Group Theory Notes

Leon Lee

September 19, 2024

Contents

1 Recapping from previous courses **3**
1.1 Groups, Subgroups, Cosets, oh my! 3
1.2 Group Homomorphisms 6

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 $\langle g \rangle = \{g, g^2, \ldots, g^n = e\}$ 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 $\{1, 2, \ldots, n\}$. 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 $C_n = \{g, g^2, \dots, g^n = e\}$. 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.

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

□

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 $(g, h) * (g', h') = (gg', hh')$