IB Groups, Rings and Modules

Martin von Hodenberg (mjv43@cam.ac.uk)

January 20, 2022

Contents

§0 Introduction

This course will contain several sections:

1. Groups; this will be a continuation from IA, focusing on simple groups, p-groups, and p-subgroups. The main result in this part of the course will be the Sylow theorems.
2. Rings; these are sets where you can add, subtract and multiply (e.g $\mathbb{Z}$ or $\mathbb{C}[X]$). We will study rings of integers such as $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$. These also generalise to polynomial rings. We will also study fields, which are rings where you can divide (e.g $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime).
3. Modules; these are an analogue of vector spaces where the scalars belong to a ring instead of a field. We will classify modules over certain "nice" rings. This allows us to prove Jordan Normal Form, and classify finite abelian groups.

§1 Groups

§1.1 Recall of IA Groups

Definition 1.1 (Group)

A group is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)
2. $\exists e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (identity)
3. $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ (inverses)

Remark.

- In practice, one often needs to check closure in order to check that $\cdot$ is well-defined.
- If using additive (respectively multiplicative) relations, we will often write 0 (or 1) for the identity.
- We write $|G|$ for the number of elements in G.

Definition 1.2 (Subgroup)

A subset $H \subseteq G$ is a subgroup (written $H \leq G$) if H is closed under $\cdot$ and $(H, \cdot)$ is a group.

Remark. A non-empty subset H of G is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$ (see IA Groups for the proof).

Example 1.3 (Examples of groups)

Groups we have already seen include:

- Additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
- Cyclic and dihedral groups C_n and D_{2n}.

- Abelian groups: those groups G such that $a \cdot b = b \cdot a$ for all $a, b \in G$.
- Symmetric and alternating groups $S_n =$ group of all permutations of $\{1, \dots, n\}$ and $A_n \leq S_n$, the group of all even permutations.
- Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ where i, j, k are quaternions.
- General and special linear groups $GL_n(\mathbb{R}) = n \times n$ matrices on $\mathbb{R}$ with $\det \neq 0$, where the group operation is matrix multiplication. This contains the subgroup $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$, which is the subgroup of matrices with $\det = 1$.

Definition 1.4 (Direct product)

The direct product of groups G and H is the set $G \times H$ with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Theorem 1.5 (Lagrange's theorem)

Let $H \leq G$. Then the left cosets of H in G are the sets $gH = \{gh : h \in H\}$ for $g \in G$. These partition G, and each has the same cardinality as H. From this we can deduce Lagrange's theorem:

If G is a finite group and $H \leq G$, then $|G| = |H|[G : H]$ where $[G : H]$ is the number of left cosets of H in G (the index of H in G).

Remark. Can also carry this out with right cosets. A corollary of Lagrange's theorem is thus that the number of left cosets = number of right cosets.

Definition 1.6 (Order of an element)

Let $g \in G$. If $\exists n \geq 1$ such that $g^n = 1$, then the least such n is the order of g in G. If no such n exists, g has infinite order.

Remark. If g has order d, then

- $g^n = 1 \implies d | n$.
- $\{1, g, \dots, g^{d-1}\} \leq G$ and so if G is finite, then $d \,|\, |G|$ (Lagrange).

Definition 1.7 (Normal subgroup)

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

Proposition 1.8

If $H \trianglelefteq G$ then the set G/H of left cosets of H in G is a group (called the quotient group) with operation

$$g_1 H \cdot g_2 H = g_1 g_2 H.$$

Proof. Check $\cdot$ is well-defined:

Suppose $g_1 H = g_1' H$ and $g_2 H = g_2' H$ for some $g_1, g_1' \in G$. Then $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$. Therefore

$$\begin{aligned} g_1' g_2' &= g_1 h_1 g_2 h_2 \\ &= g_1 g_2 \underbrace{(g_2{}^{-1} h_1 g_2)}_{\in H} \underbrace{h_2}_{\in H} \end{aligned}$$

Therefore $g_1' g_2' H = g_1 g_2 H$. Associativity is inherited from G, the identity is $H = eH$, and the inverse of gH is $g^{-1} H$. □

Definition 1.9 (Homomorphism)

If G, H are groups, then a function $\phi : G \to H$ is a group homomorphism if $\phi(g_1 g_2) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. It has kernel

$$\ker \phi = \{g \in G : \ \phi(g) = e\} \leq G.$$

and image

$$\operatorname{Im} \phi = \{\phi(g) : \ g \in G\} \leq H.$$

Remark. If $a \in \ker \phi$ and $g \in G$, then

$$\begin{aligned} \phi(g^{-1} a g) &= \phi(g^{-1})\phi(a)\phi(g) \\ &= \phi(g^{-1})\phi(g) \\ &= \phi(g^{-1} g) = \phi(e) = e. \end{aligned}$$

So $g^{-1} a g \in \ker \phi$ and hence $\ker \phi$ is a normal subgroup of G.