

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 Probability 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	Groups and Rings	1
1	Quotient groups	3
1.1	Group homomorphisms	3
1.2	Normal subgroups	3
1.3	Quotient groups	3
1.4	Isomorphism theorems	3
1.5	Centres	4
1.6	Commutators	5
1.7	p -primary subgroups	5
1.8	Generators	5
2	Group actions	5
2.1	Actions	5
2.2	Orbit-stabiliser theorem	5
2.3	p -groups	5
2.4	Jordan's theorem	5
3	Finitely generated Abelian groups	5
3.1	Smith normal form	5
3.2	Classification of finitely generated Abelian groups	5
4	Rings	5
4.1	Rings	5
4.2	Ring homomorphisms	5
4.3	Ideals	5
5	Integral domains	5
5.1	Integral domains	5
5.2	Characteristic	5
5.3	Vector spaces	5
6	PIDs and UFDs	5
6.1	Polynomial rings	5
6.2	Euclidian domains	5
6.3	Principal ideal domains	5
6.4	Unique factorisation domains	5
7	Fields	5
7.1	Field extensions	5
7.2	Constructing fields	5
7.3	Existence of finite fields	5

1 Quotient groups

1.1 Group homomorphisms

Definition 1.1.1 (Group isomorphism). Given groups G, H , a function $f : G \rightarrow H$ 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. $\text{Aut } G$ (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 subgroup 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 $f : G \rightarrow H$ is a group homomorphism, $G/\ker f \cong \text{im } f$.

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

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

$$\begin{array}{ccc} G & & \\ \pi \downarrow & \searrow \phi & \\ G/N & \xrightarrow{\tilde{f}} & H \end{array}$$

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

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

1.5 Centres

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

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. Have $\phi : G \rightarrow \text{Aut } G$ with $\phi : g \mapsto \text{conjugation by } g$, $\ker \phi = Z(G)$.

□

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

Proof.

□

- 1.6 Commutators
- 1.7 p -primary subgroups
- 1.8 Generators
- 2 Group actions
 - 2.1 Actions
 - 2.2 Orbit-stabiliser theorem
 - 2.3 p -groups
 - 2.4 Jordan's theorem
- 3 Finitely generated Abelian groups
 - 3.1 Smith normal form
 - 3.2 Classification of finitely generated Abelian groups
- 4 Rings
 - 4.1 Rings
 - 4.2 Ring homomorphisms
 - 4.3 Ideals
- 5 Integral domains
 - 5.1 Integral domains
 - 5.2 Characteristic
 - 5.3 Vector spaces
- 6 PIDs and UFDs
 - 6.1 Polynomial rings
 - 6.2 Euclidian domains
 - 6.3 Principal ideal domains
 - 6.4 Unique factorisation domains
- 7 Fields
 - 7.1 Field extensions
 - 7.2 Constructing fields
 - 7.3 Existence of finite fields