Group Theory Notes

Leon Lee

October 7, 2024

Contents

1 Recapping from previous courses

1.1 Groups, Subgroups, Cosets, oh my!

Definition 1.1.1: Group

A **group** consists of a set G together with a function $G \times G \to G$ which maps an ordered pair $(g, h) \in G \times G$ to an element $g * h \in G$. The following axioms must be satisfied:

1. **Associativity**: $(g * h) * k = g * (h * k)$ for each triple $(g, h, k) \in G \times G \times G$
2. **Identity**: There is an element $e \in G$ s.t. $e * g = g = g * e$ for each element $g \in G$
3. **Inverse**: To each element $g \in G$ there is an element $h \in G$ s.t. $gh = e = hg$

Every single course seems to have its own definition for a group, this one is a bit more compact than others. FPM had the **closure** axiom, but that is satisfied by the definition of the function $G \times G \to G$

Note on notation: Usually just write gh instead of $g * h$. Additionally g^{-1} is the inverse of g

Definition 1.3.1: Subgroups

If H is a nonempty subset of G, then H is a **subgroup** provided that

1. $hk \in H$ for all $h, k \in H$
2. $h^{-1} \in H$ for each $h \in H$

Alternatively, we can say "H is closed under the group operation"

Notation

- $H \leq G$ means H is a subgroup of G, whereas $H \subseteq G$ means H is a subset of G.
- $H < G$ means that H is a subgroup of G and also $H \neq G$.
- A subgroup is **proper** if $H \neq G$
- A subgroup is **non-trivial** if $H \neq \{e\}$

Note: $e \in H$ follows from the definition, and associativity follows from the fact that G is a group. Any subgroup H of G is a group using the same product as G

Definition 1.3.6: Cosets

Let $H \leq G$ and let $g \in G$. Then the **left coset of H determined by** g is the set $gH := \{gh : h \in H\}$. $Hg := \{hg : h \in H\}$ is the **right coset of H determined by** g

Notation

- The set of left cosets of H is denoted G/H, the set of right cosets is denoted $H\backslash G$.
- The number of elements in a group G is denoted by $\#G$ or $|G|$, and is known as the **order** of G. We will use $|G|$ in this course.
- The number of left cosets of a subgroup H of G is the **index** of H in G and is denoted by $|G : H|$ or $[G : H]$ (That is, $[G : H] = |G/H|$). We will use $[G : H]$ in this course.

Theorem 1.1.1: Coset Lemmas

If H if finite, $|gH| = |H|$
If $g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$

Theorem 1.3.8: Lagrange's Theorem

Let H be a subgroup of a finite group G. Then

$$|G| = [G : H] \cdot |H|$$

Consequences and Results

- The order of a subgroup must divide the order of the group, e.g. A group of order 12 cannot have a subgroup of order 8
- The converse of Lagrange's Theorem is false, e.g. there is a group of order 12 that doesn't have a subgroup of order 6

Example: If $G = S_3$ and $H = \{e, (12)\}$, what are the left cosets of H?

$$H = eH = \{e, (12)\} \quad \{(23), (132)\} \quad \{(13), (123)\}$$

Example: If $H \triangle G$ then the left cosets are right cosets

Proof.

$$gH = \{gh : h \in H\} = \{(ghg^{-1})g : h \in H\} \subseteq Hg$$

□

Theorem 1.3.9: Cauchy's Theorem

If G is a finite group and p is a prime that divides the order of G, then G has a subgroup of order p

Definition 1.3.10: Order of an element

Let $g \in G$. The **order** of g is the least positive integer such that $g^n = g$ or ∞ if such n does not exist. We write the order of g as $o(g)$. Note that $o(g) = |\langle g \rangle|$.
It thus follows from Lagrange's Theorem that the order of an element of G must divide $|G|$, since if $o(g) = n$ then $\langle g \rangle = \{g, g^2, \dots, g^n = e\}$ is a subgroup of G. We also have:

Corollary 1.3.11: If $|G|$ is prime, then G is cyclic

Example A: Examples of Groups and Subgroups

- $\mathbb{Z}/n$ under addition, where $a * b = a + b \mod n$
- $(\mathbb{R}\backslash\{0\}, \times)$, or $K\backslash\{0\}$ for any field K
- Alternating group: $A_n \subset S_n$ - permutations from an even number of transpositions?

1.2.1 S_n, the n**-th symmetric group** is the group of permutations of $\{1, 2, \dots, n\}$. The group operation is composition of fucntions

1.2.6 A group $(G, *)$ is **abelian** if $g * h = h * g$ for all $g, h \in G$

- Let F be a field
  - The **general linear group** $GL(n, F)$ is the set of all invertible $n \times n$ matrices
  - The **special linear group** $SL(n, F)$ is the set of all invertible $n \times n$ matrices with determinant equal to 1

1.3.5 Let G be a group and let $g \in G$. Then $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G. It is called the **subgroup generated by** g. If $G = \langle g \rangle$ for some $g \in G$, then G is referred to as **cyclic**

1.3.7 A *subgroup* $H \leq G$ is **normal** if $gH = Hg$ for all $g \in G$. In this case we write $H \trianglelefteq G$

1.2 Group Homomorphisms

Definition 1.4.1: Group Homomorphism

Let G, H be groups. A function $\phi : G \to H$ such that

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$ is a **group homomorphism**

Example: If ϕ is a group homomorphism then $\phi(e) = e$

Proof.

$$\begin{aligned} \phi(e \cdot e) &= \phi(e)\phi(e) \\ \implies \phi(e) &= \phi(e)\phi(e) \\ \text{multiply by } \phi(e)^{-1} \quad e &= \phi(e)^{-1}\phi(e)\phi(e) = \phi(e) \end{aligned}$$

□

Example: Show $\phi(g^{-1}) = \phi(g)^{-1}$

Proof.

$$\begin{aligned} \phi(g \cdot g^{-1}) &= \phi(g)\phi(g^{-1}) \\ \phi(e) &= \phi(g)\phi(g^{-1}) \\ \text{Multiply by } \phi(g)^{-1} \quad \phi(g)^{-1}\phi(e) &= \phi(g)^{-1}\phi(g)\phi(g^{-1}) \\ \phi(g)^{-1} &= \phi(g^{-1}) \end{aligned}$$

□

Example 1.4.2: Cyclic Group Homomorphisms

Let C_n be the **cyclic group of order** n. We can think of C_n as the set of rotations of an equilaterial n-gon. If g is a rotation of $2\pi/n$ radians, then $C_n = \{g, g^2, \ldots, g^n = e\}$. The group C_n is cyclic since all elements are powers of a single element g. Then

$$\begin{aligned} \phi : \mathbb{Z} &\to C_n \\ a &\mapsto g^a \end{aligned}$$

is a group homomorphism. (proof in lecture notes)

Definition 1.4.3: Group Isomorphism

If G and H are groups and $\psi : G \to H$ is a bijective *group homomorphism*, we say that ψ is a **group isomorphism** and that G and H are **isomorphic**

Definition 1.4.5: Kernel of a Homomorphism

Let $\phi : G \to H$ be a group homomorphism. The **kernel** of ϕ is $\{g \to G : \phi(g) = e\}$

Definition 1.4.6: Automorphisms

Let G be a group. The st of all isomorphisms $\phi : G \to G$ is also a group. It is called the **automorphism group of** G, and is written $\mathrm{Aut}(G)$. The group operation is composition of functions

Example: What is $\mathrm{Aut}(C_3)$?

Proof.

$$C_3 = \{e, r, r^{-1}\}$$

$\square$

Definition 1.4.8: Direct Product

Let G, H be groups. The **product** (or **direct product**) $G \times H$ is a group, with group operation $*$ given by

$$(g, h) * (g', h') = (g *_G g', h *_G h')$$

Note: we usually just say that $(g, h) * (g', h') = (gg', hh')$

1.3 something...

Let $H \leq G$ (H a subgroup of G). TFAE

1. $\forall g \in G, h \in H$, $ghg^{-1} \in H$
2. $gHg^{-1} = H$, $\forall g \in G$
3. $gH = Hg$, $\forall g \in G$

Proof. Show conditions imply each other

- (2) $\implies$ (1) immediately
- (1) says that $gHg^{-1} \subseteq H$, $\forall g \in G$
  WTS: $gHg^{-1} \supseteq H$
  $$H = g^{-1}gHg^{-1}g \subseteq g^{-1}Hg, \forall g \in G$$
  replacing g with g^{-1}:
  $$H \subseteq gHg^{-1}, \forall g \in G$$
- (2) $\implies$ (3): Multiply by g on right
  (3) $\implies$ (2): Multiply by g^{-1} on left

$\square$

Theorem 1.3.1: lma

If $\phi : G \to H$ is a group homomorphism, then $\ker \phi \triangle G$

Proof. If $\phi(x) = e$, then

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g) = \phi(g)e\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$$

$\square$

Theorem 1.3.2

If $N \leq G$, then $N \triangleleft G$ iff $\exists \phi : G \to H$ s.t. $N = \ker \phi$

Proof. $\ker \phi$ is normal by the above lemma
Conversely, given $N \triangleleft G$, we can form **factor group** G/N
G/N is the set of left cosets, with:

- Identity N
- Inverses $(gN)^{-1} : g^{-1}N$
- Multiplication: $(g_1N) \times (g_2N) := g_1g_2N$

Check that the group is well defined

1. If $gN = g'N$, then $g' = gx$ for $x \in N$

$$(g'N)^{-1} = (g')^{-1}N = (gx)^{-1}N = x^{-1}g^{-1}N$$

   As N is normal, $gx^{-1}g^{-1} \in N$

$$\implies x^{-1}g^{-1}N = g^{-1}(gx^{-1}g^{-1})N = g^{-1}N, \text{ as } gx^{-1}g^{-1} \in N$$

2. If $g_1N = g_1'N$ and $g_2N = g_2'N$, then $g_1' = g_1x$ and $g_2' = g_2y$ for $x, y \in N$

$$(g_1'N) \times (g_2'N) = g_1'g_2'N = g_1xg_2yN$$

$$yN = N, \quad \text{so} \quad g_1xg_2y_1N = g_1xg_2N$$

   N normal, so $g_2^{-1}xg_2 \in N \implies g_1g_2(g_2^{-1}xg_2)N = g_1g_2N$

then prove the group axioms lol

Define $\text{can} : G \to G/N$, $g \mapsto gN$. This is a group homomorphism

$$\text{can}(g_1g_2) = g_1g_2N = (g_1N) * (g_2N) = \text{can}(g_1) * \text{can}(g_2)$$

Kernel of can

$$\ker(\text{can}) = \{g \in G : \text{can}(g) = N\} = \{g \in G : gN = N\} = N$$

□

Example: If $G = \mathbb{Z}$, (normal) subgroups are $n\mathbb{Z} = \{ni : i \in \mathbb{Z}\}$. What is $\mathbb{Z}/n\mathbb{Z}$?
Elements of $\mathbb{Z}/n\mathbb{Z}$ are cosets, $i + n\mathbb{Z}$ (fixed i), or $\{x \in \mathbb{Z} : x \equiv i \mod n\}$
Group operation: $(i + n\mathbb{Z}) * (j + n\mathbb{Z}) = i + j + n\mathbb{Z} = i + j \mod n$
soooo... $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n$, where elements are $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}$
lol !

1.4 First Isomorphism Theorem and stuff

Theorem 1.4.1: First Isomorphism Theorem

If $\theta : G \to H$ a group homomorphism, then:

- $\mathrm{im}(\theta)$ is a subgroup of H
- $\ker(\theta) \triangleleft G$
- $\exists$ a group homomorphism $\overline{\theta} : \theta / \ker\theta \tilde{\to} \mathrm{im}(\theta)$

Proof. Prove all 3

- If $\theta(a), \theta(b) \in \mathrm{im}(\theta)$, then $\theta(a)\theta(b) = \theta(ab) \in \mathrm{im}(\theta)$
  $\theta(a)^{-1} = \theta(a^{-1}) \in \mathrm{im}(\theta)$ thererfore $\mathrm{im}(\theta) \leq H$
- Already $\ker(\theta) \triangleleft G$
- Let $N = \ker(\theta)$. Then $gN \in G/N$. Define $\overline{\theta}(gN) := \theta(g)$.
  Well defined: If $gN = g'N$, then $g' = gx$ for some $x \in N$. Then $\overline{\theta}(g'N) = \theta(g') = \theta(g)\theta(x) = \theta(g)e$ as $x \in \ker(\theta) = \theta(g)$

$\square$

Ex 1: $\theta : \mathbb{C} \to \mathbb{C}\ \{0\}$

Theorem 1.4.2: Property of Finite Groups

Lf $N \triangleleft$, then for any homomorphism $\psi : G \to H$ with $N \subseteq \ker\psi$. $\exists$ a group homomorphism $\overline{\psi} : G/N \to H$ s.t. $\psi = \overline{\psi} \circ \mathrm{can}$

If $\psi : G \to K$ surjective...? $\psi : G \to H$ with $\ker\phi \subseteq \ker\psi$, then @$\exists$ $\overline{\psi} : K \to H$ s.t. $\psi = \overline{\psi} \circ \psi$

Theorem 1.4.3

Let $N \triangleleft G$, can $G \to G/N$ and $K \leq G/N$

1. $\mathrm{can}^{-1}(K) \leq G$ with $\mathrm{can}^{-1}(K) \geq N$
2. $\mathrm{can}^{-1}(K) \triangleleft G \iff K \triangleleft G/N$

Theorem 1.4.4: Correspondence Theorem

If we have $N \triangleleft G$, $\mathrm{can} : G \to G/N$, then:

- $H \to \mathrm{can}(H)$ gives a bijection between subgroups of G/N and subgroups of G containing N
- Normal subgroups of G containing $N \iff$ normal subgroups of G/N
- If $A, B \leq G$ with $N \subseteq A, N \subseteq B$, then: $A \subseteq B$ iff $\mathrm{can}(A) \subseteq \mathrm{can}(B)$

Proof. Given $K < G/N$, $can^{-1}K \leq G$ and $N \leq \text{can}^{-1} K$ since $\text{can}^{-1}\{e\} = N$
Last prop says: $\text{can}^{-1}\text{can}(H) = H$ when $N \subseteq H$

$$\text{can}(\text{can}^{-1} K) \subseteq K$$

Since can is surjective, $\forall x \in K$, $\exists y \in G$ s.t. $\text{can}(y) = x$. Then $y \in can^{-1}K$ so $x \in \text{can}(\text{can}^{-1} K)$
So, $\text{can}(\text{can}^{-1} K) = K$ since can is surjective. Therefore can & can^{-1} give a bijection

$$\{\text{subgroups of } G \text{ containing } N\} \leftrightsquigarrow \{\text{subgroups of } G/N\}$$

$\square$

1.4.5 Recap of last time (which is not on the notes)

- $\text{can}(H) \triangleleft G/N \iff H \triangleleft G$
- If $A \subseteq B$ then $\text{can}(K) \subseteq \text{can}(B)$
  Conversely, if $\text{can}(A) \subseteq \text{can}(B)$ then $\text{can}^{-1} \underbrace{\text{can}}_{=A}(A) \subseteq can^{-1} \underbrace{\text{can}}_{=B}(B)$

Definition 1.4.6: Random notation

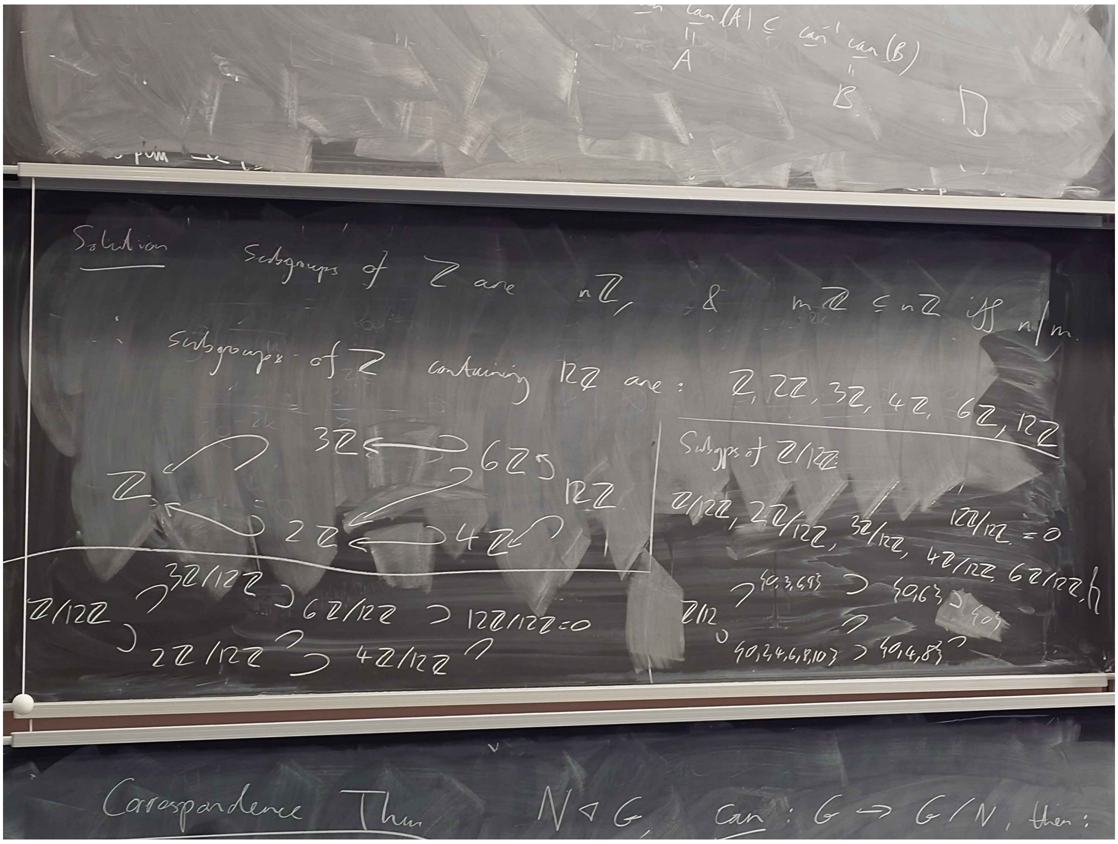
- $\exists$: There exists
- $\exists!$: There exists unique
- $\nexists$: there does not exist

Example: Let $G = \mathbb{Z}$, $N = 12\mathbb{Z}$.

- Find all subgroups of G containing N and all inclusions between them
- Find all subgroups of $\mathbb{Z}/12$

Solution: Subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. $m\mathbb{Z} \subseteq n\mathbb{Z}$ iff n/m
Therefore, subgroups of $\mathbb{Z}$ containing $12\mathbb{Z}$ are:

$$\mathbb{Z},\ 2\mathbb{Z},\ 3\mathbb{Z},\ 4\mathbb{Z},\ 6\mathbb{Z},\ 12\mathbb{Z}$$



Subgroups of $\mathbb{Z}/12\mathbb{Z}$:

$$12\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},\ 2\mathbb{Z}/12\mathbb{Z},\ 3\mathbb{Z}/12\mathbb{Z},\ 4\mathbb{Z}/12\mathbb{Z},\ 6\mathbb{Z}/12\mathbb{Z}$$

some working out

Theorem 1.4.7: Third Isomorphism Theorem

If $N, H \triangleleft G$, with $N \leq H$, then

$$(G/N)/(H/N) \cong G/H$$

Proof. $N \leq \ker(\mathrm{can}_H) = H$, so $\exists! \pi$ by universal property of finite groups
π is surjective, because can_H is isomorphic
Explicitly,

$$\pi(gN) = gH = \pi(\mathrm{can}_N(g)) = \mathrm{can}_H(g)$$

$\ker(\pi) = \{gN : g \in H\} = H/N$
By the first isomorphism theorem,

$$G/H \equiv (G/N)/\ker \pi = (G/N)/(H/N)$$

$\square$

Theorem 1.4.8: Second Isormorphism Theorem

Let $N \triangleleft G$ and $H \leq G$. Then:

1. $HN \leq G$
2. $N \triangleleft HN$
3. $H \cap N \triangleleft H$
4. $HN/N \equiv H/H \cap N$

Proof. Let $h_1 h_2 \in H$, $n_1 n_2 \in N$

1. $$h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{(h_2^{-1} n_1 h_2) n_2}_{\in N}$$
$$(hn)^{-1} = n^{-1} h^{-1} = \underbrace{h^{-1}}_{\in H} \underbrace{(hn^{-1} h^{-1})}_{\in N}$$

2. If $g \in HN$ and $n \in N$, then $g \cap g^{-1} \in n$ since $g \in G$

3. If $x \in H \cap N$ and $h \in H$, then $\underbrace{hxh^{-1}}_{N \triangleleft G} \in N$ and $\underbrace{hxh^{-1}}_{x \in H} \in H$

4. Need $\theta : H \to HN/N$ surjective with kernel $H \cap N$

   Let $\theta(h) = hN$ i.e. $\theta = \mathrm{can}_N \big|_H$, $(\mathrm{can}_N\, G \to G/N)$

   Surjective: cosets of HN/N are cosets xN for $x \in HN$ but $x = hn$, $h \in H$, $n \in N$ and $xN = hN = \theta(n)$ (wtf?)

   Kernel: If $\theta(h) = e$, $kN = N$, so $h \in N$, so $\ker \theta = H \cap N$, so by the correspondence theorem,
   $$H/H \cap N \subseteq HN/N$$

□

2 Group Actions

Definition 2.0.1: Free Group

The **free group on generators** $x_1, \ldots, x_m$ is the group whose elements are words in the symbols $x_1, \ldots, x_m, x_1^{-1}, \ldots, x_m^{-1}$, subject to the group axioms and all logical consequences. The group operation is concatenation. The free group is written

$$\langle x_1, \ldots, x_m \rangle$$

Example: Find presentations for:

- $\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle = \langle x, y \mid xyx^{-1}y^{-1} = e \rangle \cong \{x^i y^i = i, j \in \mathbb{Z}\}$

Example 2.0.2: Random group action E

Let

$$E = \langle a, b \mid a^2, b^5, (ab)^2 \rangle$$

Lemma 2.0.3

Any element $x \in E$ can be written $x = a^i b^j$, where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4\}$

Lemma 2.0.4

Group homomorphisms

$$\phi : \langle x_1, \ldots, x_n \mid r_1(\underline{x}), \ldots, r_n(\underline{x}) \rangle \to G$$

correspond to multiples $(g_1, \ldots, g_m) \in G^m$ s.t. $r_1(\underline{g}) = e, \ldots, r_n(\underline{g})$

Example: For $E = \langle a, b \mid a^2, b^5, (ab)^2 \rangle$
Group homomorphism - $Q : E \to G$ correspond to:

$$(g, h) \in G \times G \quad \text{s.t.} \quad g^2 = e,\, h^5 = e,\, (gh)^2 = e$$

In particular, we have:

$$\begin{aligned} \phi : E &\to D_5 \\ b &\mapsto \text{rotation} \\ a &\mapsto \text{reflection} \end{aligned}$$

We also have that $\text{im}(Q) = D_5$, and Q surjective

Definition 2.0.5: Reduced Word

A word $x^{m_1} y^{n_1} x^{m_2} y^{n_2} \ldots x^{m_k} y^{n_k}$ is **reduced** if no $m_i, n_j = 0$ except possibly for m_1 or n_k (That is, a word doesn't need to start with a power of x or end with a power of y)

Lemma 2.0.6

Every element of $\langle x, y \rangle$ has a unique expansion as a reduced word