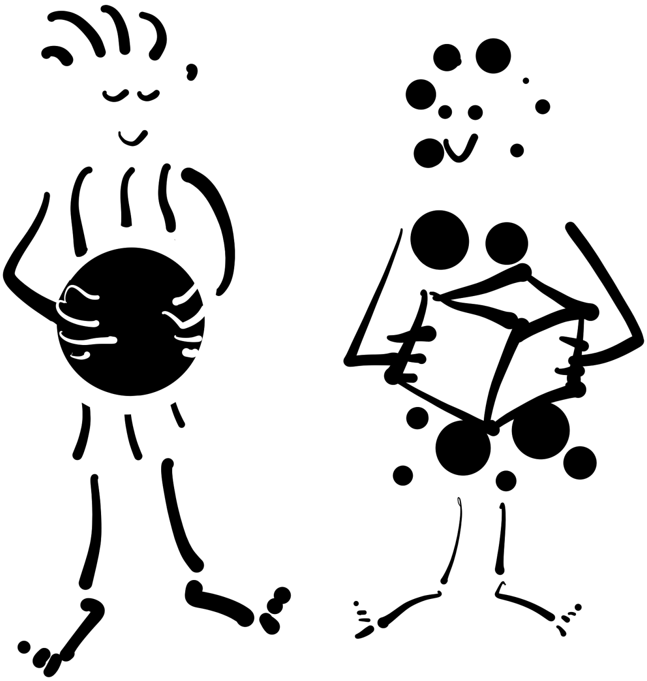
1

Background



https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.1 Basic Notation

The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the sets of natural, whole, rational, real, and complex numbers, respectively. We assume that $\mathbb{N}$ contains the number 0.

For real numbers $a, b \in \mathbb{R}$ we use $a \wedge b = \min\{a, b\}$ and $a \vee b = \max\{a, b\}$.

For sets A, B the notation A^B is used to denote all functions from B to A.

$A \uplus B$ is used to denote disjoint unions; that is, this notation includes the claim that $A \cap B = \emptyset$.

We use $\mathbf{1}_A$ to denote the indication function of a set A; so $\mathbf{1}_A(\omega) = 1$ for $\omega \in A$ and $\mathbf{1}_A(\omega) = 0$ for $\omega \notin A$.

For linear operators we use I to denote the identity operator.

In a generic probability space, we use $\mathbb{P}$ to denote the probability measure and $\mathbb{E}$ to denote expectation.

A graph is a pair (V, E) where V is a set (whose elements are called *vertices*) and $E \subset \{\{x, y\} \subset G\}$. A subset $\{x, y\} \in E$ is called an *edge*. Sometimes we write $x \sim y$ to denote the case that $\{x, y\} \in E$. A graph is naturally equipped with the notion of paths: A finite *path* in a graph G is a sequence $x_0, \ldots, x_n$ of vertices such that $x_j \sim x_{j+1}$ for all $0 \leq j < n$. For such a sequence, n is the *length* of the path; this is the number of edges traversed by the path. An infinite such sequence is called an infinite path. A graph is *connected* if for every $x, y \in G$ there is some finite path starting at x and ending at y. A connected graph comes with a natural metric on it: $\text{dist}_G(x, y)$ is the minimal length of a path between x and y.

For a sequence $(a_n)_n$ we use the notation $a[m, n] = (a_m, \ldots, a_n)$.

For two measures μ, ν on a measurable space $(\Omega, \mathcal{F})$, we write $\mu \ll \nu$ if μ is absolutely continuous with respect to ν. That is, for any $A \in \mathcal{F}$ it holds that if $\nu(A) = 0$ then $\mu(A) = 0$.

If μ is a probability measure on a measurable space $(\Omega, \mathcal{F})$, then an i.i.d.-μ sequence of elements means a sequence of elements $(\omega_t)_t$ such that each one has law μ and that are all independent. (Sometimes this is just called i.i.d., omitting μ from the notation; "i.i.d." stands for *independent and identically distributed*.)

In a group G we use 1 and sometimes 1_G to denote the identity element. For elements $x, y \in G$ we denote $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$. The latter is called the *commutator* of x, y. Iterated commutators are defined inductively by $[x_1, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n]$. The **centralizer** of $x \in G$ is defined to be $C_G(x) = \{y \in G : [x, y] = 1\}$.

For $A \subset G$ we write $A^x = \{a^x : a \in A\}$ and $A^{-1} = \left\{a^{-1} : a \in A\right\}$. A is called **symmetric** if $A = A^{-1}$. A group G is **generated** by a subset $S \subset G$ if every element of G can be written a product of finitely many elements from

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

$S \cup S^{-1}$. Also, $\langle A \rangle$ denotes the subgroup generated by the elements of A; that is, all elements that can be written as a product of finitely many elements from $A \cup A^{-1}$. For two subsets $A, B \subset G$ we write $[A, B] = \langle [a, b] : a \in A\,,\ b \in B \rangle$ (note that this is the group generated by all commutators, not just the set of commutators). We also denote $AB = \{ab : a \in A\,,\ b \in B\}$.

1.2 Spaces of Sequences

Let G be a countable set. Let us briefly review the formal setup of the canonical probability spaces on $G^{\mathbb{N}}$. This is the space of sequences $(\omega_n)_{n=0}^{\infty}$ where $\omega_n \in G$ for all $n \in \mathbb{N}$. A cylinder set is a set of the form

$$C(J, \omega) = \left\{ \eta \in G^{\mathbb{N}} \mid \forall\, j \in J\,,\ \eta_j = \omega_j \right\}, \qquad J \subset \mathbb{N},\, 0 < |J| < \infty, \quad \omega \in G^{\mathbb{N}}.$$

It is also natural to define $C(\emptyset, \omega) = G^{\mathbb{N}}$. Let $X_j \colon G^{\mathbb{N}} \to G$ be the map $X_j(\omega) = \omega_j$ projecting onto the jth coordinate. For times $t > s$ we also use the notation $X[s, t] = (X_s, X_{s+1}, \ldots, X_t)$.

Define the **cylinder σ-algebra**

$$\mathcal{F} = \sigma(X_0, X_1, X_2, \ldots) = \sigma\left(X_n^{-1}(g) \mid n \in \mathbb{N}\,,\ g \in G\right).$$

Exercise 1.1 Show that

$$\mathcal{F} = \sigma(X_0, X_1, X_2, \ldots) = \sigma\left(C(J, \omega) \mid 0 < |J| < \infty\,,\ J \subset \mathbb{N}, \quad \omega \in G^{\mathbb{N}}\right)$$
$$= \sigma\left(C(\{0, \ldots, n\}, \omega) \mid n \in \mathbb{N} \quad \omega \in G^{\mathbb{N}}\right).$$

Show that $\eta \in C(J, \omega)$ if and only if $C(J, \omega) = C(J, \eta)$.

For $t \geq 0$ we denote

$$\mathcal{F}_t = \sigma(X_0, \ldots, X_t).$$

Exercise 1.2 Show that $\mathcal{F}_t \subset \mathcal{F}_{t+1} \subset \mathcal{F}$. (A sequence of σ-algebras with this property is called a *filtration*.) Conclude that

$$\mathcal{F} = \sigma\Big(\bigcup_t \mathcal{F}_t\Big).$$

Theorems of Carathéodory and Kolmogorov tell us that the probability measure $\mathbb{P}$ on $\left(G^{\mathbb{N}}, \mathcal{F}\right)$ is completely determined by knowing the marginal probabilities $\mathbb{P}[X_0 = g_0, \ldots, X_n = g_n]$ for all $n \in \mathbb{N}, g_0, \ldots, g_n \in G$. That is, when G is countable, Kolmogorov's extension theorem implies the following:

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Theorem 1.2.1 *Let $(P_t)_t$ be a sequence of probability measures, where each P_t is defined on $\mathcal{F}_t$. Assume that these measures are consistent in the sense that for all t,*

$$P_{t+1}(\{(X_0,\ldots,X_t)=(g_0,\ldots,g_t)\}) = P_t(\{(X_0,\ldots,X_t)=(g_0,\ldots,g_t)\}) \tag{1.1}$$

for any $g_0,\ldots,g_t \in G$. Then, there exists a unique probability measure $\mathbb{P}$ on $\left(G^{\mathbb{N}},\mathcal{F}\right)$ such that for any $A \in \mathcal{F}_t$ we have $\mathbb{P}(A) = P_t(A)$.

Details can be found in Durrett (2019, appendix A).

Exercise 1.3 Let $(P_t)_t$ be a sequence of probability measures, where each P_t is defined on $\mathcal{F}_t$. Show that (1.1) holds if and only if for any $t < s$ and any $A \in \mathcal{F}_t$, we have $P_s(A) = P_t(A)$.

The space $G^{\mathbb{N}}$ comes equipped with a natural *shift operator*: $\theta\colon G^{\mathbb{N}} \to G^{\mathbb{N}}$ given by $\theta(\omega)_t = \omega_{t+1}$ for all $t \in \mathbb{N}$.

Exercise 1.4 Show that $\theta^t(A) \in \mathcal{F}$ for any $A \in \mathcal{F}$. ▷ solution ◁

Exercise 1.5 Let $\mathcal{K} \subset \mathcal{F}$ be a collection of events. Show that if $\mathcal{G} = \sigma(\mathcal{K})$ is the σ-algebra generated by $\mathcal{K}$, then $\theta^{-t}\mathcal{G} := \{\theta^{-t}(A) : A \in \mathcal{G}\}$ is a σ-algebra, and in fact $\theta^{-t}\mathcal{G} = \sigma\left(\theta^{-t}(K) \colon K \in \mathcal{K}\right)$. ▷ solution ◁

Exercise 1.6 Show that $\theta^{-1}(A) \in \mathcal{F}$ for any $A \in \mathcal{F}$. ▷ solution ◁

Exercise 1.7 Define

$$\sigma(X_t, X_{t+1}, \ldots) = \sigma\left(X_{t+j}^{-1}(g) \colon g \in G\,,\ j \geq 0\right).$$

Show that $\sigma(X_t, X_{t+1}, \ldots) = \theta^{-t}\mathcal{F} = \{\theta^{-t}(A) : A \in \mathcal{F}\}$. ▷ solution ◁

Exercise 1.8 If $\sim$ is an equivalence relation on Ω, we say that a subset $A \subset \Omega$ **respects** $\sim$ if for any $\omega \sim \eta \in \Omega$ we have $\omega \in A \iff \eta \in A$.

Show that the collection of subsets A that respect the equivalence relation $\sim$ forms a σ-algebra on Ω.

Exercise 1.9 Define an equivalence relation on $G^{\mathbb{N}}$ by $\omega \sim_t \omega'$ if $\omega_j = \omega'_j$ for all $j = 0, 1, \ldots, t$.

Show that this is indeed an equivalence relation.

Show that $\sigma(X_0, X_1, \ldots, X_t) = \{A : A \text{ respects } \sim_t\}$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.3 Group Actions

A (left) group action $G \curvearrowright X$ is a function from $G \times X$ to X, $(\gamma, x) \mapsto \gamma.x$, that is *compatible* in the sense that $(\gamma\eta).x = \gamma.(\eta.x)$, and such that $1.x = x$ for all $x \in X$. We usually denote $\gamma.x$ or γx for the action of $\gamma \in G$ on $x \in X$.

A *right* action is analogously defined for $(x, \gamma) \mapsto x.\gamma$ and compatibility is $x.(\gamma\eta) = (x.\gamma).\eta$ (and $x.1 = x$ for all $x \in X$).

Exercise 1.10 Let $G \curvearrowright X$ be a left group action. For any $\gamma \in G$ and $x \in X$ define $x.\gamma := \gamma^{-1}.x$. Show that this defines a right action of G on X.

Conversely, show that if G acts on X from the right, then defining $\gamma.x = x.\gamma^{-1}$ is a left action.

The bijections on a set X form a group with the group operation given by composition of functions. A (left) group action $G \curvearrowright X$ can be thought of as a homomorphism from the group into the group of bijections on X.

Sometimes, we wish to restrict to some subgroup of bijections on X when X has some additional structure. For example, if X is a topological space, we say that G acts on X by homeomorphisms if every element of G is a homeomorphism of X, when thinking of elements of G as identified with their corresponding bijection of X. That is, an action by homeomorphisms is a group homomorphism from G into the set of homeomorphisms of X.

Similarly, if $\mathbb{H}$ is some Hilbert space, then a group G acts on $\mathbb{H}$ by unitary operators if every element of G is mapped to a unitary operator of $\mathbb{H}$. This is just a group homomorphism from G into the group of unitary operators on $\mathbb{H}$.

Exercise 1.11 Show that any group acts on itself by left multiplication; that is, $G \curvearrowright G$ by $x.y := xy$.

Exercise 1.12 Let $\mathbb{C}^G$ be the set of all functions from $G \to \mathbb{C}$. Show that $G \curvearrowright \mathbb{C}^G$ by $(x.f)(y) := f\left(x^{-1}y\right)$.

Show that $f^x(y) := f\left(yx^{-1}\right)$ defines a *right* action.

Exercise 1.13 Generalize the previous exercise as follows:

Suppose that $G \curvearrowright X$. Consider $\mathbb{C}^X$, all functions from $X \to \mathbb{C}$. Show that $G \curvearrowright \mathbb{C}^X$ by $\gamma.f(x) := f\left(\gamma^{-1}.x\right)$, for all $f \in \mathbb{C}^X, \gamma \in G, x \in X$.

Show that the action $G \curvearrowright \mathbb{C}^X$ is *linear*; that is, $\gamma.(\zeta f + h) = \zeta(\gamma.f) + h$, for all $f, h \colon X \to \mathbb{C}$, $\zeta \in \mathbb{C}$, and $\gamma \in G$.

Show that $f^\gamma(x) := f(\gamma.x)$ defines a right action of G on $\mathbb{C}^X$. Show that this right action is linear as well.

Exercise 1.14 Let $G \curvearrowright X$. Let $\mathcal{M}_1(X)$ be the set of all probability measures on $(X, \mathcal{F})$, where $\mathcal{F}$ is some σ-algebra on X. Suppose that for any $g \in G$ the function $g \colon X \to X$ given by $g(x) = g.x$ is a measurable function. (In this case we say that G acts on X by measurable functions.)

Show that $G \curvearrowright \mathcal{M}_1(X)$ by

$$\forall\, A \in \mathcal{F} \qquad g.\mu(A) := \mu\left(g^{-1}A\right),$$

where $g^{-1}A := \left\{g^{-1}.x \colon x \in A\right\}$.

Exercise 1.15 Let $F = \{f \colon G \to \mathbb{C} : f(1) = 0\}$. Show that

$$(x.f)(y) := f\left(x^{-1}y\right) - f\left(x^{-1}\right)$$

defines a left action of G on F.

Notation Throughout this book, unless specified otherwise, we will always use the left action $\gamma.f(x) = f\left(\gamma^{-1}x\right)$ for $G \curvearrowright X$ and $f \colon X \to \mathbb{C}$.

Definition 1.3.1 Let $G \curvearrowright X$ be a (left) action. For $A \subset X$ and $\gamma \in G$ define $\gamma.A = \{\gamma.x : x \in A\}$. For $F \subset G$ denote $F.A = \{\gamma.x : \gamma \in F,\ x \in A\}$.

A subset $A \subset X$ is called ***G*-invariant** if $\gamma.A \subset A$ for all $\gamma \in G$; equivalently, $G.A = A$.

Definition 1.3.2 For a group action $G \curvearrowright X$ and some $x \in X$, the set $G.x := \{g.x : g \in G\}$ is called the **orbit** of x under G. The **stabilizer** of x is the subgroup $\mathsf{stab}(x) = \{g \in G : g.x = x\}$.

Exercise 1.16 Show that for $G \curvearrowright X$ any stabilizer $\mathsf{stab}(x)$ is indeed a subgroup.

▷ solution ◁

Exercise 1.17 (Orbit-Stabilizer theorem) Let $G \curvearrowright X$.

Show that $|G.x| = [G : \mathsf{stab}(x)]$. ▷ solution ◁

One nice consequence of the orbit-stabilizer theorem is that intersections of finite-index subgroups have finite index.

Proposition 1.3.3 *Let G be a group and $H, N \leq G$ be subgroups.*

Then, $[G : H \cap N] \leq [G : H] \cdot [G : N]$.

Proof If either $[G : H] = \infty$ or $[G : N] = \infty$ there is nothing to prove because the right-hand side is infinite. So assume that $[G : H] < \infty$ and $[G : N] < \infty$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Let $X = G/H \times G/N$. That is, elements of X are pairs of cosets $(\alpha H, \beta N)$. Therefore, X is finite, since $|X| = |G/H| \cdot |G/N|$.

The group G acts on X by $g.(\alpha H, \beta N) = (g\alpha H, g\beta N)$. The stabilizer of (H, N) may easily be computed: $\mathsf{stab}(H, N) = H \cap N$. Thus, $[G : H \cap N] \leq |X| \leq [G : H] \cdot [G : N]$. □

1.4 Discrete Group Convolutions

Throughout this book we will almost exclusively deal with countable groups. Given a countable group G, one may define the **convolution** of functions $f, g \colon G \to \mathbb{C}$ as follows.

Definition 1.4.1 Let G be a countable group. Let $f, g \colon G \to \mathbb{C}$. The **convolution** of f and g is the function $f * g \colon G \to \mathbb{C}$ defined by

$$(f * g)(x) := \sum_y f(y) g\left(y^{-1}x\right) = \sum_y f(y)(y.g)(x),$$

as long as the above sum converges absolutely.

This is the analogue of the usual convolution of functions on the group $\mathbb{R}$:

$$(f * g)(x) = \int f(y) g(x - y) dy.$$

However, the convolution is not necessarily commutative, as is the case for Abelian groups.

Exercise 1.18 Show that

$$(f * g)(x) = \sum_y f\left(xy^{-1}\right) g(y).$$

Give an example for which $f * g \neq g * f$.

Exercise 1.19 (Left action and convolutions) Show that $x.(f * g) = (x.f * g)$ for the canonical left action $x.f(y) = f\left(x^{-1}y\right)$.

When G is countable, a probability measure μ on G may be thought of as a function $\mu \colon G \to [0, 1]$ so that $\mu(A) = \sum_{a \in A} \mu(a)$.

Exercise 1.20 Let μ be a probability measure on a countable group G, and let X be a random element of G with law μ. Show that

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

$$\mathbb{E}\left[f\left(x\cdot X^{-1}\right)\right] = (f*\mu)(x)$$

whenever the above quantities are well defined.

Definition 1.4.2 Let μ be a probability measure on G. We will use the notation μ^t to denote the t-fold convolution of μ with itself. Specifically, $\mu^1 = \mu$ and $\mu^{t+1} = \mu * \mu^t = \mu^t * \mu$.

Exercise 1.21 Let G be a countable group. Let μ, ν be probability measures on G. Let X, Y be independent random elements in G such that X has law μ, and Y has law ν.

Show that the law of $X \cdot Y$ is $\mu * \nu$. ▷ solution ◁

Exercise 1.22 Show that for any $p \geq 1$ we have $||x.f||_p = ||f||_p$. Here, $||f||_p^p = \sum_x |f(x)|^p$ and $||f||_\infty = \sup_x |f(x)|$.

Show that $||\check{f}||_p = ||f||_p$, where $\check{f}(x) = f\left(x^{-1}\right)$.

Exercise 1.23 Prove *Young's inequality for products*: For all $a, b \geq 0$ and any $p, q > 0$ such that $p + q = 1$, we have $ab \leq pa^{1/p} + qb^{1/q}$. ▷ solution ◁

Exercise 1.24 Prove the *generalized Hölder inequality*: for all $p_1, \ldots, p_n \in [1, \infty]$ such that $\sum_{j=1}^n \frac{1}{p_j} = 1$, we have

$$||f_1 \cdots f_n||_1 \leq \prod_{j=1}^n ||f_j||_{p_j}.$$ ▷ solution ◁

Exercise 1.25 Prove *Young's inequality for convolutions*: For any $p, q \geq 1$ and $1 \leq r \leq \infty$ such that $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$, we have

$$||f * g||_r \leq ||f||_p \cdot ||g||_q.$$ ▷ solution ◁

1.5 Basic Group Notions

Here we briefly recall some basic notions and examples from group theory. Further depth on any of these notions can be found in any basic textbook on group theory.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.5.1 Basic Linear Groups

If R is a ring we use the notation $\mathsf{M}_n(R)$ to denote the set of $n \times n$ matrices with entries in R. For example, $\mathsf{M}_n(\mathbb{Z})$ is the set of all $n \times n$ matrices with integer entries. These do not necessarily form a group. By $\mathsf{GL}_n(\mathbb{R})$ we denote the group of $n \times n$ invertible matrices with real entries. The group operation here is matrix multiplication. In more generality, $\mathsf{GL}_n(\mathbb{C})$ is the group of $n \times n$ matrices with complex entries, so that $\mathsf{GL}_n(\mathbb{R}) \leq \mathsf{GL}_n(\mathbb{C})$.

Exercise 1.26 Show that $\mathsf{GL}_2(\mathbb{R}) \cap \mathsf{M}_2(\mathbb{Z})$ is not a group with matrix multiplication. ▷ solution ◁

A nontrivial fact is that if we restrict to integer entries with determinant ±1, we do have a group. We denote

$$\mathsf{GL}_n(\mathbb{Z}) = \{M \in \mathsf{M}_n(\mathbb{Z}) : |\det(M)| = 1\}.$$

Proposition 1.5.1 $\mathsf{GL}_n(\mathbb{Z})$ *is a group with matrix multiplication.*

Proof The main property we will use is that for any $M \in \mathsf{GL}_n(\mathbb{Z})$ the number $\det(M)$ is invertible in the ring $\mathbb{Z}$. (This proof generalizes to matrices over a commutative ring with unit such that the determinants are invertible in the ring; see Exercise 1.102.)

Recall Cramer's Rule: For $b \in \mathbb{R}^d$ and $A \in \mathsf{GL}_n(\mathbb{R})$, we may compute the solution to $Ax = b$ by $x_i = \frac{\det(A(i,b))}{\det(A)}$ for each $i = 1, \ldots, n$, where $A(i, b)$ is the matrix A with ith column replaced by the vector b.

Let e_i denote the standard basis for $\mathbb{R}^n$. So e_i is a vector with 1 in the ith position, and 0 everywhere else.

Now let $A \in \mathsf{GL}_n(\mathbb{Z})$. We want to compute A^{-1} and show that it has integer entries. Let x_i be the ith column of A^{-1}. Then $Ax_i = e_i$. Consequently,

$$\left(A^{-1}\right)_{i,j} = (x_i)_j = \frac{\det(A(j, e_i))}{\det(A)}.$$

Note that since A, e_i have integer entries, then so does $A(j, e_i)$. Since $\det(A) \in \{-1, 1\}$, we conclude that A^{-1} has integer entries.

Thus, if $A \in \mathsf{GL}_n(\mathbb{Z})$ then $A^{-1} \in \mathsf{GL}_n(\mathbb{Z})$.

The fact that $\mathsf{GL}_n(\mathbb{Z})$ is closed under matrix multiplication is easy to prove, and is left to the reader. □

The following notation is also standard. Define:

$$\mathsf{SL}_n(\mathbb{Z}) = \{A \in \mathsf{GL}_n(\mathbb{Z}) \mid \det(A) = 1\}.$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.27 Show that $\mathsf{SL}_n(\mathbb{Z}) \lhd \mathsf{GL}_n(\mathbb{Z})$ and that $[\mathsf{GL}_n(\mathbb{Z}) : \mathsf{SL}_n(\mathbb{Z})] = 2$.

▷ solution ◁

Exercise 1.28 For $1 \leq i, j \leq n$ let $E_{i,j}$ denote the $n \times n$ matrix with 1 only in the (i, j) entry, and 0 in all other entries.

Show that $\mathsf{SL}_n(\mathbb{Z}) = \left\langle I + E_{i,j} \mid 1 \leq i \neq j \leq n \right\rangle$, where I is the $n \times n$ identity matrix. ▷ solution ◁

1.5.2 Abelian Groups

A group G is called **Abelian**, or **commutative**, if $xy = yx$ for all $x, y \in G$.

A group G is called **finitely generated** if there exists a finite generating set for G. That is, if there exists a finite set $S \subset G$, $|S| < \infty$, such that for any $x \in G$ there are $s_1, \ldots, s_n \in S \cup S^{-1}$ such that $x = s_1 \cdots s_n$. We will come back to finitely generated groups in Section 1.5.7.

Exercise 1.29 Show that the group $\mathbb{Z}^d$ (with vector addition as the group operation) is a finitely generated Abelian group, with the standard basis serving as a finite generating set.

Finitely generated Abelian groups have a special structure. The classification of these groups is given by the so-called *fundamental theorem of finitely generated Abelian groups*. We will prove a simplified version of this theorem.

Theorem 1.5.2 *Let G be a finitely generated Abelian group. Then there exists a finite Abelian group F and some integer $d \geq 0$ such that $G \cong \mathbb{Z}^d \times F$. Also, $d > 0$ if and only if $|G| = \infty$.*

Proof Let $U = \{u_1, \ldots, u_n\}$ be a finite generating set for G. Consider the vector space $V = \mathbb{Q}^n$. Define a map $\psi : \mathbb{Z}^n \to G$ by

$$\psi(z_1, \ldots, z_n) = (u_1)^{z_1} \cdots (u_n)^{z_n}.$$

Note that since G is Abelian and since U generates G, the map ψ is surjective. Also, it is simple to check that because G is Abelian we have that ψ is a homomorphism.

Let $K = \mathsf{Ker}\psi = \{\vec{z} \in \mathbb{Z}^n : \psi(\vec{z}) = 1\}$. Let $W = \mathsf{span}(K)$, which is a subspace of V. The quotient vector space V/W has dimension $d \leq n$, so we can choose $\vec{b}_1, \ldots, \vec{b}_d \in V$ such that $\{b_j + W : 1 \leq j \leq d\}$ forms a (linear) basis for V/W. Let $\vec{w}_1, \ldots, \vec{w}_k$ be a basis for W. By multiplying by a large enough integer,

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

we can assume without loss of generality that $\vec{b}_j \in \mathbb{Z}^n$ for all $1 \leq j \leq d$ and $\vec{w}_j \in \mathbb{Z}^n$ for all $1 \leq j \leq k$.

Define $s_j = \psi(\vec{b}_j)$ for all $1 \leq j \leq d$ and $f_j = \psi(\vec{w}_j)$ for all $1 \leq j \leq k$.

We claim that the map $(z_1, \ldots, z_d) \mapsto (s_1)^{z_1} \cdots (s_d)^{z_d}$ is an isomorphism from $\mathbb{Z}^d$ onto $Z = \langle s_1, \ldots, s_d \rangle$. It is immediate to verify that this is a surjective homomorphism. To show it is injective, assume that $(s_1)^{z_1} \cdots (s_d)^{z_d} = 1$. Then,

$$\psi\left(z_1\vec{b}_1 + \cdots + z_d\vec{b}_d\right) = (s_1)^{z_1} \cdots (s_d)^{z_d} = 1,$$

implying that $z_1\vec{b}_1 + \cdots + z_d\vec{b}_d \in K \subset W$. Since $\vec{b}_1 + W, \ldots, \vec{b}_d + W$ are linearly independent, it must be that $z_1 = \cdots = z_d = 0$. This proves injectivity, showing that $Z \cong \mathbb{Z}^d$.

Now fix some $\vec{z} \in \mathbb{Z}^n \cap W$. Then since $W = \mathsf{span}(K)$, there exist some $q_1, \ldots, q_m \in \mathbb{Q}$ and $\vec{z}_1, \ldots, \vec{z}_m \in K$ such that $\vec{z} = q_1\vec{z}_1 + \cdots + q_m\vec{z}_m$. So there exists a large enough integer $r \neq 0$ such that $r\vec{z} \in K$, implying that $\psi(\vec{z})^r = \psi(r\vec{z}) = 1$. This implies that any element of $F = \langle f_1, \ldots, f_k \rangle$ is *torsion*; that is, for any $x \in F$ there exists an integer $r \neq 0$ such that $x^r = 1$. (One can check that in fact F is exactly the subgroup of all torsion elements of G.) So we may take $r > 0$ large enough so that $(f_j)^r = 1$ for all $1 \leq j \leq k$. Since F is generated by $f_1, \ldots, f_k$, and since F is Abelian, we have that the map $\{0, \ldots, r-1\}^k \to F$ given by $(a_1, \ldots, a_k) \mapsto (f_1)^{a_1} \cdots (f_k)^{a_k}$ is surjective, and thus F is a finite group.

Let $x \in Z \cap F$. So $x^r = 1$ for some integer $r > 0$. Then

$$\psi\left(rz_1\vec{b}_1 + \cdots + rz_d\vec{b}_d\right) = ((s_1)^{z_1} \cdots (s_d)^{z_d})^r = x^r = 1,$$

for some integers $z_1, \ldots, z_d \in \mathbb{Z}$. This implies that $rz_1\vec{b}_1 + \cdots + rz_d\vec{b}_d \in K \subset W$, and as before we get that $z_1 = \cdots = z_d = 0$, so that $x = 1$. That is, we have shown that $Z \cap F = \{1\}$.

Finally, recall that the map $\psi \colon \mathbb{Z}^n \to G$ is surjective. Any $\vec{z} \in \mathbb{Z}^n$ can be written as $\vec{z} = \vec{v} + \vec{w}$ where $\vec{v} = z_1\vec{b}_1 + \cdots + z_d\vec{b}_d$ and $\vec{w} = a_1\vec{w}_1 + \cdots + a_k\vec{w}_k$ for integers $z_1, \ldots, z_d, a_1, \ldots, a_k$. Thus, for any $x \in G$ there exist $\psi(\vec{v}) \in Z$ and $\psi(\vec{w}) \in F$ such that $x = \psi(\vec{v}) \cdot \psi(\vec{w})$.

To conclude, we have $Z \lhd G$ with $Z \cong \mathbb{Z}^d$ and $F \lhd G$ with $|F| < \infty$, and these have the following properties:

- $G = ZF = \{zf : z \in Z\,,\ f \in F\}$,
- $Z \cap F = \{1\}$,
- and for any $z \in Z$, $f \in F$ we have $zf = fz$.

It is an exercise to show that this implies that $G \cong Z \times F$. □

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.30 Let G be a group and let Z, F be subgroups such that $G = ZF$, $Z \cap F = \{1\}$, and $zf = fz$ for all $z \in Z$, $f \in F$.

Show that $G \cong Z \times F$.

1.5.3 Virtual Properties

A **group property** is a class of groups $\mathcal{P}$ such that if $G \cong H$ and $G \in \mathcal{P}$, then also $H \in \mathcal{P}$. For $G \in \mathcal{P}$ we sometimes say that G **is** $\mathcal{P}$.

For a group property $\mathcal{P}$, we may define the property **virtually** $\mathcal{P}$. A group G is **virtually** $\mathcal{P}$ if there exists a finite index subgroup $[G : H] < \infty$ such that H is $\mathcal{P}$.

Example 1.5.3 A group G is virtually finitely generated if there exists a finite index subgroup $H \leq G$, $[G : H] < \infty$ such that H is finitely generated. △▽△

Exercise 1.31 Show that if G is virtually finitely generated then G is finitely generated. ▷ solution ◁

Example 1.5.4 A group G is called **indicable** if there exists a surjective homomorphism from G onto $\mathbb{Z}$.

A group G is therefore **virtually indicable** if there exists a finite index subgroup $[G : H] < \infty$ and a surjective homomorphism $\varphi \colon H \to \mathbb{Z}$. △▽△

Exercise 1.32 Show that if G is finitely generated and there exists a homomorphism $\varphi \colon G \to A$ where A is an Abelian group and $|\varphi(G)| = \infty$, then G is indicable. ▷ solution ◁

Exercise 1.33 Let G be a finitely generated group. Show that $|G/[G, G]| = \infty$ if and only if there exists a surjective homomorphism $\varphi \colon G \to \mathbb{Z}$. ▷ solution ◁

Every group $G \in \mathcal{P}$ is also virtually $\mathcal{P}$, as it has index 1 in itself. But not every property $\mathcal{P}$ is the same as virtually $\mathcal{P}$.

For example: the *infinite dihedral group* D_∞, see Exercise 1.72, is virtually $\mathbb{Z}$ (i.e. contains a finite index subgroup isomorphic to $\mathbb{Z}$) but is not Abelian, and so definitely not isomorphic to $\mathbb{Z}$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.5.4 Nilpotent Groups

Definition 1.5.5 For a group G, we define the **lower central series** inductively as follows: $\gamma_0 = \gamma_0(G) = G$ and $\gamma_{n+1} = \gamma_{n+1}(G) = [\gamma_n(G), G]$ for all $n \geq 0$.

We define the **upper central series** as: $Z_0 = \{1\}$ and for all $n \geq 0$,

$$Z_{n+1} = Z_{n+1}(G) := \{x \in G : \forall\, y \in G\ [x, y] \in Z_n\}.$$

$Z_1 = Z_1(G)$ is called the **center** of G, and is sometimes denoted just $Z(G)$.

Exercise 1.34 Assume that $G = \langle S \rangle$, for some set of elements $S \subset G$.

Show that

$$\gamma_n(G) = \left\langle [s_0, \ldots, s_n]^x : s_0, \ldots, s_n \in S\,,\ x \in G \right\rangle.$$ ▷ solution ◁

Exercise 1.35 Let φ be an automorphism of a group G. Show that $\varphi(\gamma_n(G)) = \gamma_n(G)$ and that $\varphi(Z_n(G)) = Z_n(G)$.

Conclude that $\gamma_n(G), Z_n(G)$ are normal subgroups of G. ▷ solution ◁

Exercise 1.36 Show that for $k \leq n$ we have $Z_k(G) \lhd Z_n(G)$.

Show that $Z_n(G)/Z_k(G) = Z_{n-k}(G/Z_k(G))$. ▷ solution ◁

Exercise 1.37 Show that if $\gamma_n(G) = \{1\}$ then $Z_n(G) = G$. ▷ solution ◁

Exercise 1.38 Show that if $Z_n(G) = G$ then $\gamma_n(G) = \{1\}$. ▷ solution ◁

Exercise 1.39 Show that if G is finitely generated, then γ_k/γ_{k+1} is also finitely generated for any $k \geq 0$. ▷ solution ◁

Definition 1.5.6 A group G is called n-step nilpotent if $\gamma_n(G) = \{1\}$ and $\gamma_{n-1}(G) \neq \{1\}$. (By convention, 0-step nilpotent is just the trivial group.)

A group is called **nilpotent** if it is n-step nilpotent for some $n \geq 0$.

Note that 0-step nilpotent is the trivial group $\{1\}$. Note too that 1-step nilpotent is just Abelian.

Exercise 1.40 Show that a group is n-step nilpotent if and only if $Z_n(G) = G$ and $Z_{n-1}(G) \neq G$.

Show that G is $(n + 1)$-step nilpotent if and only if $G/Z_1(G)$ is n-step nilpotent. ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.41 Show that $G/\gamma_n(G)$ is at most n-step nilpotent. ▷ solution ◁

Exercise 1.42 Show that if G is a nilpotent group and $H \leq G$, then H is nilpotent as well. ▷ solution ◁

Exercise 1.43 Show that if G is nilpotent and $N \lhd G$, then G/N is also nilpotent. ▷ solution ◁

Let us go through some basic examples of nilpotent groups.

Some readers may have seen the following definition: An $n \times n$ matrix $M \in \mathsf{M}_n(\mathbb{R})$ is called k**-step nilpotent** if $M^{k-1} \neq 0$ and $M^k = 0$. This is related to nilpotence of groups, as the following exercises show.

Exercise 1.44 Let $T_n(\mathbb{R})$ denote all $n \times n$ upper triangular matrices with real entries. For $1 \leq k \leq n$ define

$$D_k = \{M \in T_n(\mathbb{R}) : \forall\, j \leq i + k - 1,\ M_{i,j} = 0\}.$$

That is, all the first k diagonals of M are 0. (So e.g. $D_0 = T_n(\mathbb{R})$.)

Show that if $M \in D_k, N \in D_\ell$ then $MN \in D_{k+\ell}$. ▷ solution ◁

Exercise 1.45 Fix $n > 1$. Let $T_n(\mathbb{R})$ denote all $n \times n$ upper triangular matrices. For $1 \leq k \leq n$ define

$$D_k = \{M \in T_n(\mathbb{R}) : \forall\, j \leq i + k - 1,\ M_{i,j} = 0\},$$

and define $D_k(\mathbb{Z}) = D_k \cap \mathsf{M}_n(\mathbb{Z})$ (recall that $\mathsf{M}_n(\mathbb{Z})$ is the set of $n \times n$ matrices with integer entries).

Set

$$Q_{n,k} = \{I + N : N \in D_k(\mathbb{Z})\}.$$

Show that $Q_{n,k}$ is a group (with the usual matrix multiplication). ▷ solution ◁

Exercise 1.46 Let $n > 1$. Let $H_n(\mathbb{Z})$ be the collection of all upper triangular $n \times n$ matrices, with 1 on the diagonal, and only integer entries.

Show that $H_n(\mathbb{Z})$ is a group (with the usual matrix multiplication).

Show that for $0 \leq k \leq n - 1$ we have

$$\gamma_k(H_n(\mathbb{Z})) \subset Q_{n,k+1} \subset Z_{n-k-1}(H_n(\mathbb{Z})).$$ ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.5.5 Solvable Groups

Definition 1.5.7 Let G be a group. The **derived series** is defined inductively as follows: $G^{(0)} = G$, and $G^{(n+1)} = \left[G^{(n)}, G^{(n)}\right]$.

Definition 1.5.8 A group G is n**-step solvable** if $G^{(n)} = \{1\}$ and $G^{(n-1)} \neq \{1\}$. (By convention, 0-step solvable is the trivial group.)

A group is **solvable** if it is solvable for some $n \geq 0$.

Note that the properties of 1-step solvable, 1-step nilpotent, and Abelian all coincide.

Exercise 1.47 Show that any nilpotent group is solvable. ▷ solution ◁

Exercise 1.48 Show that if G is 2-step solvable, then $G^{(1)}$ is Abelian. ▷ solution ◁

Exercise 1.49 Show that the following are equivalent:

- G is a solvable group.
- $G^{(n)}$ is solvable for all $n \geq 0$.
- $G^{(n)}$ is solvable for some $n \geq 0$. ▷ solution ◁

Exercise 1.50 Show that if G is solvable and infinite then $[G : [G, G]] = \infty$.

▷ solution ◁

Exercise 1.51 Show that if G is a solvable group and $H \leq G$ then H is solvable.

▷ solution ◁

Exercise 1.52 Let Δ_n^+ denote the collection of all $n \times n$ diagonal matrices with real entries and only positive values on the diagonal.

Show that Δ_n^+ is an Abelian group (with the usual matrix multiplication).

▷ solution ◁

Exercise 1.53 Fix $n > 1$, and recall D_k, the collection of all $n \times n$ upper triangular matrices, with first k diagonals equal to 0 (from Exercise 1.44).

Recall also Δ_n^+, the collection of all $n \times n$ diagonal matrices with only positive values on the diagonal.

For $k \geq 1$ define

$$P_{n,k} = P_{n,k} := \{T + M : T \in \Delta_n^+ \,,\ M \in D_k\}.$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Show that $P_{n,k}$ is a group (with the usual matrix multiplication).
Show that $[P_{n,k}, P_{n,k}] \subset \{I + M \colon M \in D_k\}$.
Show that $P_{n,k}$ is solvable, of step at most $\lceil \log_2(n) \rceil + 1$.
Show that $P_{n,k}$ is not nilpotent when $k < n$. ▷ solution ◁

Exercise 1.54 Let $r > 1$ and consider $\omega = e^{2\pi i/r}$, the rth root of unity. Define

$$D = \left\{ \sum_{k=0}^{r-1} a_k \omega^k : a_k \in \mathbb{Z} \right\}$$

and

$$G = \left\{ \begin{bmatrix} \omega^z & d \\ 0 & 1 \end{bmatrix} : z \in \mathbb{Z},\ d \in D \right\}.$$

Show that G is a finitely generated virtually Abelian group that is not nilpotent.

▷ solution ◁

1.5.6 Free Groups

Let S be a finite set. For each element $s \in S$, consider a new element $\bar{s}$, and define $\bar{S} = \{\bar{s} : s \in S\}$. Consider all possible finite words in the letters $S \cup \bar{S}$, including the empty word $\varnothing$, and denote this set by Ω_S. That is,

$$\Omega_S := \{a_1 \cdots a_n : n \in \mathbb{N},\ a_j \in S \cup \bar{S}\} \cup \{\varnothing\}.$$

Define the *reduction operation* $R \colon \Omega_S \to \Omega_S$ as follows: Call a word $a_1 \cdots a_n \in \Omega_S$ **reduced** if for all $1 \le j < n$ we have that $(a_j, a_{j+1}) \notin \{(s, \bar{s}), (\bar{s}, s) : s \in S\}$. The empty word $\varnothing$ is reduced by convention. Let $\mathbb{F}_S$ denote the collection of all reduced words. Now, for a word $\omega \in \mathbb{F}_S$, define $R(\omega) = \omega$. For a word $a_1 \cdots a_n \notin \mathbb{F}_S$, let j be the smallest index for which $(a_j, a_{j+1}) \in \{(s, \bar{s}), (\bar{s}, s) : s \in S\}$, and define $R(a_1 \cdots a_n) = a_1 \cdots a_{j-1} a_{j+2} \cdots a_n$ (if $j = 1$ this means $R(a_1 \cdots a_n) = a_3 \cdots a_n$).

It is easy to see that for any word $a_1 \cdots a_n \in \Omega_S$, at most n applications of R will result in a reduced word. Let $R^\infty(a_1 \cdots a_n)$ denote this reduced word. So $R^\infty \colon \Omega_S \to \mathbb{F}_S$, which fixes any word in $\mathbb{F}_S$.

Define a product structure on $\mathbb{F}_S$: For two reduced words $a_1 \cdots a_n$ and $b_1 \cdots b_m$ define

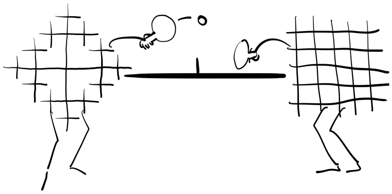
$$\varnothing a_1 \cdots a_n = a_1 \cdots a_n \varnothing = a_1 \cdots a_n$$

and

$$a_1 \cdots a_n \cdot b_1 \cdots b_m = R^\infty(a_1 \cdots a_n b_1 \cdots b_m).$$

It is easily verified that this turns $\mathbb{F}_S$ into a group with identity element $\varnothing$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press



Definition 1.5.9 $\mathbb{F}_S$ is called the **free group** on generators S.

Since the actual letters generating the free group are not important, we will usually write $\mathbb{F}_d$ for the free group generated by d elements.

If G is a finitely generated group, generated by a finite set S, then consider $\mathbb{F}_S$ and define a map $\varphi\colon \mathbb{F}_S \to G$ by $\varphi(\varnothing) = 1$, for $s \in S$ we set $\varphi(s) = s$ and $\varphi(\bar{s}) = s^{-1}$, and finally for general reduced words set $\varphi(a_1 \cdots a_n) = \varphi(a_1) \cdots \varphi(a_n)$. This is easily seen to be a surjective homomorphism, so $G \cong \mathbb{F}_S/\mathsf{Ker}\varphi$.

Remark 1.5.10 Let G be a group generated by a finite set S. We have seen that there exists a normal subgroup $R \lhd \mathbb{F}_S$ such that $\mathbb{F}_S/R \cong G$. In this case we write $G = \langle S \mid R \rangle$.

Moreover, suppose there exist $(r_n)_n \subset R$ such that R is the smallest normal subgroup containing all $(r_n)_n$. Then we write $G = \langle S \mid (r_n)_n \rangle$.

We will come back to this *presentation* in Section 1.5.8.

There is a classical method of proving that certain groups (or subgroups) are isomorphic to a free group. We will not require it but include it for the educational value.

Exercise 1.55 (Ping-pong lemma) Let G be a group acting on some set X. Let $a, b \in G$.

Suppose that there exist disjoint non-empty subsets $A, B \subset X$, $A \cap B = \emptyset$ such that for all $0 \neq z \in \mathbb{Z}$ we have $a^z(B) \subset A$ and $b^z(A) \subset B$. (This is known as: *a, b play ping-pong*.)

Then $H = \langle a, b \rangle \leq G$ is isomorphic to $\mathbb{F}_2$. ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.56 Consider $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ in $\mathsf{SL}_2(\mathbb{Z})$.

Show that $S = \langle a, b\rangle$ is a free group generated by 2 elements. ▷ solution ◁

Remark 1.5.11 The group S above, generated by $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$, is sometimes called the *Sanov subgroup*.

Note that $\mathsf{SL}_2(\mathbb{Z})$ is generated by $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $y = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and that $a = x^2$ and $b = y^2$.

Exercise 1.57 Let $I \in \mathsf{SL}_2(\mathbb{Z})$ denote the 2×2 identity matrix. Show that $\{-I, I\} \lhd \mathsf{SL}_2(\mathbb{Z})$.

Denote $\mathsf{PSL}_2(\mathbb{Z}) = \mathsf{SL}_2(\mathbb{Z})/\{-I, I\}$.

Exercise 1.58 Let $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $y = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and let $a = x^2, b = y^2$. Set $t = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $s = xt$.

Show that $t^2 = s^3 = -I$, where I is the 2×2 identity matrix.

Show that $x = -st$ and $y = -s^2t$.

Let $\pi \colon \mathsf{SL}_2(\mathbb{Z}) \to \mathsf{PSL}_2(\mathbb{Z})$ be the canonical homomorphism. Show that $\mathsf{PSL}_2(\mathbb{Z}) = \langle \pi(t), \pi(s)\rangle$.

Show that for any $z \in \mathsf{SL}_2(\mathbb{Z})$ there exist $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ and $\alpha, \beta \in \{0, 1\}$ such that $z \equiv t^\alpha s^{\varepsilon_1} t s^{\varepsilon_2} \cdots t s^{\varepsilon_n} t^\beta \pmod{\{-I, I\}}$.

Exercise 1.59 Let x, y, a, b, s, t be as in Exercise 1.58.

Let $S = \langle a, b\rangle \leq \mathsf{SL}_2(\mathbb{Z})$ be the Sanov subgroup (from Exercise 1.56).

Show that $a = stst$ and $b = s^2ts^2t$.

Let $\pi \colon \mathsf{SL}_2(\mathbb{Z}) \to \mathsf{PSL}_2(\mathbb{Z})$ be the canonical projection.

Show that for any $z \in \mathsf{SL}_2(\mathbb{Z})$ there exist $w \in S$ and $p \in \left\{1, s, s^2, t, st, s^2t\right\}$ such that $\pi(z) = \pi(w)\pi(p)$.

Show that $[\mathsf{PSL}_2(\mathbb{Z}) : \pi(S)] \leq 6$.

Conclude that $[\mathsf{SL}_2(\mathbb{Z}) : S] \leq 12$. ▷ solution ◁

1.5.7 Finitely Generated Groups

Exercise 1.60 Let $H \leq G$ and let S be a finite generating set for G. Let T be a *right-traversal* of H in G; that is, a set of representatives for the right-cosets of H containing $1 \in T$. So $G = \biguplus_{t \in T} Ht$.

Show that H is generated by $TST^{-1} \cap H$. ▷ solution ◁

Exercise 1.61 Show that a finite index subgroup of a finitely generated group is also finitely generated.

Exercise 1.62 Let $H \lhd G$ and let $\pi \colon G \to G/H$ be the canonical projection.

Assume that H is generated by U and G/H is generated by $\tilde{S}$.

Show that if $S \subset G$ is such that $\pi(S) = \tilde{S}$, then $U \cup S$ generates G.

Conclude that if H and G/H are finitely generated, then so is G. ▹ solution ◃

A nice property of finitely generated groups is that there cannot be too many finite index subgroups of a given index.

Theorem 1.5.12 *Let G be a finitely generated group, generated by d elements. Then for any n, the set* $\{H \leq G \mid [G:H] = n\}$ *has size at most* $(n!)^d$.

Proof Assume that $S \subset G$ is a finite generating set for G of size $|S| = d$.

Let Π_n be the group of permutations of the set $\{1, 2, \ldots, n\}$.

Let $X = \{H \leq G : [G:H] = n\}$. If $X = \emptyset$ then it is of course finite. So assume that $X \neq \emptyset$.

Consider $H \in X$. Write $G/H = \{xH : x \in G\} = \{x_1H, x_2H, \ldots, x_nH\}$, where $x_1 = 1$. G acts on G/H by $x(yH) = xyH$. Define $\psi_H \colon G \to \Pi_n$ by $x \mapsto \pi_x \in \Pi_n$, where π_x is the permutation for which $\pi_x(i) = j$ for the unique $1 \leq i, j \leq n$ such that $xx_iH = x_jH$. Note that $\pi_x(1) = 1$ if and only if $x \in H$.

It is easy to see that ψ_H is a homomorphism from G into Π_n.

We claim that $H \mapsto \psi_H$ is an injective map from X into $\mathsf{Hom}(G, \Pi_n)$. Indeed, if $H \neq K \in X$, then without loss of generality we may take $x \in H \backslash K$ (otherwise $x \in K \backslash H$, and reverse the roles of H and K in what follows). Let $\pi = \psi_H(x)$ and $\sigma = \psi_K(x)$. Since $x \in H$ we have that $\pi(1) = 1$. Since $x \notin K$ we have that $\sigma(1) \neq 1$. So $\psi_H(x) \neq \psi_K(x)$, implying that $\psi_H \neq \psi_K$.

We conclude that $|X| \leq |\mathsf{Hom}(G, \Pi_n)|$, so we only need to bound the size of this last quantity.

Any homomorphism $\psi \in \mathsf{Hom}(G, \Pi_n)$ is completely determined by the values $\{\psi(s) : s \in S\}$. Thus,

$$|\mathsf{Hom}(G, \Pi_n)| \leq \left|(\Pi_n)^S\right| = (n!)^d. \qquad \square$$

1.5.8 Finitely Presented Groups

Definition 1.5.13 Let G be a group generated by a finite set S. Consider the free group on the generators S, $\mathbb{F}_S$. If it is possible to find a normal subgroup $R \lhd \mathbb{F}_S$ and finitely many $r_1, \ldots, r_k \in R$ such that R is the smallest normal subgroup

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

containing $r_1, \ldots, r_k$, we write $G = \langle S \mid r_1, \ldots, r_k \rangle$, and in this special case we say that G is **finitely presented**.

The elements of S are called **generators** of G, and the elements of R are called **relations** of G.

The next lemma shows how the property of finite presentation can be moved from quotients by finitely presented groups to the mother group.

Lemma 1.5.14 *Let G be a group and $N \lhd G$. Assume that both N and G/N are finitely presented. Then, G is finitely presented as well.*

Proof Assume that

$$N = \langle s_1, \ldots, s_k \mid r_1, \ldots, r_\ell \rangle \qquad \text{and} \qquad G/N = \langle a_1, \ldots, a_d \mid p_1, \ldots, p_m \rangle .$$

Let $\mathbb{F} = \mathbb{F}_{d+k}$ be the free group on $d + k$ generators. Denote the generators of $\mathbb{F}$ by $\{f_1, \ldots, f_d, t_1, \ldots, t_k\}$. Let $F = \langle f_1, \ldots, f_d \rangle \le \mathbb{F}$ and $T = \langle t_1, \ldots, t_k \rangle \le \mathbb{F}$. So F is a free group on d generators, and T is a free group on k generators.

For any $1 \le j \le d$ choose an element $g_j \in G$ such that g_j is mapped to a_j under the canonical projection $G \to G/N$ (i.e. $a_j = N g_j$).

Let $\varphi \colon \mathbb{F} \to G$ be the homomorphism defined by $\varphi(f_j) = g_j$ for $1 \le j \le d$ and $\varphi(t_j) = s_j$ for $1 \le j \le k$. By our assumptions on the presentation for N, there exist words $r_1, \ldots, r_\ell \in T$ such that if R is the smallest normal subgroup of T containing $r_1, \ldots, r_k$, then $\varphi|_T : T \to N$ with $\mathsf{Ker}(\varphi|_T) = \mathsf{Ker}\varphi \cap T = R$.

Also, by our assumptions on the presentation of G/N, there exist words $p_1, \ldots, p_m \in F$ such that if P is the smallest normal subgroup of F containing $p_1, \ldots, p_m$, then $\varphi^{-1}(N) \cap F = P$

For any $1 \le i \le k$ and $1 \le j \le d$, we have that $\varphi\left((t_i)^{f_j}\right) = (n_i)^{g_j} \in N$. So there exists $u_{i,j} \in T$ such that $\varphi\left((t_i)^{f_j}\right) = \varphi(u_{i,j})$. Define $q_{i,j} = (t_i)^{f_j}(u_{i,j})^{-1}$. Observe that $q_{i,j} \in \mathsf{Ker}\varphi$ for all i, j.

For any $1 \le j \le m$ we have that $\varphi(p_j) \in N$, by our assumptions on the presentation of G/N. So there exists $w_j \in T$ such that $\varphi(p_j) = \varphi(w_j)$. Define $z_j = p_j(w_j)^{-1}$. Observe that $z_j \in \mathsf{Ker}\varphi$ for all j.

Denote $K := \mathsf{Ker}\varphi$. Let Q be the smallest normal subgroup of $\mathbb{F}$ containing $\{q_{i,j} : 1 \le i \le k\ ,\ 1 \le j \le d\}$. Let Z be the smallest normal subgroup of $\mathbb{F}$ containing $z_1, \ldots, z_m$.

Let $M \lhd \mathbb{F}$ be any normal subgroup containing

$$\{r_1, \ldots, r_\ell, z_1, \ldots, z_m\} \bigcup \{q_{i,j} : 1 \le i \le k\ ,\ 1 \le j \le d\} \subset M .$$

Since M is an arbitrary normal subgroup containing the above relations, we only need to show that $K \lhd M$ for all such M, which will prove that G is finitely presented, since $G \cong \mathbb{F}/K$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

To this end, we will prove that

$$K \subset RQZ := \{rqz : r \in R\,,\ q \in Q\,,\ z \in Z\} \subset M. \tag{1.2}$$

We move to prove (1.2). It will be convenient to use the notations

$$AB = \{ab : a \in A\,,\ b \in B\} \qquad \text{and} \qquad A^B = \{a^b : a \in A\,,\ b \in B\}$$

for subsets $A, B \subset \mathbb{F}$.

Step I. Let $t \in T$ and $f \in F$. Then replacing $(t_i)^{f_j} = u_{i,j}q_{i,j}$, since $Q \lhd \mathbb{F}$, we have that $t^f = uq$ for some $u \in T$ and $q \in Q$. That is, $T^F \subset TQ$.

Step II. For any $1 \leq j \leq m$, and any $f \in F$, we have that $(p_j)^f = (w_j z_j)^f$. Since $Z \lhd \mathbb{F}$ and since $P = \left\langle (p_j)^f : 1 \leq j \leq m\,,\ f \in F \right\rangle$, we have that $P \subset T^F Z \subset TQZ$.

Step III. For any $x \in \mathbb{F}$ we can write $x = h_1 v_1 \cdots h_n v_n$ for some $h_1, \ldots, h_n \in F$ and $v_1, \ldots, v_n \in T$. By conjugating the v_j, we have that $x = (u_1)^{d_1} \cdot (u_n)^{d_n} f$ for some $u_1, \ldots, u_n \in T$ and $d_1, \ldots, d_n, f \in F$. Since $Q \lhd \mathbb{F}$, we conclude that $\mathbb{F} \subset TQF$.

Step IV. Let $x \in K$. Write $x = tqf$ for $t \in T$, $q \in Q$, and $f \in F$. So $\varphi(tf) = 1$, implying that $f \in \varphi^{-1}(N) \cap F = P$. This implies that

$$K \subset TQP \subset TQTQZ \subset TQZ.$$

Hence, for any $x \in K$ we can write $x = tqz$ for some $t \in T$, $q \in Q$, and $z \in Z$. Since $Q, Z \subset K$, we have that $t \in T \cap K = R$. So we have shown that $K \subset RQZ$, which is (1.2). □

Theorem 1.5.15 *Suppose G is a group, and suppose that there exists a sequence of subgroups $G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\}$, with the property that every quotient H_j/H_{j+1} is finitely presented.*

Then G is finitely presented.

Proof This is proved by induction on n. If $n = 1$, then $G = H_0$ is finitely presented by assumption.

For $n > 1$, let $H = H_1$. By induction, considering the sequence $H = H_1 \rhd \cdots \rhd H_n = \{1\}$ we have that H is finitely presented. Also, by assumption G/H_1 is finitely presented. So G is finitely presented by Lemma 1.5.14, completing the induction. □

Exercise 1.63 Show that if G is a finite group then it is finitely presented.

▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.64 Assume that a group G is virtually-$\mathbb{Z}$; that is, there exists a finite index normal subgroup $H \lhd G$, $[G : H] < \infty$ such that $H \cong \mathbb{Z}$.

Show that G is finitely presented. ▷ solution ◁

Exercise 1.65 Let G be a n-step solvable group. Assume that $G^{(k)}/G^{(k+1)}$ is virtually-$\mathbb{Z}$ for every $0 \leq k < n$.

Show that G is finitely presented. ▷ solution ◁

Exercise 1.66 Show that $\mathbb{Z}^d$ is finitely presented.

Show that any finitely generated virtually Abelian group is finitely presented.

▷ solution ◁

Exercise 1.67 Show that if G is a finitely generated nilpotent group, then G is finitely presented. ▷ solution ◁

1.5.9 Semi-direct Products

In this exercise, we introduce the notion of *semi-direct products*.

Recall that a *direct product* of groups G, H is the group whose elements are the pairs $G \times H$ and the group operation is given by $(g, h)(g', h') = (gg', hh')$ for all $g, g' \in G$ and $h, h' \in H$.

Exercise 1.68 Let G, H be groups. Assume that G acts on H by automorphisms. That is, each $g \in G$ can be thought of as an automorphism of H. A different way of thinking of this is that there is a homomorphism $\rho \colon G \to \mathrm{Aut}(H)$; that is, $g.h = (\rho(g))(h)$ for any $g \in G$ and $h \in H$.

Define the **semi-direct product** of G acting on H (with respect to ρ) as the group $G \ltimes H$ (also sometimes denoted $H \rtimes_\rho G$), whose elements are $G \times H = \{(g, h) \mid g \in G\,,\ h \in H\}$ and where multiplication is defined by

$$(g, h)(g', h') = (gg', h \cdot g.h').$$

Show that this defines a group structure. Determine the identity element in $G \ltimes H$ and the inverse of (g, h).

Show that the set $\{1_G\} \times H$ is an isomorphic copy of H sitting as a normal subgroup inside $G \ltimes H$. Show that $G \ltimes H/(\{1_G\} \times H) \cong G$. ▷ solution ◁

A useful (but not completely precise) way to think about semi-direct product $G \ltimes H$ is to think of matrices of the form $\left[\begin{smallmatrix} g & h \\ 0 & 1 \end{smallmatrix}\right]$, $g \in G, h \in H$. This is especially aesthetic when H is Abelian, so that multiplication in H can be written additively. Indeed, when multiplying two such matrices we have

$$\begin{bmatrix} g & h \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} g' & h' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} gg' & gh'+h \\ 0 & 1 \end{bmatrix},$$

which is reminiscent of $(g, h)(g', h') = (gg', h + gh')$. In the non-Abelian case matrix multiplication must be interpreted properly:

$$\begin{bmatrix} g & h \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} g' & h' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} gg' & h \cdot gh' \\ 0 & 1 \end{bmatrix}.$$

Also, it may be worth pointing out that $G \ltimes H$ hints at which group is acting on which: $\ltimes$ has a small triangle, similar to the symbol $\rhd$, which reminds us that $H \cong \{1_G\} \times H \lhd G$.

Exercise 1.69 Let G, H be groups. Define an action $\rho\colon G \to \mathsf{Aut}(H)$ of G on H by $\rho(g).h = h$ for all $h \in H$ and $g \in G$.

Show that $G \ltimes H = G \times H$.

So a semi-direct product generalizes the notion of a direct product of groups.

Exercise 1.70 Recall from Sections 1.5.4 and 1.5.5 the following groups of $n \times n$ matrices: For $1 \leq k \leq n$, the group D_k is the additive group of all upper-triangular $n \times n$ real matrices A such that $A_{i,j} = 0$ for all $j \leq i + k - 1$ (so the first k diagonals are 0). Here, Δ_n^+ is the multiplicative group of diagonal matrices with only strictly positive entries on the diagonal.

Show that Δ_n^+ acts on D_k by left multiplication.

Show that $\Delta_n^+ \ltimes D_k$ is 2-step solvable.

Show that if $\Delta_n^+ \ltimes D_k$ is nilpotent, then $k \geq n$. ▷ solution ◁

Exercise 1.71 Let V be a vector space over $\mathbb{C}$. $\varphi\colon V \to V$ is an **affine transformation** if $\varphi(v) = \alpha v + u$ for some fixed scalar $0 \neq \alpha \in \mathbb{C}$ and fixed vector u (α is called the *dilation* and u the *translation*).

Let A be the collection of all affine transformations on V. Show that A is a group with multiplication given by composition.

Show that $A \cong \mathbb{C}^* \ltimes V$ where $\mathbb{C}^*$ is the multiplicative group $\mathbb{C}\backslash\{0\}$ and V is considered as an additive group.

Is A Abelian? Nilpotent? Solvable? ▷ solution ◁

Exercise 1.72 The **infinite dihedral group** is $D_\infty = \left\langle a, b \mid baba\ ,\ b^2 \right\rangle$.

Let $\varphi \in \mathsf{Aut}(\mathbb{Z})$ be given by $\varphi(x) = -x$. Let $\mathbb{Z}_2 = \{-1, 1\}$ be the group on 2 elements (the group operation given by multiplication). Show that $D_\infty \cong \mathbb{Z}_2 \ltimes \mathbb{Z}$ where $\mathbb{Z}_2$ acts on $\mathbb{Z}$ via $\varepsilon.x = \varepsilon \cdot x$ for $\varepsilon \in \{-1, 1\}$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Show that D_∞ is not nilpotent.

Show that D_∞ is 2-step solvable.

Show that D_∞ is virtually $\mathbb{Z}$. ▷ solution ◁

Exercise 1.73 Consider the following group: Let S_d be the group of permutations on d elements. Let S_d act on $\mathbb{Z}^d$ by permuting the coordinates; that is, $\sigma(z_1, \ldots, z_d) = \left(z_{\sigma^{-1}(1)}, \ldots, z_{\sigma^{-1}(d)}\right)$.

Show that this is indeed a left action.

Consider the group $G = S_d \ltimes \mathbb{Z}^d$. Show that there exist $H \lhd G$ such that $G/H \cong S_d$ and $H \cong \mathbb{Z}^d$. (Specifically H is Abelian.)

Show that G is not Abelian for $d > 2$. ▷ solution ◁

1.6 Measures on Groups and Harmonic Functions

1.6.1 Metric and Measure Structures on a Group

Definition 1.6.1 (Cayley graph) Let G be a finitely generated group. Let $S \subset G$ be a finite generating set. Assume that S is **symmetric**; that is, $S = S^{-1} := \{s^{-1} : s \in S\}$. The **Cayley graph** of G with respect to S is the graph with vertex set G and edges defined by the relations $x \sim y \iff x^{-1}y \in S$.

The distance in this Cayley graph is denoted by dist_S.

Exercise 1.74 Show that $\mathrm{dist}_S(x, y)$ is invariant under the diagonal G-action. That is, $\mathrm{dist}_S(gx, gy) = \mathrm{dist}_S(x, y)$ for any $g \in G$.

Due to this fact, we may denote $|x| = |x|_S := \mathrm{dist}_S(1, x)$. So that $\mathrm{dist}_S(x, y) = |x^{-1}y|$. Balls of radius r in this metric are denoted

$$B(x, r) = B_S(x, r) = \{y : \mathrm{dist}_S(x, y) \le r\}.$$

Throughout the book, the underlying generating set will be implicit, and we will not specify it explicitly in the notation. If we wish to stress a specific generating set (or, sometimes, a specific group), we will use the notation $\mathrm{dist}_{G,S}(x, y) = \mathrm{dist}_S(x, y) = \mathrm{dist}_G(x, y)$ and $B_{G,S}(x, r) = B_S(x, r) = B_G(x, r)$.

Exercise 1.75 Let S, T be two finite symmetric generating sets of G. Show that there exists a constant $\kappa = \kappa_{S,T} > 0$ such that for all $x, y \in G$,

$$\kappa^{-1} \cdot \mathrm{dist}_T(x, y) \le \mathrm{dist}_S(x, y) \le \kappa \cdot \mathrm{dist}_T(x, y)\,.$$

▷ solution ◁

Definition 1.6.2 Let μ be a probability measure on G.

- We say that μ is **adapted** (to G) if any element $x \in G$ can be written as a product $x = s_1 \cdots s_k$ where $s_1, \ldots, s_k \in \operatorname{supp}(\mu)$.
- μ is **symmetric** if $\mu(x) = \mu\left(x^{-1}\right)$ for all $x \in G$.
- μ has an **exponential tail** if for some $\varepsilon > 0$,

$$\mathbb{E}_\mu\left[e^{\varepsilon|X|}\right] = \sum_x \mu(x) e^{\varepsilon|x|} < \infty.$$

- We say that μ has k**th moment** if

$$\mathbb{E}_\mu\left[|X|^k\right] = \sum_x \mu(x)|x|^k < \infty.$$

By $\mathsf{SA}(G,k)$ we denote the collection of symmetric, adapted measures on G with kth moment. By $\mathsf{SA}(G,\infty)$ we denote the collection of symmetric, adapted, exponential tail measures on G.

Exercise 1.76 Show that if μ has kth moment with respect to a finite symmetric generating set S, then μ has kth moment with respect to *any* finite symmetric generating set.

Show that if μ has an exponential tail with respect to a finite symmetric generating set S, then μ has an exponential tail with respect to *any* finite symmetric generating set.

The most basic example of $\mu \in \mathsf{SA}(G,\infty)$ is when μ is the uniform measure on some finite symmetric generating set S of a finitely generated group G.

Exercise 1.77 Show that if μ is a symmetric, adapted measure on G with finite support, then $\mu \in \mathsf{SA}(G,\infty)$.

Exercise 1.78 Show that if μ, ν are symmetric probability measures on G, then $p\mu + (1-p)\nu$ is also symmetric for $p \in (0,1)$.

Exercise 1.79 Show that if μ is an adapted probability measure on G and ν is any probability measure on G, then for any $p \in (0,1]$ we have that $p\mu + (1-p)\nu$ is also adapted.

Exercise 1.80 Let $p \in (0,1)$. Show that if $\mu \in \mathsf{SA}(G,k)$ then $\nu = p\delta_1 + (1-p)\mu \in \mathsf{SA}(G,k)$. (Such a measure ν is called a *lazy version* of μ.) ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.6.2 Random Walks

Given a group G with a probability measure μ define the **μ-random walk** on G started at $x \in G$ as the sequence

$$X_t = xU_1U_2 \cdots U_t,$$

where $(U_j)_j$ are i.i.d. with law μ.

The probability measure and expectation on $G^{\mathbb{N}}$ (with the canonical cylinder-set σ-algebra) are denoted $\mathbb{P}_x, \mathbb{E}_x$. When we omit the subscript x we refer to $\mathbb{P} = \mathbb{P}_1, \mathbb{E} = \mathbb{E}_1$. Note that the law of $(X_t)_t$ under $\mathbb{P}_x$ is the same as the law of $(xX_t)_t$ under $\mathbb{P}$. For a probability measure ν on G we denote $\mathbb{P}_\nu = \sum_x \nu(x)\,\mathbb{P}_x$ and similarly for $\mathbb{E}_\nu = \sum_x \nu(x)\,\mathbb{E}_x$. More precisely, given some probability measure ν on G, we define $\mathbb{P}_\nu$ to be the measure obtained by Kolmogorov's extension theorem, via the sequence of measures

$$P_t\left(\{(X_0, \ldots, X_t) = (g_0, \ldots, g_t)\}\right) = \nu(g_0) \cdot \prod_{j=1}^{t} \mu\left(g_{j-1}^{-1} g_j\right).$$

Exercise 1.81 Show that P_t above indeed defines a probability measure on $\mathcal{F}_t = \sigma(X_0, \ldots, X_t)$.

Exercise 1.82 Show that the μ-random walk on G is a Markov chain with transition matrix $P(x, y) = \mu\left(x^{-1}y\right)$. (Markov chains will be defined and studied in Chapter 3. For the unfamiliar reader, this exercise may be skipped in the meantime.)

Show that the corresponding Laplacian operator, usually defined $\Delta := I - P$, and the averaging operator P are given by

$$Pf(x) = f * \check{\mu}(x), \qquad \Delta f(x) = f * (\delta_1 - \check{\mu})(x),$$

where $\check{\mu}(y) = \mu\left(y^{-1}\right)$.

Exercise 1.83 Consider the matrix $P(x, y) = \mu\left(x^{-1}y\right)$ from the previous exercise. Show that if P^t is the tth matrix power of P then

$$\mathbb{E}_x[f(X_t)] = \left(P^t f\right)(x).$$

Exercise 1.84 Let μ be a probability measure on G, and let $P(x, y) = \mu\left(x^{-1}y\right)$.

- Show that $P^t(1, x) = \check{\mu}^{*t}(x)$, where $\check{\mu}^t$ is convolution of $\check{\mu}$ with itself t times. $\left(\check{\mu}(y) = \mu(y^{-1})\right)$.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

- Show that μ is adapted if and only if for every $x, y \in G$ there exists $t \geq 0$ such that $P^t(x, y) > 0$. (This property is also called *irreducible*.)
- Show that μ is symmetric if and only if P is a symmetric matrix (if and only if $\check{\mu} = \mu$).

We will investigate random walks in more depth in Chapter 3.

1.6.3 Harmonic Functions

In classical analysis, a function $f \colon \mathbb{R}^n \to \mathbb{R}$ is harmonic at x if for any small enough ball around x, $B(x,r)$, it satisfies the mean value property: $\frac{1}{|\partial B(x,r)|} \int_{\partial B(x,r)} f(y)dy = f(x)$. Another definition is that $\Delta f(x) = 0$ where $\Delta = \sum_j \frac{\partial^2}{\partial x_j^2}$ is the Laplace operator. (Why these two definitions should coincide is a deep fact, outside the scope of our current discussion.)

Definition 1.6.3 Let G be a finitely generated group and μ a probability measure on G. A function $f \colon G \to \mathbb{C}$ is **μ-harmonic** (or simply, *harmonic*) at $x \in G$ if

$$\sum_y \mu(y) f(xy) = f(x)$$

and the above sum converges absolutely.

A function is harmonic if it is harmonic at every $x \in G$.

Exercise 1.85 Show that f is μ-harmonic at x if and only if $\mathbb{E}_\mu[f(xU)] = f(x)$, if and only if $\Delta f(x) = 0$. (Here $\mathbb{E}_\mu$ is expectation with respect to μ, and U is a random element of G with law μ.)

Exercise 1.86 Prove the *maximum principle* for harmonic functions:

Consider an adapted probability measure μ on G. If f is harmonic, and there exists x such that $f(x) = \sup_y f(y)$, then f is constant.

Exercise 1.87 (L^2 harmonic functions) Consider the space $\ell^2(G)$ of functions $f \colon G \to \mathbb{C}$ such that $\sum_y |f(y)|^2 < \infty$. This space is a Hilbert space with the inner product $\langle f, g \rangle = \sum_y f(y)\overline{g(y)}$.

Prove the following "integration by parts" identity: for any $f, g \in \ell^2(G)$,

$$\sum_{x,y} P(x,y)(f(x) - f(y))(\bar{g}(x) - \bar{g}(y)) = 2 \langle \Delta f, g \rangle .$$

(The left-hand side above is $\langle \nabla f, \nabla g \rangle$, appropriately interpreted, hence the name

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

"integration by parts". This is also sometimes understood as Green's identity.) Here as usual, $P(x, y) = \mu\left(x^{-1}y\right)$ for a symmetric measure μ.

Show that any $f \in \ell^2(G)$ that is harmonic must be constant. ▷ solution ◁

Example 1.6.4 Consider the group $\mathbb{Z}$ and the measure $\mu = \frac{1}{2}\delta_1 + \frac{1}{2}\delta_{-1}$. Suppose that f is a μ-harmonic function. Then, for any $z \in \mathbb{Z}$, $f(z-1)+f(z+1) = 2f(z)$, which implies that

$$\begin{aligned} f(z+1) &= 2f(z) - f(z-1), \\ f(z-1) &= 2f(z) - f(z+1). \end{aligned}$$

So the values of f are determined by the two numbers $f(0), f(1)$. This implies that the space $\mathsf{HF}(\mathbb{Z}, \mu) = \{f : \mathbb{Z} \to \mathbb{C} : \Delta f \equiv 0\}$ of all harmonic functions has dimension at most 2.

Moreover, any function $f(z) = \alpha z + \beta$, is a μ-harmonic function (check this!).

Thus, we conclude that $\mathsf{HF}(\mathbb{Z}, \mu)$ is the (2-dimensional) space of all linear maps $z \mapsto \alpha z + \beta$ for $\alpha, \beta \in \mathbb{C}$. △▽△

Exercise 1.88 Show that if $G = \mathbb{Z}$ and μ is uniform measure on $\{-1, 1, -2, 2\}$ then the space of all μ-harmonic functions has dimension at least 2.

Is this dimension finite? ▷ solution ◁

Exercise 1.89 Consider the group $G = \mathbb{Z}^2$ and the measure μ, which is uniform on the standard generators $\{(\pm 1, 0), (0, \pm 1)\}$.

Show that the functions $f(x, y) = x$, $h(x, y) = y$ and $g(x, y) = x^2 - y^2$ and $k(x, y) = xy$ are all μ-harmonic.

Consider a different measure ν, which is uniform on $\{(\pm 1, 0), (0, \pm 1), \pm(1, 1)\}$. Which of the above functions is harmonic with respect to ν? ▷ solution ◁

Exercise 1.90 Let G be a finitely generated group. Let $\mu \in \mathsf{SA}(G, 1)$. Show that any homomorphism from G to the additive group $(\mathbb{C}, +)$ is a μ-harmonic function. ▷ solution ◁

Exercise 1.91 Let μ be a symmetric and adapted probability measure on a finitely generated group G. Let $p \in (0, 1)$ and let $\nu = p\delta_1 + (1 - p)\mu$ be a lazy version of μ. Show that any function $f : G \to \mathbb{C}$ is μ-harmonic if and only if it is ν-harmonic. ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

1.7 Bounded, Lipschitz, and Polynomial Growth Functions

1.7.1 Bounded Functions

Recall for $f \colon G \to \mathbb{C}$ and $p > 0$ we have

$$||f||_p^p = \sum_x |f(x)|^p,$$

$$||f||_\infty = \sup_x |f(x)|.$$

Recall that $||x.f||_p = ||f||_p$ for all $p \in (0, \infty]$.

Exercise 1.92 Show that $||f||_\infty \leq ||f||_p$ for any $p > 0$.

For a finitely generated group G and a probability measure μ on G, we use $\mathsf{BHF}(G, \mu)$ to denote the set of bounded μ-harmonic functions on G; that is,

$$\mathsf{BHF}(G, \mu) = \{f \colon G \to \mathbb{C} : ||f||_\infty < \infty \,,\ \Delta f \equiv 0\}.$$

Exercise 1.93 Show that $\mathsf{BHF}(G, \mu)$ is a vector space over $\mathbb{C}$. Show that it is a G-invariant subspace; that is, $G.\mathsf{BHF}(G, \mu) \subset \mathsf{BHF}(G, \mu)$.

Any constant function is in $\mathsf{BHF}(G, \mu)$, so $\dim \mathsf{BHF}(G, \mu) \geq 1$. The question of whether $\mathsf{BHF}(G, \mu)$ consists of more than just constant functions is an important one, and we will dedicate Chapter 6 to this investigation.

1.7.2 Lipschitz Functions

For a group G and a function $f \colon G \to \mathbb{C}$, define the right-derivative at y

$$\partial^y f \colon G \to \mathbb{C} \qquad \text{by} \qquad \partial^y f(x) = f\left(xy^{-1}\right) - f(x).$$

Given a finite symmetric generating set S, define the gradient $\nabla f = \nabla_S f \colon G \to \mathbb{C}^S$ by $(\nabla f(x))_s = \partial^s f(x)$. We define the Lipschitz semi-norm by

$$||\nabla_S f||_\infty := \sup_{s \in S} \sup_{x \in G} |\partial^s f(x)|.$$

Definition 1.7.1 A function $f \colon G \to \mathbb{C}$ is called **Lipschitz** if $||\nabla_S f||_\infty < \infty$.

Exercise 1.94 Show that for any two symmetric generating sets S_1, S_2, there exists $C > 0$ such that

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

$$||\nabla_{S_1} f||_\infty \leq C \cdot ||\nabla_{S_2} f||_\infty .$$

Conclude that the definition of *Lipschitz function* does not depend on the choice of specific generating set.

Exercise 1.95 What is the set $\left\{ f \in \mathbb{C}^G : ||\nabla_S f||_\infty = 0 \right\}$?

We use $\mathsf{LHF}(G, \mu)$ to denote the set of Lipschitz μ-harmonic functions; that is,

$$\mathsf{LHF}(G, \mu) = \{ f \colon G \to \mathbb{C} : ||\nabla_S f||_\infty < \infty \, , \; \Delta f \equiv 0 \}.$$

Exercise 1.96 Show that $\mathsf{LHF}(G, \mu)$ is a G-invariant vector space, by showing that

$$\forall \, x \in G \qquad ||\nabla_S x.f||_\infty = ||\nabla_S f||_\infty .$$

Exercise 1.97 (Horofunctions) Let G be a finitely generated group with a metric given by some fixed finite symmetric generating set S.

Consider the space

$$L = \{ h \colon G \to \mathbb{C} : ||\nabla_S h||_\infty \leq 1 \, , \; h(1) = 0 \}.$$

Show that L is compact under the topology of pointwise convergence.

Show that $x.h(y) = h\left(x^{-1}y\right) - h\left(x^{-1}\right)$ defines a left action of G on L.

Show that if h is fixed under the G-action (i.e. $x.h = h$ for all $x \in G$) then h is a homomorphism from G into the group $(\mathbb{C}, +)$.

Show that if h is a homomorphism from G into $(\mathbb{C}, +)$, then there exists $\alpha > 0$ such that $\alpha h \in L$.

For every $x \in G$ let $b_x(y) = \mathrm{dist}_S(x, y) - \mathrm{dist}_S(x, 1) = \left|x^{-1}y\right| - |x|$. Show that $b_x \in L$ for any $x \in G$. Prove that the map $x \mapsto b_x$ from G into L is an injective map.

▷ solution ◁

1.7.3 Polynomially Growing Functions

Let S be a finite, symmetric generating set for a group G. For $f \colon G \to \mathbb{C}$ and $k \geq 0$, define the kth degree **polynomial semi-norm** by

$$||f||_{S,k} := \limsup_{r \to \infty} r^{-k} \cdot \sup_{|x| \leq r} |f(x)|.$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Let

$$\mathsf{HF}_k(G,\mu) = \left\{ f \in \mathbb{C}^G \ : \ f \text{ is } \mu\text{-harmonic}, \ ||f||_{S,k} < \infty \right\}.$$

Exercise 1.98 Show that $|| \cdot ||_{S,k}$ is indeed a semi-norm.

Show that $||x.f||_{S,k} = ||f||_{S,k}$.

Show that $\mathsf{HF}_k(G,\mu)$ is a G-invariant vector space. ▷ solution ◁

Exercise 1.99 Show that if S, T are two finite symmetric generating sets for G then there exists some constant $C = C(S,T,k) > 0$ such that for any $f : G \to \mathbb{C}$ we have $||f||_{S,k} \leq C \cdot ||f||_{T,k}$.

Specifically, the space $\mathsf{HF}_k(G,\mu)$ does not depend on the specific choice of generating set. ▷ solution ◁

Exercise 1.100 Show that if $||f||_{S,k} < \infty$ then there exists $C > 0$ such that for all $x \in G$ we have $|f(x)| \leq C \left(|x|^k + 1 \right)$.

Exercise 1.101 Show that

$$\mathbb{C} \leq \mathsf{BHF}(G,\mu) \leq \mathsf{LHF}(G,\mu) \leq \mathsf{HF}_1(G,\mu) \leq \mathsf{HF}_k(G,\mu) \leq \mathsf{HF}_{k+1}(G,\mu),$$

for all $k \geq 1$.

1.8 Additional Exercises

Exercise 1.102 Let R be a commutative ring. Define $\mathsf{GL}_n(R)$ to be the collection of all $n \times n$ matrices M with entries in R such that $\det(M)$ is an invertible element in R.

Show that $\mathsf{GL}_n(R)$ is a group. ▷ solution ◁

Exercise 1.103 Let I be the $n \times n$ identity matrix. Show that $\{I, -I\} \lhd \mathsf{GL}_n(\mathbb{Z})$.

Define $\mathsf{PGL}_n(\mathbb{Z}) = \mathsf{GL}_n(\mathbb{Z})/\{-I, I\}$.

Show that $\mathsf{GL}_{2n+1}(\mathbb{Z}) \cong \{-1, 1\} \times \mathsf{PGL}_{2n+1}(\mathbb{Z})$.

Show that $\mathsf{SL}_{2n+1}(\mathbb{Z}) \cong \mathsf{PGL}_{2n+1}(\mathbb{Z})$. ▷ solution ◁

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Exercise 1.104 Let $S \leq \mathsf{SL}_2(\mathbb{Z})$ be the Sanov subgroup (see Exercise 1.56 and Remark 1.5.11). Show that if $A \in S$ then

$$A = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix}$$

for some integers $n, m, k, \ell \in \mathbb{Z}$. ▷ solution ◁

Exercise 1.105 Show that the Sanov subgroup is exactly

$$S = \left\{ A = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix} \mid \det(A) = 1, \ k, \ell, n, m \in \mathbb{Z} \right\}.$$

▷ solution ◁

Exercise 1.106 Show that the Sanov subgroup S has finite index in $\mathsf{SL}_2(\mathbb{Z})$. (Hint: use the map taking the matrix entries modulo 4.) ▷ solution ◁

1.9 Solutions to Exercises

Solution to Exercise 1.4 :(
Let $\mathcal{G} = \{A : \theta^t(A) \in \mathcal{F}\}$. $\mathcal{G}$ is easily seen to be a σ-algebra. For any $t \leq n \in \mathbb{N}$ and $g \in G$, we have that

$$\theta^t\left(X_n^{-1}(g)\right) = \{\theta^t(\omega) \colon \omega_n = g\} = X_{n-t}^{-1}(g) \in \mathcal{F},$$

and if $t > n \in \mathbb{N}$ then $\theta^t\left(X_n^{-1}(g)\right) = G^{\mathbb{N}} \in \mathcal{F}$.

So $X_n^{-1}(g) \in \mathcal{G}$ for all $n \in \mathbb{N}$ and $g \in G$. This implies that $\mathcal{F} \subset \mathcal{G}$, which completes the proof. :) ✓

Solution to Exercise 1.5 :(
$\theta^{-t}\mathcal{G}$ is a σ algebra because $\theta^{-t}\left(G^{\mathbb{N}}\right) = G^{\mathbb{N}}$ and $\theta^{-t}(\cup_n A_n) = \cup_n \theta^{-t}(A_n)$ and $\theta^{-t}(A^c) = (\theta^{-t}(A))^c$.

For any $k \in \mathcal{K}$ we have that $\theta^{-t}(K) \in \theta^{-t}\mathcal{G}$ by definition. So let $\mathcal{H}$ be any σ-algebra containing $\{\theta^{-t}(K) : K \in \mathcal{K}\}$. Define $\mathcal{G}' = \{A : \theta^{-t}(A) \in \mathcal{H}\}$. Then, similarly to the above, it is easy to see that $\mathcal{G}'$ is a σ-algebra. Moreover, $\mathcal{K} \subset \mathcal{G}'$, so it must be that $\mathcal{G} \subset \mathcal{G}'$. But then, $\theta^{-t}\mathcal{G} \subset \theta^{-t}\mathcal{G}' \subset \mathcal{H}$. Since $\mathcal{H}$ was any σ-algebra containing $\{\theta^{-t}(K) : K \in \mathcal{K}\}$, this implies that $\theta^{-t}\mathcal{G} = \sigma(\theta^{-t}(K) : K \in \mathcal{K})$. :) ✓

Solution to Exercise 1.6 :(
This is immediate from

$$\theta^{-1}\mathcal{F} = \sigma\left(\theta^{-1}(X_n(g)) : n \in \mathbb{N}, \ g \in G\right) = \sigma(X_{n+1}(g) : n \in \mathbb{N}, \ g \in G) \subset \mathcal{F}. \qquad :) ✓$$

Solution to Exercise 1.7 :(
Note that

$$\theta^{-t}\left(X_n^{-1}(g)\right) = \left\{\omega : \theta^t(\omega) \in X_n^{-1}(g)\right\} = \{\omega : \omega_{t+n} = g\} = X_{t+n}^{-1}(g).$$

Since $\mathcal{F} = \sigma\left(X_n^{-1}(g) : n \in \mathbb{N}, \ g \in G\right)$ we have that

$$\theta^{-t}\mathcal{F} = \sigma\left(\theta^{-t}X_n^{-1}(g) : n \in \mathbb{N}, \ g \in G\right) = \sigma\left(X_{n+t}^{-1}(g) : n \in \mathbb{N}, \ g \in G\right) = \sigma(X_t, X_{t+1}, \ldots). \quad :) ✓$$

Solution to Exercise 1.16 :(
If $g, \gamma \in \mathsf{stab}(x)$, then $\gamma g.x = \gamma.x = x$, and also $g^{-1}.x = g^{-1}g.x = x$. :) ✓

Solution to Exercise 1.17 :(

Let $x \in X$ and $S = \mathsf{stab}(x)$. The map of cosets of S into $G.x$ given by $gS \mapsto g.x$ is a well-defined bijection.

Indeed, if $gS = \gamma S$ then $g = \gamma s$ for some $s \in S$. So $g.x = \gamma s.x = \gamma.x$, and the map is well defined.

It is obviously surjective, and if $g.x = \gamma.x$ then $\gamma^{-1}g \in S$, so $gS = \gamma S$, implying that the map is injective as well. :) ✓

Solution to Exercise 1.21 :(

Compute:

$$\mathbb{P}[X \cdot Y = z] = \sum_x \mathbb{P}\left[X = x\,,\ Y = x^{-1}z\right] = \sum_x \mu(x)\nu\left(x^{-1}z\right) = (\mu * \nu)(z). \qquad :)\ ✓$$

Solution to Exercise 1.23 :(

If $a = 0$ or $b = 0$ there is nothing to prove. So assume that $a, b > 0$. Consider the random variable X that satisfies $\mathbb{P}\left[X = a^{1/p}\right] = p, \mathbb{P}[X = b^{1/q}] = q$. Then $\mathbb{E}[\log X] = \log a + \log b$. Also, $\mathbb{E}[X] = pa^{1/p} + qb^{1/q}$. Jensen's inequality tells us that $\mathbb{E}[\log X] \leq \log \mathbb{E}[X]$, which results in $\log(ab) = \log a + \log b \leq \log\left(pa^{1/p} + qb^{1/q}\right)$.

:) ✓

Solution to Exercise 1.24 :(

The proof is by induction on n. For $n = 1$ there is nothing to prove. For $n = 2$, this is the "usual" Hölder inequality, which is proved as follows: denote $f = f_1$, $g = f_2$, $p = p_1$, $q = p_2$ and $\tilde{f} = \frac{f}{||f||_p}$, $\tilde{g} = \frac{g}{||g||_q}$. Then,

$$\begin{aligned} ||fg||_1 &= ||f||_p \cdot ||g||_q \cdot \sum_x |\tilde{f}(x)| \cdot |\tilde{g}(x)| \leq ||f||_p \cdot ||g||_q \cdot \sum_x \tfrac{1}{p} |\tilde{f}(x)|^p + \tfrac{1}{q} |\tilde{g}(x)|^q \\ &= ||f||_p \cdot ||g||_q \cdot \left(\tfrac{1}{p} ||\tilde{f}||_p^p + \tfrac{1}{q} ||\tilde{g}||_q^q\right) = ||f||_p \cdot ||g||_q, \end{aligned}$$

where the inequality is just Young's inequality for products: $ab \leq pa^{1/p} + qb^{1/q}$. A similar (and simpler) argument proves the case where $p = 1, q = \infty$.

Now for the induction step, $n > 2$. Let $q_n = \frac{p_n}{p_n - 1}$ and $q_j = p_j \cdot \left(1 - \frac{1}{p_n}\right) = \frac{p_j}{q_n}$ for $1 \leq j < n$. Then, $\frac{1}{p_n} + \frac{1}{q_n} = 1$ and

$$\sum_{j=1}^{n-1} \frac{1}{q_j} = \left(1 - \frac{1}{p_n}\right)^{-1} \cdot \sum_{j=1}^{n-1} \frac{1}{p_j} = 1.$$

By the induction hypothesis (for $n = 2$ and $n - 1$),

$$\begin{aligned} ||f_1 \cdots f_n||_1 &\leq ||f_n||_{p_n} \cdot ||f_1 \cdots f_{n-1}||_{q_n} = ||f_n||_{p_n} \cdot \left(|||f_1|^{q_n} \cdots |f_{n-1}|^{q_n}||_1\right)^{1/q_n} \\ &\leq ||f_n||_{p_n} \cdot \left(\prod_{j=1}^{n-1} |||f_j|^{q_n}||_{q_j}\right)^{1/q_n} = ||f_n||_{p_n} \cdot \prod_{j=1}^{n-1} ||f_j||_{p_j}. \qquad :)\ ✓ \end{aligned}$$

Solution to Exercise 1.25 :(

For any x, since $\frac{1}{r} + \frac{r-p}{pr} + \frac{r-q}{qr} = \frac{1}{p} + \frac{1}{q} - \frac{1}{r} = 1$,

$$\begin{aligned} |f * g(x)| &\leq \sum_y \left|f(y)g\left(y^{-1}x\right)\right| = \sum_y \left(|f(y)|^p \left|g\left(y^{-1}x\right)\right|^q\right)^{1/r} \cdot |f(y)|^{(r-p)/r} \left|g\left(y^{-1}x\right)\right|^{(r-q)/r} \\ &= ||f_1 \cdot f_2 \cdot f_3||_1 \leq ||f_1||_r \cdot ||f_2||_{pr/(r-p)} \cdot ||f_3||_{qr/(r-q)}, \end{aligned}$$

where the second inequality is the generalized Hölder inequality with

$$\begin{aligned} f_1(y) &= \left(|f(y)|^p \left|g\left(y^{-1}x\right)\right|^q\right)^{1/r}, \\ f_2(y) &= |f(y)|^{(r-p)/r}, \\ f_3(y) &= \left|g\left(y^{-1}x\right)\right|^{(r-q)/r}. \end{aligned}$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Now,

$$||f_1||_r = \Big(\sum_y |f(y)|^p \left|g\left(y^{-1}x\right)\right|^q \Big)^{1/r},$$

$$||f_2||_{pr/(r-p)} = \left(\sum_y |f(y)|^p \right)^{(r-p)/pr} = ||f||_p^{(r-p)/r},$$

$$||f_3||_{qr/(r-q)} = \left(\sum_y \left|g(y^{-1}x)\right|^q \right)^{(r-q)/qr} = ||x.\check{g}||_q^{(r-q)/r} = ||g||_q^{(r-q)/r},$$

recalling that $\check{g}(z) = g\left(z^{-1}\right)$ and that $||x.\check{g}||_q = ||g||_q$. Combining all the above,

$$\begin{aligned} ||f * g||_r^r &= \sum_x |f * g(x)|^r \leq \sum_{x,y} |f(y)|^p \left|g\left(y^{-1}x\right)\right|^q \cdot ||f||_p^{r-p} \cdot ||g||_q^{r-q} \\ &= ||f||_p^{r-p} \cdot ||g||_q^{r-q} \cdot \sum_y |f(y)|^p \cdot ||y.g||_q^q \\ &= ||g||_q^r \cdot ||f||_p^{r-p} \cdot \sum_y |f(y)|^p = ||g||_q^r \cdot ||f||_p^r. \end{aligned}$$

:) ✓

Solution to Exercise 1.26 :(

Inverses of invertible matrices with integer entries do not necessarily have to have integer entries. For example, take $M = \left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]$. The inverse is $M^{-1} = \frac{1}{3}\left[\begin{smallmatrix} -1 & 2 \\ 2 & -1 \end{smallmatrix}\right]$. :) ✓

Solution to Exercise 1.27 :(

The map $A \mapsto \det(A)$ is a homomorphism from $\mathsf{GL}_n(\mathbb{Z})$ onto $\{-1, 1\}$. $\mathsf{SL}_n(\mathbb{Z})$ is the kernel of this map. :) ✓

Solution to Exercise 1.28 :(

We use $e_1, \ldots, e_n$ to denote the standard basis of $\mathbb{R}^n$.

For a matrix A we write $c_j(A)$ for the jth column of A, and $r_j(A)$ for the jth row of A.

It is easy to see that $AE_{i,j}$ is a matrix with $c_k(AE_{i,j}) = 0$ for $k \neq j$ and $c_j(AE_{i,j}) = c_i(A)$. Thus, multiplying A on the right by $I + E_{i,j}$ results in adding $c_i(A)$ to $c_j(A)$. That is,

$$c_k(A(I + E_{i,j})) = \begin{cases} c_k(A) & \text{for } k \neq j, \\ c_j(A) + c_i(A) & \text{for } k = j. \end{cases}$$

Specifically, $(I + E_{i,j})^{-1} = I - E_{i,j}$. Applying $(I + E_{i,j})^z$ we see that we can add a z-multiple of column i to column j.

By transposing the matrices, we see that

$$r_k((I + E_{i,j})A) = \begin{cases} r_k(A) & \text{for } k \neq j, \\ r_i(A) + r_j(A) & \text{for } k = i. \end{cases}$$

Thus, we can add a multiple of some row i to another row j.

Also, for $i \neq j$, set $S_{i,j} = (I + E_{i,j})(I - E_{j,i})(I + E_{i,j})$. One may compute that

$$c_k(AS_{i,j}) = \begin{cases} c_k(A) & \text{for } k \notin \{i, j\}, \\ -c_j(A) & \text{for } k = i, \\ c_i(A) & \text{for } k = j. \end{cases}$$

That is, we can swap columns at the price of changing the sign of one of them. Multiplying by $S_{i,j}$ on the left we can also swap rows, changing the sign of one.

Denote $G_k = \left\langle I + E_{i,j} \mid 1 \leq i \neq j \leq k \right\rangle$.

We claim by induction on k that for any $A \in \mathsf{GL}_k(\mathbb{Z})$ there exist $M, N \in G_k$ such that for any diagonal $(n-k) \times (n-k)$ matrix D with integer entries, if we consider the $n \times n$ matrix $A' = \left[\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right]$, we find that

$MA'N$ is a diagonal matrix. The base case, where $k = 1$, is just the case where A' is already diagonal, so we may choose $M = N = I$.

So assume $1 < k \leq n$, and let $A \in \mathsf{GL}_k(\mathbb{Z})$. Let D be any diagonal $(n-k) \times (n-k)$ matrix D with integer entries, and define $A' = \left[\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right]$. By swapping columns and/or rows, we may assume without loss of generality that $A'_{k,k} \neq 0$. Now, suppose that $A'_{i,k} \neq 0$ for some $1 \leq i < k$. Adding appropriate multiples of $r_k(A')$ to $r_i(A')$ and appropriate multiples of $r_i(A')$ to $r_k(A')$ sequentially, we arrive at a matrix $M \in G_k$ for which $(MA')_{k,k} \neq 0$ and $(MA')_{i,k} = 0$. Continuing this way for all $1 \leq i < k$, we find that there exists $M \in G_k$ such that $(MA')_{k,k} \neq 0$ and $(MA')_{i,k} = 0$ for all $1 \leq i < n$. The same procedure with columns instead of rows yields a matrix $N \in G_k$ such that $(MA'N)_{k,k} \neq 0$ and $(MA'N)_{i,k} = (MA'N)_{k,i} = 0$ for all $1 \leq i < n$.

Let B be the $(k-1) \times (k-1)$ matrix given by $B_{i,j} = (MA'N)_{i,j}$ for all $1 \leq i, j \leq k-1$. Let D' be the $(n-k+1)\times(n-k+1)$ diagonal matrix given by $D'_{1,1} = (MA'N)_{k,k}$ and $D'_{1+i,1+i} = (MA'N)_{k+i,k+i} = D_{i,i}$ for all $1 \leq i \leq n-k$. We find that

$$MA'N = \left[\begin{smallmatrix} B & 0 \\ 0 & D' \end{smallmatrix}\right].$$

Moreover,

$$\det(A) \cdot \det(D) = \det(A') = \det(MA'N) = \det(B) \cdot (MA'N)_{k,k} \cdot \det(D),$$

which implies that $\det(B) \cdot (MA'N)_{k,k} = \det(A)$. As these are all integers, and $|\det(A)| = 1$, we also find that $|\det(B)| = 1$, so that $B \in \mathsf{GL}_{k-1}(\mathbb{Z})$. By induction, there exist $M', N' \in G_{k-1}$ such that $M'MA'NN'$ is a diagonal matrix. Since $G_{k-1} \leq G_k$, we have that $M'M, MN' \in G_k$, completing the induction step.

Taking $k = n$ from the above induction claim, we see that for any $A \in \mathsf{GL}_n(\mathbb{Z})$ there exist $M, N \in G_n$ such that MAN is a diagonal matrix. Since $\det(A) = \det(MAN)$, and since MAN has integer entries, we find that $a_i := (MAN)_{i,i} \in \{-1, 1\}$ for all $1 \leq i \leq n$. Also, $\det(A) = \prod_{i=1}^n a_i$.

Now, if $A \in \mathsf{SL}_n(\mathbb{Z})$, then $\prod_{i=1}^n a_i = 1$. Let $J = \{1 \leq i \leq n : a_i = -1\}$.

If $J \neq \emptyset$, then since $(-1)^{|J|} = \prod_{j \in J} a_j = 1$, it must be that $|J| \geq 2$. Take any $i \neq j \in J$ and consider the matrix $B = S_{j,i}MANS_{i,j}$. B is a diagonal matrix, with $B_{j,j} = -a_i = 1$ and $B_{i,i} = -a_j = 1$ and $B_{k,k} = a_k$ for all $k \notin \{i,j\}$. Continuing this way, we find some matrices $S, T \in G_n$ such that $TMANS = I$. So $A = M^{-1}T^{-1}S^{-1}N^{-1} \in G_n$, and we are done. :) ✓

Solution to Exercise 1.31 :(

Let G be virtually finitely generated. So there exists $H \leq G$, $[G : H] < \infty$ such that H is finitely generated.

Let $R \subset G$ be a set of representatives for the cosets of H in G; that is $G = \biguplus_{r \in R} Hr$, and $|R| = [G : H]$. Let S be a finite symmetric generating set for H.

Let $x \in G$. There are unique $y \in H$ and $r \in R$ such that $x = yr$. Since S generates H, there are $s_1, \ldots, s_n \in S$ such that $y = s_1 \cdots s_n$. Thus, $x = s_1 \cdots s_n \cdot r$.

This implies that $S \cup R$ is a finite generating set for G. :) ✓

Solution to Exercise 1.32 :(

Since G is finitely generated, the image $\varphi(G)$ is a finitely generated Abelian group. By Theorem 1.5.2, $\varphi(G) \cong \mathbb{Z}^d \times F$ for a finite Abelian group F. If $d = 0$ then $|\varphi(G)| < \infty$. So under our assumptions, $d > 0$.

Since $|\varphi(G)| = \infty$, there must exist $0 \neq z \in \mathbb{Z}^d$ and $f \in F$ such that $(z, f) \in \varphi(G) \leq \mathbb{Z}^d \times F$. Since $z \neq 0$, there must exist $1 \leq j \leq d$ such that $z_j \neq 0$. Let $\pi \colon \mathbb{Z}^d \times F \to \mathbb{Z}$ be the homomorphism given by $\pi(w, f) = w_j$ for all $w \in \mathbb{Z}^d$ and $f \in F$. Then, $\psi = \pi \circ \varphi$ is a homomorphism from G into $\mathbb{Z}$. Since $0 \neq z_j \in \psi(G)$, we obtain that $z_j\mathbb{Z} \leq \psi(G)$, implying that $|\psi(G)| = \infty$. Since $\psi(G) \leq \mathbb{Z}$ it can only be trivial, or isomorphic to $\mathbb{Z}$. Thus, ψ maps G onto the group $\psi(G) \cong \mathbb{Z}$. :) ✓

Solution to Exercise 1.33 :(

Let $\pi \colon G \to G/[G,G]$ be the canonical projection. If $G/[G,G]$ is infinite, then $\pi(G)$ is an infinite Abelian group, so Exercise 1.32 provides a surjective homomorphism onto $\mathbb{Z}$.

If on the other hand there exists a surjective homomorphism $\varphi \colon G \to \mathbb{Z}$, then $[G,G] \lhd \mathsf{Ker}\varphi$. Thus, $[G : [G,G]] \geq [G : \mathsf{Ker}\varphi] = \infty$. :) ✓

Solution to Exercise 1.34 :(

We prove this by induction on n.

Note that

$$[xy, z] = y^{-1}x^{-1}z^{-1}xyz = ([x,z])^y \cdot [y,z],$$

so if $x = s_1 \cdots s_m$ then for any $y \in G$, there exist $z_1, \ldots, z_m$ such that

$$[x, y] = ([s_1, y])^{z_1} \cdots ([s_m, y])^{z_m} .$$

Expanding out y in a similar fashion shows that

$$\gamma_1(G) = \langle [s, s']^x : s, s' \in S,\ x \in G \rangle,$$

proving the claim for $n = 1$.

Assume now that $n > 1$. Recall that

$$\gamma_n(G) = \langle [x, z] : x \in \gamma_{n-1}(G)\, ,\ z \in G \rangle\, .$$

By induction on n, any $x \in \gamma_{n-1}(G)$ can be written as

$$x = [s_{1,1}, \ldots, s_{n-1,1}]^{z_1} \cdots [s_{1,m}, \ldots, s_{n-1,m}]^{z_m}$$

for $s_{i,j} \in S$ and $z_j \in G$. Thus, for any $s \in S$ there exist $w_1, \ldots, w_m \in G$ such that

$$[x, s] = [s_{1,1}, \ldots, s_{n-1,1}, s]^{w_1} \cdots [s_{1,m}, \ldots, s_{n-1,m}, s]^{w_m} .$$

Also, for any $y = r_1 \cdots r_\ell$ with $r_j \in S$ there exist $u_1, \ldots, u_\ell$ such that

$$[x, y]^{-1} = [y, x] = [r_1, x]^{u_1} \cdots [r_\ell, x]^{u_\ell} .$$

All this implies that for any $x \in \gamma_{n-1}(G)$ and any $y \in G$ we can write $[x, y]$ as a finite product of elements of the form $[s_1, \ldots, s_n]^z$ where $s_j \in S$ and $z \in G$. In other words, this proves the induction step. :) ✓

Solution to Exercise 1.35 :(

This is shown by induction on n.

For $n = 0$ it is immediate that we have $\varphi(\gamma_0(G)) = \varphi(G) = G$ and $\varphi(Z_0(G)) = \varphi(\{1\}) = \{1\}$.

For $n > 0$, note that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ for all $x, y \in G$. So by induction

$$\varphi([\gamma_{n-1}(G), G]) = [\varphi(\gamma_{n-1}(G)), \varphi(G)] = [\gamma_{n-1}(G), G] = \gamma_n(G).$$

Also by induction, $[\varphi(x), y] \in Z_{n-1}(G)$ for all $y \in G$ if and only if $\varphi([x, y]) \in Z_{n-1}(G) = \varphi(Z_{n-1}(G))$ for all $y \in G$, which is if and only if $[x, y] \in Z_{n-1}(G)$ for all $y \in G$. So $\varphi(Z_n(G)) = Z_n(G)$.

This completes the proof by induction.

Finally, for any $y \in G$, the map $\varphi_y(x) = x^y$ is an automorphism of G, so that $\gamma_n(G)^y = \gamma_n(G)$ and $Z_n(G)^y = Z_n(G)$ for all $y \in G$; that is, these are normal subgroups. :) ✓

Solution to Exercise 1.36 :(

Since $Z_k(G)$ is a normal subgroup, for any $x \in Z_k(G)$ and any $y \in G$ we have that $[x, y] = x^{-1}x^y \in Z_k(G)$. So $Z_k(G) \lhd Z_{k+1}(G)$. This proves the first assertion.

Now, the second assertion we prove by induction on $m := n - k$. Fix $k \geq 0$. The base step is $m = 0$, which is just $Z_k(G)/Z_k(G) = \{1\} = Z_0(G/Z_k(G))$.

For the induction step, let $m > 0$. Let $H = G/Z_k(G)$ and let $\pi : G \to H$ be the canonical projection. Since $Z_k(G) \lhd Z_{k+m}(G)$, it suffices to prove that $\pi(Z_{k+m}(G)) = Z_m(H)$. Indeed, we have by induction that for $x, y \in G$,

$$[x, y] \in Z_{k+m-1}(G) \iff [\pi(x), \pi(y)] = \pi([x, y]) \in Z_{k+m-1}(G)/Z_k(G) = Z_{m-1}(H),$$

so

$$\begin{aligned}\pi(Z_{k+m}(G)) &= \{\pi(x) : \forall\, y \in G\ [x, y] \in Z_{k+m-1}(G)\} \\ &= \{\pi(x) : \forall\, z \in H\ [\pi(x), z] \in Z_{m-1}(H)\} = Z_m(H),\end{aligned}$$

completing the induction step. :) ✓

Solution to Exercise 1.37 :(

We do this by induction on n. For $n = 0$ this is obvious.

For $n > 0$, assume that $\gamma_n = \{1\}$. Then, $[\gamma_{n-1}, G] = \{1\}$ implies that $\gamma_{n-1} \lhd Z_1$. Let $H = G/Z_1$, and let

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

$\pi : G \to H$ be the canonical projection. It is easy to verify that for all $k \geq 1$, we have

$$\pi(\gamma_k) = [\pi(\gamma_{k-1}), \pi(G)] = [\gamma_{k-1}(H), H] = \gamma_k(H),$$

so $\gamma_{n-1}(H) = \{1\}$. By induction and a previous exercise,

$$G/Z_1 = H = Z_{n-1}(H) = Z_{n-1}(G/Z_1) = Z_n/Z_1.$$

As $Z_1 \lhd Z_n$, this can only happen if $G = Z_n$. :) ✓

Solution to Exercise 1.38 :(
Again this is by induction, where the base step $n = 0$ is obvious.

Assume for $n > 0$ that $Z_n = G$. Set $H = G/Z_1$. Since $Z_{n-1}(H) = Z_n/Z_1 = H$, we have by induction that $\gamma_{n-1}(H) = \{1\}$. As before, if $\pi : G \to H$ is the canonical projection, then $\pi(\gamma_{n-1}) = \gamma_{n-1}(H) = \{1\}$, so $\gamma_{n-1} \lhd Z_1$. Thus,

$$\gamma_n = [\gamma_{n-1}, G] \lhd [Z_1, G] = \{1\}.$$:) ✓

Solution to Exercise 1.39 :(
Let $k \geq 1$. We know that $\gamma_k = \langle [x, y] : x \in \gamma_{k-1},\ y \in G\rangle$. Consider γ_k/γ_{k+1} as a subgroup of G/γ_{k+1}. Note that since $[\gamma_k, G] = \gamma_{k+1}$, we have that $\gamma_k/\gamma_{k+1} \leq Z(G/\gamma_{k+1})$. Thus, for any $x \in \gamma_{k-1}, y, z \in G$ we get that

$$[x, yz] = x^{-1}z^{-1}y^{-1}xyz = [x, z]z^{-1}[x, y]z \equiv [x, z] \cdot [x, y] \pmod{\gamma_{k+1}}.$$

Also, if $x, y \in \gamma_{k-1}$ and $z \in G$ then

$$[xy, z] = y^{-1}x^{-1}z^{-1}xyz = y^{-1}[x, z]z^{-1}yz \equiv [x, z] \cdot [y, z] \pmod{\gamma_{k+1}}.$$

We conclude that if $\gamma_{k-1} = \langle X\rangle$ and $G = \langle S\rangle$ then

$$\gamma_k/\gamma_{k+1} = \langle [\gamma_{k+1}x, \gamma_{k+1}s] : x \in X,\ s \in S\rangle.$$

By induction on k, this proves that as long as G is finitely generated, the group γ_k/γ_{k+1} is finitely generated for all k. :) ✓

Solution to Exercise 1.40 :(
G is n-step nilpotent if and only if $\gamma_n(G) = \{1\}$ and $\gamma_{n-1}(G) \neq \{1\}$, which, by Exercises 1.37 and 1.38, is if and only if $Z_n = G$ and $Z_{n-1} \neq G$.

The second assertion follows from the fact that $Z_{n+1}(G) = Z_n(G/Z_1)$ and $Z_n(G) = Z_{n-1}(G/Z_1)$. :) ✓

Solution to Exercise 1.41 :(
One verifies that $\gamma_k(G/\gamma_n) \leq \gamma_k/\gamma_n$, so $\gamma_n(G/\gamma_n) = \{1\}$. :) ✓

Solution to Exercise 1.42 :(
This follows from $\gamma_n(H) \leq \gamma_n(G)$ for all n, which is easily shown by induction, since for any subgroups $A \leq B \leq G$ and $C \leq D \leq G$ we have $[A, C] \leq [B, D]$. :) ✓

Solution to Exercise 1.43 :(
Let $\pi : G \to G/N$ be the canonical projection. Note that $\gamma_k(G/N) \leq \pi(\gamma_k(G))$. So if $\gamma_n(G) = \{1\} \leq N$, then $\gamma_n(G/N) = \{1\}$. :) ✓

Solution to Exercise 1.44 :(
Let $1 \leq j \leq i + k + \ell - 1 \leq n$. Compute for $M \in D_k, N \in D_\ell$:

$$(MN)_{i,j} = \sum_{t=1}^{n} M_{i,t}N_{t,j}\mathbf{1}_{\{t \geq i+k\}}\mathbf{1}_{\{j \geq t+\ell\}} = 0,$$

because $j - \ell < i + k$. :) ✓

Solution to Exercise 1.45 :(
If $M, N \in D_k(\mathbb{Z})$ then

$$(I + M)(I + N) = I + M + N + MN \in Q_{n,k}$$

because $MN \in D_{2k}(\mathbb{Z}) \subset D_k(\mathbb{Z})$.

Moreover, since D_n contains only the 0 matrix, we have that for any $N \in D_k(\mathbb{Z})$ we may choose $M = \sum_{j=1}^{n-1}(-N)^j \in D_k(\mathbb{Z})$, and we have that

$$(I+N)(I+M) = (I+N) \cdot \sum_{j=0}^{n-1}(-N)^j = I,$$

implying that $(I+N)^{-1} = I+M$ for this choice of M.

This proves that $Q_{n,k}$ is a group. :) ✓

Solution to Exercise 1.46 :(
Let $H = H_n(\mathbb{Z})$. Note that $H = Q_{n,1}$ from the previous exercise, so it is indeed a group.

We now show that for $0 \le k \le n-1$ we have $\gamma_k(H) \subset Q_{n,k+1} \subset Z_{n-k-1}(H)$.

The case $k=0$ is exactly what was shown above. For $k>0$, if $I+M \in H$, $N \in D_k(\mathbb{Z})$ then

$$\begin{aligned}[(I+M),(I+N)] &= (I+M)^{-1}(I+N)^{-1}(I+N+M(I+N)) \\ &= (I+M)^{-1}\left(I+((I+N)^{-1}-I)M(I+N)+M(I+N)\right) \\ &= (I+M)^{-1}((I+M)+L+MN) = I+(I+M)^{-1}(L+MN),\end{aligned}$$

where

$$L = \left((I+N)^{-1}-I\right)M(I+N) = \sum_{j=1}^{n}(-N)^j M(I+N) \in D_{k+1}(\mathbb{Z}).$$

Since $MN \in D_{k+1}(\mathbb{Z})$ as well, we conclude inductively that $\gamma_k(H) \subset Q_{n,k+1}$.

Also, since D_n only contains the 0 matrix, it is immediate that $Q_{n,k+1} \subset Z_{n-k-1}(H)$ holds when $k=n-1$. For $k<n-1$ and $N \in D_{k+1}(\mathbb{Z})$, for any $I+M \in H$, we have seen that $[(I+M),(I+N)] \in Q_{n,k+2} \subset Z_{n-k-2}(H)$ (inductively). Thus, $I+N \in Z_{n-k-1}(H)$ for any $N \in D_{k+1}(\mathbb{Z})$, as required. :) ✓

Solution to Exercise 1.47 :(
This follows since if $H \le G$ then $[G,H] \le [G,G]$.

So for any group G we have that $G^{(n)} \le \gamma_n(G)$, inductively. :) ✓

Solution to Exercise 1.48 :(
If G is 2-step solvable then $\left[G^{(1)},G^{(1)}\right] = G^{(2)} = \{1\}$. :) ✓

Solution to Exercise 1.49 :(
This follows since $\left(G^{(n)}\right)^{(k)} = G^{(n+k)}$. :) ✓

Solution to Exercise 1.50 :(
There exists n such that $G^{(n)} \ne \{1\} = G^{(n+1)}$.

We prove this by induction on n. If $n=0$ then G is infinite Abelian, in which case $[G,G]=\{1\}$.

For $n>0$, let $H = G/G^{(n)}$. We have that $H^{(n)} = \{1\}$, so by induction $[H:[H,H]] = \infty$. Also, $[H,H] = G^{(1)}/G^{(n)}$, so $[G:[G,G]] = [H:[H,H]] = \infty$, completing the induction. :) ✓

Solution to Exercise 1.51 :(
This follows from $H^{(n)} \le G^{(n)}$, which can be easily shown inductively. :) ✓

Solution to Exercise 1.52 :(
For $A,B \in \Delta_n^+$ we have that

$$(AB)_{i,j} = \sum_{\ell=1}^{n} A_{i,\ell}B_{\ell,j} = \mathbf{1}_{\{i=j\}}A_{i,i}B_{i,i}.$$

This immediately shows that $AB = BA$.

Also, since $A_{i,i} > 0$ for all i, we can choose $B_{i,i} = \frac{1}{A_{i,i}}$, to get $AB = I$, so $B = A^{-1}$. :) ✓

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Solution to Exercise 1.53 :(

For $T+M, S+N \in P_{n,k}$ we have $(T+M)(S+N) = TS+TN+MS+MN$. Since $TN, MS, MN \in D_k$ we get that $P_{n,k}$ is closed under matrix multiplication.

Choosing $M = \sum_{j=1}^{n} \left(-S^{-1}N\right)^j \cdot S^{-1}$ and $T = S^{-1}$ will give us that

$$(T+M)(S+N) = I + S^{-1}N + M\left(I + S^{-1}N\right) = I,$$

so $(S+N)^{-1} = S^{-1} + M$ for this choice of M.

Now consider the map $\varphi\colon P_{n,k} \to \Delta_n^+$ given by $\varphi(T+M) = T$. One easily check that this is a surjective homomorphism, and that $\mathsf{Ker}\varphi = \{I+N : N \in D_k\}$. Since Δ_n^+ is an Abelian group, it must be that $[P_{n,k}, P_{n,k}] \lhd \mathsf{Ker}\varphi$.

As in Exercise 1.46, we compute commutators: for any $M \in D_\ell$, $N \in D_k$ we have $[(I+M),(I+N)] = I + (I+M)^{-1}(L+MN)$, where

$$L = \sum_{j=1}^{n} (-N)^j M(I+N) \in D_{\ell+k}$$

and also $MN \in D_{\ell+k}$ (by Exercise 1.44).

This implies inductively that

$$(P_{n,k})^{(\ell+1)} = ([P_{n,k}, P_{n,k}])^{(\ell)} \lhd \{I+N : N \in D_{2^\ell k}\}$$

for all $\ell \geq 0$. Since D_n contains only the 0 matrix, $P_{n,k}$ is solvable of step at most $\lceil \log_2(n/k) \rceil + 1$.

Finally, to show that $P_{n,k}$ is not nilpotent, we will show that $Z_1(P_{n,k}) = \{1\}$, which implies that $Z_\ell(P_{n,k}) = \{1\}$ for all $\ell \geq 0$. Indeed,

$$(T+M)(S+N) - (S+N)(T+M) = TN - NT + MS - SM + MN - NM.$$

If $S+N \in Z_1(P_{n,k})$, then by choosing $M \in D_{n-1}$, we have that $NM = MN = 0$. Also, an easy computation gives

$$MS - SM = (S_{n,n} - S_{1,1}) \cdot M.$$

Also, there exist t, s such that $N_{t,s} \neq 0$. Necessarily $s > t$. We choose $M_{i,j} = \mathbf{1}_{\{i=j=n\}}$ and $T_{i,j} = \alpha \cdot \mathbf{1}_{\{i=j=t\}}$ for some $\alpha > 0$. Then

$$(TN - NT)_{i,j} = \alpha\left(\mathbf{1}_{\{i=t\}} - \mathbf{1}_{\{j=t\}}\right) N_{i,j}.$$

Hence

$$((T+M)(S+N) - (S+N)(T+M))_{t,s} = \alpha N_{t,s} + S_{n,n} - S_{1,1}.$$

Since we can choose $\alpha > 0$ such that this is nonzero, we find that $S+N$ does not commute with $T+M$ in this case. :) ✓

Solution to Exercise 1.54 :(

It is easy to compute that

$$\begin{bmatrix} \omega^z & d \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \omega^w & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \omega^{z+w} & \omega^z c + d \\ 0 & 1 \end{bmatrix},$$

so that $\begin{bmatrix} \omega^z & d \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \omega^{-z} & -\omega^{-z} d \\ 0 & 1 \end{bmatrix}$ showing that G is a group.

For $d = \sum_{k=0}^{r-1} a_k \omega^k$ where $a_0, \ldots, a_{r-1} \in \mathbb{Z}$, and $z \in \mathbb{Z}$, we have that

$$\begin{bmatrix} \omega^z & d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \cdot \left(\begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix}\right)^z = \prod_{k=0}^{r-1} \begin{bmatrix} 1 & a_k \omega^k \\ 0 & 1 \end{bmatrix} \cdot \left(\begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix}\right)^z = \prod_{k=0}^{r-1} \left(\begin{bmatrix} 1 & \omega^k \\ 0 & 1 \end{bmatrix}\right)^{a_k} \cdot \left(\begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix}\right)^z,$$

implying that G is generated by the finite set

$$G = \left\langle \begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \omega^k \\ 0 & 1 \end{bmatrix} : 0 \leq k \leq r-1 \right\rangle.$$

Computing commutators we see that

$$\left[\begin{bmatrix} \omega^z & d \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \omega^w & c \\ 0 & 1 \end{bmatrix}\right] = \begin{bmatrix} \omega^{-z-w} & -\omega-z-wc-\omega^{-z}d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \omega^{z+w} & \omega^z c+d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \omega^{-z-w}((\omega^z-1)c-(\omega^w-1)d) \\ 0 & 1 \end{bmatrix}.$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

As above, this shows that G is 2-step solvable, but not nilpotent, since $Z_1(G) = \{1\}$.

However, consider the map $\varphi \colon G \to \{0, 1, \ldots, r-1\}$ given by $\varphi\left(\left[\begin{smallmatrix} \omega^z & d \\ 0 & 1 \end{smallmatrix}\right]\right) = z \pmod{r}$. This is easily seen to be a well-defined surjective homomorphism, so $[G : \mathsf{Ker}\varphi] = r$. Moreover, $\left[\begin{smallmatrix} \omega^z & d \\ 0 & 1 \end{smallmatrix}\right] \in \mathsf{Ker}\varphi$ if and only if $z = 0 \pmod{r}$. Thus

$$\mathsf{Ker}\varphi = \left\{\left[\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right] : d \in D\right\},$$

which is an Abelian group of finite index in G. :) ✓

Solution to Exercise 1.55 :(

Let $S = \{a, b\}$. Define $\varphi \colon \mathbb{F}_S \to H$ by $\varphi(a) = a$ and $\varphi(b) = b$ and extending in the canonical way to words in $\mathbb{F}_S$. This is a surjective homomorphism, and we want to show that it is injective as well.

Step I. Let $h = a^{z_1} b^{w_1} \cdots a^{z_n}$ be an element in H such that $z_n, z_k, w_k \in \mathbb{Z} \setminus \{0\}$ for all $1 \le k \le n-1$. For any $x \in B$,

$$h.x = a^{z_1} b^{w_1} \cdots a^{z_n}.x \in a^{z_1} b^{w_1} \cdots a^{z_{n-1}} b^{z_{n-1}}(A) \subset A,$$

so it is impossible that $h.x = x$, implying that $h \neq 1$.

Step II. Now, for a general element $h = a^{z_1} b^{w_1} \cdots a^{z_n} b^{w_n}$, where $w_1, z_n, z_k, w_k \in \mathbb{Z} \setminus \{0\}$ for $2 \le k \le n-1$, but possibly $z_1 = 0$ or $w_n = 0$. In this case we can define:

$$g = \begin{cases} a^{-z_n} h a^{z_n} & \text{if } z_1 = w_n = 0, \\ a^{-1} h a & \text{if } z_1 = 0 \neq w_n, \\ h & \text{if } z_1 \neq 0 = w_n. \end{cases}$$

We see that in each of the above cases, the element g falls into the conditions of Step I. So $g \neq 1$. Since every time g is a conjugate of h, also $h \neq 1$. :) ✓

Solution to Exercise 1.56 :(

$\mathsf{SL}_2(\mathbb{Z})$ acts on $\mathbb{Z}^2$. Let $A = \left\{(x, y) \in \mathbb{Z}^2 : |y| < |x|\right\}$ and $B = \left\{(x, y) \in \mathbb{Z}^2 : |x| < |y|\right\}$.

Note that $a^z = \left[\begin{smallmatrix} 1 & 2z \\ 0 & 1 \end{smallmatrix}\right]$ and $b^z = \left[\begin{smallmatrix} 1 & 0 \\ 2z & 1 \end{smallmatrix}\right]$ for any $z \in \mathbb{Z}$.

We have that $a^z(x, y) = (x + 2zy, y)$. So if $(x, y) \in B$, since $|y| > |x|$ we get that

$$|x + 2zy| \ge 2|z||y| - |x| > (2|z| - 1)|y| \ge |y|$$

if $z \neq 0$. So $a^z(x, y) \in A$ for all $z \neq 0$ and $(x, y) \in B$.

Similarly, if $(x, y) \in A$ then

$$|2zx + y| \ge 2|z||x| - |y| > (2|z| - 1)|x| \ge |x|,$$

so $b^z(x, y) \in B$ for all $z \neq 0$ and $(x, y) \in A$.

This implies that $\langle a, b \rangle$ is isomorphic to $\mathbb{F}_2$ by the Ping-Pong Lemma. :) ✓

Solution to Exercise 1.59 :(

It was shown in Exercise 1.58 that $a = x^2 = (-st)^2 = stst$ and $b = y^2 = (-s^2t)^2 = s^2ts^2t$.

Now, let $z \in \mathsf{SL}_2(\mathbb{Z})$. By Exercise 1.58, there exist $n \ge 0$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ and $\alpha, \beta \in \{0, 1\}$ such that $z \equiv t^\alpha s^{\varepsilon_1} t s^{\varepsilon_2} \cdots t s^{\varepsilon_n} t^\beta \pmod{\{-I, I\}}$. Choose a minimal $n = n(z)$ as above. We prove the assertion that there exist $w \in S$ and $p \in \left\{1, s, s^2, t, ts, ts^2\right\}$ such that $z \equiv wp \pmod{\{-I, I\}}$ by induction on n.

The base case is $n(z) = 0$, for which $z \equiv t^{\alpha+\beta} \pmod{\{-I, I\}}$ for some $\alpha, \beta \in \{0, 1\}$. In all cases one sees that the assertion holds with $w = 1$ and $p \in \{1, t\}$.

For the induction step, we have that $z \equiv t^\alpha s^{\varepsilon_1} t s^{\varepsilon_2} \cdots t s^{\varepsilon_n} t^\beta \pmod{\{-I, I\}}$ and $n \ge 1$. Set $\tilde{z} = t^\alpha s^{\varepsilon_1} t s^{\varepsilon_2} \cdots s^{\varepsilon_{n-1}} t$. By induction, there exist $\tilde{w} \in S$ and $\tilde{p} \in \left\{1, s, s^2, t, st, s^2t\right\}$ such that $\tilde{z} \equiv \tilde{w}\tilde{p} \pmod{\{-I, I\}}$. Note that modulo $\{-I, I\}$,

$$\tilde{p}s^{-1}t \equiv \begin{cases} s^{-1}t \equiv s^2t & \tilde{p} = 1, \\ t & \tilde{p} = s, \\ st & \tilde{p} = s^2, \\ ts^{-1}t \equiv a^{-1}s & \tilde{p} = t, \\ sts^{-1}t \equiv ab^{-1}s^2 & \tilde{p} = st, \\ s^2ts^{-1}t \equiv b & \tilde{p} = s^2t, \end{cases} \qquad \tilde{p}st \equiv \begin{cases} st & \tilde{p} = 1, \\ s^2t & \tilde{p} = s, \\ t & \tilde{p} = s^2, \\ tst \equiv b^{-1}s^2 & \tilde{p} = t, \\ stst = a & \tilde{p} = st, \\ s^2tst \equiv ba^{-1}s & \tilde{p} = s^2t, \end{cases}$$

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

which completes the induction step.

This immediately shows that the number of cosets of $\pi(S)$ is at most 6, that is, $[\mathsf{PSL}_2(\mathbb{Z}) : \pi(S)] \leq 6$.

Finally, we also have that for any $z \in \mathsf{SL}_2(\mathbb{Z})$ there exist $w \in S$ and $p \in \left\{1, s, s^2, t, st, s^2t\right\}$ such that $\pi(z) = \pi(wp)$. This implies that for some $\varepsilon \in \{-1, 1\}$ we have that $z = \varepsilon wp$. Hence, there are at most 12 cosets for S in $\mathsf{SL}_2(\mathbb{Z})$; that is, $[\mathsf{SL}_2(\mathbb{Z}) : S] \leq 12$. :) ✓

Solution to Exercise 1.60 :(
For every $x \in G$ there are unique elements $y_x \in H$ and $t_x \in T$ such that $x = y_x t_x$. For any $u \in T$ and $s \in S$ one has that $us(t_{us})^{-1} = y_{us} \in TST^{-1} \cap H$.

We will show that $\{y_{us} : u \in T,\ s \in S\}$ generate H. To this end, fix some $x \in G$ and write $x = s_1 \cdots s_n$ for $s_j \in S$. Define inductively $u_1 = s_1$ and $u_{k+1} = t_{u_k} s_{k+1}$. Then,

$$x = y_{s_1} t_{s_1} s_2 \cdots s_n = y_{u_1} y_{u_2} t_{u_2} s_3 \cdots s_n = \cdots = y_{u_1} y_{u_2} \cdots y_{u_n} t_{u_n}.$$

Note that $u_j \in TS$ so $y_{u_j} \in TST^{-1} \cap H$. Specifically, if $x \in H$ then it must be that $t_{u_n} = 1$ and $x = y_{u_1} \cdots y_{u_n}$. :) ✓

Solution to Exercise 1.62 :(
For any $x \in G$, we can write $\pi(x) = \pi(s_1) \cdots \pi(s_n)$ for some $s_j \in S$. Thus, there exists $h \in H$ such that $x = hs_1 \cdots s_n$. Writing $h = u_1 \cdots u_m$ for $u_i \in U$, we have that $U \cup S$ generates G. :) ✓

Solution to Exercise 1.63 :(
Let $G = \{g_1, \ldots, g_n\}$. Let $\mathbb{F} = \mathbb{F}_n$ be the free group on n generators, and denote the generators by $\{s_1, \ldots, s_n\}$. Consider the homomorphism $\varphi \colon \mathbb{F} \to G$ defined by setting $\varphi(s_j) = g_j$.

For every $1 \leq i, j \leq n$ there exists $1 \leq k = k(i,j) \leq n$ such that $g_i g_j = g_k$. Define the relation $r_{i,j} = s_i s_j (s_k)^{-1}$ for $k = k(i,j)$.

Let $K = \mathsf{Ker}\varphi$ and let $R \lhd \mathbb{F}$ be the smallest normal subgroup containing $\{r_{i,j} : 1 \leq i, j \leq n\}$. Note that $R \lhd K$.

Let $\pi \colon \mathbb{F}/R \to G$ be the homomorphism defined by $\pi(Rx) = \varphi(x)$. This is well defined because $R \lhd K$. So $\mathbb{F}/R$ and K/R are finite groups. Since $(\mathbb{F}/R)/(K/R) \cong \mathbb{F}/K \cong G$, we have that $|G| \leq \frac{|G|}{|K/R|}$, which can only mean that $K = R$. Hence $G = \left\langle s_1, \ldots, s_n \mid r_{i,j}\ 1 \leq i, j \leq n \right\rangle$ is a finitely presented group. :) ✓

Solution to Exercise 1.64 :(
$\mathbb{Z}$ is finitely presented, as it is just the free group on 1 generator. Since G/H is finite, it is also finitely presented. Thus, G is finitely presented by Lemma 1.5.14. :) ✓

Solution to Exercise 1.65 :(
This follows directly from Theorem 1.5.15 and the fact that virtually-$\mathbb{Z}$ groups are finitely presented. :) ✓

Solution to Exercise 1.66 :(
If $e_1, \ldots e_d$ are the standard basis vectors spanning $\mathbb{Z}^d$, then defining $H_k = \langle e_1, \ldots, e_{d-k} \rangle$ for $0 \leq k < d$, and $H_d = \{1\}$, we have that $H_{k+1} \lhd H_k$ and $H_k/H_{k+1} \cong \mathbb{Z}$ for all $0 \leq k < d$. Thus $\mathbb{Z}^d$ is finitely presented by Theorem 1.5.15.

If G is a finitely generated virtually Abelian group, then $G \cong \mathbb{Z}^d \times F$ for some d and some finite group F (by Theorem 1.5.2). Thus, there exists a normal subgroup $N \lhd G$ such that $N \cong \mathbb{Z}^d$ and $G/N \cong F$. Since both N and F are finitely presented, so is G by Lemma 1.5.14. :) ✓

Solution to Exercise 1.67 :(
Assume that G is n-step nilpotent. We prove the claim by induction on n.

If $n = 1$ then G is Abelian, and since it was assumed to be finitely generated, G is finitely presented, completing the induction base.

For $n > 1$, consider the lower central series $G = \gamma_0 \rhd \gamma_1 \rhd \cdots \rhd \gamma_n = \{1\}$. Consider the group $H = \gamma_{n-1}$. Since $[G, H] = \{1\}$, we have that H is Abelian. By Exercise 1.39, $H \cong \gamma_{n-1}/\gamma_n$ is finitely generated. Thus, H is finitely presented. Also, G/H is at most $(n-1)$-step nilpotent and finitely generated, so G/H is finitely presented by induction. Thus, G is also finitely presented, completing the induction step. :) ✓

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

Solution to Exercise 1.68 :(
Multiplication is associative since

$$((g,h)(g',h'))(g'',h'') = (gg', hg(h'))(g'',h'') = (gg'g'', hg(h')gg'(h'')),$$
$$(g,h)((g',h')(g'',h'')) = (g,h)(g'g'', h'g'(h'')) = (gg'g'', hg(h')gg'(h'')).$$

The identity is easily seen to be $(1_G, 1_H)$. Inverses are given by $(g,h)^{-1} = \left(g^{-1}, g^{-1}(h^{-1})\right)$.

The map $(g,h) \mapsto g$ is a homomorphism onto G with kernel $\{(1,h) \mid h \in H\}$, which is isomorphic to H. :) ✓

Solution to Exercise 1.70 :(
Since $TM \in D_k$ for all $T \in \Delta_n^+$ and $M \in D_k$, it is obvious that Δ_n^+ acts on the set D_k. Also, $T(M+N) = TM + TN$ so this action is indeed a group automorphism (recall that D_k has an additive operation).

For $T \in \Delta_n^+$, $M \in D_k$ define a $2n \times 2n$ matrix by $\Psi(T,M) = \left[\begin{smallmatrix} T & M \\ 0 & I \end{smallmatrix}\right]$. Multiplying two such matrices by blocks gives $\Psi(T,M)\Psi(S,N) = \Psi(TS, TN+M)$. This immediately leads to the conclusion that $\Delta_n^+ \ltimes D_k \cong G := \{\Psi(T,M) : T \in \Delta_n^+,\ M \in D_k\}$.

Now, since $\Psi(T,M)^{-1} = \Psi\left(T^{-1}, -T^{-1}M\right)$, we have that

$$\begin{aligned}[\Psi(T,M), \Psi(S,N)] &= \Psi\left(T^{-1}S^{-1}, -T^{-1}S^{-1}N - T^{-1}M\right)\Psi(TS, TN+M) \\ &= \Psi\left(I, T^{-1}S^{-1}(TN+M) - T^{-1}S^{-1}N - T^{-1}M\right) \\ &= \Psi\left(I, (I-T^{-1})S^{-1}N - (I-S^{-1})T^{-1}M\right).\end{aligned}$$

Thus, $G^{(1)} \subset \{\Psi(I,M) : M \in D_k\}$. However, computing the commutator again (when $S = T = I$) we get that $G^{(2)} = \{I\}$, so G is 2-step solvable.

If $k \geq n$ then D_k is just the 0 matrix, so $\Delta_n^+ \ltimes D_k \cong \Delta_n^+$, which is Abelian.

To show that G is not nilpotent when $k < n$, we first compute the center $Z = Z_1(G)$. If $\Psi(S,N) \in Z$, then the commutator computation above implies that $(T-I)N = (S-I)M$ for all $T \in \Delta_n^+$, $M \in D_k$. Choosing $T = I$ and $M_{i,j} = \mathbf{1}_{\{j \geq i+k\}}$, we get that $S_{j,j} = 1$ for all $j \leq n-k$. Thus, $(S-I)M = 0$ for any $M \in D_k$. This leads to $(T-I)N = 0$ for all $T \in \Delta_n^+$, which cannot hold unless $N = 0$. We conclude that

$$Z = \{\Psi(S,0) : \forall\, j \leq n-k\,,\ S_{j,j} = 1\}.$$

Now, we compute the second center $Z_2 = Z_2(G) = \{x \in G : \forall\, y \in G\ [x,y] \in Z_1(G)\}$. Using the commutator formula above, we see that if $\Psi(S,N) \in Z_2$, then again $(T-I)N = (S-I)M$ for all $T \in \Delta_n^+$, $M \in D_k$, which leads to $N = 0$ and $S_{j,j} = 1$ for all $j \leq n-k$, as before. But then we get that $Z_2 = Z$, so the upper-central series stabilizes at Z, and G cannot be nilpotent. :) ✓

Solution to Exercise 1.71 :(
For $\alpha \neq 0$ and $u \in V$, denote the transformation $v \mapsto \alpha v + u$ by the "matrix" $\left[\begin{smallmatrix} \alpha & u \\ 0 & 1 \end{smallmatrix}\right]$. (If V is finite dimensional, then this is an actual $(\dim V + 1) \times (\dim V + 1)$ matrix.)

One sees that the usual matrix multiplication provides us with composition of transformations:

$$\left[\begin{smallmatrix} \alpha & u \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} \beta & v \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} \alpha\beta & \alpha v + u \\ 0 & 1 \end{smallmatrix}\right].$$

The inverse transformation is given by

$$\left[\begin{smallmatrix} \alpha & u \\ 0 & 1 \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} \alpha^{-1} & -\alpha^{-1}u \\ 0 & 1 \end{smallmatrix}\right].$$

This provides the group structure for the affine transformations of V.

In fact, note that the multiplicative group $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ acts on the additive group V, so the collection of affine transformations is just $\mathbb{C}^* \ltimes V$.

It is now straightforward to compute commutators:

$$\left[\left[\begin{smallmatrix} \alpha & u \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} \beta & v \\ 0 & 1 \end{smallmatrix}\right]\right] = \left[\begin{smallmatrix} \alpha^{-1}\beta^{-1} & -\alpha^{-1}\beta^{-1}v - \alpha^{-1}u \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} \alpha\beta & \alpha v + u \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & \alpha^{-1}\beta^{-1}((\alpha-1)v - (\beta-1)u) \\ 0 & 1 \end{smallmatrix}\right].$$

Just as before, one sees that $\mathbb{C}^* \ltimes V$ is 2-step solvable, if $V \neq \{0\}$.

Also, if $\left[\begin{smallmatrix} \alpha & u \\ 0 & 1 \end{smallmatrix}\right] \in Z = Z_1(\mathbb{C}^* \ltimes V)$, then $(\alpha - 1)v = (\beta - 1)u$ for all $\beta \in \mathbb{C}^*$, $v \in V$. If $V \neq \{0\}$, this is only possible if $u = 0$ and $\alpha = 1$. Hence $Z = \{1\}$. That is, the only case where $\mathbb{C}^* \ltimes V$ is nilpotent is when $V = \{0\}$ and $\mathbb{C}^* \ltimes V \cong \mathbb{C}^*$, which is Abelian. :) ✓

Solution to Exercise 1.72 :(
First, note that the collection $\{a^x b^\eta : \eta \in \{0, 1\},\ x \in \mathbb{Z}\}$ forms a subgroup of D_∞. Since the generators a, b of D_∞ are contained in this subgroup, we get that any element of D_∞ is of the form $a^x b^\eta$ for some $\eta \in \{0, 1\}$ and $x \in \mathbb{Z}$.

It is not difficult to verify that the map $(\varepsilon, x) \mapsto a^x b^{(1+\varepsilon)/2}$ is a surjective homomorphism with trivial kernel.

Now,

$$\begin{aligned}
[(\varepsilon, x), (\delta, y)] &= (\varepsilon, -\varepsilon x)(\delta, -\delta y)(\varepsilon, x)(\delta, y) \\
&= (\varepsilon\delta, -\varepsilon x - \varepsilon\delta y)(\varepsilon\delta, x + \varepsilon y) \\
&= \left(\varepsilon^2\delta^2, -\varepsilon x - \varepsilon\delta y + \varepsilon\delta x + \varepsilon^2\delta y\right) \\
&= (1, \varepsilon(\delta - 1)x + \delta(1 - \varepsilon)y).
\end{aligned}$$

Thus $[(1, x), (-1, 0)] = (1, -2x)$ and $[(-1, x), (1, 1)] = (1, 2)$. Hence $Z(\mathbb{Z}_2 \ltimes \mathbb{Z}) = \{(1, 0)\}$, so $D_\infty \cong \mathbb{Z}_2 \ltimes \mathbb{Z}$ is not nilpotent.

Also, the above commutator calculation shows that $[(1, x), (1, y)] = (1, 0)$, so $D_\infty \cong \mathbb{Z}_2 \ltimes \mathbb{Z}$ is 2-step solvable.

Finally, the surjective homomorphism $(\varepsilon, x) \mapsto \varepsilon$ shows that $H = \{(1, x) : x \in \mathbb{Z}\}$ is a normal subgroup of $\mathbb{Z}_2 \ltimes \mathbb{Z}$ isomorphic to $\mathbb{Z}$, and of index 2 because $\mathbb{Z}_2 \ltimes \mathbb{Z}/H \cong \mathbb{Z}_2$. :) ✓

Solution to Exercise 1.73 :(
The group structure is easy to verify. The identity in G is $1_G = (1_{S_d}, 0)$ and $(\sigma, z)^{-1} = \left(\sigma^{-1}, -\sigma^{-1}z\right)$.

Now, note that

$$(\sigma, z)^{(\tau,w)} = \left(\tau^{-1}, -\tau^{-1}w\right)(\sigma\tau, z + \sigma w) = \left(\sigma^\tau, \tau^{-1}z + \sigma^\tau\tau^{-1}w - \tau^{-1}w\right).$$

Let $H = \{(1_{S_d}, z) \colon z \in \mathbb{Z}^d\}$. Then it is immediate that $H \cong \mathbb{Z}^d$ and from the above, $\left(1_{S_d}, z\right)^{(\tau,w)} = \left(1_{S_d}, \tau^{-1}z\right)$, so $H \lhd G$. Also, the map $\pi \colon G \to S_d$ given by $(\sigma, z) \mapsto \sigma$ is a homomorphism with kernel H. So $G/H \cong S_d$.

Finally,

$$[(\sigma, z), (\tau, w)] = \left(\sigma^{-1}, -\sigma^{-1}z\right)\left(\sigma^\tau, \tau^{-1}z + \sigma^\tau\tau^{-1}w - \tau^{-1}w\right) = \left([\sigma, \tau], -\sigma^{-1}z + \tau^\sigma w - \sigma^{-1}\tau^{-1}w\right).$$

Since S_d is non-Abelian (for $d > 2$) we may find $\sigma, \tau \in S_d$ such that $[\sigma, \tau] \neq 1_{S_d}$. :) ✓

Solution to Exercise 1.75 :(
It suffices to show only one inequality, as the other will follow by reversing the roles of S, T.

For any $t \in T$ let $s_{t,1}, \ldots, s_{t,n(t)} \in S$ be such that $s_{t,1} \cdots s_{t,n(t)} = t$ and $n(t) = |t|_S = \mathrm{dist}_S(1, t)$. Let $\kappa = \max_{t \in T} n(t)$.

Now, for any $x \in G$ let $t_1, \ldots, t_m \in T$ be such that $t_1 \cdots t_m = x$ and $m = |x|_T = \mathrm{dist}_T(1, x)$. Then,

$$x = t_1 \cdots t_m = s_{t_1,1} \cdots s_{t_1,n(t_1)} \cdot s_{t_2,1} \cdots s_{t_2,n(t_2)} \cdots s_{t_m,1} \cdots s_{t_m,n(t_m)},$$

so

$$|x|_S \leq \sum_{j=1}^{m} \sum_{k=1}^{n(t_j)} |s_{t_j,k}| \leq \kappa \cdot m = \kappa \cdot |x|_T.$$

Hence, for general $x, y \in G$ we have that

$$\mathrm{dist}_S(x, y) = \left|x^{-1}y\right|_S \leq \kappa \cdot \left|x^{-1}y\right|_T = \mathrm{dist}_T(x, y). \qquad \text{:) ✓}$$

Solution to Exercise 1.80 :(
Symmetry and adaptedness of ν follow from the previous exercises. Let U be a random element of law μ, and let $V = U$ with probability $1 - p$, and $V = 1$ with probability p. Then,

$$\mathbb{E}\left[|V|^k\right] = (1 - p)\,\mathbb{E}\left[|U|^k\right] < \infty,$$

implying that $\nu \in \mathsf{SA}(G, k)$. :) ✓

Solution to Exercise 1.87 :(
Compute using the symmetry of P:

$$\begin{aligned}2\langle \Delta f, g\rangle &= 2\sum_x \Delta f(x)\bar{g}(x) = 2\sum_x\sum_y P(x,y)(f(x)-f(y))\bar{g}(x)\\ &= \sum_{x,y} P(x,y)(f(x)-f(y))\bar{g}(x) + \sum_{y,x} P(y,x)(f(y)-f(x))\bar{g}(y)\\ &= \sum_{x,y} P(x,y)(f(x)-f(y))(\bar{g}(x)-\bar{g}(y)).\end{aligned}$$

We have used that $f, g \in \ell^2$, so that the above sums converge absolutely, and so can be summed together.

Thus, if f is ℓ^2 and harmonic we have that

$$\sum_{x,y} P(x,y)|f(x)-f(y)|^2 = 2\langle \Delta f, f\rangle = 0.$$

Thus, $|f(x)-f(y)|^2 = 0$ for all x, y such that $P(x,y) > 0$. Since P is irreducible (i.e. μ is adapted) this implies that f is constant. :) ✓

Solution to Exercise 1.88 :(
Note that any linear map $z \mapsto \alpha z + \beta$ is still harmonic with respect to this μ.

The dimension is at most 4 since the linear map $f \mapsto (f(-1), f(0), f(1), f(2))$ from the space $\mathsf{HF}(\mathbb{Z}, \mu)$ to $\mathbb{C}^4$ is injective (it has a trivial kernel). Indeed, for any μ-harmonic function f, and any z we have that

$$\begin{aligned}f(z+2) &= 4f(z) - f(z-1) - f(z+1) - f(z-2),\\ f(z-2) &= 4f(z) - f(z-1) - f(z+1) - f(z+2).\end{aligned}$$

So if $f(z-1) = f(z) = f(z+1) = f(z+2) = 0$ for any z then $f \equiv 0$ is identically 0. :) ✓

Solution to Exercise 1.89 :(
It is easy to verify μ-harmonicity.

As for ν, one may check that f, h are ν-harmonic. Also,

$$\begin{aligned}g * \check{\nu}(x,y) &= \tfrac{1}{6}\big((x+1)^2 - y^2 + (x-1)^2 - y^2 + x^2 - (y+1)^2 + x^2 - (y-1)^2\\ &\qquad + (x+1)^2 - (y+1)^2 + (x-1)^2 - (y-1)^2\big)\\ &= x^2 - y^2 + \tfrac{1}{6}(2 - 2 + 1 + 2x - 1 - 2y + 1 - 2x - 1 + 2y) = x^2 - y^2 = g(x,y),\\ k * \check{\nu}(x,y) &= \tfrac{1}{6}\big((x+1)y + (x-1)y + x(y+1) + x(y-1) + (x+1)(y+1) + (x-1)(y-1)\big)\\ &= xy + \tfrac{1}{6}(y - y + x - x + x + y + 1 - x - y + 1) = xy + \tfrac{1}{3},\end{aligned}$$

so g is ν-harmonic, but k is not ν-harmonic. :) ✓

Solution to Exercise 1.90 :(
Let $\varphi \colon G \to \mathbb{C}$ be a homomorphism. Then, using the symmetry of μ,

$$\sum_y \mu(y)\varphi(xy) = \varphi(x) + \sum_y \mu(y)\tfrac{1}{2}\left(\varphi(y) + \varphi(y^{-1})\right) = \varphi(x).$$

The above sum converges absolutely because μ has finite first moment, and since $|\varphi(xy)| \leq |\varphi(x)| + |\varphi(y)| \leq \max_{s\in S} |\varphi(s)| \cdot (|x| + |y|)$, where S is the finite symmetric generating set used to determine the metric on G. :) ✓

Solution to Exercise 1.91 :(
For any $x \in G$,

$$\sum_y \nu(y)f(xy) = pf(x) + (1-p)\sum_x \mu(y)f(xy),$$

where the sums on both sides converge absolutely together. :) ✓

Solution to Exercise 1.97 :(
The fact that L is compact is basically the Arzelà–Ascoli theorem. However, let us give a self-contained proof.

The space L with the topology of pointwise convergence is metrizable; for example, one may consider the metric

$$\mathrm{dist}(f,h) = \exp(-R(h,f)), \qquad R(h,f) := \sup\{r \geq 0 : \forall\ |x| \leq r\ ,\ h(x) = f(x)\}.$$

So compactness will follow by showing that any sequence has a converging subsequence.

Let $(f_n)_n$ be a sequence in L. Denote $G = \{x_1, x_2, \ldots\}$.

We will inductively construct a sequence of subsets $\mathbb{N} \supset I_1 \supset I_2 \supset I_3 \supset \cdots$, all infinite $|I_j| = \infty$, such that for all $m \geq 1$ the limits $\lim_{I_j \ni k \to \infty} f_k(x_j)$ exist.

Indeed, if $m = 1$ then since $|f_n(x)| \leq |x|$ for all n, the sequence $(f_n(x_1))_n$ is bounded, and thus has a converging subsequence. Let I_1 be the indices of this converging subsequence.

For $m > 1$, given I_{m-1}, we consider $(f_k(x_m))_{k \in I_{m-1}}$. Since this sequence is bounded, it too has a converging subsequence, and we denote by $I_m \subset I_{m-1}$ the indices of this new subsequence.

With this construction, we now write $I_m = (n_k^{(m)})_k$, for each $m \geq 1$. Consider the sequence $h_k = f_{n_k^{(k)}}$.

For any $m \geq 1$, the sequence $(h_k)_{k \geq m}$ is a subsequence of $(f_k)_{k \in I_m}$. Thus, $h(x_m) := \lim_{k\to\infty} h_k(x_m)$ exists.

This shows that $(h_k)_k$ converges pointwise to h, proving that L is compact.

The fact that $x.h(y) = h\left(x^{-1}y\right) - h\left(x^{-1}\right)$ is a left action is easily shown.

Also, if $x.h = h$ for all $x \in G$, then $h(xy) = x^{-1}.h(y) + h(x) = h(y) + h(x)$ for all $x, y \in G$.

If $h \colon G \to \mathbb{C}$ is a homomorphism, then choose $\alpha = \frac{1}{\max_{s\in S}|h(s)|}$. Then

$$||\nabla_S h||_\infty = \sup_{s\in S}\sup_{x\in G}|h(xs) - h(x)| = \max_{s\in S}|h(s)|,$$

so that $||\nabla_S \alpha h||_\infty = 1$. Hence, $\alpha h \in L$.

Now for the functions b_x. Note that

$$z.b_x(y) = b_x\left(z^{-1}y\right) - b_x\left(z^{-1}\right) = \left|x^{-1}z^{-1}y\right| - \left|x^{-1}z^{-1}\right| = b_{zx}(y).$$

By the triangle inequality, $|b_x(y)| \leq |y|$. So,

$$|b_x(ys) - b_x(y)| = \left|y^{-1}.b_x(s)\right| = |b_{y^{-1}x}(s)| \leq |s|,$$

which implies that $||\nabla_S b_x||_\infty \leq 1$.

Finally, if $b_x = b_y$, then

$$\mathrm{dist}_S(x,y) = b_x(y) + |x| = b_y(y) + |x| = |x| - |y|.$$

Reversing the roles of x, y we have that $\mathrm{dist}_S(x,y) = -\mathrm{dist}_S(x,y)$, implying that $\mathrm{dist}_S(x,y) = 0$, so that $x = y$. :) ✓

Solution to Exercise 1.98 :(
The fact that $||\cdot||_{S,k}$ is a semi-norm is easy to verify.

For $f \colon G \to \mathbb{C}$ and $x \in G$ note that

$$||x.f||_{S,k} = \limsup_{r\to\infty} r^{-k} \sup_{|y|\leq r}\left|f\left(x^{-1}y\right)\right| \leq \limsup_{r\to\infty}(r + |x|)^{-k} \sup_{|z|\leq r+|x|}|f(z)| \cdot \left(\tfrac{r+|x|}{r}\right)^k = ||f||_{S,k}.$$

Repeating this for x^{-1}, we have that $||x.f||_{S,k} \leq ||f||_{S,k} = \left\|x^{-1}.x.f\right\|_{S,k} \leq ||x.f||_{S,k}$, which implies equality.

It is now immediate that $\mathsf{HF}_k(G,\mu)$ is a G-invariant vector space. :) ✓

Solution to Exercise 1.99 :(
We know that there exists $\kappa > 0$ such that $|x|_T \leq \kappa|x|_S$ for all $x \in G$. Hence,

$$||f||_{S,k} = \limsup_{r\to\infty} r^{-k} \sup_{|x|_S\leq r}|f(x)| \leq \limsup_{r\to\infty} r^{-k} \sup_{|x|_T\leq \kappa r}|f(x)| \leq \kappa^k ||f||_{T,k}.$$:) ✓

Solution to Exercise 1.102 :(
This is similar to the proof of Proposition 1.5.1.

Let $M \in \mathsf{GL}_n(R)$. Let us recall the *cofactor matrix* $c(M)$ and the *adjugate matrix* $\mathsf{adj}(M)$ given as follows: For every $1 \leq i, j \leq n$ let $M^{i,j}$ be the $(n-1) \times (n-1)$ matrix obtained from M by deleting the ith row and jth column. Define $c(M)$ to be the $n \times n$ matrix given by $c(M)_{i,j} = (-1)^{i+j} \det(M^{i,j})$. It is well known that for any fixed $1 \leq i \leq n$ we have $\det(M) = \sum_{j=1}^{n} M_{i,j} C_{i,j}$. Define $\mathsf{adj}(M) = c(M)^\tau$ (the transpose). Thus, $M\mathsf{adj}(M) = \mathsf{adj}(M)M = \det(M) \cdot I$ where I is the $n \times n$ identity matrix.

This implies that if $\det(M)$ is invertible in R, then $M^{-1} = (\det(M))^{-1} \cdot \mathsf{adj}(M)$. :) ✓

Solution to Exercise 1.103 :(
It is easy to see that $I, -I$ commute with any $A \in \mathsf{GL}_n(\mathbb{Z})$. Thus, $\{I, -I\} \lhd \mathsf{GL}_n(\mathbb{Z})$.

For $A \in \mathsf{GL}_{2n+1}(\mathbb{Z})$ we have that $\det(\det(A) \cdot A) = \det(A)^{2n+1} \cdot \det(A) = 1$. Thus, the map $A \mapsto (\det(A), \det(A) \cdot A)$ is an isomorphism from $\mathsf{GL}_{2n+1}(\mathbb{Z})$ onto $\{-1, 1\} \times \mathsf{SL}_{2n+1}(\mathbb{Z})$.

Also, the map $A \mapsto \{-I, I\}A$ is an isomorphism from $\mathsf{SL}_{2n+1}(\mathbb{Z})$ onto $\mathsf{PGL}_{2n+1}(\mathbb{Z})$. :) ✓

Solution to Exercise 1.104 :(
Since S is generated by $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$, it suffices to show that for any matrix $A = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix}$, we have that Aa and Ab are both still of this form.

For A as above, compute,

$$Aa = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4k+1 & 2(4k+1)+2n \\ 2m & 2\cdot 2m+4\ell+1 \end{bmatrix} = \begin{bmatrix} 4k+1 & 2(4k+1+n) \\ 2m & 4(m+\ell)+1 \end{bmatrix},$$

which is of the correct form. Similarly,

$$Ab = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 4k+1+2\cdot 2n & 2n \\ 2m+2(4\ell+1) & 4\ell+1 \end{bmatrix} = \begin{bmatrix} 4(k+n)+1 & 2n \\ 2(m+4\ell+1) & 4\ell+1 \end{bmatrix},$$

completing the proof. :) ✓

Solution to Exercise 1.105 :(
Let

$$H = \left\{ A = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix} \mid \det(A) = 1\,,\ k, \ell, n, m \in \mathbb{Z} \right\}.$$

We have already seen that $S \subset H$.

Let $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ be the generators of S.

Let $A = \begin{bmatrix} 4k+1 & 2n \\ 2m & 4\ell+1 \end{bmatrix}$. Denote $||A|| = \max\{|4k+1|, |4\ell+1|\}$. Since $A^{-1} = \begin{bmatrix} 4\ell+1 & -2n \\ -2m & 4k+1 \end{bmatrix}$, by possibly replacing A with A^{-1}, we may assume that $|4k+1| \geq |4\ell+1|$, so that $||A|| = |4k+1|$.

We will prove by induction on $||A||$ that if $\det(A) = 1$ then $A \in S$.

The base case is where $||A|| = 1$, which is $k = \ell = 0$. Then $1 = \det(A) = 4(\ell - mn) + 1$ implies that $\ell = nm$, so that either $n = 0$ or $m = 0$. If $n = 0$ then $A = b^m \in S$ and if $m = 0$ then $A = a^n \in S$. This completes the base case.

For $||A|| > 1$ we proceed by induction as follows.

Note that $\det(A) = 1$ implies that $|(4k+1)(4\ell+1)| = |4nm+1|$. If $2\min\{|n|, |m|\} > |4k+1|$ then

$$|4k+1|^2 \geq |(4k+1)(4\ell+1)| \geq 4|nm| - 1 \geq (|4k+1|+1)^2 - 1 > |4k+1|^2,$$

a contradiction! So it must be that

$$2\min\{|n|, |m|\} \leq |4k+1|.$$

Since $2\min\{|n|, |m|\}$ is even, and $|4k+1|$ is odd, equality cannot hold, so we conclude that

$$2\min\{|n|, |m|\} < |4k+1|.$$

We now have two cases.

Case I. $2|n| < |4k+1|$. In this case we see that for some $z \in \{-1, 1\}$ we have $|4(k+zn)+1| < |4k+1|$. Since

$$Ab^z = \begin{bmatrix} 4(k+zn)+1 & 2n \\ 2(m+z(4\ell+1)) & 4\ell+1 \end{bmatrix},$$

if $|4\ell+1| < |4k+1|$, then $||Ab^z|| < ||A||$, and by induction $Ab^z \in S$, implying that $A \in S$ as well.

https://doi.org/10.1017/9781009128391.003 Published online by Cambridge University Press

If $|4\ell + 1| = |4k + 1|$, then we can find $w \in \{-1, 1\}$ such that $|4(\ell + wn) + 1| < |4\ell + 1|$. So the matrix $b^w Ab^z$ admits that

$$||b^w Ab^z|| = \max\{|4(k + zn) + 1|, |4(\ell + wn) + 1|\} < ||A||.$$

Again by induction $b^w Ab^z \in S$ so that $A \in S$ as well.

Case II. $2|m| < |4k + 1|$. Similarly to the previous case, taking $z \in \{-1, 1\}$ such that $|4(k + zm) + 1| < |4k + 1|$, we find that

$$a^z A = \begin{bmatrix} 4(k+zm)+1 & 2(n+z(4\ell+1)) \\ 2m & 4\ell+1 \end{bmatrix}.$$

If $|4\ell + 1| < |4k + 1|$ then $||a^z A|| < ||A||$, so that $a^z A \in S$ by induction, implying that $A \in S$.

If $|4\ell + 1| = |4k + 1|$, then taking $w \in \{-1, 1\}$ such that $|4(\ell + wm) + 1| < |4\ell + 1|$, we obtain that $||a^z Aa^w|| = \max\{|4(k + zm) + 1|, |4(\ell + wm) + 1|\} < ||A||$. As before, by induction $a^z Aa^w \in S$ so that $A \in S$ as well. :) ✓

Solution to Exercise 1.106 :(

Let $\varphi\colon \mathsf{SL}_2(\mathbb{Z}) \to \mathsf{SL}_2(\mathbb{Z}/4\mathbb{Z})$ be the map given by taking the matrix entries modulo 4. This is easily seen to be a surjective homomorphism.

Let $K = \mathsf{Ker}\varphi \lhd \mathsf{SL}_2(\mathbb{Z})$. By the above exercises, $K \lhd S$. So $[\mathsf{SL}_2(\mathbb{Z}) : S] = [\mathsf{SL}_2(\mathbb{Z})/K : S/K] = [\mathsf{SL}_2(\mathbb{Z}/4\mathbb{Z}) : \varphi(S)] < \infty$. :) ✓