Groups, Rings, and Modules

Jonathan Gai

January 26, 2022

Contents

Lecture 1: Groups

20 Jan. 12:00

Introduction

0.1 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.

0.2 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*. example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime.

0.3 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.

1 Groups

1.1 Revision and Basic Theory

We revisit basic properties and definition from Part 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. (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 1.2 (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 1.3 (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 1.1 (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 1.4 (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 1.5 (Normal Subgroup). A subgroup $H \leq G$ is *normal* if $g^{-1}Hg = H \; \forall g \in G$. We write $H \trianglelefteq G$.

Proposition 1.1. 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 $g_2H = g_2'$. 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 1.6 (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* $\text{Im}(\phi) = \{\phi(y) \mid y \in G\} \leq H$.

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. ∎

Lecture 2: Isomorphism Theorems

22 Jan. 12:00

We will next talk about a special kind of homomorphism.

Definition 1.7. An *isomorphism* of groups is a group homomorphism that is also a bijection.

We say that G and H are isomorphic (written $G \cong H$) if there exists an isomorphism $\phi : G \to H$.

Exercise. Check that $\phi^{-1} : H \to G$ is a group homomorphism.

Theorem 1.2 (First Isomorphism Theorem). Let $\phi : G \to H$ be a group homomorphism. Then $\ker(\phi) \trianglelefteq$ and ${}^{G}/_{\ker(\phi)} \cong \mathrm{Im}(\phi)$.

Proof. Let $K = \ker(\phi)$. We already checked that K is normal.

Define $\Phi : {}^{G}/_{K} \to \mathrm{Im}(\phi)$, $gK \mapsto \phi(g)$. We need to check that Φ is well-defined first.

$$\begin{aligned}g_1K = g_2K &\iff g_2^{-1}g_1 \in K\\ &\iff \phi(g_2^{-1}g_1) = 1\\ &\iff \phi(g_1) = \phi(g_2).\end{aligned}$$

Note that we showed that Φ is injective at the same time because we can just go the other way.

Next, we show that Φ is a group homomorphism.

$$\begin{aligned}\Phi(g_1Kg_2K) &= \Phi(g_1g_2K)\\ &= \phi(g_1g_2)\\ &= \Phi(g_1K)\Phi(g_2K).\end{aligned}$$

Lastly, we show that Φ is surjective. Let $x \in \mathrm{Im}(\phi)$, say $x = \phi(g)$ for some $g \in G$, then $x = \Phi(gK)$. So it is indeed an isomorphism. ∎

Example. If we consider the function

$$\begin{aligned}\phi\colon \mathbb{C} &\longrightarrow \mathbb{C}^{\times}\\ z &\longmapsto e^{z}\end{aligned}$$

Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +) \to (\mathbb{C}, \times)$. It is well known that

$$\begin{aligned} \ker(\phi) &= 2\pi i\mathbb{Z}, \\ \operatorname{Im}(\phi) &= \mathbb{C}^\times \quad \text{by existence of } \log . \end{aligned}$$

Thus, $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^\times$.

From the naming for the First Isomorphism Theorem, we have the following Isomorphism Theorems as well.

Theorem 1.3 (Second Isomorphsim Theorem). Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk \mid h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. Let $h_1k_1, h_2k_2 \in HK$ with $h_1, h_2 \in H$, $g_1, g_2 \in G$. It suffices to show that

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{H}\underbrace{(h_2k_1k_2^{-1}h_2^{-1})}_{K} \in HK.$$

Thus, $HK \leq G$ by remark from last lecture. Let

$$\begin{aligned} \phi \colon H &\longrightarrow G/K \\ h &\longmapsto hK. \end{aligned}$$

This is the composition of inclusion map $H \to G$ and quotient map $G \to G/K$ hence ϕ is a group homomorphism.

$$\begin{aligned} \ker(\phi) &= \{h \in H \mid hK = K\} = H \cap K \trianglelefteq H, \\ \operatorname{Im}(\phi) &= \{hK \mid h \in H\} = HK/K. \end{aligned}$$

First isomorphism theorem gives

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

■

Remark. Suppose $K \trianglelefteq G$, there is a bijection

$$\begin{aligned} \{\text{Subgroups of } G/K\} &\longleftrightarrow \{\text{Subgroups of } G \text{ containing } K\}, \\ x &\longmapsto \{g \in G \mid gK \in X\}, \\ H/K &\longleftarrow H. \end{aligned}$$

Restricts to a bijection between the normal subgroups.

$$\{\text{Normal subgroups of } G/K\} \longleftrightarrow \{\text{Normal subgroups of } G \text{ containing } K\}.$$

Theorem 1.4 (Third Isomorphism Theorem). Let $K \leq H \leq G$ be normal subgroups of G. Then

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Proof. Let

$$\begin{aligned} \phi\colon G/K &\longrightarrow G/H \\ gK &\longmapsto gH. \end{aligned}$$

If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \leq H \implies g_1H = g_2H$. So ϕ is well-defined.

ϕ is a surjective group homomorphism with $\ker(\phi) = H/K$.

Now apply First Isomorphism Theorem. ■

1.2 Simple Groups

If $K \trianglelefteq G$, then studying the group K and G/K gives some information about G.

This approach is not always available.

Definition 1.8 (Simple Group). A group G is *simple* if $\mathbf{1}$ (the trivial subgroup) and G are its only normal subgroups.

Notation. We do not consider the trivial group to be a simple group.

Similar to the prime numbers, we can think of finite simple groups as the building block of finite groups. One of the greatest achievements in math is that we classified *all* finite simple groups!

Lemma 1.1. Let G be an Abelian group. G is simple if and only if $G \cong C_p$ for some prime p.

Proof. We prove the $\impliedby$ direction first. Let $H \leq C_p$. Lagrange's Theorem tells us

$$|H|\big||C_p| = p.$$

So $|H| = 1$ or p by primality of p. That is, $H = \{1\}$ or C_p. Thus, C_p is simple.

To prove the $\implies$ direction. Let $1 \neq g \in G$. G contains the subgroup

$$\langle g \rangle = \langle \ldots, g^{-2}, g^{-1}, e, g, g, \ldots \rangle$$

which is the subgroup generated by g. It is normal in G since G is Abelian. Since G simple, $\langle g \rangle = G$.

If G is infinite, $G \cong (\mathbb{Z}, +)$ which cannot be true by simplicity of G because $2\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Otherwise, $G \cong C_n$ for some n, let g be a generator. If $m \mid n$, then $g^{n/m}$ generates a subgroup of order m. Because G is simple, the order of the subgroup can only be 1 or n. So the only factors of n is 1 and n, and we have n prime. ■

Lemma 1.2. If G is a finite group, then it has a composition series

$$\mathbf{1} \cong G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m \cong G$$

with each quotient ${}^{G_{i+1}}/{}_{G_i}$ simple.

Note that G_i need not be normal in G.

Lecture 3

25 Jan. 1:00

Proof. Induct on $|G|$. When $|G| = 1$, the statement is obviously true.

If $|G| > 1$, let G_{m-1} be a normal subgroup of the largest possible order that is not $|G|$. By the correspondence theorem, ${}^{G}/{}_{G_{m-1}}$ is simple.

Apply inductively to G_{m-1}. ■

1.3 Group Action

Definition 1.9. For X a set, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition. The identity is $id = id_X$.

A group G is a *permutation group* of degree n if $G \leq$ X with $|Z| = n$.

Example.

1. $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n, as is $A_n \leq S_n$.
2. D_{2n}, the symmetries of regular n-gon, is a subgroup of $\mathrm{Sym}(n)$.

Definition 1.10. An *action* of a group G on a set X is a function $* : G \times X \to X$ satisfying

1. $e * x = x$ for all $x \in X$,
2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G, x \in X$.

Proposition 1.2. An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. For each $g \in G$ let $\phi_g : X \to X$, $x \mapsto g * x$. We have

$$\begin{aligned}\phi_{g_1 g_2}(x) &= (g_1 g_2) * x \\ &= g_1 * (g_2 * x) \\ &= \phi_{g_1}(g_2 * x) \\ &= \phi_{g_1} \circ \phi_{g_2}(x).\end{aligned}$$

Thus, $\phi_{g_1 g_2} = \phi_{g_1}\phi_{g_2}$.

In particular $\phi_{g_1} \circ \phi_{g_1^{-1}} = \phi_{g_1^{-1}} \circ \phi_{g_1} = \phi_e = id_X$.

Because ϕ_g has an inverse, it is bijective. So $\phi_g \in \mathrm{Sym}(X)$. Define

$$\begin{aligned}\phi\colon G &\longrightarrow \mathrm{Sym}(X) \\ g &\longmapsto \phi_g\end{aligned}$$

which is indeed a group homomorphism.

Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a gruop homomorphism.

Define

$$\begin{aligned}*\colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto \phi(g)(x).\end{aligned}$$

Then it does satisfy the requirements for a group action,

1. $e * x = \phi(e)(x) = id_X(x) = x$,
2. $\begin{aligned}(g_1 g_2) * x &= \phi(g_1 g_2)(x) \\ &= \phi(g_1)(\phi(g_2)(x)) \\ &= g_1 * (g_2 * x).\end{aligned}$

■

Definition 1.11. We say $\phi : G \to \mathrm{Sym}(X)$ is a *permutation representation* of G.

Definition 1.12. Let G act on a set X.

1. The *orbit* of $x \in X$ is $\mathrm{orb}_G(x) = \{g * x \mid g \in G\} \subseteq X$
2. the *stabilizer* of $x \in X$ is $G_x = \{g \in G \mid g * x = x\} \leq G$.

Recalled from IA, we have the Orbit-Stabilizer Theorem. There is a bijection $\mathrm{orb}_G(x) \leftrightarrow {}^{G}/_{G_x}$, the set of left cosets in G.

In particular, if G is finite, then

$$|G| = |\mathrm{orb}_G(x)||G_x|.$$

Example. Let G be the group of all symmetries of a cube, and X be the set of vertices. Let $x \in X$ be any vertex $|\mathrm{orb}_G(x)| = 8, |G_x| = 8$. So $|G| = 48$.

Remark.

1. $\ker \phi = \cap_{x \in X} G_x$ is called the *kernel* of the group action.
2. The orbits partition X. We say that the action is *transitive* if there is just one orbit.
3. $G_{g*x} = gG_x g^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilizers are conjugate.

Example.

1. Let G act on itself by left multiplication. That is, $g * x = gx$. The kernel of this action is

$$\{g \in G \mid g * x = x \ \forall x \in G\} = \mathbf{1}.$$

Thus, G injects into $\mathrm{Sym}(G)$. This proves,

Theorem 1.5 (Cayley's Theorem). Any finite group G is isomorphic to a subgroup of S_n for some n (take $n = |G|$).

2. Let $H \leq G$, G acts on ${}^{G}/_{H}$, the set of left cosets, by left multiplication. That is $g * xH = gxH$.

This action is transitive (since $(x_2 x_1^{-1}) x_1 H = x_2 H$) with

$$\begin{aligned} G_{xH} &= \{g \in G \mid gxH = xH\} \\ &= \{g \in G \mid x^{-1} g x \in H\} \\ &= xHx^{-1}. \end{aligned}$$

Thus, $\ker(\phi) = \cap_{x \in G} xHx^{-1}$. This is the largest normal subgroup of G that is contained in H

Theorem 1.6. Let G be a non-Abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq 5$ and G is isomorphic to a subgroup of A_n.

Proof. Let G act on $X = {}^{G}/_{H}$ by left coset multiplication, and let $\phi : G \to \mathrm{Sym}(X)$ be associated permutation representation.

As G is simple, $\ker(\phi) = \mathbf{1}$ or G. Since G acts transitively on X and $|X| > 1$, $\ker(\phi) = \mathbf{1}$ and $G \cong \mathrm{Im}(\phi) \leq S_n$.

Since $G \leq S_n$ and A_n is a normal subgroup of S_n. The Second Isomorphism Theorem gives $G \cap A_n \cong {}^{GA_n}/_{A_n} \leq {}^{S_n}/_{A_n} \cong C_2$. Because G is simple, we have $G \cap A_n = 1$ or G. If the intersection is trivial, we have an injection into C_2 by First Isomorphism Theorem, but G is non-Abelian. So we must have

$$G \cap A_n = G \implies G \leq A_n.$$

Finally, if $n \leq 4$, it is easy to check that A_n does not have non-Abelian simple subgroups. So we must have $n > 5$. ■