

MAT3004 Lecture 7 Notes: Homomorphisms, Cosets, and Lagrange's Theorem

Transcription

1 Recall: Homomorphisms and Isomorphisms

Let $\phi : G \rightarrow H$ be a **homomorphism**.

$$\text{If } \phi(g_1 \times g_2) = \phi(g_1) \star \phi(g_2).$$

If ϕ is bijective, then ϕ is an **isomorphism**, and we write:

$$G \cong H$$

If $G \cong H$, then:

$$G \text{ is abelian} \iff H \text{ is abelian}$$

$$G \text{ is cyclic} \iff H \text{ is cyclic}$$

The algebraic structure of G and H are the same.

—

2 Classification Theorems

Some classification theorems classifying G up to isomorphism.

2.1 1. If G is Cyclic

$$G \cong \mathbb{Z} \quad \text{or} \quad G \cong \mathbb{Z}_n$$

Example 1. $A_3 = \{e, (123), (132)\} \neq \mathbb{Z}_3$ (as sets), but $A_3 \cong \mathbb{Z}_3$.

Sketch Proof: Let $G = \langle g \rangle$.

Case 1: $|G| = \infty$. Then $\text{ord}(g) = \infty$. Consider $\psi : \mathbb{Z} \rightarrow G$ defined by $\psi(j) = g^j$. Then ψ is a homomorphism and surjective. Suppose on the contrary ψ is NOT injective, then $\psi(j) = g^j = g^k = \psi(k)$ for $j \neq k$. This leads to a contradiction regarding the infinite order.

Case 2: $|G| = n$. Then $\text{ord}(g) = n$. $G = \{e, g, g^2, \dots, g^{n-1}\}$. Consider $\phi : G \rightarrow \mathbb{Z}_n$ defined by $\phi(g^i) = [i]_n$.

2.2 2. If $|G| = p$ (p is prime)

$$G \cong \mathbb{Z}_p$$

(This follows from Lagrange's Theorem).

2.3 3. If $|G| = p^2$ (p is prime)

$$G \cong \mathbb{Z}_{p^2} \quad \text{or} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

(Recall from last lecture: $\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \times \mathbb{Z}_p$).

2.4 Question: How about $|G| = pq$ where $p \neq q$ are primes?

e.g., $|G| = 6$.

$$G \cong \mathbb{Z}_6 \quad \text{or} \quad G \cong S_3$$

2.5 4. Finite Abelian Groups

If $|G| < \infty$ and G is abelian. (To be covered later in this course).

—

3 Lagrange's Theorem and Equivalence Relations

3.1 Recap: Equivalence Class on a Set

Let S be a set. " \sim " is an **equivalence relation** on S if $\forall a, b, c \in S$:

- (i) $a \sim a$ (Reflexivity)

- (ii) $a \sim b \implies b \sim a$ (Symmetry)
- (iii) If $a \sim b$ and $b \sim c \implies a \sim c$ (Transitivity)

3.2 Examples

(1) Let $S = \mathbb{R}^2$. For $x, y \in \mathbb{R}^2$:

$$x \sim y \iff |x| = |y|$$

This is an equivalence relation.

$$x \sim y \iff |x| = |y|$$

$$y \sim z \iff |y| = |z|$$

$$x \sim z \iff |x| = |z|$$

(2) Let $S = S_n$. For $\sigma, \tau \in S_n$:

$$\sigma \sim \tau \iff \sigma \cdot \tau \text{ is even}$$

(Note: This implies they have the same parity).

- e.g., for all $\sigma \in S_n$, $\sigma \cdot \sigma$ is always even $\implies \sigma \sim \sigma$.

3.3 Equivalence Classes

Definition 1. Let \sim be an equivalence relation on S . An **equivalence class** (representative $a \in S$) is:

$$C_a = \{b \in S \mid a \sim b\}$$

Examples revisited:

(1) As before, $S = \mathbb{R}^2$.

$$C_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \left\{ \vec{x} \in \mathbb{R}^2 \mid |\vec{x}| = \left| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| = 1 \right\}$$

$C_{(a>0)} = \{x \mid |x| = a\}$. *Pictorially:* These form concentric circles around the origin.

(2) As before, $S = S_n$. If $\sigma \in S_n$ is even, then:

$$C_\sigma = \{\tau \mid \sigma\tau \text{ is even}\} = \{\text{all even permutations}\} = A_n$$

Similarly, if σ' is odd, then:

$$C_{\sigma'} = \{\text{all odd permutations}\} = S_n \setminus A_n$$

Remark 1. • If $a \sim a'$, then $C_a = C_{a'}$.

• If $a \not\sim a'$, then $C_a \cap C_{a'} = \emptyset$ (is disjoint).

So we can partition S into disjoint equivalence classes:

$$S = C_a \sqcup C_b \sqcup C_c \sqcup \dots$$

—

4 Equivalence Relation in Groups

Proposition 1. Let G be a group and $H \leq G$ (H is a subgroup of G). For $a, b \in G$:

$$a \sim b \iff a^{-1}b \in H$$

is an equivalence relation on $S = G$.

Proof. (i) **Reflexive:** $a \sim a$

$$a^{-1}a = e \in H \implies a \sim a$$

(Since $H \leq G$, it contains the identity).

(ii) **Symmetric:** $a \sim b \implies b \sim a$

$$a \sim b \iff a^{-1}b \in H$$

Since H is a subgroup, it is closed under inverses:

$$\begin{aligned} (a^{-1}b)^{-1} \in H &\implies b^{-1}(a^{-1})^{-1} \in H \implies b^{-1}a \in H \\ &\iff b \sim a \end{aligned}$$

(iii) **Transitive:** $a \sim b$ and $b \sim c \implies a \sim c$. (Proof omitted in notes, but follows from closure of H). \square

—

5 Left Cosets

Definition 2. Let $H \leq G$ be given. A **Left Coset** with representative $a \in G$ is the equivalence class:

$$\begin{aligned} aH &:= C_a = \{b \mid a \sim b\} \\ &= \{b \mid a^{-1}b = h, \text{ for some } h \in H\} \\ &= \{b \mid b = ah, h \in H\} \\ &= \{ah \mid h \in H\} \end{aligned}$$

5.1 Examples of Cosets

(1) $G = (\mathbb{Z}, +)$ (or $G = \mathbb{Z}_n$ contextually). Let $H = \langle 7 \rangle = 7\mathbb{Z}$. Then:

$$\begin{aligned} 1 + H &= \{1 + h \mid h \in H\} \\ \implies 1 + 7\mathbb{Z} &= \{1 + 7k \mid k \in \mathbb{Z}\} \end{aligned}$$

(Note that $1 \sim 8$, since $-1 + 8 = 7 \in 7\mathbb{Z}$. So $1 + 7\mathbb{Z} = 8 + 7\mathbb{Z}$ as in the Remark).

Also, we have the partition:

$$\mathbb{Z} = (0 + 7\mathbb{Z}) \sqcup (1 + 7\mathbb{Z}) \sqcup \cdots \sqcup (6 + 7\mathbb{Z})$$

(2) $G = S_3$, $H = \langle (13) \rangle = \{e, (13)\}$. Then the left cosets are:

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

(3) $G = S_n$, $H = A_n$. Then:

$$\begin{aligned} eA_n &= \{e\sigma \mid \sigma \text{ is even}\} = \{\text{all even perms}\} \\ &= (\sigma A_n \text{ for even } \sigma) \end{aligned}$$

And for τ a transposition (odd):

$$\tau A_n = \{\tau\sigma \mid \sigma \text{ is even}\} = \{\text{all odd permutations}\}$$

Question: Let $\gamma \in S_n$ be odd. Can we express $\gamma = \tau\sigma$ for some σ even?

Answer: Yes, take $\sigma = \tau^{-1}\gamma$. Since τ is a transposition (odd) and γ is odd:

$$\text{odd}^{-1} \cdot \text{odd} \implies \text{odd} \cdot \text{odd} = \text{even}$$

Therefore:

$$S_n = eA_n \sqcup \tau A_n$$

6 Right Cosets

Remark 2. Similarly, we can define another equivalence relation:

$$a \sim_R b \iff ba^{-1} \in H$$

In this case, the equivalence classes are called **right cosets**:

$$Ha := \tilde{C}_a = \{ha \mid h \in H\}$$

—

7 Lagrange's Theorem

Theorem 1 (Lagrange). *Let G be a finite group, and $H \leq G$ be any subgroup. Then $|H|$ divides $|G|$ ($|H| \mid |G|$).*

Example 2. *If $|G| = 10$, there are no $H \leq G$ with $|H| = 3, 4, 6$.*

Proof. Partition G into left cosets (we can do so since left cosets are equivalence classes):

$$G = eH \sqcup a_2H \sqcup \cdots \sqcup a_mH$$

This implies:

$$|G| = |eH| + |a_2H| + \cdots + |a_mH|$$

Claim 1. $|a_iH| = |eH| = |H|$ for all i . (All cosets have the same size).

Therefore:

$$\begin{aligned} |G| &= |H| + |H| + \cdots + |H| \quad (m \text{ times}) \\ &= m|H| \end{aligned}$$

Which implies $|H| \mid |G|$. □