other hand:

1. *Not all subgroups in the lamplighter group G are finitely generated:* the subgroup $\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_2$ of G is not finitely generated.

2. *The lamplighter group G is not virtually torsion-free:* For any finite-index subgroup $H \leqslant G$, $H \cap \bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_2$ has finite index in $\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_2$; in particular this intersection is infinite and contains elements of order 2.

   Both (1) and (2) imply that the lamplighter group is *not polycyclic*.

3. The commutator subgroup G' of the lamplighter group G coincides with the following subgroup of $\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_2$:

   $$C = \{f : \mathbb{Z} \to \mathbb{Z}_2 \mid \mathrm{Supp}(f) \text{ has even cardinality}\}\,, \tag{13}$$

   where $\mathrm{Supp}(f) = \{n \in \mathbb{Z} \mid f(n) = 1\}$.

   [*NB. The notation here is additive, the identity element is* 0.]

   In particular, G' *is not finitely generated* and the group G is metabelian (since G' abelian).

We prove (3). First of all, C is clearly a subgroup. Note also that

$$(f,m)^{-1} = (-\varphi(-m)f, -m)\,,$$

where φ is the action of $\mathbb{Z}$ on the space of functions $f : \mathbb{Z} \to \mathbb{Z}_2$ via *shift*: For $m \in \mathbb{Z}$,

$$\varphi(m) : f(x) \mapsto f(x+m).$$

If we think of functions f as biinfinite sequences, then $\varphi(m)$ acts on a sequence via shifting all the indices by m. A straightforward calculation gives

$$[(f,m),(g,n)] = (f - g - \varphi(n)f + \varphi(m)g\,,\, 0)\,.$$

Now, observe that either $\mathrm{Supp}(f)$ and $\mathrm{Supp}(\varphi(n)f)$ are disjoint, in which case $\mathrm{Supp}(f - \varphi(n)f)$ has cardinality twice the cardinality of $\mathrm{Supp}\, f$, or they overlap on a set of cardinality k; in the latter case, $\mathrm{Supp}(f - \varphi(n)f)$ has cardinality twice the cardinality of $\mathrm{Supp}\, f$ minus $2k$. The same holds for $\mathrm{Supp}(-g + \varphi(m)g)$. Since C is a subgroup,

$$(f - g - \varphi(n)f + \varphi(m)g) = (f - \varphi(n)f - (g - \varphi(m)g)) \in C.$$

This shows that $G' \leqslant C$.

Consider the opposite inclusion. The subgroup C is generated by functions $f : \mathbb{Z} \to \mathbb{Z}_2\,, \mathrm{Supp}\, f = \{a,b\}$, where a, b are distinct integers; thus, it suffices to show that $(f,0) \in G'$. Let $\delta_a : f : \mathbb{Z} \to \mathbb{Z}_2\,,\, \mathrm{Supp}\, \delta_a = \{a\}$. Then

$$[(\delta_a, 0), (0, b-a)] = (\delta_a - \varphi(b-a)\delta_a, 0) = (f, 0)$$

which implies that $(f,0) \leqslant G'$.

We conclude this section by noting that, unlike polycyclic groups, solvable groups may not be finitely presented. An example of such a group is the wreath product $\mathbb{Z} \wr \mathbb{Z}$ [Bie79]. We refer to the same paper for a survey on finitely presented solvable groups. Nevertheless, a solvable group may be finitely presented without being polycyclic; for instance the Baumslag–Solitar group

$$G = BS(1,p) = \left\langle a, b | aba^{-1} = b^p \right\rangle$$

is metabelian but not polycyclic (for $|p| \geqslant 2$). The derived subgroup G' of G is isomorphic to the additive group of p-adic rational numbers, i.e. rational numbers whose denominators are powers of p. In particular, G' is not finitely generated. Hence, in view of Proposition 5.38, G is not polycyclic.

Exercise 5.68. Show that the group $G = BS(1,p)$ is metabelian.

6 Linear groups

6.1 Preliminary results

In this section, $\mathbb{K}$ will denote an algebraically closed field (e.g. $\mathbb{C}$) and V a finite-dimensional vector space over $\mathbb{K}$.

We let $End(V)$ denote the algebra of (linear) endomorphisms of V and $GL(V)$ the group of invertible endomorphisms of V. Linear actions of groups G on V are called *representations* of G on V.

A group G that is isomorphic to a subgroup of $GL(V)$ for some V, is called a *matrix group* or a *linear group*.

We recall a few standard facts, either seen in courses in past years, or easily found in textbooks. Some of the proofs being more elaborate and beyond the scope of this course, we will not give them here, but simply assume the results and use them.

Lemma 6.1. *The bilinear form on $End(V)$, regarded as a vector space over $\mathbb{K}$, defined by*

$$\tau : End(V) \times End(V) \to \mathbb{K}, \tau(A, B) = \mathrm{tr}(AB^T)$$

is non-degenerate.

Proof. Representing A and B by their matrix entries $(a_{ij}), (b_{kl})$, we obtain:

$$tr(AB^T) = \Sigma_{i,j} a_{ij}\, b_{ij}).$$

Therefore, if for some $i, j, a_{ij} \neq 0$, we take B such that $b_{kl} = 0$ for all $(k, l) \neq (i, j)$ and $b_{ij} = 1$. Then $tr(AB^T) = a_{ij} \neq 0$. □

Fixing a basis for V determines:

- an isomorphism of groups $GL(V) \simeq GL_n(\mathbb{K})$, where $GL_n(\mathbb{K})$, the general linear group, is the group of all invertible $n \times n$ matrices over $\mathbb{K}$;
- an isomorphism of algebras $End(V) \simeq M_n(\mathbb{K})$, where the latter is the algebra of all $n \times n$ matrices over $\mathbb{K}$.

We use the following notation:

- $SL_n(\mathbb{K}) = \{g \in GL_n(\mathbb{K}) \mid \det(g) = 1\}$ for the special linear group;
- $T_n(\mathbb{K})$ for the group of invertible upper-triangular $n \times n$ matrices with entries in the field $\mathbb{K}$;
- $U_n(\mathbb{K})$ for the upper unitriangular group, that is the subgroup of $T_n(\mathbb{K})$ composed of matrices with all diagonal entries equal to 1.

The subalgebra of $End(V)$ generated by a linear group G will be denoted by $\mathbb{K}[G]$; this is just the linear span of G over $\mathbb{K}$.

If V is a vector space and $A \subset End(V)$ is a subgroup, then A is said to act *irreducibly* on V if V contains no proper subspace $\{0\} \subsetneq V' \subsetneq V$ such that $aV' \subset V'$ for all $a \in A$.

We say that the action of A on V is *completely reducible* if V decomposes as a direct sum of irreducible subspaces.

A linear group $G \leq GL(V)$ is called *triangularizable* if there exists a basis of V with respect to which G is represented by upper-triangular matrices.

If G is triangularizable then G' is unipotent, hence nilpotent. So G is solvable. The converse can be easily proven in the particular case of abelian groups, as follows.

Lemma 6.2. *If A is an abelian group acting irreducibly on V then V has dimension* 1.

Proof. As $\mathbb{K}$ is algebraically closed, every $a \in A$ has at least an eigenvalue. The corresponding space of eigenvectors is b-invariant for every $b \in A$, hence it must coincide with V. Thus, every $a \in A$ is a multiple of the identity map on V, hence by irreducibility V must have dimension 1. □

Lemma 6.2 and an easy induction on the dimension of V give the following.

Lemma 6.3. *If A is an abelian group acting on V then there exists a basis of V with respect to which A becomes upper triangular.*

A proof of the following theorem can be found, for instance, in [Lan02, Chapter XVII, §3, Corollary 3.3]:

Theorem 6.4 (Burnside's theorem)**.** *If $A \subset End(V)$ is a subalgebra which acts absolutely irreducibly on a finite-dimensional vector space V, then $A = End(V)$. In particular, if $G \subset End(V)$ is a subsemigroup acting irreducibly, then G spans $End(V)$ as a vector space, i.e. $\mathbb{K}[G] = End(V)$.*

Corollary 6.5. *If G is irreducible then the only matrices commuting with all the elements of G are the identity and its scalar multiples.*

Theorem 6.6. *Suppose that $G \leq \mathrm{GL}_n(\mathbb{K})$ is irreducible and that*

$$|\{\mathrm{tr}(g) \mid g \in G\}| = q < \infty.$$

Then $|G| \leq q^{n^2}$.

Proof. By the preceding theorem, G contains $m = n^2$ linearly independent matrices $w(1), \ldots, w(m)$. For $\underline{\mu} \in k^m$ let

$$G(\underline{\mu}) = \{g \in G \mid \mathrm{tr}(w(s)g) = \mu_s \ (s = 1, \ldots, m)\}.$$

Observe that $g = (g_{ij}) \in G(\underline{\mu})$ if and only if it satisfies the equations

$$\sum_{i=1}^{n} \sum_{l=1}^{n} w(s)_{il} g_{li} = \mu_s \quad (s = 1, \ldots, m).$$

This is a system of $m = n^2$ linearly independent equations, so it has at most one solution (g_{ij}). The result follows as there are just q^{n^2} possibilites for $\underline{\mu}$. □

Corollary 6.7. *Suppose that $G \leq \mathrm{GL}_n(k)$ is completely reducible and that $g^e = 1 \ \forall g \in G$. Then $|G| \leq e^{n^3}$.*

Proof. See Ex. Sheet 4. □

6.2 Virtually nilpotent and solvable subgroups of $GL_n(\mathbb{K})$

In this section we collect various properties about virtually nilpotent and solvable subgroups of $GL(n, \mathbb{K})$ for arbitrary fields $\mathbb{K}$ (not necessarily algebraically closed).

In what follows, V will denote a finite-dimensional vector space over a field $\mathbb{K}$.

Recall that an endomorphism $h \in End(V)$ of V is *nilpotent* if $h^k = 0$ for some $k > 0$. Equivalently, in some basis, h can be written as an upper triangular matrix with zeroes on the diagonal.

Automorphisms of V of the form $I+h$, with h nilpotent, are called *unipotent*. Here and in what follows, I is the identity map $V \to V$. An automorphism g of V is called *quasiunipotent* if all the eigenvalues of g are roots of unity in $\bar{\mathbb{K}}$. Equivalently, g is quasiunipotent if g^k is unipotent for some $k > 0$.

A subgroup $G < GL(V)$ is *unipotent* (respectively, *quasiunipotent*) if every element of G is unipotent (respectively, quasiunipotent).

Theorem 6.8 (Kolchin's theorem)**.** *Suppose that $\mathbb{K} = \bar{\mathbb{K}}$ and $G < GL(V)$ is a unipotent subgroup. Then G is conjugate to a subgroup of the group of invertible upper-triangular matrices $\mathcal{T}_n(\mathbb{K})$.*

Proof. The proof is by induction on the dimension n of V. The claim is clear for $n = 1$, hence, we assume that $n > 1$. The statement of the theorem amounts to the claim that G preserves a full flag

$$0 \subset V_1 \subset \ldots \subset V_{n-1} \subset V,$$

where $i = \dim(V_i)$ for each i. Indeed, given such a flag, we will inductively pick basis elements $\mathbf{e}_i \in V_i$ such that $\{\mathbf{e}_1, \ldots, \mathbf{e}_i\}$ is a basis in V_i. With respect to this basis, each subgroup of $GL(V)$ preserving the flag will be contained in $\mathcal{T}_n(\mathbb{K})$.

Suppose first that the action of G on V is reducible, that is G preserves a proper subspace $V' \subset V$. Then we obtain two induced actions of G on V' (by restriction) and on $V'' = V/V'$ (by projection). Since both actions preserve full flags in V', V'' (by the induction hypothesis), the combination of these flags yields a full G-invariant flag in V.

Therefore, we will assume that the action of G on V is irreducible. For each $g \in G$ the endomorphism $g' = g - I$ is nilpotent, hence, has zero trace. Therefore, for all $x \in G$, we have

$$tr(g'x) = tr(gx - x) = tr(I) - tr(I) = 0.$$

Since, by Burnside's theorem, G spans $End(V)$, we conclude that for each $x \in End(V)$ and each $g \in G$,

$$tr(g'x) = 0.$$

Using the fact that τ is a nondegenerate pairing on $End(V)$ (Lemma 6.1), we conclude that $g' = 0$ for all $g \in G$, i.e. $G = \{1\}$. □

The following theorem is a minor variation on Kolchin's theorem.

Proposition 6.9. *Suppose that $\mathbb{K} = \bar{\mathbb{K}}$, $G < GL(V)$ is quasiunipotent and, moreover, there exists an upper bound α on the orders of all eigenvalues of elements $g \in G$. Then G contains a finite index subgroup conjugate into the group of upper triangular matrices $\mathcal{T}_n(\mathbb{K})$. The index depends only on V and on α.*

Proof. The proof follows closely the proof of Kolchin's Theorem. As in Kolchin's Theorem, the proof is by induction on the dimension of V and it suffices to consider the case of subgroups acting irreducibly on V. For each $g \in G$ define a linear map

$$T_g : End(V) \to \mathbb{K}, \quad T_g(x) = tr(gx).$$

Since τ, $\tau(A, B) = tr(AB)$, is a nondegenerate pairing on $End(V)$ (see Lemma 6.1), for $g_1 \neq g_2 \in G$, we get $T_{g_1} \neq T_{g_2}$. As we assumed that the orders of the eigenvalues of elements of G are uniformly bounded, the set of traces of elements of G is finite. Therefore, for each $g \in G$, the set

$$\{T_g(x) : x \in G\}$$

is a certain finite set $C \subset \mathbb{K}$, independent of g. By Burnside's Theorem, G spans the algebra $End(V)$, which implies that for each $g \in G$, the map T_g is determined by its restriction to G. Thus, the set

$$\{T_g : End(V) \to \mathbb{K} | g \in G\}$$

is finite. We, therefore, conclude that the group G is finite. □

Suppose that $G < \mathcal{T}_n(\mathbb{K})$ is quasiunipotent with an upper bound on the orders of the eigenvalues. Then there exists $k > 0$ such that g^k is unipotent for each $g \in G$. Therefore, G contains a finite index subgroup G_1 contained in $\mathcal{U}_n(\mathbb{K})$. Since (see Example 5.7) the group $\mathcal{U}_n(\mathbb{K})$ is nilpotent, we obtain:

Corollary 6.10. *Suppose that $G < GL(V)$ is quasiunipotent and, moreover, there exists an upper bound α on the orders of all the eigenvalues of elements $g \in G$. Then G is virtually nilpotent. Moreover, the index of the nilpotent subgroup in G depends only on V and α.*

As far as linear solvable groups are concerned, we have the following results, which we give here without proof.

Theorem 6.11. (Lie-Kolchin-Mal'cev Theorem) *Let G be a solvable linear group of degree n. Then G has a triangularizable normal subgroup K of finite index at most $\mu(n)$, a number that depends only on n.*

Definition 6.12. Given two classes of groups $\mathcal{X}$ and $\mathcal{Y}$ we say that a group G is $\mathcal{X}$-by-$\mathcal{Y}$ if there exists a short exact sequence

$$\{1\} \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow \{1\},$$

such that $N \in \mathcal{X}$ and $Q \in \mathcal{Y}$.

Corollary 6.13. *Let G be a solvable linear group of degree n.*

(i) G is virtually unipotent-by-abelian;

(ii) the derived length of G is at most $\beta(n) := n + \log_2 \mu(n)$.

Claim (ii) is the *Zassenhaus Theorem*.

This can be combined with the following general result.

Theorem 6.14 (see [Rag72])**.** *Every nilpotent subgroup of $GL(n, \mathbb{Z})$ is finitely generated.*

Corollary 6.13 and Theorem 6.14 imply the following.

Corollary 6.15. *Every finitely generated solvable group linear over $\mathbb{Z}$ is polycyclic.*

Proof. By Corollary 6.13 such a group G has a finite index subgroup that is unipotent-by-abelian, hence a finite index normal subgroup N that is polycyclic by Theorem 6.14.

The quotient G/N is solvable and finite, hence noetherian, hence polycyclic. Proposition 5.38, (5), implies that G is polycyclic. □

It is also true, conversely, that *every polycyclic group is linear over $\mathbb{Z}$* (theorem of L. Auslander).

Theorem 6.16 (Auslander's Theorem)**.** *Every polycyclic group is linear over $\mathbb{Z}$.*

For a proof we refer to [Seg05, Chapter 5].

Corollary 6.17. *Every polycyclic group is virtually nilpotent-by-abelian.*

We have thus obtained the following way of distinguishing polycyclic groups among solvable groups.

Theorem 6.18. *A finitely generated solvable group is polycyclic if and only if it is linear over $\mathbb{Z}$.*

7 Solvable versus nilpotent: growth of groups

7.1 The growth function

Definition 7.1. We introduce the following *asymptotic inequality* between functions $f, g : X \to \mathbb{R}$ with $X \subset \mathbb{R}$: we write $f \preceq g$ if there exist $a, b > 0$, $c \geqslant 0$ and $x_0 \in \mathbb{R}$ such that for all $x \in X$, $x \geqslant x_0$, we have $bx + c \in X$ and

$$f(x) \leqslant ag(bx + c).$$

If $f \preceq g$ and $g \preceq f$ then we write $f \asymp g$ and we say that f and g are *asymptotically equal*.

Suppose that G is a finitely generated group endowed with a word metric dist_S associated to a finite generating set S, with the usual assumptions that $S^{-1} = S$ and $1 \notin S$.

We define the *growth function*

$$\mathfrak{G}_{G,S}(R) := \mathrm{card}\ \bar{B}(1, R),$$

the cardinality of the closed R-ball centered at 1 with respect to the metric dist_S.

Lemma 7.2. *Assume that (G, dist_S) and (H, dist_X) are two groups with word metrics that are bi-Lipschitz equivalent to each other, i.e. there exists $L > 0$ and a bijection $f : G \to H$ such that*

$$\frac{1}{L}\mathrm{dist}_S(g, g') \leqslant \mathrm{dist}_X(f(g), f(g')) \leqslant L\mathrm{dist}_S(g, g')\,, \forall g, g' \in G\,. \qquad (14)$$

Then $\mathfrak{G}_{G,S} \asymp \mathfrak{G}_{H,X}$.

This is in particular true when $(H, \mathrm{dist}_X) = (G, \mathrm{dist}_{S'})$, for another finite set S' generating G.

Proof. Let $\bar{f} : H \to G$ be the inverse of f.

Let $D = \max(\mathrm{dist}_X(f(1_G), 1_H), \mathrm{dist}_S(1_G, \bar{f}(1_H))$. Then for each $R > 0$,

$$f(\bar{B}(1_G, R)) \subset \bar{B}(1_H, LR + D), \quad \bar{f}(\bar{B}(1_H, R)) \subset \bar{B}(1_G, LR + D).$$

It follows that

$$\mathrm{card}\ \bar{B}(1_G, R) \leqslant \mathrm{card}\, \bar{B}(1_H, LR + D)$$

and

$$\mathrm{card}\ \bar{B}(1_H, R) \leqslant \mathrm{card}\ \bar{B}(1_G, LR + D). \quad \square$$

Corollary 7.3. *If S, S' are two finite generating sets of G then $\mathfrak{G}_S \asymp \mathfrak{G}_{S'}$. Thus one can speak about the growth function $\mathfrak{G}_G$ of a group G, well defined up to the equivalence relation $\asymp$.*

Examples 7.4.

1. If $G = \mathbb{Z}^k$ then $\mathfrak{G}_S \asymp x^k$ for every finite generating set S.

2. If $G = F_k$ is the free group of finite rank $k \geqslant 2$ and S is the set of k generators then

$$\mathfrak{G}_S(n) = 1 + (q^n - 1)\frac{q+1}{q-1}, \quad q = 2k - 1.$$

Exercise 7.5.

1. Prove the two statements above.

2. Conclude that $\mathbb{Z}^m$ is bi-Lipschitz equivalent to $\mathbb{Z}^n$ if and only if $n = m$.

3. Compute the growth function for the group $\mathbb{Z}^2$ equipped with the generating set x, y, where $\{x, y\}$ is a basis of $\mathbb{Z}^2$.

Proposition 7.6. *1. If G is infinite, $\mathfrak{G}_S|_{\mathbb{N}}$ is strictly increasing.*

2. The growth function is sub-multiplicative*:*

$$\mathfrak{G}_S(r+t) \leqslant \mathfrak{G}_S(r)\mathfrak{G}_S(t)\,.$$

3. For each finitely generated group G, $\mathfrak{G}_G(r) \preceq 2^r$.

Proof. (1) Consider two integers $n < m$. As G is infinite there exists $g \in G$ at distance $d \geqslant m$ from 1. The shortest path joining 1 and g in $\mathrm{Cayley}(G,S)$ can be parameterized as an isometric embedding $p : [0,d] \to \mathrm{Cayley}(G,S)$. The vertex $p(n+1)$ is an element of $\bar{B}(1,m) \setminus \bar{B}(1,n)$.

(2) follows immediately from the fact that

$$\bar{B}(1,n+m) \subseteq \bigcup_{y \in \bar{B}(1,n)} \bar{B}(y,m)\,.$$

(3) follows from the existence of an epimorphism $\pi_S : F(S) \to G$, where S is a finite generating set of G. □

The property (2) implies that the function $\ln \mathfrak{G}_S(n)$ is sub-additive, hence by the Fekete's Lemma, see e.g. [HP74, Theorem 7.6.1], there exists a (finite) limit

$$\lim_{n\to\infty} \frac{\ln \mathfrak{G}_S(n)}{n}.$$

Hence, we also get a finite limit

$$\gamma_S = \lim_{n\to\infty} \mathfrak{G}_S(n)^{\frac{1}{n}}\,,$$

called *growth constant*. The property (1) implies that $\mathfrak{G}_S(n) \geqslant n$; whence, $\gamma_S \geqslant 1$.

Definition 7.7. If $\gamma_S > 1$ then G is said to be of *exponential growth*. If $\gamma_S = 1$ then G is said to be of *sub-exponential growth*.

Note that by Corollary 7.3, if there exists a finite generating set S such that $\gamma_S > 1$ then $\gamma_{S'} > 1$ for every other finite generating set S'. Likewise for the equality to 1.

Exercise 7.8. Prove that, for every $n \geqslant 2$, the group $SL(n,\mathbb{Z})$ has exponential growth.

Proposition 7.9. *(a) If H is a finitely generated subgroup in a finitely generated group G then $\mathfrak{G}_H \preceq \mathfrak{G}_G$.*

(b) If H is a subgroup of finite index in G then $\mathfrak{G}_H \asymp \mathfrak{G}_G$.

(c) If N is a normal subgroup in G then $\mathfrak{G}_{G/N} \preceq \mathfrak{G}_G$

(d) If N is a finite normal subgroup in G then $\mathfrak{G}_{G/N} \asymp \mathfrak{G}_G$.

Proof. (a) If X is a finite generating set of H and S is a finite generating set of G containing X then Cayley(H, X) is a subgraph of Cayley(G, S) and $\mathrm{dist}_X(1, h) \geqslant \mathrm{dist}_S(1, h)$ for every $h \in H$. In particular the closed ball of radius r and center 1 in Cayley(H, X) is contained in the closed ball of radius r and center 1 in Cayley(G, S).

The proofs of (b) and (d) are variations of the proof of Lemma 7.2.

(c) Let S be a finite generating set in G, and let $\bar{S} = \{sN \mid s \in S, s \notin N\}$ be the corresponding finite generating set in G/N. The epimorphism $\pi : G \to G/N$ maps the ball of center 1 and radius r onto the ball of center 1 and radius r. □

Question 7.10 (J. Milnor [Mil68b]). Is it true that the growth of a finitely generated group is either polynomial (i.e. $\mathfrak{G}_S(t) \preceq t^d$ for some integer d) or exponential (i.e. $\gamma_S > 1$)?

R. Grigorchuk in [Gri84] proved that Milnor's question has a negative answer, by constructing finitely generated groups of *intermediate growth*, i.e. their growth is superpolynomial but subexponential. More precisely, Grigorchuk proved that for every sub-exponential function f there exists a group G_f of intermediate growth equipped with a finite generating set S_f whose growth function $\mathfrak{G}_{S_f}(n)$ is larger than $f(n)$ for infinitely many n. The first explicit computations of growth functions (up to the equivalence relation $\asymp$) for some groups of intermediate growth were done by L. Bartholdi and A. Erschler in [BE12]. For every $k \in \mathbb{N}$, they constructed examples of torsion groups G_k and of torsion-free groups H_k such that their growth functions satisfy

$$\mathfrak{G}_{G_k}(x) \asymp \exp\left(x^{1-(1-\alpha)^k}\right),$$

and

$$\mathfrak{G}_{H_k}(x) \asymp \exp\left(\log x \cdot x^{1-(1-\alpha)^k}\right),$$

Here α is the number satisfying $2^{3-\frac{3}{\alpha}} + 2^{2-\frac{2}{\alpha}} + 2^{1-\frac{1}{\alpha}} = 2$.

We note that all currently known groups of intermediate growth have growth larger than $2^{\sqrt{n}}$. Existence of finitely presented groups of intermediate growth is unknown.

One can easily see that every abelian group has polynomial growth. It is a more difficult theorem (proven independently by Hyman Bass [Bas72] and Yves Guivarc'h [Gui70, Gui73]) that all nilpotent groups also have polynomial growth.

Definition 7.11. Let G be a finitely generated nilpotent group of class k. Let m_i denote the free rank of the abelian group $C^iG/C^{i+1}G$; define the *homogeneous dimension* of G,

$$d(G) = \sum_{i=1}^{k} i m_i.$$

Theorem 7.12 (Bass–Guivarc'h Theorem)**.** *The growth function of G satisfies*

$$\mathfrak{G}_G(n) \asymp n^d\,. \tag{15}$$

7.2 Wolf's Theorem

In this section we classify (virtually) polycyclic groups according to their growth. We first discuss a particular case for which the proof contains all the ideas used in the general case.

Notation 7.13. If G is a group, a semidirect product $G \rtimes_\Phi \mathbb{Z}$ is defined by a homomorphism $\Phi : \mathbb{Z} \to \mathrm{Aut}\,(G)$. The latter homomorphism is entirely determined by $\Phi(1) = \varphi$. We set

$$S = G \rtimes_\varphi \mathbb{Z} := G \rtimes_\Phi \mathbb{Z}$$

7.3 Automorphisms of $\mathbb{Z}^n$

Theorem 7.14. *The group of automorphisms of $\mathbb{Z}^n$ is isomorphic to $GL(n,\mathbb{Z})$.*

Proof. Consider the basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ of $\mathbb{Z}^n$, where

$$\mathbf{e}_i = (\underbrace{0,\dots,0}_{i-1 \text{ times}}, 1, \underbrace{0,\dots,0}_{n-i \text{ times}})\,.$$

Let $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ be an automorphism. Set

$$\phi(\mathbf{e}_i) = \sum_{j=1}^{n} m_{ij}\mathbf{e}_j. \tag{16}$$

We thus obtain a map $\mu : \phi \mapsto M_\phi = (m_{ij})$, where M_ϕ is a matrix with integer entries. We leave it to the reader to check that $\mu(\phi \circ \psi) = M_\phi M_\psi$. It follows that $\mu(\phi) \in GL(n,\mathbb{Z})$ for every $\phi \in Aut(\mathbb{Z}^n)$.

Given a matrix $M \in GL(n,\mathbb{Z})$, we define an endomorphism

$$\phi : \mathbb{Z}^n \to \mathbb{Z}^n,$$

using the equation (16). Since the map $\nu : M \mapsto \phi$ respects the composition, it follows that $\nu : GL(n,\mathbb{Z}) \to Aut(\mathbb{Z}^n)$ is a homomorphism and $\mu = \nu^{-1}$. □

Below we establish several properties of automorphisms of free abelian groups.

Lemma 7.15. *Let* $\mathbf{v} = (v_1, .., v_n) \in G = \mathbb{Z}^n$ *be a vector with* $\gcd(v_1, \dots, v_n) = 1$. *Then* $H = G/\langle \mathbf{v} \rangle$ *is free abelian of rank* $n-1$. *Moreover, there exists a basis* $\{\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_{n-1}, \mathbf{v}\}$ *of* G *such that* $\{\mathbf{y}_1 + \langle \mathbf{v} \rangle, \dots, \mathbf{y}_{n-1} + \langle \mathbf{v} \rangle\}$ *is a basis of* H.

Proof. First, let us show that the group H is free abelian; since this group is finitely generated, it suffices to verify that it is torsion-free. We will use the notation $x \mapsto \bar{x}$ for the quotient map $G \to H$.

Let $u \in G$ be such that $\bar{u} \in H$ has finite order k. Then $ku \in \langle \mathbf{v} \rangle$, i.e. $ku = m\mathbf{v}$ for some $m \in \mathbb{Z}$. Since $\gcd(v_1, \dots, v_n) = 1$, it follows that $k|m$ and, hence, $u \in \langle \mathbf{v} \rangle$, $\bar{u} = \bar{1}$.

Thus, $H = \mathbb{Z}^n/\langle \mathbf{v} \rangle$ is torsion-free, and, hence, it is free abelian of finite rank m. Next, the homomorphism $G \to H$ extends to a surjective linear map $\mathbb{R}^n \to \mathbb{R}^m$, whose kernel is the line spanned by v. Therefore, $m = n - 1$.

Let $\{\bar{x}_1, \dots, \bar{x}_{n-1}\}$ be a basis on H. The map

$$\bar{x}_i \mapsto x_i, i = 1, \dots, n-1,$$

extends to a group monomorphism $H \to G$; thus, the set $\{x_1, \dots, x_{n-1}, v\}$ generates $\mathbb{Z}^n$. It follows that $\{x_1, \dots, x_{n-1}, v\}$ is a basis of G. □

Lemma 7.16. *If a matrix* M *in* $GL(n, \mathbb{Z})$ *has all eigenvalues equal to* 1 *then there exists a finite ascending series of subgroups*

$$\{1\} = \Lambda_0 \leqslant \Lambda_1 \leqslant \cdots \leqslant \Lambda_{n-1} \leqslant \Lambda_n = \mathbb{Z}^n$$

such that $\Lambda_i \simeq \mathbb{Z}^i$, $\Lambda_{i+1}/\Lambda_i \simeq \mathbb{Z}$ *for all* $i \geqslant 0$, $M(\Lambda_i) = \Lambda_i$ *and* M *acts on* Λ_{i+1}/Λ_i *as the identity.*

Proof. Since M has eigenvalue 1, there exists a vector $v = (v_1, .., v_n) \in \mathbb{Z}^n$ such that $\gcd(v_1, .., v_n) = 1$ and $Mv = v$. Then M induces an automorphism of $H = \mathbb{Z}^n/\langle v \rangle \simeq \mathbb{Z}^{n-1}$ and the matrix $\bar{M}$ of this automorphism has only 1 as an eigenvalue. This follows immediately when writing the matrix of the automorphism M with respect to a basis $\{x_1, x_2, \dots, x_{n-1}, v\}$ of $\mathbb{Z}^n$ as in Lemma 7.15 and looking at the characteristic polynomial. Now, lemma follows by induction on n. □

The following lemma is a special case of a classical result of L. Kronecker; see [Kro57] or Proposition 1.2.1 in [GdlHJ89]. Our proof follows Kronecker's original argument.

Lemma 7.17. *Let* $M \in GL(n, \mathbb{Z})$ *be a matrix such that each eigenvalue of* M *has absolute value* 1. *Then all the eigenvalues of* M *are roots of unity.*

Proof. Recall that for each $n \times n$ matrix A with the eigenvalues $\mu_1, \dots, \mu_n$ (here and below, we repeat the eigenvalues if necessary, according to their multiplicities) the characteristic polynomial $p_A(t)$ equals

$$\sum_{i=0}^{n} a_{n-i} t^i,$$

where, by Vieta's formulae,

$$a_i = \det(A)(-1)^n \sigma_i(\mu_1, \ldots, \mu_n),$$

and σ_i is the ith *elementary symmetric polynomial*:

$$\sigma_i(x_1, \ldots, x_n) = \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant n} x_{j_1} \ldots x_{j_i}.$$

We now return to the integer square matrix M as in lemma and let $\lambda_1, \ldots, \lambda_n$ denote its eigenvalues. Consider the sequence of matrices $M^k, k \in \mathbb{N}$. The eigenvalues of M^k are $\lambda_1^k, \ldots, \lambda_n^k$, which, by the assumption, all have the absolute value 1. Therefore, the coefficients of the characteristic polynomials $p_k(t) := p_{M^k}(t)$ of M^k are uniformly bounded, independently on k. Since the matrices M^k belong to $GL(n, \mathbb{Z})$, there are only finitely many distinct characteristic polynomials of the matrices M^k. Hence, there exists an infinite sequence $k_1 < k_2 < k_3 < \ldots$, such that

$$p_{k_1}(t) = p_{k_2}(t) = p_{k_3}(t) = \ldots.$$

It follows that there are distinct members of this sequence, $q < r$, such that

$$\lambda_1^q = \lambda_1^r, \ldots, \lambda_n^q = \lambda_n^r.$$

Hence, for each $i = 1, \ldots, n$

$$\lambda_i^{r-q} = 1,$$

which means that each eigenvalue of M is a root of unity. □

Lemma 7.18. *If a matrix M in $GL(n, \mathbb{Z})$ has one eigenvalue λ of absolute value at least 2 then there exists a vector $\mathbf{v} \in \mathbb{Z}^n$ such that the following map is injective:*

$$\begin{array}{rcl} \Phi : \bigoplus\limits_{n \in \mathbb{Z}_+} \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}^n \\ \Phi : (s_n)_n & \mapsto & s_0 v + s_1 M\mathbf{v} + \ldots + s_n M^n \mathbf{v} + \ldots . \end{array} \tag{17}$$

Proof. The matrix M defines an automorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$, $\varphi(\mathbf{v}) = M\mathbf{v}$. The dual map φ^* has the matrix M^T in the dual canonical basis. Therefore, it also has the eigenvalue λ and, hence, there exists a linear form $f : \mathbb{C}^n \to \mathbb{C}$ such that $\varphi^*(f) = f \circ \varphi = \lambda f$.

Take $\mathbf{v} \in \mathbb{Z}^n \setminus \operatorname{Ker} f$. Assume that the map Φ is not injective. It follows that there exist some $(t_n)_n$, $t_n \in \{-1, 0, 1\}$, such that

$$t_0\mathbf{v} + t_1 M\mathbf{v} + \ldots + t_n M^n \mathbf{v} + \ldots = 0.$$

Let N be the largest integer such that $t_N \neq 0$. Then

$$M^N \mathbf{v} = r_0\mathbf{v} + r_1 M\mathbf{v} + \ldots + r_{N-1} M^{N-1}\mathbf{v}$$

where $r_i \in \{-1, 0, 1\}$. By applying f to the equality we obtain

$$\left(r_0 + r_1\lambda + \cdots + r_{N-1}\lambda^{N-1}\right) f(\mathbf{v}) = \lambda^N f(\mathbf{v}),$$

whence

$$|\lambda|^N \leqslant \sum_{i=1}^{N-1} |\lambda|^i = \frac{|\lambda|^N - 1}{|\lambda| - 1} \leqslant |\lambda|^N - 1\,,$$

a contradiction. □

7.3.A Wolf's Theorem for semidirect products $\mathbb{Z}^n \rtimes \mathbb{Z}$

In this section we explain how to provide an affirmative answer to Question 7.10 in the case of semidirect products $\mathbb{Z}^n \rtimes \mathbb{Z}$. This easy example helps to understand the general case of polycyclic groups and the general Wolf Theorem.

Note that the semidirect product is defined by a homomorphism $\varphi : \mathbb{Z} \to Aut(\mathbb{Z}^n) = GL(n, \mathbb{Z})$, and the latter is determined by $\theta = \varphi(1)$, which is represented by a matrix $M \in GL(n, \mathbb{Z})$. Therefore the same semidirect product is also denoted $\mathbb{Z}^n \rtimes_\theta \mathbb{Z} = \mathbb{Z}^n \rtimes_M \mathbb{Z}$.

Proposition 7.19. *A semidirect product $G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is*

1. *either virtually nilpotent (when M has all eigenvalues of absolute value 1);*
2. *or of exponential growth (when M has at least one eigenvalue of absolute value $\neq 1$).*

Remarks 7.20. 1. The group $G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is nilpotent if M has all eigenvalues equal to 1 (see Case (1) of the proof of the proposition).

2. The same is not in general true if M has all eigenvalues of absolute value 1. The group $G = \mathbb{Z} \rtimes_M \mathbb{Z}$ with $M = (-1)$ is a counter-example: It admits a quotient which is the infinite dihedral group and the latter is not nilpotent. In this example, the group $G = \mathbb{Z} \rtimes_M \mathbb{Z}$ is polycyclic, virtually nilpotent but not nilpotent. In particular, the statement (1) in Proposition 7.19 cannot be improved to '$G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is nilpotent'.

Proof. Note that $\mathbb{Z}^n \rtimes_{\theta^N} \mathbb{Z}$ is a subgroup of finite index in $G = \mathbb{Z}^n \rtimes_\theta \mathbb{Z}$ (corresponding to the replacement of the second factor $\mathbb{Z}$ by $N\mathbb{Z}$). Thus, we may replace M by some power of M, and replace G with a finite-index subgroup. We will retain the notation G and M for the finite-index subgroup and the power of M. Then the matrix $M \in GL(n, \mathbb{Z})$ will have no non-trivial roots of unity as eigenvalues. In view of Lemma 7.17, this means that for every eigenvalue $\lambda \neq 1$ of M, $|\lambda| \neq 1$.

Of the two cases to consider, case (1) appears as an exercise on Ex. Sheet 4. We therefore only prove (2).

Assume thus that M has an eigenvalue with absolute value strictly greater than 1. After replacing θ with its power θ^N if necessary, we may assume that the matrix M has an eigenvalue with absolute value at least 2.

Lemma 7.18 applied to M implies that there exists an element $v \in \mathbb{Z}^n$ such that distinct elements $s = (s_k) \in \bigoplus_{k \geqslant 0} \mathbb{Z}_2$ define distinct vectors

$$s_0 v + s_1 M v + \ldots + s_n M^k v + \ldots$$

in $\mathbb{Z}^n$. With the multiplicative notation for the binary operation in G, the above vectors correspond to distinct elements

$$g_s = v^{s_0} (tvt^{-1})^{s_1} \cdots (t^k v t^{-k})^{s_k} \cdots \in G.$$

Now, consider the set Σ_K of sequences $s = (s_k)$ for which $s_k = 0\,, \forall k \geqslant K+1$. Then the map

$$\Sigma_K \to G, \quad s \mapsto g_s$$

is injective and its image consists of 2^{K+1} distinct elements g_s. Assume that the generating set of G contains the elements t and v. With respect to this generating set, the word-length $|g_s|$ is at most $3K+1$ for every $s \in \Sigma_K$. Thus, for every K we obtain 2^{K+1} distinct elements of G of length at most $3K+1$, whence G has exponential growth. □

7.3.B The general Wolf Theorem

Theorem 7.21 (Wolf's Theorem)**.** *A polycyclic group is either virtually nilpotent or has exponential growth.*

The main ingredient in the proof of Theorem 7.21 is the following generalization of Proposition 7.19.

Proposition 7.22. *Let G be a finitely generated nilpotent group and let $\varphi \in Aut(G)$. Then the polycyclic group $P = G \rtimes_\varphi \mathbb{Z}$ is*

1. *either virtually nilpotent;*
2. *or has exponential growth.*

Remark 7.23. The statement (1) in Proposition 7.22 cannot be improved to 'P is nilpotent', see Remark 7.20, Part (2).

Proof. See Ex. Sheet 4. □

Proof of Theorem 7.21. According to Proposition 5.45, it suffices to prove the statement for poly-C_∞ groups. Let G be a poly-C_∞ group, and consider a finite subnormal descending series

$$G = N_0 \geqslant N_1 \geqslant \ldots \geqslant N_n \geqslant N_{n+1} = \{1\}$$

such that $N_i / N_{i+1} \simeq \mathbb{Z}$ for every $i \geqslant 0$. We argue by induction on n. For $n = 0$ the group G is infinite cyclic and the statement is obvious. Assume that the assertion of the theorem holds for n and consider the case of $n+1$. By

the induction hypothesis, the subgroup $N_1 \leqslant G$ is either virtually nilpotent or has exponential growth. In the second case the group G itself has exponential growth.

Assume that N_1 is virtually nilpotent. Corollary 3.17 implies that G decomposes as a semidirect product $N_1 \rtimes_\theta \mathbb{Z}$, corresponding to a homomorphism $\Psi : \mathbb{Z} \to \mathrm{Aut}\,(N_1)$, $\theta = \Psi(1)$.

By hypothesis, N_1 contains a nilpotent subgroup H of finite index. We may moreover assume that H is characteristic in N_1. In particular H is invariant under the automorphisms ψ. We retain the notation θ for the restriction $\theta\big|_H$. Therefore, $H \rtimes_\theta \mathbb{Z}$ is a normal subgroup of G. Moreover, $H \rtimes_\theta \mathbb{Z}$ has finite index in G, since $G/(H \rtimes_\theta \mathbb{Z})$ is the quotient of the finite group N_1/H.

By Proposition 7.22, $H \rtimes_\theta \mathbb{Z}$ is either virtually nilpotent or of exponential growth. Therefore, the same alternative holds for $N_1 \rtimes_\theta \mathbb{Z} = G$. □

7.4 Milnor's theorem

Theorem 7.24 (J. Milnor, [Mil68a])**.** *A finitely generated solvable group is either polycyclic or has exponential growth.*

We begin the proof by establishing a property of conjugates implied by sub-exponential growth:

Lemma 7.25. *If a finitely generated group G has sub-exponential growth then for all $\beta_1, \ldots, \beta_m, g \in G$, the set of conjugates*

$$\{g^k \beta_i g^{-k} \mid k \in \mathbb{Z}, i = 1, \ldots, m\}$$

generates a finitely generated subgroup $N \leqslant G$.

Proof. Exercise on Ex. Sheet 4. □

Exercise 7.26. Use Lemma 7.25 to prove that the finitely generated group H described in Example 3.8 has exponential growth.

We now are ready to prove Theorem 7.24; our proof is by induction on the derived length d of G. For $d = 1$ the group G is finitely generated abelian and the statement is immediate. Assume that the alternative holds for finitely generated solvable groups of derived length $\leqslant d$ and consider G of derived length $d + 1$. Then $H = G/G^{(d)}$ is finitely generated solvable of derived length d. By the induction hypothesis, either H has exponential growth or H is polycyclic. If H has exponential growth then G has exponential growth too (see statement (c) in Proposition 7.9).

Assume therefore that H is polycyclic. In particular, H is finitely presented by Proposition 5.48. Theorem 7.24 will follow from:

Lemma 7.27. *Consider a short exact sequence*

$$1 \to A \to G \xrightarrow{\pi} H \to 1\,, \quad \textit{with } A \textit{ abelian and } G \textit{ finitely generated.} \tag{18}$$

If H is polycyclic then G is either polycyclic or has exponential growth.

Proof. We assume that G has sub-exponential growth and will prove that G is polycyclic. The group G is polycyclic iff A is finitely generated. Since H is polycyclic, it has the bounded generation property (see Proposition 5.38); hence, there exist finitely many elements $h_1, \ldots, h_q$ in H such that every element $h \in H$ can be written as

$$h = h_1^{m_1} h_2^{m_2} \cdots h_q^{m_q}\,, \text{ with } m_1, m_2, \ldots, m_q \in \mathbb{Z}\,.$$

Choose $g_i \in G$ such that $\pi(g_i) = h_i$ for every $i \in \{1, 2, \ldots, q\}$. Then every element $g \in G$ can be written as

$$g = g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q} a\,, \text{ with } m_1, m_2, \ldots, m_q \in \mathbb{Z} \text{ and } a \in A\,. \tag{19}$$

Since H is finitely presented, by Lemma 3.42 there exist finitely many elements $a_1, \ldots, a_k$ in A such that every element in A is a product of G-conjugates of $a_1, \ldots, a_k$. According to (19), all the conjugates of a_j are of the form

$$g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q} a_j \left(g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q}\right)^{-1}\,. \tag{20}$$

By Lemma 7.25, the subgroup A_q generated by the conjugates $g_q^m a_j g_q^{-m}$ with $m \in \mathbb{Z}$ and $j \in \{1, \ldots, k\}$ is finitely generated. Let S_q be its finite generating set. Then the conjugates $g_{q-1}^n g_q^m a_j g_q^{-m} g_{q-1}^{-n}$ with $m, n \in \mathbb{Z}$ and $j \in \{1, \ldots, k\}$ are in the subgroup A_{q-1} of A generated by $g_{q-1}^n s g_{q-1}^{-n}$ with $n \in \mathbb{Z}$ and $s \in S_q$. Again Lemma 7.25 implies that the subgroup A_{q-1} is finitely generated. Continuing inductively, we conclude that the group A generated by all the conjugates in (20), is finitely generated. Hence, G is polycyclic. □

This also concludes the proof of Milnor's theorem, Theorem 7.24. □

By combining the theorems of Milnor and Wolf we obtain:

Theorem 7.28. *Every finitely generated solvable group either is virtually nilpotent or it has exponential growth.*

References

[Bas72] H. Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. London Math. Soc. **25** (1972), 603–614.

[BE12] L. Bartholdi and A. Erschler, *Growth of permutational extensions*, Invent. Math. **189** (2012), no. 2, 431–455.

[Bie79] R. Bieri, *Finitely presented soluble groups*, Séminaire d'Algèbre Paul Dubreil 31ème année (Paris, 1977–1978), Lecture Notes in Math., vol. 740, Springer, Berlin, 1979, pp. 1–8.

[BW11] M. Bridson and H. Wilton, *On the difficulty of presenting finitely presentable groups*, Groups Geom. Dyn. **5** (2011), no. 2, 301–325.

[DK] C. Druţu and M. Kapovich, *Geometric Group Theory*, Colloquium Publications, Amer. Math. Soc.

[GdlHJ89] F. M. Goodman, P. de la Harpe, and V. Jones, *Coxeter graphs and towers of algebras*, Mathematical Sciences Research Institute Publications, vol. 14, Springer-Verlag, New York, 1989.

[Gri84] R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no. 5, 939–985.

[Gui70] Y. Guivarc'h, *Groupes de Lie à croissance polynomiale*, C. R. Acad. Sci. Paris, Ser. A—B **271** (1970), A237–A239.

[Gui73] ———, *Croissance polynomiale et périodes des fonctions harmonique*, Bull. Soc. Math. France **101** (1973), 333–379.

[Hal76] M. Hall, *The theory of groups*, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition.

[Hir38] K. A. Hirsch, *On infinite soluble groups, II*, Proc. Lond. Math. Soc. **44** (1938), 336–344.

[HP74] E. Hille and R. Phillips, *Functional analysis and semi-groups*, American Mathematical Society, Providence, R. I., 1974, Third printing of the revised edition of 1957, American Mathematical Society Colloquium Publications, Vol. XXXI.

[Kro57] L. Kronecker, *Zwei Sätze Über Gleichungen mit ganzzahligen Coefficienten*, J. für Reine und Angewandte Mathematik **53** (1857), 173–175.

[Lan02] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 2002.

[Mal40] A. I. Mal'cev, *On isomorphic matrix representations of infinite groups*, Mat. Sbornik **8** (1940), 405–422.

[Mal49] ———, *Generalized nilpotent algebras and their associated groups*, Mat. Sbornik **25** (1949), 347–366.

[Mil68a] J. Milnor, *Growth of finitely generated solvable groups*, J. Diff. Geom. **2** (1968), 447–449.

[Mil68b] ———, *A note on curvature and fundamental group*, J. Diff. Geom. **2** (1968), 1–7.

[Mil79] J. J. Millson, *Real vector bundles with discrete structure group*, Topology **18** (1979), no. 1, 83–89.

[Ol′91] A. Yu. Ol′shanskiĭ, *Geometry of defining relations in groups*, Mathematics and its Applications (Soviet Series), vol. 70, Kluwer Academic Publishers Group, Dordrecht, 1991.

[Rag72] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Springer-Verlag, 1972.

[Seg05] D. Segal, *Polycyclic groups*, Cambridge University Press, Cambridge, 2005.

[Sel60] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to Function Theory (K. Chandrasekhadran, ed.), Tata Inst. of Fund. Research, Bombay, 1960, pp. 147–164.