Groups, Rings, and Modules

Jonathan Gai

January 20, 2022

Contents

Lecture 1: Groups

20 Jan. 12:00

1 Introduction

1.1 Groups

Continuation from IA, focussing on

1. Simple groups, p-groups, p-subgroups.
2. Main results in this part of the course will be the Sylow Theorems.

1.2 Rings

Sets where you can add, subtract and multiply.

Example. Examples of rings include,

1. $\mathbb{Z}$ or $\mathbb{C}[X]$.
2. Rings of integers $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ (More in Part II Number Fields).
3. Polynomial rings $\mathbb{C}[x_1, \ldots, x_2]$ (More in Part II Algebraic Geometry).

A ring where you can divide is called a *field*. Eg. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime.

1.3 Modules

An analogue of vector space where the scalars belong to a ring instead of a field.

We will classify modules over certain nice rings.

Allows us to prove Jordan normal form, and classify finite Abelian groups.

2 Groups

2.1 Revision and Basic Theory

We revisit basic properties and definition from Part IA Groups.

Definition 2.1 (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. (Associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. (Identity) $\exists a \in G$ s.t. $e \cdot g = g \cdot e = g \ \forall g \in G$.
3. (Inverses) $\forall g \in G, \exists y^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remark. Some things to note form definition of a group.

1. *Closure* is included implicitly in the definition of a binary operation. In checking $\cdot$ well-defined, we need to check closure, i.e. $a, b \in G \implies a \cdot b \in G$.
2. If using additive (or multiplicative) notation, often write 0 (or 1) for identity.

Definition 2.2 (Subgroup). A subset $H \subset G$ is a *subgroup* (written $H \leq G$) if $h \cdot h^{-1} \in H, \forall h, h' \in H$, and $(H, \cdot)$ is a group. Remark: A non-empty subset H of G is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$

Example. Here we list some common groups and their subgroups.

1. Additive $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
2. Cyclic and dihedral group, $C_n \leq D_{2n}$.
3. Abelian groups - those $(G, \cdot)$ such that $a \cdot b = b \cdot a \ \forall a, b \in G$
4. Symmetric and Alternating groups, $A_n \leq S_n$.
5. Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
6. General and Special Linear Groups, $SL_n(\mathbb{R}) \leq SL_n(\mathbb{R})$.

Definition 2.3 (Direct Product). The *(direct) product* of groups G and H is the set $G \times H$ with operation given by

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

Let $H \leq G$, the *left cosets* of H in G are the sets $gH = \{gh \mid h \in H\}$ for $g \in G$. These partition G, and each coset has the same cardinality as H. So we can deduce.

Theorem 2.1 (Lagrange's Theorem). Let G be a finite group and $H \leq G$, Then $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the number of left cosets of H in G. $[G : H]$ is the *index* of H in G.

Remark. Can also carry this out with right cosets. Lagrange's Theorem then implies that the number of left cosets is the same as the number of right cosets.

Definition 2.4 (Order). Let $g \in G$. If $\exists n \geq 1$ s.t. $g^n = 1$ then the least such n is the *order* of g, otherwise we say that g has infinite order.

Remark. If g has order d, then

1. $g^n = 1 \implies d \mid n$.
2. $\{1, g, \ldots, g^{d-1}\} \leq G$ and so if G is finite, then $d \mid |G|$ (by Lagrange's Theorem).

Definition 2.5 (Normal Subgroup). A subgroup $H \leq G$ is *normal* if $g^{-1}Hg = H \ \forall g \in G$. We write $H \trianglelefteq G$.

Proposition 2.1. 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

$$g_1H \cdot g_2H = g_1g_2H.$$

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

Suppose $g_1H = g_1'H$ and $g_2H = g_2'$ for some $h_1, h_2 \in H$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$, we have

$$\begin{aligned} g_1'g_2' &= g_2h_1g_2h_2 \\ &= g_1g_2(g_2^{-1}h_2g_2)h_2 \end{aligned}$$

so $g_1'g_2'H = g_1g_2H$.

Associativity is inherited from G, the identity is $H = eH$, and the inverse of gH is $g^{-1}H$. ■

Definition 2.6 (Homomorphism). G, H groups. A function $\phi : G \to H$ is a group homomorphism if $\phi(g_1g_2) = \phi(g_1)\phi(g_2) \forall g_1, g_2 \in G$. It has *kernel*

$$\ker(\phi) = \{y \in G \mid \phi(y) = 1\} \trianglelefteq G,$$

and *image* $\mathrm{Im}(\phi) = \{\phi(y) \mid y \in G\} \leq H$.

Proof. If $a \in \ker(\phi)$ and $g \in G$, then

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

So it is indeed a normal subgroup. ■