Last class we determined all automorphisms of a cyclic group.

- If $ord(a)=n$ and α an autom. of $\langle a \rangle$
  $\Rightarrow \exists j$ with $gcd(j,n)=1$ s.t.
  $$\alpha(a) = a^j$$
  $$(\Rightarrow \quad \alpha(a^k) = \alpha(a)^k = (a^j)^k = a^{jk})$$
  (prop. of isom.)
- $ord(a)=\infty$
  $\Rightarrow$ either $\alpha = id$ for $\langle a \rangle$
  or $\alpha(a^k) = a^{-k} = (a^k)^{-1}$.

Observation: if α and β are autom. of G

$\Rightarrow$ $\alpha \circ \beta$ is an autom.

$\alpha \circ \beta (g) = \alpha(\beta(g))$

can show

Theorem: The set $Aut(G) = \{\alpha : G \to G \text{ autom.}\}$ forms a group with operation = concatenation of maps

Proof easy (identity elem: $id: G \to G$, $g \to g$

inverse of α = inverse map (exists because α is 1-1 and onto))

Remark: Can show:

If $G = \mathbb{Z}_n$ then $|Aut(G)| = \phi(n)$ (show last time)

Recall: $|u(n)| = \phi(n) = \#\{j, 0 < j < n, \gcd(j,n) = 1\}$

One can show: $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$

isom. given by $\Phi: j \in U(n) \longrightarrow \alpha_j : k \in \mathbb{Z}_n \longrightarrow jk \bmod n.$

Lagrange's Theorem

Def. $H \subset G$ a subset (not necessarily a subgroup)

Then define for $a \in G$ given

$$aH = \{ah, h \in H\}$$
$$Ha = \{ha, h \in H\}$$

If $H \subset G$ is a subgroup then we call

aH a left coset of H.

Ha a right coset

Example: ① $H = \langle (12) \rangle = \{ id, (12) \}$

$G = S_3$

left cosets:

$id \cdot H = H = \{ id, (12) \} =$

$(12)H = \{ \underbrace{(12)id}_{(12)}, \underbrace{(12)(12)}_{=id} \} = \{ id, (12) \}$ } same

$(13)H = \{ (13)id, (13)(12) \} = \{ (13), (123) \}$

$(123)H = \{ (123)id, (123)(12) \} = \{ (123), (13) \}$ } same

$(23)H = \{ (23), (132) \}$

$(132)H = \{ (132), (23) \}$ } same

intersections of distinct left cosets are empty

---

similar for right cosets: e.g.

$H(13) = \{ id(13), (12)(13) \} = \{ (13), (132) \}$

observe: $(13)H \neq H(13)$

② $G = \mathbb{Z}_6$ $\quad H = \langle 2 \rangle = \{0, 2, 4\} \subset \mathbb{Z}_6$

(use add. notation):

$H = 0+H = 2+H = 4+H$ (even numbers mod 6)

$1+H = 3+H = 5+H$ (odd numbers mod 6)

here $1+H = H+1$

Properties of cosets (Lemma)

① $a \in aH$ (follows from $a = ae$, $e \in H$)

② $aH = H \iff a \in H$

("$\Leftarrow$" $a \in H \Rightarrow ah \in H$ $\forall h \in H \Rightarrow aH \subset H$

check: $aH \supset H$ i.e.

given $h \in H$, $h = a(a^{-1}h) \in aH$ ($a^{-1}h \in H$)

"$\Rightarrow$" $\Rightarrow aH = H$.

"$\Rightarrow$" $a = a \cdot e \in aH = H \Rightarrow a \in H$.

③ $(ab)H = a(bH)$

(because $\{(ab)h, h \in H\}$ $= \{a(bh), h \in H\}$)

(5) we have either $aH = bH$ or $aH \cap bH = \emptyset$

proof assume $aH \cap bH \neq \emptyset$

$\Rightarrow \exists\ c \in aH \cap bH$

$\Rightarrow c = ah_1 = bh_2$ with $h_1, h_2 \in H$

multiply by a^{-1} from left:

$\Rightarrow h_1 = a^{-1}ah_1 = a^{-1}bh_2 \Rightarrow a^{-1}b = h_1 h_2^{-1} \in H$

($h_1 \in H$, $a^{-1}bh_2 \in H$)

$\Rightarrow b = aa^{-1}b = a(\underbrace{a^{-1}b}_{\in H}) \in aH$

$\Rightarrow bH = a(\underbrace{a^{-1}b}_{\in H})H = aH$

(7) $|aH| = |H|$ for all $a \in G$

proof. the map $h \in H \to ah \in aH$ is onto by def.

it is 1-1 by left cancellation

$\Rightarrow$ map gives us bijection between elements of H and aH.

Lagrange's Theorem

If G is a finite group and $H \subset G$ a subgroup

$\Rightarrow |H| \mid |G|$

proof. let $a_1H, a_2H, \ldots a_rH$ be all left cosets in G (*)

$\Rightarrow G = a_1H \cup a_2H \cup \ldots \cup a_rH$

(any $a \in G$ is in a left coset namely aH)

$|G| = |a_1H| + |a_2H| + \ldots + |a_rH|$ (because $a_iH \cap a_jH = \emptyset$ $i \neq j$)

$= |H| + |H| + \ldots + |H|$

$\overset{(+)}{=} r|H|$ ✓

Applications:

Cor 2 If G is finite group, $a \in G$

$\Rightarrow \operatorname{ord}(a) \mid |G|$

proof. $\operatorname{ord}(a) = |\langle a \rangle| \mid |G|$

↑ Lagrange's Theorem.

Cor 3 If $|G| = p$ prime

$\Rightarrow$ G is cyclic