Feb 22

1. Every permutation in S_n can be uniquely factorized as prod. of disjoint cycles. each cycle is product of transpositions.
2. Review the def. of left cosets G_0 through section 2.9.
3. Review def. of gp. hom. 2 examples 2.5.13 / 2.10.6.

1. Def 1.5.11 (sign of permutations).

For $p \in S_n$. a basis $\{e_1, \cdots, e_n\}$ of n-dim V.

p acts $\{e_1, \cdots, e_n\}$ by $e_i \longmapsto e_{p(i)}$

$\Rightarrow$ p gives a linear transformation $V \to V$

$\Rightarrow$ p can be written into an $n \times n$ - matrix, denoted by P.

$\operatorname{sign} p \triangleq \det P = \{\pm 1\}$.

Example: $p = (1\ 2) \Rightarrow$ $\begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} = P$. $\operatorname{sign} p = \det P = -1$.

If $\operatorname{sign} p = -1$. it is called odd.
$\operatorname{sign} p = 1$. it is called even.

Prop: Every permutation in S_n can be uniquely factorized as prod. of disjoint cycles. each cycle is product of transpositions.

Pf: Given a permutation $p \in S_n$.
Define an equivalence relation on $\{1, 2, \cdots, n\} = S$.

$x \sim y$ iff $x = p^k y$. $k \in \mathbb{Z}$.

If $x \sim y$. $y \sim z$ $x = p^k y$, $y = p^{k'} z$ $\Rightarrow$ $x = p^{k+k'} z$. $x \sim z$
If $x \sim y$, $x = p^k y$ $\Rightarrow$ $y = p^{-k} x$. $\Rightarrow$ $y \sim x$.
$x = x$ $\Rightarrow$ $x \sim x$.

$\Rightarrow$ "$\sim$" is an equi. relation.

By Prop 2.7.4. An equi. relation on a set S determines a partition of S. and conversely.

Suppose S is divided into k parts by "$\sim$". pick representative elements $a_1, \cdots, a_k$.

$a_1, p(a_1), p^2(a_1), \cdots$ At some $n_k \in \mathbb{N}$, $p^{n_k} a_1 = a_1$

The permutation p restricted on $\{a_1, p(a_1), p^2(a_1), \cdots, p^{n_1-1}(a_1)\}$ is a cycle $= (a_1\ p(a_1)\ \cdots\ p^{n_1-1}(a_1))$.

$p = (a_1\ p(a_1)\ \cdots\ p^{n_1-1}(a_1))(a_2\ p(a_2)\ \cdots\ p^{n_2-1}(a_2)) \cdots (a_k\ p(a_k)\ \cdots\ p^{n_k-1}(a_k))$.

$\{a_1', \cdots, a_k' \mid a_i' \sim a_i\}$. $(a_i'\ p(a_i')\ \cdots\ p^{n_i-1}(a_i'))$.

Since $a_i' \sim a_i$ $a_i' = p^\lambda a_i$

$\Rightarrow (p^\lambda a_i\ p^{\lambda+1} a_i\ \cdots\ p^{\lambda+n_i-1} a_i) = (a_i\ p(a_i)\ \cdots\ p^{n_i-1}(a_i))$

$\Rightarrow$ The factorization of p into disjoint cycles is unique. ▨

Prop: Every cycle can be written as prod. of transpositions.

Pf: Given a cycle $(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$

$= (i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_2)$. ▨

Therefore we can conclude that every permutation in S_n is prod. of transpositions.

2. Def: (Left cosets): If H is a subgp. of G. $a \in G$.

$aH \triangleq \{ah \mid h \in H\}$. (left coset of H)

$Ha \triangleq \{ha \mid h \in H\}$.

Left cosets in G are equi. classes for the congruence relation

Given $a, b \in G$. $a \equiv b$ iff $\exists h \in H$ s.t. $ah = b$.

- $a \equiv b$, $b \equiv c$. $\Leftrightarrow \exists h, h' \in H$ $ah = b$ $bh' = c$.
  $\Rightarrow (ah)h' = c$.
  $\Rightarrow a(hh') = c$. $\Rightarrow a \equiv c$. ($hh' \in H$)
- $a \equiv b$. $\exists h$ s.t. $ah = b$. $\Rightarrow a = bh^{-1}$ ($h^{-1} \in H$) $\Rightarrow b \equiv a$.
- $a = ae$ ($e \in H$) $\Rightarrow a \equiv a$.

Therefore. congruence relation is an equivalence relation.

§2.3. Modular arithmetic.

The case of $\mathbb{Z}$

For two integers a, b, they are said to be congruent mod n ($a \equiv b \bmod n$) iff n divides $a-b$.

This is an equi. relation. The equi. class of a as $\bar{a}$.

$$\bar{a} = \{\cdots, a-n, a, a+n, a+2n, \cdots\}$$

Prop. If $a \equiv a' \bmod n$, $b \equiv b' \bmod n$, then $a+b \equiv a'+b' \bmod n$
$ab \equiv a'b' \bmod n$.

Pf: $a - a' = kn$, $k \in \mathbb{Z}$; $b - b' = ln$.

$\Leftrightarrow a = a' + kn$, $b = b' + ln$. $\Rightarrow a+b = a'+b'+kn+ln$
$= a'+b'+(k+l)n$. $\Rightarrow a+b \equiv a'+b'$

$\Rightarrow ab = (a'+kn)(b'+ln)$
$= a'b' + knb' + lna' + kln^2$
$= a'b' + (kb' + la' + kln)\,n$

Thus $ab \equiv a'b' \bmod n$. ∎

3. Def (gp. hom.). G, G' are gps. $\varphi: G \to G'$ is a map.

φ is a gp. hom. iff $\forall a, b \in G$. $\varphi(ab) = \varphi(a)\varphi(b)$.

Properties (Cor 2.8.13). Let $\varphi: G \to G'$ be a hom. of finite gp.s Then:

- $|G| = |\ker\varphi|\,|\mathrm{Im}\varphi|$
- $|\ker\varphi|$ divides $|G|$
- $|\mathrm{Im}\varphi|$ divides both $|G|$ and $|G'|$.

An example of gp. hom.: (Example 2.5.13).

$\varphi: S_4 \to S_3$. $S = \{1, 2, 3, 4\}$. There're 3 ways to partition it into two parts with each part has 2 elements.

$\Pi_1 = \{1,2\} \cup \{3,4\}$.
$\Pi_2 = \{1,3\} \cup \{2,4\}$
$\Pi_3 = \{1,4\} \cup \{2,3\}$.

For a permutation $\rho \in S_4$. Its action on S will give a permutation on $\{\Pi_1, \Pi_2, \Pi_3\}$.

$p=(1\,2)$. $\pi_1 \longmapsto \{2\ 1\}\ \{3\ 4\} = \pi_1$
$\pi_2 \longmapsto \{2\ 3\}\ \{1\ 4\} = \pi_3$
$\pi_3 \longmapsto \{2\ 4\}\ \{1\ 3\} = \pi_2$

$\Big\}\ p=(1\,2) \longmapsto (2\,3) \in S_3$.
$\varphi(p)=(2\,3)$.

Given $p, q \in S_4$. $\pi_1 \longmapsto \pi_{\varphi(p)(1)} = \{p(1)\ p(2)\} \cup \{p(3)\ p(4)\}$.

$\pi_{\varphi(q)\varphi(p)(1)} = \{q(p(1))\ q(p(2))\} \cup \{q(p(3))\ q(p(4))\}$.

$= \{qp(1)\ qp(2)\} \cup \{qp(3)\ qp(4)\}$.

$= \pi_{\varphi(qp)(1)}$

$\Rightarrow \varphi(q)\varphi(p) = \varphi(qp)$.

- This hom. is surjective

$S_3 = (1)\ (1\,2)\ (2\,3)\ (3\,1)$

$(1\,2\,3)\ (1\,3\,2)$.

$(1\,2\,3) \in S_4$ ↑ $(1\,2\,4) \in S_4$

$\varphi: S_4 \to S_3$ is surjective. it is not injective $|S_4| = 24$, $|S_3| = 6$.

- $|\ker\varphi| = 4$. $\ker\varphi = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

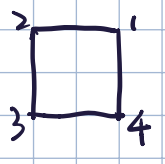
Example 2.10.b. S_3 has a subgp. of order 3.

3 subgp.s of order 2.

By the correspondence theorem. S_4 has a subgroup of order $12 = 3 \times 4 = |\ker\varphi|$.

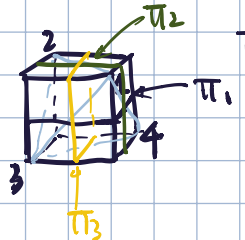
has 3 subgroups of order 8.

There're no other subgroups containing $\ker\varphi$.



reflection

rotation S_4



π_1, π_2, π_3.

By the 1st iso. thm. $S_4/\ker\varphi \cong S_3$.