Sections 8 & 9

Last time: Let A be a set. **Permutation of A** is function $\phi: A \longrightarrow A$, which is one-to-one & onto.

Notation: If A finite, $A = \{a_1, \ldots, a_n\}$, write

$$\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \phi(a_1) & \phi(a_2) & \cdots & \phi(a_n) \end{pmatrix}.$$

S_A = set of permutations of A. Binary operation

$$\sigma\tau = \sigma \circ \tau$$

makes S_A a group (identity $\iota: A \to A$, $\iota(x) = x$, inverse to ϕ is ϕ^{-1}).

Example: $A = \{a, b, c\}$, $\sigma = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ $\tau = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

$$\sigma\tau = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \quad \text{since} \quad \begin{aligned} \sigma(\tau(a)) &= c \\ \sigma(\tau(b)) &= b \\ \sigma(\tau(c)) &= a. \end{aligned}$$

Def: If $A = \{1, 2, \ldots, n\}$, write S_n for S_A, the "symmetric group on n letters".

$|S_n|$ = # of permutations of $\{1, 2, \ldots, n\} = n!$

$S_1 = \{e\} = \{(1)\}$. $S_2 = \left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\} \simeq (\mathbb{Z}_2, +_2)$.

$S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$

$\rho_0 = e$

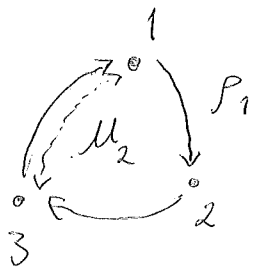
$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$



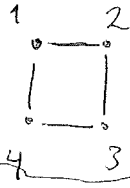
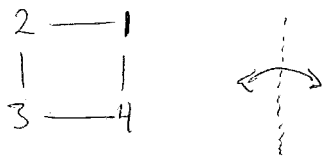
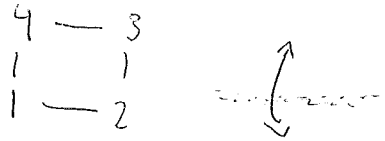
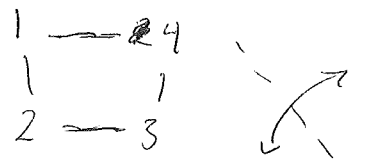
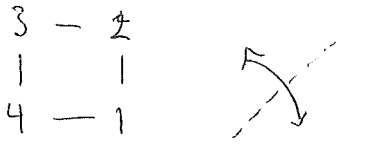
$$\rho_1 \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \mu_3$$

$$\neq \mu_1 \Rightarrow S_3 \text{ is not abelian.}$$

$$\mu_1 \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \mu_2$$

Example $D_4 < S_4$, group of symmetries of the square,

$\sigma \in D_4 \iff \sigma$ obtained by picking up a square and setting it down in some orientation.

Elements	
$\rho_0 = e$	
$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	
$\rho_2 = \rho_1^2$	
$\rho_3 = \rho_1^3$	
$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$	
$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$	
$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$	
$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$	

Are subgroups of S_n "special"? No.

Thm (Cayley) Every group G is isomorphic to a subgroup of S_G.

Def A, B sets, $f: A \to B$, *image of f*, denoted $f(A) \subseteq B$ is

$$f(A) = \{ f(a) \mid a \in A \}.$$

Def If G, H are groups, $\phi: G \to H$ is a *homomorphism* if $\phi(xy) = \phi(x)\phi(y) \quad \forall x, y \in G$.

(Recall "isomorphism", means ϕ is one-to-one, onto & a homomorphism).

Lemma Let G, H be groups $\phi: G \to H$ be a one-to-one homomorphism. Then $\phi(G)$ is a subgroup of H & ϕ gives isomorphism $G \cong \phi(G)$.

Proof $\phi(G)$ a subgroup: • $\phi(G)$ is closed, since $y_1, y_2 \in \phi(G)$

$\Rightarrow y_i = \phi(x_1), \; y_2 = \phi(x_2), \; x_i \in G$

$\Rightarrow y_1 y_2 = \phi(x_1)\phi(x_2) = \phi(x_1 x_2) \in \phi(G)$

• Identity: Let $e_G \in G$, $e_H \in H$ be identities. Have

$$\phi(e_G)\phi(e_G) = \phi(e_G e_G) = \phi(e_G) = \phi(e_G) e_H$$

$\Rightarrow$ (left cancellation)

$$\phi(e_G) = e_H.$$

• Inverses: $\phi(x^{-1}) = \phi(x)^{-1}$.

Now $\phi: G \to \phi(G)$ is one-to-one, onto, & a homomorphism

$\Rightarrow$ an isomorphism.

Proof of Cayley: Need $\phi: G \to S_G$, one-to-one homomorphism.

For $x \in G$, let $\lambda_x : G \to G$ be

$$\lambda_x(g) = xg.$$

This is a permutation ($xg = h$ admits unique solution in g), so get $\lambda_x \in S_G$. Have $\lambda_x \lambda_y = \lambda_{xy}$, since

$$\lambda_x(\lambda_y(g)) = \lambda_x(yg) = xyg = \lambda_{xy}(g).$$

Let $\phi: G \to S_G$ be $\phi(x) = \lambda_x$, then ϕ is homomorphism.

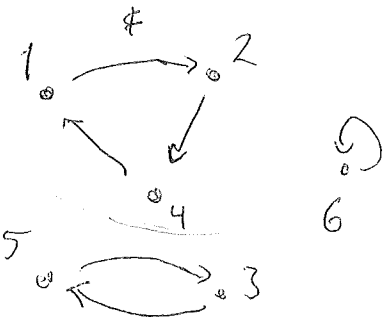
One-to-one since $\phi(x) = \phi(y) \iff \lambda_x = \lambda_y \Rightarrow \lambda_x(e) = \lambda_y(e) \Rightarrow xe = ye$

$$\Rightarrow x = y.$$

□

Orbits & cycles

Example $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$

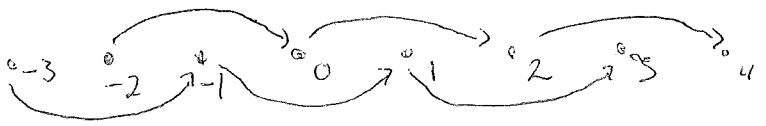


Let $\sigma \in S_A$. Define relation $\sim$ on A by (equivalence)

$a \sim b$ if there is an $n \in \mathbb{Z}$ such that $\sigma^n(a) = b$. The orbits of σ are the equivalence classes of $\sim$, subsets of A.

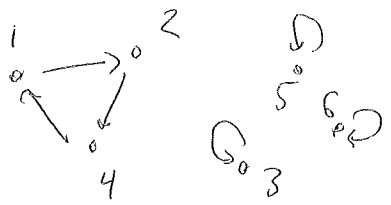
In example, orbits of σ are $\{1, 2, 4\}, \{3, 5\}, \{6\}$.

Example $A = \mathbb{Z}$, $\phi(n) = n + 2$. Orbits of ϕ are {even numbers}, {odd numbers}



Cycles Let A be finite set. A cycle is a $\sigma \in S_A$ which has at most one orbit of size >1. V

Example $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$ is a cycle.



Notation: If σ is a cycle, write $\sigma = (a_1, \ldots, a_k)$, where $\{a_1, \ldots, a_k\}$ is the non-trivial orbit of σ, & $\sigma(a_i) = a_{i+1}$ $1 \le i \le k-1$

Length of cycle = size of non-trivial orbit $\sigma(a_k) = a_1$

Example above: $\tau = (1\ 2\ 4)$.

Def Cycles $\sigma_1, \sigma_2 \in S_A$ are disjoint if their nontrivial orbits are disjoint sets.

Example (1 2 4) & (3 5) are disjoint.
(1 2 4) & (4 5) are not.

Thm In S_n, every σ can be written as a product of disjoint cycles, $\sigma = \sigma_1 \cdots \sigma_k$, σ_i disjoint cycles.

Example: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = (1\ 2\ 4)(3\ 5) = (3\ 5)(1\ 2\ 4)$.

Note: The cycles are determined uniquely, but not their order.

Def A cycle of length 2 is a transposition.

E.g. (3 5), (1 2), ...

Thm Every $\sigma \in S_n$ can be written as a product of transpositions.

Example $(1\ 2\ 3) = (1\ 3)(1\ 2)$.

Proof Write $\sigma = \sigma_1 \cdots \sigma_k$, where the σ_i are cycles.

If $\sigma_i = (a_1\ a_2\ \dots\ a_m)$, then also

$$\sigma_i = (a_1\ a_m)(a_1\ a_{m-1})\cdots(a_1\ a_2).$$

Replace each σ_i by product of transpositions $\Longrightarrow \sigma$ is product of transpositions. □

Can write $\sigma = \tau_1 \cdots \tau_m = \tau_1' \cdots \tau_{m'}'$ as product of transpositions in many ways, generally $m \neq m'$

Thm ⊛ m is even $\Longleftrightarrow$ m' is even.

Def $\sigma \in S_n$ is called even/odd if $\sigma = \hat{\tau}_1 \cdots \hat{\tau}_m$ with $\hat{\tau}_i$ transpositions, and m even/odd.

Identity $\iota = (12)^2$ is even

Product of even σ, σ' is even

Inverse of even σ is even

$\Longrightarrow A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$ is a subgroup of S_n, "the alternating group on n letters".

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Proof of ⊛: For $\sigma \in S_n$, define $(n \times n)$-matrix M^σ by

$$M^\sigma_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j) \\ 0 & \text{otherwise} \end{cases}$$

Example $n=3$ $M^\iota = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $M^{(1\,3\,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

Have $M^\sigma e_j = e_{\sigma(j)}$, so

$$M^{\sigma_1} M^{\sigma_2} e_j = e_{\sigma_1\sigma_2(j)} \Longrightarrow M^{\sigma_1} M^{\sigma_2} = M^{\sigma_1\sigma_2}.$$

If τ is a transposition, $\det M^{\tau} = -1$, so $\sigma = \tau_1 \cdots \tau_m = \tau_1' \cdots \tau_{m'}'$

$$\Rightarrow \det M^{\sigma} = (\det M^{\tau_1}) \cdots (\det M^{\tau_m}) = (-1)^m$$

$$(\det M^{\tau_1'}) \cdots (\det M^{\tau_{m'}'}) = (-1)^{m'}$$

$\Rightarrow m$ & m' have the same parity.

□