Automorphism Groups and Cosets - Lecture 10/03

Group of Automorphisms

- $Aut(G)$ is the group of automorphisms of G.
- Fix $g \in G$, define $\phi_g : G \to G$. $\phi_g(x) = gxg^{-1}$

  We've verified $\phi_g \in Aut(G)$. Each ϕ_g is called an inner automorphism.
- $$\begin{aligned} \Phi : \ G &\to Aut(G) \\ g &\mapsto \phi_g \end{aligned}$$
- $Inn(G) = \{ \phi_g \in Aut(G) \mid g \in G \} = Im(\Phi)$
- We know: the image of a homomorphism is a subgroup of the codomain group.
  - Φ is a homomorphism:
  - $\Phi(g_1 g_2) = \phi_{g_1 g_2}$. $\forall x \in G$. $\phi_{g_1 g_2}(x) = (g_1 g_2)(x)(g_1 g_2)^{-1}$

    $= g_1 g_2 x g_2^{-1} g_1^{-1}$

    $= g_1 (g_2 x g_2^{-1}) g_1^{-1}$

    $= \phi_{g_1}(\phi_{g_2}(x)) = \phi_{g_1} \circ \phi_{g_2}(x)$

    $= \phi_{g_1} \circ \phi_{g_2}$

    $= \Phi(g_1) \circ \Phi(g_2)$
  - So $Inn(G)$ is a subgroup of $Aut(G)$
- Furthermore, $Inn(G)$ is a normal subgroup of $Aut(G)$
  - $\forall \phi_g \in Inn(G), \forall f \in Aut(G)$ need to check : $f \circ \phi_g \circ f^{-1} \in Inn(G)$
  - $\forall x \in G,\ f \circ \phi_g \circ f^{-1}(x) = f(\phi_g(f^{-1}(x)))$

    $= f(gf^{-1}(x)g^{-1}) = f(g)f(f^{-1}(x))f(g^{-1}) = f(g)xf(g)^{-1} = \phi_{f(g)}(x)$
  - So $f \circ \phi_g \circ f^{-1} = \phi_{f(g)} \in Inn(G)$

- $\Phi : \; G \;\to\; Aut(G)$

  $\qquad g \;\mapsto\; \phi_g$

  Sometimes, different g may lead to same ϕ_g.

  For example, if G is abelian

  $\phi_g(x) = gxg^{-1} = x$

  $\phi_g = id_G, \; Inn(G) = \{id\}$
- Φ will be injective iff $Z(G) = \{1\}$
  - Q. When will Φ be injective? (i.e., $g_1 \neq g_2 \Rightarrow \phi_{g_1} \neq \phi_{g_2}$).

    $g \in \ker(\Phi) \Leftrightarrow \Phi(g) = \phi_g = id_G \Leftrightarrow \forall x \in G. \; \phi_g(x) = x \Leftrightarrow \forall x \in G. \; gxg^{-1} = x$

    $\Leftrightarrow \forall x \in G \; gx = xg$

    $\Leftrightarrow g \in Z(G)$.

    So $\ker(\Phi) = Z(G)$.

    Φ will be injective iff $Z(G) = \{1\}$.
  - E.g. $Z(S_3) = \{id\}$, so we have an injective homomorphism:

$$\Phi : S_3 \to Aut(S_3)$$
$$\Rightarrow |Aut(S_3)| \geq |S_3|$$

Quotient & Product of Groups

Cosets

G is a group, H is a subgroup of G.

Define a relation on G by $a \sim b$ if $a = bh$ ($b^{-1}a = h$) for some $h \in H$

This is an equivalence relation:

- $\forall a \in G. \; a = a \cdot 1, \; 1 \in H.$ so $a \sim a$.
- $a \sim b \Rightarrow a = bh$ for some $h \in H \Rightarrow b = ah^{-1}. \; h^{-1} \in H. \Rightarrow b \sim a$
- $a \sim b, \; b \sim c \Rightarrow a = bh_1, \; b = ch_2$ for some $h_1, h_2 \in H$

  $\Rightarrow a = (ch_2)h_1 = c(h_2h_1), \; h_2h_1 \in H. \Rightarrow a \sim c.$

Under this equivalence relation, an equivalence class is:

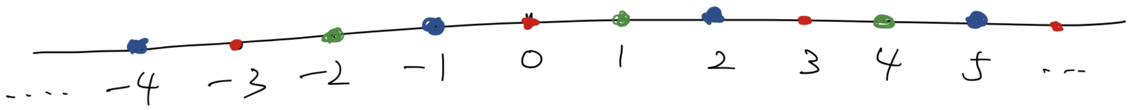
$$[g] = \{x \in G | x \sim g\} = \{x \in G | x = gh \text{ for some } h \in H\} = \{gh \in G | h \in H\} = gH$$

Such an equivalence class is called a <u>left coset</u> of H in G.

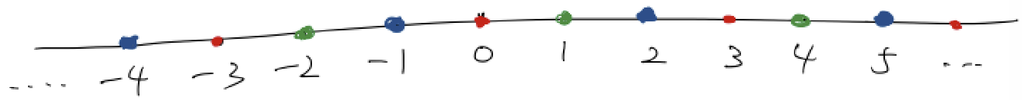
Corollary

Two left cosets of H in G are either disjoint or conincide. And G is a partition of its distinct left cosets.

Example



Example ①. $(\mathbb{Z}, +)$. $H = 3\mathbb{Z}$.



$0 + 3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\}$

$1 + 3\mathbb{Z} = \{1, 4, 7, \ldots, -2, -5, \ldots\}$

$2 + 3\mathbb{Z} = \{2, 5, 8, \ldots, -1, -4, -7, \ldots\}$

②. $G = S_3$. $H = \langle (1\ 2) \rangle$.

$1H = (1\ 2)H = \{id, (1\ 2)\}$,

$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$.

$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H$

Prop

H is a subgroup of G. $a, b \in G$. Then the following are equivalent:

1. $aH = bH$
2. $a = bh$ for some $h \in H$
3. $b^{-1}a \in H$
4. $a \in bH$

Remark. We can also construct right cosets in a similar way:
$Hg = \{hg \in G \mid h \in H\}$ (start from defining $a \sim b$ if $a = hb$ for some $h \in H$)

But in general, gH and Hg may be different sets.

Index

H is a subgroup of G.

Define the number of distinct left cosets of H in G to be the index of H in G.

Denoted by $[G : H]$.

Ex.

1. $(\mathbb{Z}, +),\ H = 3\mathbb{Z}$. We see $[\mathbb{Z} : 3\mathbb{Z}] = 3$
2. $S_3,\ H =< (1\ 2) >$. We see $[S_3 : H] = 3$

Lagrange Theorem

If G is a finite group of H is a subgroup of G, then

$$[G : H] = \frac{|G|}{|H|}$$

Proof:

Pf. We know G is the disjoint union of distinct left cosets of H in G, and there're $[G:H]$ left cosets.

For each coset gH, it has same number of elements as that of H, since we can construct a bijection

$$\boxed{\begin{aligned} H &\longrightarrow gH \\ h &\longmapsto gh \end{aligned}}$$

So $|G| = (\#\text{ left cosets}) \times (\#\text{ elements in each coset})$

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

$\Rightarrow \boxed{\frac{|G|}{|H|} = [G:H]}$.

Remark:

Remark ① When $|G| = \infty$, we can understand $|G| = [G:H] \cdot |H|$ as at least one of $[G:H]$ and $|H|$ is infinite.

② When $|G|$ and $|H|$ are infinite, it's possible $[G:H] < \infty$.

For example, $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z}$.

Cor

Cor. If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

e.g. $G = K_4 = \{1, a, b, c\}$. Find all subgroups of K_4.

$|K_4| = 4$. H is a subgroup of K_4. $|H| \mid 4 \Rightarrow |H| = 1, 2, 4$.

- $|H| = 1$: $H = \{1\}$. • $|H| = 4$: $H = K_4$.
- $|H| = 2$: $\{1, a\}, \{1, b\}, \{1, c\}$

$$\begin{array}{ccc} \{1,a\} & \{1,b\} & \{1,c\} \\ \| & \| & \| \\ \langle a \rangle & \langle b \rangle & \langle c \rangle \end{array}$$

Cor. If $x \in G$, G is a finite group. then $|x|$ divides $|G|$.

Pf. $|x| = |\langle x \rangle|$. by the above Cor., it divides $|G|$.

Prop

If G is a group, $|G|$ is prime, then G is a cyclic group

Prop. If G is a group. $|G|$ is prime, then G is a cyclic group.

Pf. $|G| \neq 1$. so $\exists\, g \in G$. $g \neq 1$. $|g| \neq 1$.

$|g| \,\big|\, |G| = p$, a prime. so $|g| = 1$ or p. $\Rightarrow |g| = p$.

(impossible)

Then $|\langle g \rangle| = |g| = p = |G|$. $\Rightarrow G = \langle g \rangle$.

Remark ① If $|G| = p$ is prime, then any non-identity element of G can be the generator of G.

② If $|G| \neq 1$ or prime. then we can find non-cyclic group G.

For example. $|G| = 4$. K_4 is non-cyclic

$|G| = 6$. S_3 is non-cyclic.