

§9 (cont.) Alternating groups

Fix n (non-neg. integer)

The n -th alternating group (or alt. grp. of n letters) is $A_n = \{ \sigma \in S_n \mid \text{even permutation} \}$

Ex. $A_3 = \{ e, (1, 2, 3), (3, 2, 1) \} \cong \mathbb{Z}_3$

Why are the A_n interesting?

they are simple groups ($n=3$ or $n \geq 5$)

... as groups they cannot decompose into easier structures (& how to combine such)

glueing data

simplicity of A_5 will lead to the Abel-Ruffini th'm

§10 Cosets and Lagrange's th'm

Suppose G is a finite group, $H \leq G$ a subgrp.
we want to compare $|G|$ (= num. of elems in G ,
order of G)

and $|H|$

"Lagrange's theorem": $\exists$ pos. integer r s.t. $|G| = r|H|$
write $r = [G:H]$, the index of H in G

Example $G = \mathbb{Z}_6$ $|G| = 6$
possibilities for H : $H = \{0\} \rightarrow |H| = 1$, $H = \{0, 2, 4\} \rightarrow |H| = 3$, $H = \{0, 3\} \rightarrow |H| = 2$
 $H = G \rightarrow |H| = 6$

In general: look for some "things" s.t. r is the number of them

$\leadsto$ cosets for G and H are such "things"

(G, H fixed for now) write

$a \sim_L b$ for $a, b \in G$ when $b = ah$ for some $h \in H$
 $a \sim_R b$ - - - - $b = ha$ for some $h \in H$

we can write these as $a^{-1}b = h$, $ab^{-1} = h'$

Ex. $G = \mathbb{Z}$, $H = m\mathbb{Z} = \{km \mid k: \text{integer}\}$

then $a \sim_L b$ means $a \equiv b \pmod{m}$

same for $a \sim_R b$

a left coset of H is a subset of G of the form

$$\{b \in G \mid b \sim_L a\} \quad \text{for some fixed } a \in G$$

notation $aH = \{ah \mid h \in H\} (= \{b \mid b \sim_L a\})$

a right coset: $H_b = \{h'_b \mid h' \in H\} (= \{a \mid a \sim_R b\})$

Prop (cf. Thm 10.1) $b \in aH \Leftrightarrow bH = aH$
 $a \in Hb \Leftrightarrow Ha = Hb$

Proof (first claim)

" $\Rightarrow$ ": take $b \in aH$ i.e. $b = ah$ for some $h \in H$

then $bH = \{bh' \mid h' \in H\} = \{ahh' \mid h' \in H\}$

• $hh' \in H$ implies $bH \subset aH$

• given $h'' \in H$ $ah'' = ah \underbrace{h^{-1}h''}_{\text{use this as } h'}$ implies $aH \subset bH$

" $\Leftarrow$ ": $b \in bH$ by $b = be$ $\square$

This means two left cosets are either equal or disjoint

$\Rightarrow$ G can be partitioned as a disjoint union of

left cosets $G = \bigcup_{i \in I} a_i H$, $a_i H \cap a_j H = \emptyset$
for $i \neq j$

for some seq. $(a_i)_{i \in I}$ in G

Ex. $G = \mathbb{Z}$, $H = m\mathbb{Z}$. consider $(a_i)_{i=0}^{m-1}$, $a_i = i$

$$a_i + H = \{a_i + km \mid k \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid n \equiv i \pmod{m}\}$$

$\mathbb{Z}$ is a disj. union of these sets

Prop. each left coset aH has the same number of elements as H

Proof. $aH \leftrightarrow H$ $ah \leftrightarrow h$ gives a one-to-one correspondence $\square$

Thm 10.10 (Lagrange's thm)

Suppose $|G| < \infty$, H is a subgroup of G .

Then $|H|$ divides $|G|$ i.e. $|G| = r|H|$, r pos. int.

Pf. Write $G = \bigcup_{i \in I} a_i H$ disj. union.

each $a_i H$ has the same num. of elems. as H

$\Rightarrow r = \text{number of } a_i\text{'s}$ will do $\square$