Groups, Rings and Modules

Adam Kelly

January 22, 2021

This set of notes is a work-in-progress account of the course 'Groups, Rings and Modules', originally lectured by Dr Tom Fisher in Lent 2020 at Cambridge. These notes are not a transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are my own view of what was taught, and should be somewhat of a superset of what was actually taught. I frequently provide different explanations, proofs, examples, and so on in areas where I feel they are helpful. Because of this, this work is likely to contain errors, which you may assume are my own. If you spot any or have any other feedback, I can be contacted at ak2316@cam.ac.uk.

Contents

0 Introduction

§0.1 Structure of the Course

This course is, quite naturally, divided into three sections.

1. *Groups*

   We will be continuing on from IA Groups, paying particular attention to certain topics such as simple groups, p-groups and p-subgroups. The main highlight of this part of the course will be the Sylow theorems.

2. *Rings*

   Rings are sets where we can add, subtract and multiply (but not necessarily divide), for example, $\mathbb{Z}$. A ring where division is always possible is a field, for example $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Z}/p\mathbb{Z}$ for a prime p.

3. *Modules*

   A module is the analog of a vector space where we work over a ring, rather than a field. We will attempt to classify modules over certain 'nice' rings. This will allow us to prove the Jordan Normal theorem of matrices and to classify finite abelian groups.

§0.2 Books

As with most mathematics courses in Cambridge, you will not need a textbook to follow this course. What is covered in lectures is enough to do both the example sheets and the examinations for this course. Still, you might find that a textbook can provide a different perspective, additional worked examples, and additional material that you may find informative, helpful or fun.

In particular, the following books are quite relevant/good, but there is no expectation that you will look at these.

- P. M. Cohn, *Classical Algebra*.

  This covers the whole course (but does have some weird notation).

- Hartley & Hawkes, *Rings, Modules & Linear Algebra*.

  This is a good reference for the 'rings and modules' part of the course, but notably doesn't include any content on group theory.

You should be able to find all of these books in either your college library or the university library.

1 Groups – Revision and Basics

The first algebraic object that we shall consider in this course is one you are likely familiar with – a group.

§1.1 Definitions

We will begin by defining what a group is.

Definition 1.1.1 (Group)

A **group** is a pair $(G, *)$ consisting of a set G and a binary operation[a] $* : G \times G \to G$ satisfying the axioms:

- *Identity.* There is an element $e \in G$ such that $e * g = g * e = g$ for all $g \in G$,
- *Inverses.* For every element $g \in G$, there is an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.
- *Associativity.* The operation $*$ is associative.

[a] Some texts include an additional *closure* axiom, but this is implied by $*$ being a binary operation on G.

Remark. We will usually either use additive or multiplicative notation for groups, and in these cases we will often write 0 or 1 for the identity respectively.

Definition 1.1.2 (Subgroup)

A subset $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if it is a group with respect to the operation $*$ defined on $H \times H$.

There is a way to test the conditions needed for a subset to be a subgroup in just a few lines, but it does have limited utility.

Lemma 1.1.3 (Fast Subgroup Checking Lemma)

A nonempty subset $H \subseteq G$ is a subgroup if $a, b \in H$ implies $a * b^{-1} \in H$.

Proof Sketch. Check that this implies the definition. □

Example 1.1.4 (Examples of Groups)

The following are all examples of groups.

(i) The additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(ii) The cyclic group of order n, C_n.

(iii) The dihedral group D_{2n} of the symmetries of a regular n-gon.

(iv) The symmetric group S_n and alternating group A_n, where S_n is the group of permutations of $\{1, 2, \ldots, n\}$ and $A_n \leq S_m$ is the group of even permuations.

(v) The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = ijk = -1$.

(vi) The matrix groups over some field F, $\mathrm{GL}_n(F)$ of all $n \times n$ matrices over F with non-zero determinant, and $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$, the subgroup of matrices with determinant 1.

Definition 1.1.5 (Direct Product)

The **direct product** of groups G and H is $G \times H$ with operation $(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

For a subgroup $H \leq G$, the **left cosets** of H in G are the sets $gH = \{gh \mid h \in H\}$ where $g \in G$. Recall that these partition G, and each has the same cardinality as H. From this we deduce Lagrange's theorem.

Theorem 1.1.6 (Lagrange's Theorem)

Let G be a finite group, and H be a subgroup. Then $|G| = |H| \cdot |G : H|$ where $|G : H|$ is the **index** of H in G, the number of left cosets of H in G.

It is natural to wonder whether there is a converse to Lagrange's theorem, and it turns out that the converse is *not* true in general. There is a partial converse however.

Theorem 1.1.7 (First Sylow Theorem)

If G is a group with $|G| = p^a m$ where p is a prime and $p \nmid m$, then there exists $H \leq G$ with $|H| = p^a$.

We will prove this theorem later on.

Definition 1.1.8 (Order of an Element)

Let G be a group and $g \in G$. If there exists $n \geq 1$ such that $g^n = 1$, then the least such n is the **order** of g. If no such n exists, we say g hsa infinite order.

Remark. If g has order d, then $g^n = 1 \iff d \mid n$. The proof follows from the division algorithm. Also, $\{1, g, g^2, \ldots, g^{d-1}\} \leq G$ and so if G is finite, then by Lagrange, $d \mid |G|$.

Definition 1.1.9 (Normal Subgroup)

A subgroup $H \leq G$ is **normal** if $g^{-1} H g = H$ for all $g \in G$. We write $H \trianglelefteq G$ in this case.

Proposition 1.1.10 (Quotient Group)

If $H \trianglelefteq G$, then the set G/H of left cosets of H in G is a group called the **quotient group** with the operation $g_1 H * g_2 H = (g_1 g_2) H$.

Proof. We must check that $*$ is well defined. Suppose that $g_1H = g_1'H$ and $g_2H = g_2'H$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$. Then we get $g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H$. This is equal to g_1g_2H if and only if $(g_1g_2)^{-1}g_1h_1g_2 \in H$, that is, if $g_2^{-1}h_1g_2 \in H$, which follows from the normality of H. Now to check the group axioms, note that associativity is inherited, we have the coset H being the identity, and the inverse of gH being $g^{-1}H$. Thus G/H is a group. $\square$