- Quiz on Thursday will cover HWK 2 & 3.
- Graded Homework 3 is available for pick up in my office (after class).
- Make sure you ~~rd~~ understand the solutions of Homeworks posted online.

Example (: Cayley Theorem)

$G = (\mathbb{Z}_3, +) \qquad H \leq S_G$

$G.$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

	$\psi_{\bar{g}} : \mathbb{Z}_3 \to \mathbb{Z}_3$
$\psi_{\bar{0}} : \mathbb{Z}_3 \to \mathbb{Z}_3$	$\psi_{\bar{0}}(\bar{x}) = \bar{0} + \bar{x}$
$\psi_{\bar{1}} : \mathbb{Z}_3 \to \mathbb{Z}_3$	$\psi_{\bar{1}}(\bar{x}) = \bar{1} + \bar{x}$
$\psi_{\bar{2}} : \mathbb{Z}_3 \to \mathbb{Z}_3$	$\psi_{\bar{2}}(\bar{x}) = \bar{2} + x$

$H \leq S_G$ = set of bijections on G

$g \in G$
$\psi_g(x) = gx \quad \forall x \in G$

$H = \{\psi_{\bar{0}}, \psi_{\bar{1}}, \psi_{\bar{2}}\}$
is isomorphic to $\mathbb{Z}_3$. $\qquad S_{\mathbb{Z}_3}$

$\psi_{\bar{0}} : \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{0} & \bar{1} & \bar{2} \end{pmatrix} \qquad \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{1} & \bar{0} & 0 \end{pmatrix}$

$\psi_{\bar{1}} : \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{1} & \bar{2} & \bar{0} \end{pmatrix} \qquad \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{0} & \bar{2} & 1 \end{pmatrix}$

$\psi_{\bar{2}} : \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{2} & \bar{0} & \bar{1} \end{pmatrix} \qquad \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} \\ \bar{2} & \bar{1} & \bar{0} \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$

Cycles, and the Alternating Groups

Definition and notation

Let $\sigma = (i_1, \ldots, i_m) \in S_n$ be the permutation of sending $\sigma(i_1) = i_2, \ldots, \sigma(i_{m-1}) = i_m$, and $\sigma(i_m) = i_1$, and $\sigma(j) = j$ for all other j.

We call σ an m-cycle in S_n. A 1-cycle is a fixed point, a two cycle is called a **transposition**. (i, j)

two elements exchange

Examaple ... (2)

Theorems 5.1–5.4 Consider S_n with $n > 1$.

(a) Disjoint cycles in S_n commute.

(b) Every permutation in S_n is a product of disjoint cycles.

(c) The order of $\sigma \in S_n$ is the lcm of the cycle lengths in its disjoint cycle decomposition.

(d) Every permutation is a product of transpositions.

$\sigma = (1, 3, 7, 10, 100) \in S_{100}$ a 5-cycle in S_{100}

$\sigma(1) = 3$

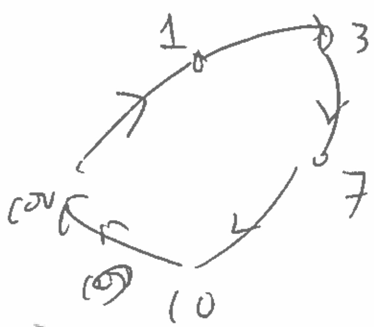
$\sigma(3) = 7$

$\sigma(7) = 10$

$\sigma(10) = 100$

$\sigma(100) = 1$

$\sigma(x) = x$ otherwise



$\underbrace{\sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma}_{5} = I$, identity of S_{100} is the identity function $I(x) = x \;\; \forall x \in \{1, \ldots, 100\}$

(a) Suppose $\sigma = (j_1, \ldots, j_\ell)$

$\hat{\sigma} = (k_1, \ldots, k_m) \in S_n$

Such that $\{j_1 \ldots j_\ell\} \cap \{k_1, \ldots, k_m\} = \phi$.

Then both $\sigma \circ \hat{\sigma}$ & $\hat{\sigma} \circ \sigma$ will fix $x \notin \{j_1 \ldots j_\ell\} \cup \{k_1, \ldots k_m\}$

& move j_1 to j_2, j_2 to j_3, ..., $j_{\ell-1}$ to j_ℓ, j_ℓ to j_1,

and k_1 to k_2, ..., k_{m-1} to k_m, k_m to k_1;

$\therefore \sigma \circ \hat{\sigma} = \hat{\sigma} \circ \sigma$

(b) Proof: Let $\sigma \in S_n$.

Consider $\sigma(1), \sigma^2(1), \sigma^3(1), \cdots, \sigma^k(1) = 1$. for the first time.

We can get a cycle of length k

$$(1, \sigma(1), \cdots, \sigma^{k-1}(1)) = (i_1 \cdots i_k).$$

If there are other number $j_1 \notin \{i_1, \cdots, i_k\}$.
then we can construct

$(j_1, j_2, \cdots, j_\ell)$ by a similar argument.

Note: $\{i_1 \cdots i_k\} \cap \{j_1 \cdots j_\ell\} = \phi$.

If there is $p \notin \{i_1 \cdots i_k\} \cup \{j_1, \cdots, j_\ell\}$
we can construct yet another cycle disjoint from the previous one.

Repeating this process, we get disjoint cycles, including one-cycles, that take into account of all elements $1, 2, \cdots, n$.

(c) Proof: Suppose $\sigma = C_1 \circ C_2 \circ \cdots \circ C_k$. $C_1 = (j_1 \cdots, j_{\ell_1})$, $C_2 = (\hat{j}_1 \cdots \hat{j}_{\ell_2})$
for k-disjoint cycles of lengths $\ell_1, \cdots, \ell_k$.

The order of σ, i.e. the minimum positive integer m, s.t. $\sigma^m = I$, the identity, is the smallest positive integer m s.t. $C_1^m = I$, $C_2^m = I$, $\cdots$, $C_k^m = I$

$\therefore$ m has to be a common multiple of $\ell_1, \ell_2, \cdots, \ell_k$.

So m is the lcm of $\ell_1, \cdots, \ell_k$.

(d) $(i_1 i_2 i_3 \cdots i_m) = (i_1 i_m) \cdots (i_1 i_3)(i_1 i_2)$.

Example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 7 & 5 & 2 & 11 & 9 & 4 & 8 & 6 & 1 & 10 & 12 \end{pmatrix}$$

$$= (1,3,5,11,10)(2,7,4)(6,9)(8)(12)$$

order of σ : $\mathrm{lcm}(5,3,2) = 30$.

Question: In S_n, what is σ with max order.

$$\sigma = (1,3,5,11,10) = \boxed{(1,10)(1,11)(1,5)(1,3)}$$

$$(3,5,11,10,1) = (3,1)(3,10)(3,11)(3,5)$$

σ: $(i,j)^{-1} = (j,i)$

$\sigma = \tau_1\tau_2\tau_3\tau_4 \quad \sigma^{-1} = \tau_4^{-1}\tau_3^{-1}\tau_2^{-1}\tau_1^{-1}$

$= \tau_4\tau_3\tau_2\tau_1$

$$\sigma^{-1} = (10,11,5,3,1) = \underline{(1,3)(1,5)(1,11)(1,10)}$$

Question: Do $\sigma_1 \circ \sigma_2$ & $\sigma_2 \circ \sigma_1$ always have the same order?

$$\underbrace{(1,3)(1,5)(1,11)}(1,10)\underbrace{(1,10)(1,11)(1,5)}_{\sigma}(1,3)$$

τ

$(1,3,4,5,7)(2,3,6,7) = (\cancel{1,3,6,7,2,7})(1,3,6)(2,4,5,7)$

$\boxed{(2,3,6,7)(1,3,4,5,7)} = \boxed{(1,6,7)\ \circ\ (2,3,4,5)}$

$3 + 4 = 7$ transpositions $\qquad 2 + 3 = 5$ transpositions

Even and odd permutations

Definition A permutation is even (odd) if it is a product of even (odd) number of transpositions.

Theorem 5.5 A permutation is either even or odd. The identity permutation ε is even.

Proof. (1) Use isomorphism to the group of permutations and determinant theory.

$S_n \cong$ set of permutation matrices, i.e., the set of (0,1) matrices with one 1 in each row and each column.

Example:

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\2\\3\end{bmatrix},\quad \underset{\sigma_1}{\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\3\\1\end{bmatrix},\quad \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\1\\2\end{bmatrix}$$

ε

$$\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\1\\3\end{bmatrix},\quad \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\3\\2\end{bmatrix},\quad \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\2\\1\end{bmatrix}$$

(2) p.107–110 in the book. Key step. Proof by induction that if $\varepsilon = \beta_1 \cdots \beta_r$, then $\varepsilon = \hat\beta_1 \cdots \hat\beta_{r-2}$ by the following trick if $r \geq 3$.

Let $\beta_r = (ab)$. Move $\beta_r = (ab)$ to the left until we see $\beta_1\eta_j$ has the following form so that we can apply the reduction:

$$(ab)(ab) = \varepsilon, \quad (ac)(ab) = (ab)(bc), \quad (bc)(ab) = (ac)(cb), \quad (cd)(ab) = (ab)(cd).$$

Eventually, ...

Every $\sigma \in S_n$ corresponds to P_σ, a ~~permutation~~ matrix i.e.

If $\sigma = \tau_1 \cdots \tau_k$ a product of ~~permutation~~ transposition

then $P_\sigma = P_{\tau_1} \cdots P_{\tau_k}$.

Notice that if τ_1 is a transposition then P_{τ_1} has det. -1 $\square$

because

$$\det \begin{bmatrix}0&\cdots&1\\ \vdots&&\vdots\\1&\cdots&0\end{bmatrix}$$

det $=$ [ ]

$\det = \begin{bmatrix}0&1\\1&0\end{bmatrix} = -1$

Theorem 5.7 The set A_n of even permutations in S_n form a subgroup of order $n!/2$.

Proof. Use bijection to count!

So if $\sigma \in S_n$, and $\sigma = \tau_1 \cdots \tau_k = \hat\tau_1 \cdots \hat\tau_\ell$,

we have $\det P_\sigma = \det P_{\tau_1} \cdots \det P_{\tau_k}$

$$= \det P_{\hat\tau_1} \cdots \det P_{\hat\tau_\ell} = \begin{cases} 1 & \text{if } k, \ell \text{ are even,} \\ -1 & \text{if } k, \ell \text{ are odd} \end{cases}$$

S_n: A_n, L_1