Lecture 2 Cosets, quotient groups, homomorphisms

Development of mathematical concepts

Vector spaces	Groups
direct sums	direct product of groups ✓
subspaces	subgroups ✓
linear isomorphism	isomorphism ✓
affine translates of subspaces	cosets
quotient spaces	quotient groups
linear maps	homomorphisms

Definition Let H be a subgroup of G, A (left) coset (左陪集) is a set of the form for some $g \in G$, $gH := \{gh;\ h \in H\}$. ← kind of "product of two sets"

gH = left coset of g.

(in particular, if $g \in H$, $gH = H$.)

A right coset (右陪集) is a set of the form, for some $g \in G$

$$Hg := \{hg\ ;\ h \in H\}$$

Remark: For abelian groups, there's no distinction between left and right cosets

(If using additive convention, it is written $g+H$.)

Proposition. Two (left) cosets g_1H and g_2H are

either equal $\Leftrightarrow g_1^{-1}g_2 \in H$

or disjoint $\Leftrightarrow g_1^{-1}g_2 \notin H$

Proof: Need to prove $g_1H \cap g_2H \neq \phi \overset{①}{\Longrightarrow} g_1^{-1}g_2 \in H \overset{②}{\Longrightarrow} g_1H = g_2H$

obvious

② If $g_1^{-1}g_2 \in H \Rightarrow g_1H = g_1(\underbrace{g_1^{-1}g_2}\cdot H) = g_2H$

↳ b/c any element $h \in H$, $hH = H$

① If $g_1H \cap g_2H \neq \phi$, say $x = g_1h_1 = g_2h_2$ for $h_1, h_2 \in H$

Then $g_1 = xh_1^{-1}$, $g_2 = xh_2^{-1} \Rightarrow g_1^{-1}g_2 = (xh_1^{-1})^{-1}xh_2^{-1}$

$= h_1 \cdot x^{-1}xh_2^{-1} = h_1h_2^{-1} \in H$ □

Definition. Write $G/H := \{gH \mid g \in G\}$ for the set of left cosets

Similarly, $H\backslash G = \{Hg \mid g \in G\}$

Lemma $\Rightarrow$ $G = \coprod_{gH \in G/H} gH$ is a disjoint union

We call $\#(G/H) =: [G:H]$ the index of H as a subgroup of G.

Lagrange's Theorem. If G is a finite group and $H \leqslant G$, then $\#H \mid \#G$

Proof: In fact, $\#(G/H) = \#G/\#H$. □

Cor. (1) If G is a finite group, then $|x| \mid \#G$

Proof: $|x| = \#\langle x \rangle \mid \#G$. □

(2) $x^{\#G} = e$.

Example. $G = (\mathbb{Z}/N\mathbb{Z})^{\times} = \{a \bmod N \mid \gcd(a,N) = 1\}$, $\#G = \varphi(N)$

Then for every $a \in (\mathbb{Z}/N\mathbb{Z})^{\times}$, $a^{\varphi(N)} \equiv 1 \bmod N$ (Euler's theorem)

Cor. If $\#G = p$ is a prime, then G is cyclic ($\Rightarrow$ abelian)

Proof: Take $\overset{\overset{e}{\times}}{x} \in G$, then $\overset{\overset{1}{\times}}{|x|} \,\Big|\, \#G = p$, $\Rightarrow |x| = p \Rightarrow G = \langle x \rangle$.

<u>Definition</u> Let G be a group, $a, g \in G$, gag^{-1} is called the <u>conjugate of a by g</u> (共轭)

<u>Lemma</u>. If H is a subgroup of G and $g \in G$, then gHg^{-1} is a subgroup

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

called the <u>conjugate of H by g</u>

Proof: Given $gag^{-1}, gbg^{-1} \in gHg^{-1}$,

$$(gag^{-1})(gbg^{-1})^{-1} = ga\cancel{g^{-1}\cdot(g^{-1})^{-1}}b^{-1}g^{-1} = gab^{-1}g^{-1} \in gHg^{-1} \ \checkmark \quad \square$$

<u>Definition</u>. A subgroup $H \leqslant G$ is <u>normal</u> if $\forall g \in G$, $H = gHg^{-1}$

(i.e. all conjugates of H are just H itself.)

($\Leftrightarrow gH = Hg$, so left coset of g is the same as right coset of g.)

- We write $H \trianglelefteq G$ to indicate normal subgroups.

  (E.g. $\{1\} \trianglelefteq G$, $G \trianglelefteq G$)

- In particular, all subgroups of an abelian group are normal.

- In this case, for $a, b \in G$, $aH \cdot bH = \{k\ell \mid k \in aH, \ell \in bH\}$
$$= abH \cdot H = abH$$

i.e. we have a well-defined group structure on G/H

(The identity is $eH = H$; the inverse of aH is $a^{-1}H$.)

We call G/H the <u>quotient group</u>/<u>factor group</u> (商群)

* <u>Some technical constructions</u>

Proposition. Let H, K be subgroups of a group G, define $HK := \{hk \mid h \in H, k \in K\}$.

When G is finite, $$\#(HK) = \frac{\#H \cdot \#K}{\#(H \cap K)}.$$

Proof: HK is a (disjoint) union of left cosets of K
$$HK = h_1K \sqcup h_2K \sqcup \cdots \sqcup h_nK$$

Claim. For the same h_i, $H = h_1(H \cap K) \sqcup \cdots \sqcup h_n(H \cap K)$

Then $$\frac{\#HK}{\#K} = n = \frac{\#H}{\#(H \cap K)}$$

Proof: For every $h, h' \in H$,
$$hK = h'K \iff h^{-1}h' \in K \iff h^{-1}h' \in H \cap K \iff h(H \cap K) = h'(H \cap K)$$

So $HK = \bigcup_{h \in H} hK = h_1K \sqcup \cdots \sqcup h_nK$

corresponds to $H = \bigcup_{h \in H} h(H \cap K) = h_1(H \cap K) \sqcup \cdots \sqcup h_n(H \cap K)$. $\square$

(In fact, we proved a natural bijection
$$H/H \cap K \xrightarrow{\sim} HK/K \qquad \text{well-defined, bijection}$$
$$h(H \cap K) \longmapsto hK \qquad)$$

Rmk: HK need not be a group above.

E.g. In $G = S_3$, $H = \langle (12) \rangle$, $K = \langle (13) \rangle$, then $\#HK = \#H \cdot \#K = 4$

HK can't be a subgroup of G b/c $4 \nmid 6$

Lemma If $KH = HK$ as a set, then HK is a subgroup of G

i.e. every product hk can be written as $k'h'$, and vice versa.

(e.g. when H is a normal subgroup, $\forall h \in H$, $hK = Kh$, so $HK = KH$.)

Proof: For $h_1, h_2 \in H$, $k_1, k_2 \in K$,

$$h_1 k_1 (h_2 k_2)^{-1} = h_1 \underbrace{k_1 k_2^{-1} h_2^{-1}}_{= h' k'} = (h_1 h') k' \in HK.$$

$\square$

Lemma. If both H and K are normal subgroups of G, then so is HK

Proof: $\forall g \in G$, $gHK = HgK = HKg$. $\square$

A special case above: $G = HK = KH \Rightarrow \#G \cdot \#(H \cap K) = \#H \cdot \#K$.

* Group homomorphism (to relate two groups)

Definition. Let $(G, *)$ and $(H, \circ)$ be groups. A map $\varphi: G \to H$ is called a homomorphism (同态)

if $\forall x, y \in G$, $\varphi(x * y) = \varphi(x) \circ \varphi(y)$

$$(\text{Rmk: } \underbrace{\varphi(e_G * e_G)}_{= \varphi(e_G)} = \varphi(e_G) \circ \varphi(e_G) \Rightarrow \varphi(e_G) = e_H$$

$$e_H = \varphi(e_G) = \varphi(g * g^{-1}) = \varphi(g) \circ \varphi(g^{-1}) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}.$$

- In particular, a bijective group homomorphism is an isomorphism.

Examples (1) $\phi: \mathbb{Z} \to \mathbb{Z}_n$, $\phi(m) = m \bmod n$ is a homomorphism

(2) When $H \trianglelefteq G$ is a normal subgroup, there's a natural homomorphism

$$\begin{aligned} G &\xrightarrow{\pi} G/H \\ a &\longmapsto aH \end{aligned}$$

← This homomorphism is surjective.

Definition. For a homomorphism $\varphi: G \to H$ of groups,

the kernel is $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$ (同态的核)

Lemma. (1) The image $\varphi(G)$ is a subgroup of H

(2) The kernel $\ker\varphi$ is a normal subgroup of G.

Proof: (1) Note $\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1}) \in \varphi(G)$

(2) If $g_1, g_2 \in \ker\varphi$, then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H \cdot e_H = e_H$

$\Rightarrow g_1 g_2^{-1} \in \ker\varphi$. So $\ker\varphi$ is a subgroup.

For any $g' \in G$, $g \in \ker\varphi$, $\varphi(g' g g'^{-1}) = \varphi(g')\varphi(g)\varphi(g')^{-1}$

$= \varphi(g') e_H \varphi(g')^{-1} = e_H$

So $g' g g'^{-1} \in \ker\varphi \Rightarrow \ker\varphi$ is normal

Lemma. A homomorphism $\varphi: G \to H$ of groups is injective if and only if $\ker\varphi = \{e_G\}$

Proof: injective $\Rightarrow$ $\ker\varphi$ has at most one element but $\varphi(e_G) = e_H$

$\Rightarrow \ker\varphi = \{e_G\}$.

Conversely, suppose $\ker\varphi = \{e_G\}$, WTS φ is injective.

Say $\varphi(g_1) = \varphi(g_2)$ for some $g_1, g_2 \in G$

Then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$

$\Rightarrow g_1 g_2^{-1} \in \ker\varphi = \{e_G\} \Rightarrow g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2$ $\square$

* **How to specify a homomorphism?**

Suppose $G = \langle s_1, \cdots, s_n \mid R_1, \cdots, R_m \rangle$

Then to specify a homomorphism $\phi: G \to H$, it is enough to give

$\phi(s_1), \cdots, \phi(s_n) \in H$

s.t. $\phi(R_j) = e_H$ in H

Example: Determine all homomorphisms $\phi : D_{2n} \longrightarrow \mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot)$

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1} \rangle$$

It is enough to find $\phi(r), \phi(s) \in \mathbb{C}^\times$, s.t.

$$\phi(r)^n = \phi(s)^2 = 1 \quad \text{and} \quad \phi(s)\phi(r)\phi(s) = \phi(r)^{-1}$$

$$\Downarrow$$

$$\phi(s)^2 \phi(r)^2 = 1 \Rightarrow \phi(r)^2 = 1$$

If n is odd, $\phi(r) = 1$, $\phi(s) \in \{\pm 1\}$ two such homomorphisms

If n is even, $\phi(r), \phi(s) \in \{\pm 1\}$ four such homomorphisms