Chapter 1

Groups and Rings

Lectured by Someone
Typed by Yu Coughlin
Autumn 2024

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

Contents

1 Quotient groups

1.1 Group homomorphisms

Definition 1.1.1 (Group isomorphism)**.** Given groups G, H, a function $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism. If there exists an isomorphism between groups, G is **isomorphic** to H written $G \cong H$.

Definition 1.1.2 (Group automorphism)**.** Given G a group, an isomorphism $f : G \xrightarrow{\sim} G$ is a **group automorphism**.

Theorem 1.1.3. $\operatorname{Aut} G$ (the set of automorphisms of a group G) is a group under function composition.

Proof. □

Theorem 1.1.4. Given groups G, H, if $f : G \xrightarrow{\sim} H$ then $f^{-1} : H \xrightarrow{\sim} G$.

Proof. □

1.2 Normal subgroups

Definition 1.2.1 (Normal subgroup)**.** A sugroup N of G is **normal**, written $N \trianglelefteq G$, if it satisfies any of these equal properties:

(N1) N is the kernel of some homomorphism,

(N2) N is stable under conjugations ($\forall n \in N$ and $g \in G$, $gng^{-1} \in N$),

(N3) for all $g \in G$ $gN = Ng$.

Proof of equivalence. □

1.3 Quotient groups

Definition 1.3.1 (Quotient groups)**.** Let $N \trianglelefteq G$, the **quotient group** of G modulo N, written G/N, is the group with elements as left cosets of N in G with $(g_1N) \cdot (g_2N) = (g_1g_2N)$.

Proof. One can easily check this satisfies all of the group axioms. □

Remark 1.3.2. By Lagrange's theorem $|G/N| = |G|/|N|$.

Definition 1.3.3 (Simple group)**.** A group G is **simple** if it has no normal subgroups except $\{e_G\}$ and G.

1.4 Isomorphism theorems

Theorem 1.4.1 (First isomorphism theorem)**.** If $f : G \to H$ is a group homomorphism, $G/\ker f \cong \operatorname{im} f$.

Proof. Have $\phi : G/\ker f \to \operatorname{im} f$ with $\phi : g\ker f \mapsto f(g)$. □

Theorem 1.4.2 (Universal property of quotients)**.** Let $N \trianglelefteq G$ and $f : G \to H$ be a group homomorphism such that $N \subseteq \ker f$. There exists a *unique* homomorphism $\tilde{f} : G/N \to H$ such that the diagram

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "f"] & \\ G/N \arrow[r, dashed, "\tilde{f}"'] & H \end{tikzcd}$$

commutes, (here $\pi : G \to G/N$ is the projection map with $\pi : g \to gN$).

Proof. The proof follows Theorem 1.4.1 with $H = \operatorname{im} f$. □

Definition 1.4.3 (Frobenius product)**.** Given $A, B \subseteq G$ a group, the **(Frobenius) product** of A and B is

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

Lemma 1.4.4. Given $H, N \leq G$ a group, N is normal $\implies HN \leq G$ and N, H normal $\implies HN \trianglelefteq G$.

Proof. □

Theorem 1.4.5 (Second isomorphism theorem)**.** If $H \leq G$ and $N \trianglelefteq G$, $H/(H \cap N) \cong (HN)/N$. This is ometimes called the *diamond theorem* due to the shape of the subgroup lattice it produces:

$$\begin{tikzcd}
 & G \arrow[d] & \\
 & HN \arrow[dl] \arrow[dr] & \\
H \arrow[dr] & & N \arrow[dl] \\
 & H \cap N \arrow[d] & \\
 & \{e_G\} &
\end{tikzcd}$$

where arrows point to subgroups.

Note 1.4.6. There are third and fourth isomorphism theorems that will not appear in this module.

1.5 Centres

Definition 1.5.1 (Inner automorphisms)**.** Given the group G the conjugations by elements of G form the group $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

Proof. □

Definition 1.5.2 (Centre of group)**.** Given the group G the elements of G that commute with all other elements form the **centre** of G, $Z(G) \trianglelefteq G$.

Proof of normality. Have $\phi : G \to \operatorname{Aut} G$ with $\phi : g \mapsto$ conjugation by g, $\ker \phi = Z(G)$. □

Theorem 1.5.3. If $G/Z(G)$ is cyclic, G is Abelian.

Proof. □

Definition 1.5.4 (p-group)**.** A finite group G is a **p-group** is the order of G is a power of prime p.

Theorem 1.5.5. Let G be a p-group, $Z(G) \neq \{e_G\}$.

1.6 Commutators

Definition 1.6.1 (Commutator)**.** For $a, b \in G$ a group, we have $[a, b] := aba^{-1}b^{-1}$ the **commutator** of a and b. $[G, G]$ is the smallest subgroup of G containing all commutators of elements of G, called the **commutator** of G.

Remark 1.6.2. A group G is Abelian iff $[G, G] = e_G$.

Theorem 1.6.3. Given G a group, $[G, G] \trianglelefteq G$ with its quotient in G Abelian.

Theorem 1.6.4. Let $N \trianglelefteq G$, G/N is Abelian iff $[G, G] \subseteq N$.

Theorem 1.6.5. Given a group G with $A, B \trianglelefteq G$, $A \cap B = \{e_G\}$ and $AB = G$; $A \times B \cong G$.

1.7 Torsion and p-primary subgroups

Definition 1.7.1 (Torsion subgroup)**.** Given an abelian group G, the set of elemnts of G with finite order form the **torsion subgroup** of G, denoted G_{tors}. When $G = G_{\text{tors}}$, we call G a **torsion Abelian group**.

Definition 1.7.2 (p-primary subgroups)**.** Given an abelian group G, the set of elements of g with order p (a prime) is the **p-primary subgroup** of G, written $G\{p\}$. When $G = G_G\{p\}$, we call G a **p-primary torsion Abelian group**.

Theorem 1.7.3. Let the prime factorisation of $n \in \mathbb{N}$ be $p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ with C_n the cyclic group of order n.

$$C_n \cong C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_m^{a_m}}.$$

Proof. □

1.8 Generators

Lemma 1.8.1. Given an indexing set $\mathcal{I}$, and a sequence of subgroups $(H_i)_{i\in\mathcal{I}} \leq H$, $\bigcap_{i\in\mathcal{I}} H_i \leq G$.

Definition 1.8.2 (Subgroup generated by a set)**.** Given $S \subseteq G$ a group,

$$\langle S \rangle := \left(\bigcap_{S\subseteq H\leq G} H \right) \leq G$$

is the **subgroup of** G **generated by** S. If $\langle S \rangle = G$ then we say S **generates** G and G is **finitely generated** is S is finite.

1.9 Classification of finitely generated Abelian groups

Definition 1.9.1 (Free Abelian group of rank n)**.** The **Free Abelian group of rank** n is the group $\mathbb{Z}^n$ under addition. The free abelian group of rank 0 is the trivial group.

Lemma 1.9.2. If $\mathbb{Z}^m \cong \mathbb{Z}^n$ then $n = m$, so the rank of a free abelian group is well defined.

Lemma 1.9.3. Any subgroup of $\mathbb{Z}^n$ is isomorphic to some $\mathbb{Z}^m$ for some $m \leq m$.

Theorem 1.9.4. Every finitely generated Abelian group is isomorphic to a product of finitely many cyclic groups.

Theorem 1.9.5. Every finitely generated Abelian group is isomorphic to a product of finitely many infinite cyclic groups and finitely many cyclic groups of prime order. The number of ininfite cyclic factors and the number of cclic factors of order p^r, where p is primse and $r \in \mathbb{N}$ is determined solely by the group.

Theorem 1.9.6. A finitely generated Abelian group, G, is not cyclic iff there exists a prime p such that $G \cong C_p \times C_p$.

2 Group actions

2.1 Actions

Definition 2.1.1 (Actions)**.** Given a group G and a set X, a **group action** is: a binary operation

$$\begin{array}{rcccc} \cdot & : & G \times X & \longrightarrow & X \\ & & (g, x) & \longmapsto & g \cdot x \end{array}$$

with $e_G \cdot x = x$ for all $x \in X$ and $(g_1 g_2) \cdot x = g_1 \cdot (g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$; or, equivalently, a homomorphism $\rho : G \to \mathrm{Sym}(X)$.

Definition 2.1.2 (Faithful set)**.** An action of a group G on a set X is **faithful** if the map $\rho : G \to \mathrm{Sym}(X)$ is injective.

2.2 Orbit-stabiliser theorem

Definition 2.2.1 (Orbit)**.** Given a group G acting on a set X, the G**-orbit** of $x \in X$ is

$$G(x) := \{g \cdot x : g \in G\} \subseteq X.$$

Orbits partition X into X/G.

Definition 2.2.2 (Stabiliser)**.** Given a group G acting on a set X, the **stabiliser** of $x \in X$ is

$$\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subseteq G.$$

Stabilisers also partition G.

Lemma 2.2.3. Given a group G acting on a set X, $\mathrm{Stab}_G(g \cdot x) = g \,\mathrm{Stab}_G(x) g^{-1}$

Theorem 2.2.4 (Orbit-stabiliser theorem)**.** Given a group G acting on a set X. For all $x \in X$, we have $\phi_x : G/\mathrm{Stab}(x) \xrightarrow{\sim} G(x)$ by $\phi_x : g\,\mathrm{Stab}(x) \mapsto g \cdot x$, giving $|G(x)| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|$.

Proof. asdfsd □

Corollary 2.2.5. $|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$.

Corollary 2.2.6 (Cayley's theorem)**.** Let G be a finite group of order n. Then S_n contains a finite subgroup isomorphic to G.

Corollary 2.2.7 (Cauchy's theorem)**.** Let G be a finite group of order n and let p be a prime factor of n. Then G contains an element of order p.

2.3 Jordan's theorem

Definition 2.3.1 (Transitive action)**.** Given a group G acting on a set X, if X is a G-orbit then we say G acts **transitively** on X.

Definition 2.3.2 (Fixed points)**.** Given a group G acting on a set X, an element $x \in X$ is a fixed point of $g \in G$ iff $g \cdot x = x$. We have $\mathrm{Fix}(g) \subseteq X$ the set of fixed points of $g \in G$ satisying:

$$\mathrm{Stab}(x) \xleftarrow[\pi_G]{} \{(x, g) \in X \times G;\ g \cdot x = x\} \xrightarrow[\pi_X]{} \mathrm{Fix}(g)\ .$$

Theorem 2.3.3 (Jordan's theorem)**.** Let G act transitively on a finite set X, we have

$$\sum_{g \in G} |\,\mathrm{Fix}(g)| = |G|,$$

with there being some element $g \in G$ such that $\mathrm{Fix}(g) = \emptyset$.

Corollary 2.3.4 (Burnside's lemma)**.** Given a group G acting on a finite set X:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

3 Rings

3.1 Rings

Definition 3.1.1 (Ring)**.** A ring (with 1) is a set R with elements $0, 1$ and binary operations $+, \times$ such that

1. $(R, +)$ is an abelian group with identity 0,
2. $(R, \times)$ is a semigroup with 1 as the identity,
3. both left and right multiplication are distributive over addition.

Examples 3.1.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings with their normal operations. $\mathbb{R}[x]$ is the set of real-valued polynomials and is also a ring.

Definition 3.1.3 (Subring)**.** A subset of a ring wich is itself a ring under the same operators with the same 1 is a **subring**.

Definition 3.1.4 (Commutative ring)**.** A ring, R, is **commutative** iff $a + b = b + a$ for all $a, b \in \mathbb{R}$.

Definition 3.1.5 (Invertible)**.** An element x of a ring R is invertible if there exists $y, z \in R$ with $yx = zx = 1$.

Definition 3.1.6 (Division ring)**.** A ring R is called a **division ring** if $R \backslash \{0\}$ is a group under multiplication with identity 1.

Remark 3.1.7. A commutative division ring is a field.