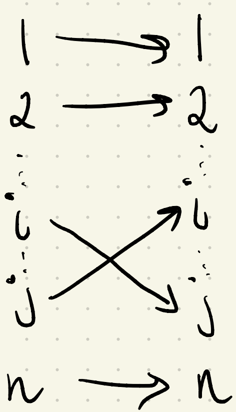
Alternating group §9 Fraleigh

Recall A cycle is a permutation with at most 1 orbit of size > 1. The length of a cycle is the size of its largest orbit.

Def 9.11 A cycle of length 2 is a transposition.

Ex.



(i, j) in cycle notation

Every cycle is a product of transpositions

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_2)$$

$$\shortparallel$$

$$(a_2, \ldots, a_k, a_1) = (a_2, a_1)(a_2, a_k) \ldots$$

Corollary 9.12 For $n \geq 2$, every element of S_n can be expressed as a product of transpositions

Proof Combine Thm 8.8 and $(a_1, \ldots, a_k) = (a_1, a_k) \cdots (a_1, a_2)$.

"every perm. is a product of cycles"

Ex. 9.13 $(1,6)(2,5,3) = (1,6)(2,3)(2,5) \cdot \underbrace{\cancel{(2,5)(2,5)}}^{e}$

$(1,4,6)(2,5,3) = (1,6)(1,4)(2,3)(2,5)$.

Ex 9.14 For S_n $n \geq 2$ the identity permutation is

$(i,j)(i,j) = e \quad \forall\ i \neq j$.

Thm 9.15 No permutation in S_n can be written as both a product of an even # of transpositions and an odd # of transpositions.

Proof 1) Using linear algebra & determinants.

$\phi: S_n \to \mathrm{Mat}_{n\times n}$ a map

$\sigma \mapsto C_\sigma$ ← matrix obtained by permuting rows of $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ according to σ.

$\sigma = (1,2)$

$C_\sigma = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ & 0 & & \ddots & \end{pmatrix}$

$\det(I) = 1$

$\det C_{(1,2)} = -1$

Then $\det(C_\sigma) = (-1)^{\left(\begin{smallmatrix}\text{\# of pairs of rows swapped}\\ \text{to obtain } C_\sigma\end{smallmatrix}\right)}$

$= (-1)^{\text{\# of transp. in a product giving } \sigma}$

$= \begin{cases} 1 & \text{if even \# of trans. to express } \sigma \\ -1 & \text{if odd \# of trans. to express } \sigma \end{cases}$

$\square$

Proof 2 counting orbits. see text.

Def 9.18 A permutation is *even* if it can be written as an even # of transpositions. It is *odd* otherwise

Claim S_n consists of equal numbers of even + odd permutations

$A_n := \{\text{even perms}\} \subseteq S_n$

$B_n := \{\text{odd perms}\} \subseteq S_n$

$\lambda_\tau : A_n \to B_n$ τ any transposition

$\sigma \mapsto \tau\sigma$

Prove λ_τ is a bijection

- If $\lambda_\tau(\mu) = \lambda_\tau(\sigma)$ $\Rightarrow \cancel{\tau}\mu = \cancel{\tau}\sigma \to \mu = \sigma$ injective
- For $\sigma \in B_n$ $\lambda_\tau(\underbrace{\tau^{-1}\sigma}_{\in A_n}) = \sigma$ surjective

$\Rightarrow |A_n| = |B_n|$ and $S_n = A_n \sqcup B_n$.

Thm 9.20 If $n \geq 2$, then $A_n = \{\text{even permutations}\}$ is a subgroup of S_n of order $\frac{|S_n|}{2} = \frac{n!}{2}$.

(called the alternating group on n letters)

Proof • A_n is closed: if σ_1, σ_2 are even then $\sigma_1\sigma_2$ is even.

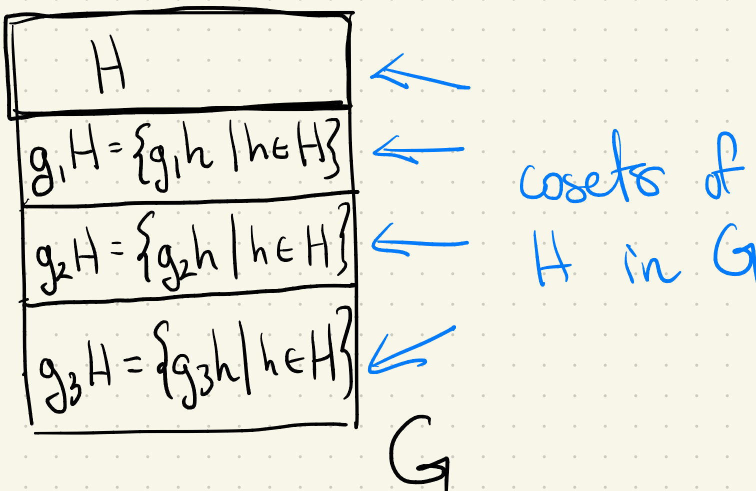
• identity $e = (i,j)(i,j) \in A_n$

• inverses: $\sigma = \tau_1 \cdots \tau_{2k}$ then $\sigma^{-1} = \tau_{2k}^{-1} \cdots \tau_1^{-1}$

moreover $(i,j)^2 = e \Rightarrow (i,j)^{-1} = (i,j)$ $\quad = \tau_{2k} \cdots \tau_1 \in A_n$

Cosets and Lagrange's Theorem §10.

Thm 10.10 (Lagrange's Thm) Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.



$$G = H \sqcup g_1H \sqcup \dots \sqcup g_kH$$

for some $g_i \in G$

and

$$|H| = |g_iH|$$

$$\Rightarrow |H| \cdot K = |G|.$$

Let H be a subgroup of G. $a, b \in G$

<u>Define</u>: left $\sim_L$ by $a \sim_L b \iff a^{-1}b \in H \iff b \in aH$

right $\sim_R$ by $b \sim_R a \iff ba^{-1} \in H \iff b \in Ha$.

<u>Thm 10.1</u> Both $\sim_L$ and $\sim_R$ are equivalence relations on G.

(see Section 1)

<u>Proof for $\sim_L$</u> <u>Reflexive</u>: For $a \in G$ $a^{-1}a = e \in H \Rightarrow a \sim_L a$.

<u>Symmetric</u>: $a \sim_L b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow b \sim_L a$.

<u>Transitive</u>: $a \sim_L b, b \sim_L c \Rightarrow a^{-1}b, b^{-1}c \in H, (a^{-1}\cancel{b}\cancel{b^{-1}}c) \in H \Rightarrow$

$a^{-1}c \in H \Rightarrow a \sim_L c$. $\square$

Def 10.2 Let $H \leq G$ the coset $aH = \{ah \mid h \in H\}$ is the left coset of H containing a.

$Ha = \{ha \mid h \in H\}$ is the right coset of H containing a.

Ex $\underset{H}{3\mathbb{Z}} \leq \underset{G}{\mathbb{Z}}$ with $+$.

left cosets

$3\mathbb{Z} = \{ \dots, -3, 0, 3, 6, \dots \}$

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

$2+3\mathbb{Z} = \{ \dots, -1, 2, 5, 8, \dots \}$

$3+3\mathbb{Z} = \{ \dots, 0, 3, 6, 9, \dots \} = H$.

left cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are

$3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}$.

What about right cosets? that group are abelian.

Try with $\underset{G}{\mathbb{Z}_6}, +_6$ and

$H_1 = \{0, 3\}$ or $H_2 = \{0, 2, 4\}$.

Ex. 10.7 $H = \langle \mu_1 \rangle \leq S_3$. $\mu_1 = (2,3)$ see Exa 8.7

$|H| = 2$.

not abelian

left cosets

$$H = \{\rho_0, \mu_1\},$$
$$\rho_1 H = \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\},$$
$$\rho_2 H = \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}.$$

osets is

right cosets.

$$H = \{\rho_0, \mu_1\},$$
$$H\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\},$$
$$H\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}.$$

10.9 Table

	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
ρ_0	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
μ_1	μ_1	ρ_0	μ_2	ρ_2	μ_3	ρ_1
ρ_1	ρ_1	μ_3	ρ_2	μ_2	ρ_0	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_0	μ_2	ρ_2
ρ_2	ρ_2	μ_2	ρ_0	μ_1	ρ_1	μ_3
μ_2	μ_2	ρ_2	μ_3	ρ_1	μ_1	ρ_0

left cosets in multiplication table.

Lemma For $H \leq G$ $|H| = |aH| = |Ha|$ for any $a \in G$.

Proof The map $\lambda_a : H \to aH$ is a bijection
$h \mapsto ah$
(recall $\lambda_\tau : A_n \to B_n$).

Inverse map is given by $\lambda_a^{-1} = \lambda_{a^{-1}}$.
check. $\square$

Thm 10.10 (Lagrange's Thm) Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.

Proof Since $\sim_L$ defines an equivalence relation the equivalence classes partition G:

$$G = H \sqcup a_1 H \sqcup \cdots \sqcup a_{k-1} H.$$ ← cosets of H in G

$a_i H \cap a_j H = \emptyset$, $i \neq j$.

$$|G| = |H| + \sum |a_i H|$$ by previous lemma $|H| = |aH|$.

$$= k|H| \Rightarrow |H| \text{ divides } |G|$$ $\square$

Corollary 10.11 Every group of prime order is cyclic

Proof If $|G| = p > 1$ and $a \in G$ then by Lagrange $|\langle a \rangle|$ divides $p \Rightarrow |\langle a \rangle| = 1$ or p. However $|\langle a \rangle| = 1 \Leftrightarrow a = e$. Since $|G| > 1$ $\exists\, a \in G$ s.t. $|\langle a \rangle| = \text{ord}(a) = p \Rightarrow G$ is cyclic of order p $\square$

$\Longrightarrow |G| = p \Rightarrow G \cong (\mathbb{Z}_p, +_p)$

Thm 10.12 The order of an element of a finite group G divides $|G|$

Proof $\text{ord}(a) = |\langle a \rangle|$ which divides $|G|$ by Lagrange $\square$

Def 10.13 Let H be a subgroup of G. The index of H is the # of left cosets of H in G

$$(G:H) := \text{index of } H \text{ in } G.$$

Thm 10.14 Suppose $K \leq H \leq G$ and $(H:K), (G:H) < \infty$

Then $(G:K) = (G:H)(H:K) < \infty$.

Proof Ex 38.