Monday Week 10, October 24, 2014

Last Time: Any permutation can be written as a product of transposition.

$$(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2)$$

Ex: write σ as a product of transpositions

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

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

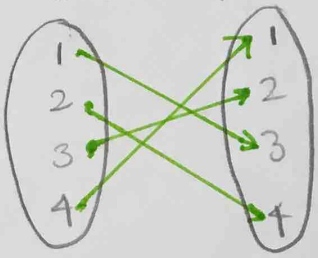
↑ first break into disjoint cycles

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

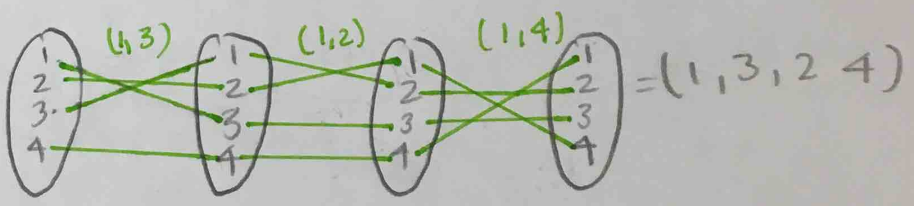
↑ write as products of transpositions.

Ex: Consider S_4

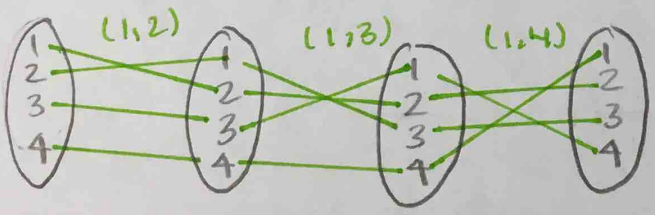
$\sigma = (1,3,2,4)$



$\sigma = (1,4)(1,2)(1,3)$



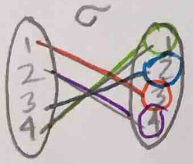
what if we flip some



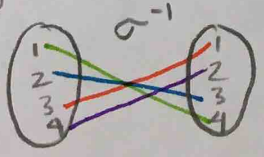
$= (1,2,3\,4) \neq \sigma$

+ order does matter

Inverse function



we go backwards



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

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$\sigma = (1,4)(1,2)(1,3)$ ⟵ 3 transpositions

$\sigma = (1,4)(2,3)(2,3)(1,2)(1,3)$ ⟵ 5 transpositions

$(2,3)^2 = i$

i = identity

transposition (a,b) where $a \neq b$

theorem: No permutation of S_n can be written as a product of an even number of transpositions and as a product of an odd number of transpositions.

Def: A Permutation of S_n is called even if it can be written as the product of an even number of transpositions. It is called odd if it can be written as the product of an odd number of transpositions.

Ex: $\sigma = (1,3,2,4) = (1,4)(1,2)(1,3)$

3 transpositions

σ is odd

Ex: $S_3 = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\}$

$S_3 = \{ i, (2,3), (1,3), (1,2), (1,2,3), (1,3,2) \}$

S_3 : Even permutations: $i = (1,3)(1,3)$, $(1,2,3) = (1,3)(1,2)$, $(1,3,2) = (1,2)(1,3)$

Odd Permutations: $(2,3)$, $(1,3)$, $(1,2)$

Theorem: Let $n \geq 2$. Let A_n be the set of even permutations from S_n. Then A_n is a subgroup of S_n and $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$

A_n is called the alternating group of size n

$$A_3 = \{i, (1,2,3), (1,3,2)\}$$

Cosets and Lagrange's Theorem

Def: Let G be a group and $H \leq G$ Let $g \in G$

The left coset of H containing g is

$$gH = \{gh \mid h \in H\}$$

The right coset of H containing g is

$$Hg = \{hg \mid h \in H\}$$

Ex: $G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$H = \langle r \rangle = \{1, r, r^2, r^3\}$

Left coset

$sH = \{s1, sr, sr^2, sr^3\} = \{s, sr, sr^2, sr^3\}$

right coset

$Hs = \{1s, rs, r^2s, r^3s\} = \{s, sr^{-1}, sr^{-2}, sr^{-3}\}$

$= \{s, sr^3, sr^2, sr\}$

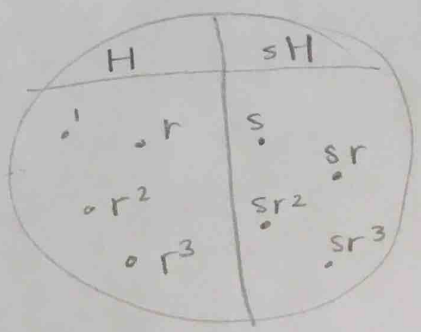
In this case $sH = Hs$, This doesn't always happen.

$rH = \{r1, rr, rr^2, \underbrace{rr^3}_{1}\} = \{r, r^2, r^3, 1\} = H$

You can check that in this example that

$H = rH = r^2H = r^3H$

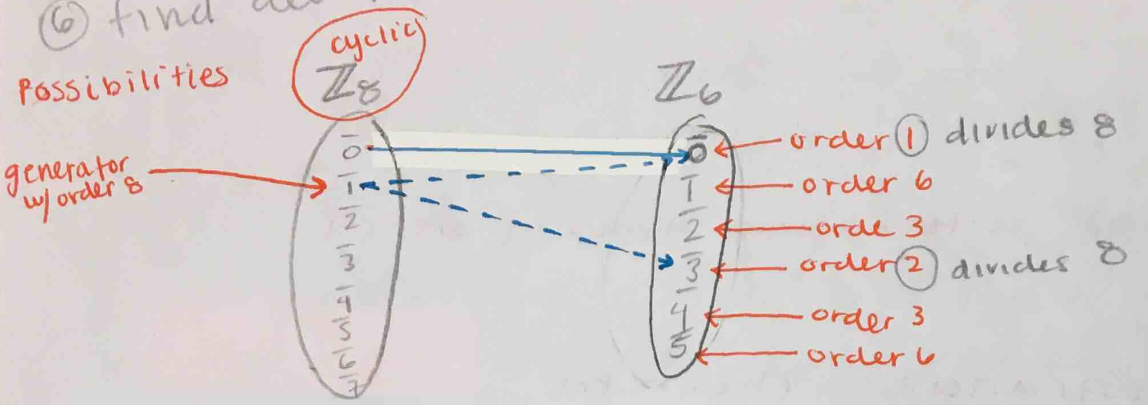
$sH = (sr)H = (sr^2)H = (sr^3)H$

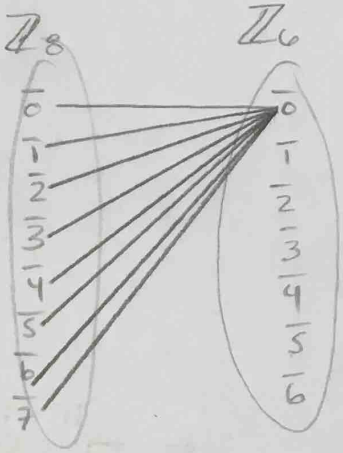


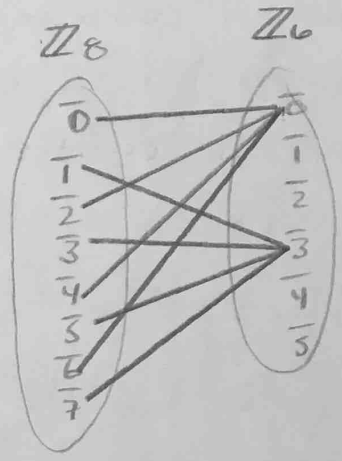
HW #4

⑥ find all homomorphisms from $\mathbb{Z}_8$ to $\mathbb{Z}_6$

Possibilities







Wednesday Week 10, October 26, 2016

HW #6 continued... Cosets

- G is a group $H \leq G$, $g \in G$

$$gH = \{gh \mid h \in H\}$$

$$Hg = \{hg \mid h \in H\}$$

Ex: $G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$$H = \{1, r, r^2, r^3\}$$

$sH = \{s, sr, sr^2, sr^3\}$ equal $rH = \{r, r^2, r^3, 1\}$

$(sr)H = \{(sr)1, (sr)r, (sr)r^2, (sr)r^3\}$

$= \{sr, sr^2, sr^3, s\}$

$(sr^2)H = sH$ $\quad r^3H = rH$

Theorem: Let G be a group, $H \leq G$, and $a, b \in G$

Then: (1) $a \in aH$

(2) $aH = bH$ iff $b^{-1}a \in H$ (or $a^{-1}b \in H$)

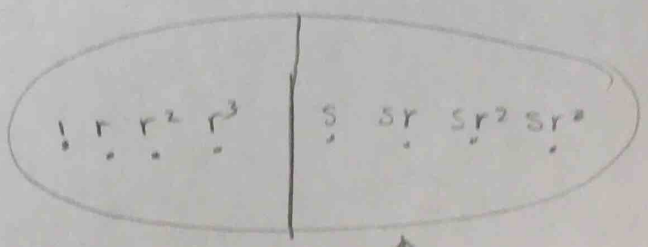
(3) $aH = bH$ iff $a \in bH$ or $(b \in aH)$

(4) $aH = bH$ iff $a = bh$ for some $h \in H$

(5) the left cosets of G partition G that is, $G = \bigcup_{g \in G} gH$ and given any two left cosets aH and bH either $aH \cap bH = \emptyset$ or $aH = bH$

(6) If H is finite, then $|H| = |aH| = |Ha|$.

D_8



$H = r^3H = r^2H = rH$ $\quad sH = (sr)H = (sr^2)H = (sr^3)H$

$D_8 = rH \cup sH$

Proof

① Let e be the identity of G, then $e \in H$, because $H \leq G$

so $ae \in aH$

so $a = ae \in aH$

② ($\Rightarrow$) Suppose $aH = bH$

From ① we know that $a \in aH$

so $a \in bH$ since $aH = bH$

Thus $a = bh$ where $h \in H$ so $b^{-1}a = h$ Thus $b^{-1}a \in H$

($\Leftarrow$) Suppose $b^{-1}a \in H$

Then $b^{-1}a = h$ where $h \in H$. So $a = bh$

lets show $aH \subseteq bH$, let $z \in aH$ so $z = ah'$ where $h' \in H$

Thus $z = ah' = bhh' = b(\underbrace{hh'}_{\text{in } H \text{ because } H \text{ is a subgroup}}) \in bH$

Now lets show $bH \subseteq aH$

let $w \in bH$

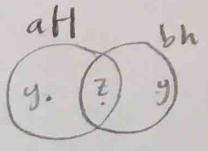
Then $w = b\hat{h}$ where $\hat{h} \in H$

so, $w = (\underbrace{ah^{-1}}_{b})\hat{h} = a(\underbrace{h^{-1}\hat{h}}_{\text{in } H \text{ since } H \leq G}) \in aH$

Therefore, $aH = bH$

③ and ④ exercises

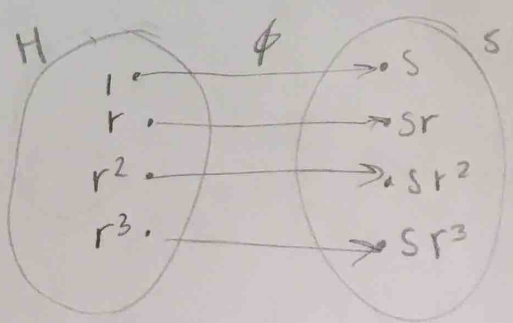
(5) Clearly $gH \subseteq G$ for any $g \in G$.
and given $g \in G$ we know from (1) that $g \in gH$. So
$G = \bigcup_{g \in G} gH$. Let $a, b \in G$. We now show that
$aH \cap bH \neq \emptyset$ iff $aH = bH$.



($\Rightarrow$) suppose $aH \cap bH \neq \emptyset$
so $\exists\ z \in aH \cap bH$ so $z = ah = bh'$ where $h, h' \in H$
Let's show $aH \subseteq bh$. Let $y \in aH$, $y = a\hat{h}$ where $\hat{h} \in H$
Thus, $y = a\hat{h} = (bh'h^{-1})\hat{h} = b(h'h^{-1}\hat{h}) \in bH$
so, $aH \subseteq bH$. Similarly you can show that
$bH \subseteq aH$ so, $aH = bH$.
($\Leftarrow$) Suppose $aH = bH$ by (1) $a \in aH$. so $a \in aH \cap bH$
Thus, $aH \cap bH \neq \emptyset$ ▨

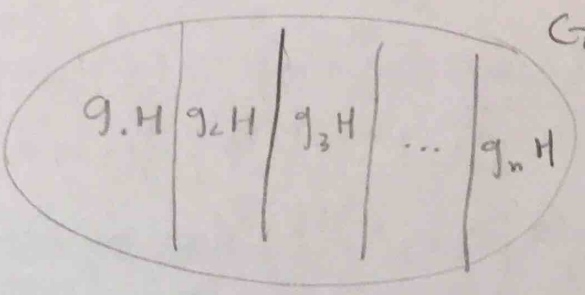
(6) Suppose H is finite. Let $a \in G$. We will show that $|H| = |aH|$ by giving a bijection between them
Define $\phi : H \to aH$ by $\phi(h) = ah$
ϕ is onto since every element of aH is of the form ah where $h \in H$
why is ϕ 1-1?
suppose $\phi(h_1) = \phi(h_2)$
where $h_1, h_2 \in H$. Then
$ah_1 = ah_2$ so $h_1 = h_2$
so ϕ is 1-1 ▨

$\phi : H \to sH$, $\phi(h) = sh$



Lagrange's Theorem

Let G be a finite group
Let H be a subgroup. Then
$|H|$ divides $|G|$



Proof:

Lagrange's Theorem Let $|H$ be a subgroup of a finite group G. Then $|H|$ is a divisor of $|G|$.

proof: Let $H, a_2H, \ldots, a_rH$ be the left cosets where $a_2, \ldots, a_r \in G$. Now,

$$G = H \amalg a_2H \amalg a_3H \amalg \ldots \amalg a_rH.$$

Let $|G| = n$, $|H| = m$. Then

$$n = |G| = m + m + m + \ldots + m = rm$$

Therefore $m \mid n \Rightarrow |H| \mid |G|$. ▨

Corollary: Every group of prime order is cyclic.

pf: Let G be a group where $|G| = p$ for some prime $p \geq 2$. Let $g \in G$ s.t. $g \neq e$. Consider $\langle g \rangle$. Then $|\langle g \rangle|$ divides $p = |G|$. Since $|\langle g \rangle| \neq 1$, we must have $|\langle g \rangle| = p$. Therefore $G = \langle g \rangle$. ▨

Remark: If $|G| = p$, then $G \simeq \mathbb{Z}_p$.