Monday Week 9, October 17, 2016

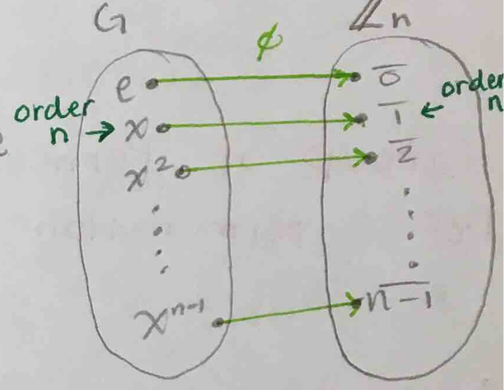
Theorem: (classification of cyclic groups up to isomorphism)

Let G be a cyclic group

If G is finite of size n, then $G \simeq \mathbb{Z}_n$

If G is infinite, then $G \simeq \mathbb{Z}$

Proof



Case 1 suppose G is finite of size n

Then $G = \langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$ where $x \in G$ and x has order n.

Define $\phi : G \to \mathbb{Z}_n$ where $\phi(x^k) = \bar{k}$

[In particular, $\phi(x) = \bar{1}$]

Theorem from last time says that ϕ is a homomorphism

From the def of ϕ, ϕ is 1-1 and onto

So ϕ is an isomorphism, so $G \simeq \mathbb{Z}_n$

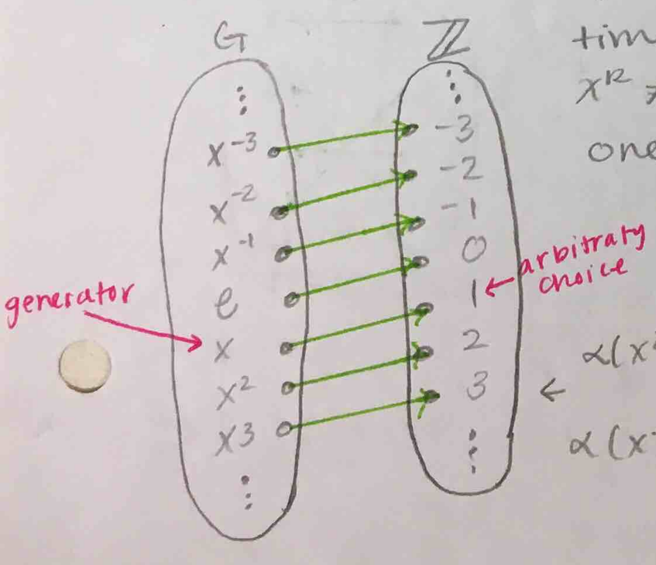
Case 2 G is infinite

Then $G = \langle x \rangle = \{\dots, x^{-3}, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}$

where $x \in G$ and x has infinite order

Define $\alpha : G \to \mathbb{Z}$ by $\alpha(x^k) = k$. From theorem from last time α is a homomorphism. Since $x^k \neq x^i$ where $i \neq k$. we have α is one-to-one and onto.

So, α is an isomorphism and $G \simeq \mathbb{Z}$ ☐



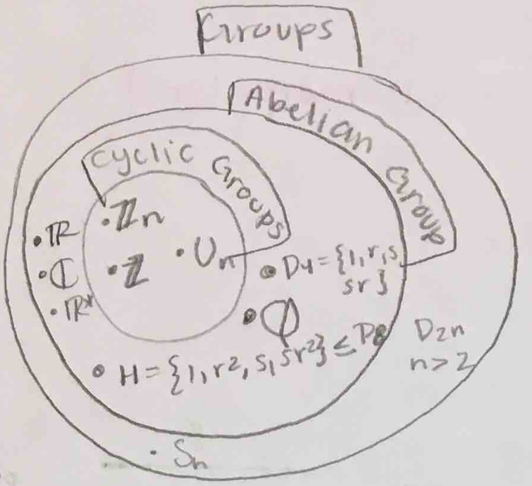
$\alpha(x^2) = \alpha(x\,x) = \alpha(x) + \alpha(x)$
$= 1 + 1 = 2$

$\alpha(x^{-1}) = [\alpha(x)]^{-1} = 1^{-1} = -1$

$G = \langle x \rangle$ is infinite

$\phi : G \to H$ pick $y \in H$

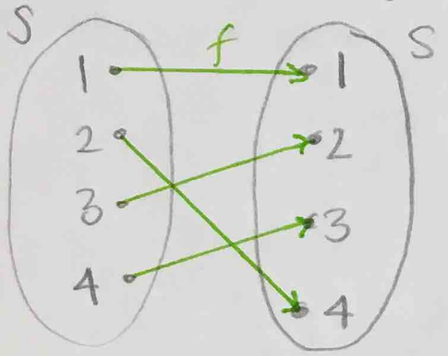
$\phi(x^k) = y^k$

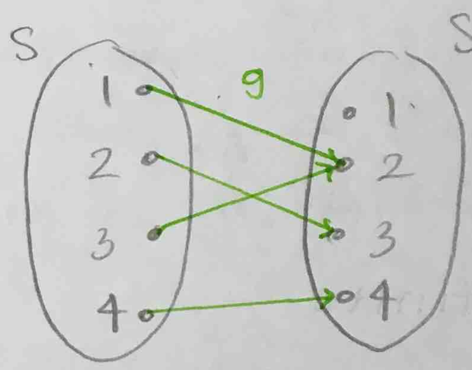


Group of Permutations

Def: A **permutation** of a set S is a function $\phi: S \to S$ where ϕ is a bijection (1-1 and onto)

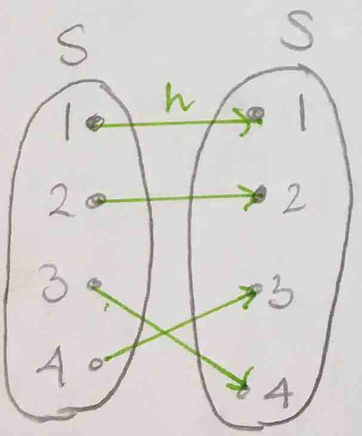
Example: $S = \{1, 2, 3, 4\}$





- f is a permutation
  f is 1-1 and onto

- g is NOT a permutation of S, not 1-1 & not onto



h is a permutation of S.

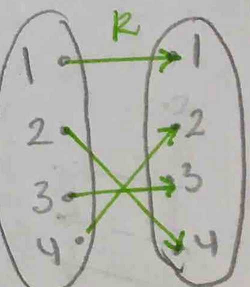
Let $k = f \circ g$

$k(1) = f(h(1)) = f(1) = 1$

$k(2) = f(h(2)) = f(2) = 4$

$k(3) = f(h(3)) = f(4) = 3$

$k(4) = f(h(4)) = f(3) = 2$



- k is also a permutation.
- we composed two bijections and it gave us a bijection.

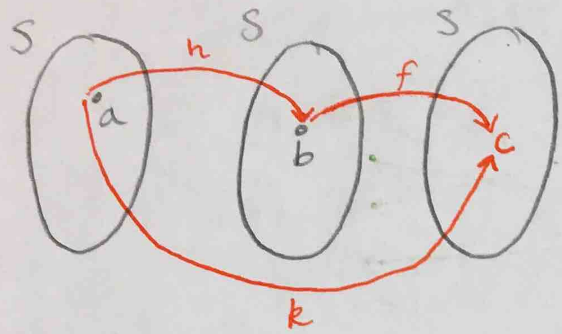
10/17 P.2

Lemma: Let f and h be permutations of a set S. Then $k \circ h$ is a permutation of S.

Proof: we must show that k is 1-1 and onto.

<u>k is onto</u>

It is given that f and h are onto S.



Let $c \in S$.

Since f is onto $\exists$ $b \in S$ s.t. $f(b) = c$

since h is onto $\exists$ $a \in S$ s.t $h(a) = b$

then $k(a) = (f \circ h)(a) = f(h(a)) = f(b) = c$

So k is onto.

<u>k is one to one</u>

Suppose $k(x) = k(y)$ where $x, y \in S$.

$(f \circ h)(x) = (f \circ h)(y)$

Thus $f(h(x)) = f(h(y))$

Since f is a permutation, f is one to one

so $h(x) = h(y)$

since h is a permutation, h is one-to-one

so $h(x) = h(y)$, we have that $x = y$.

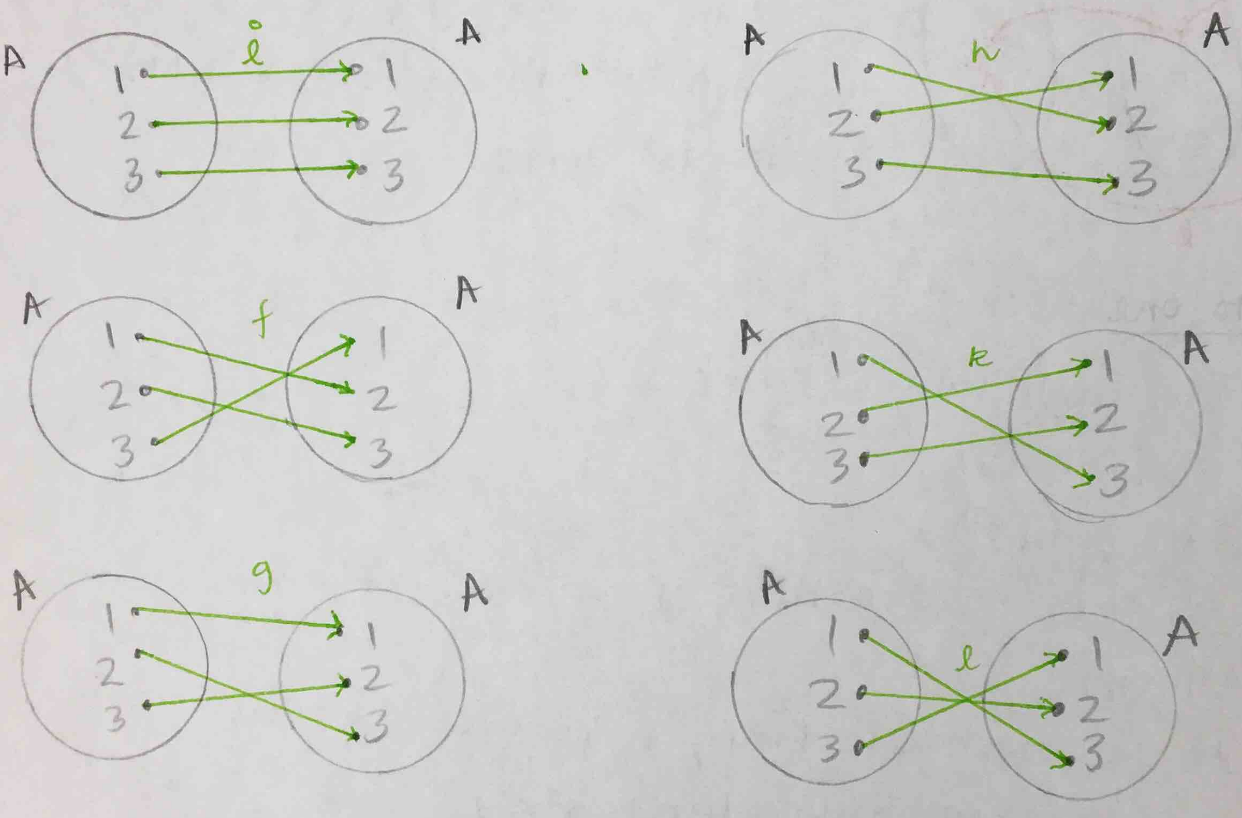
so k is one to one $\boxtimes$

Theorem: Let A be a nonempty set. Let S_A be the collection of permutations of A. Then S_A is a group under the operation of composition.

The identity of S_A is the function $i : A \to A$ where $i(x) = x \ \forall \ x \in A$

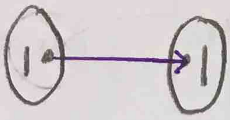
If A has size n, then we write S_n instead of S_A

Example: $A = \{1, 2, 3\}$



S_n is called the symmetric group on n letters

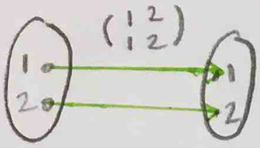
Ex: calculate the elements of S_1



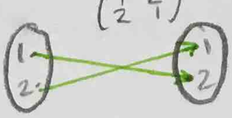
$S_1 = \{i\}$

Ex: calculate the elements of S_2

$\begin{pmatrix}1&2\\1&2\end{pmatrix}$



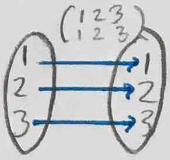
$\begin{pmatrix}1&2\\2&1\end{pmatrix}$



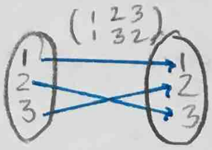
$S_2 = \left\{\begin{pmatrix}1&2\\1&2\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$

Ex: calculate the elements of S_3

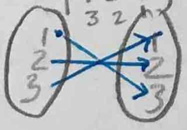
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$



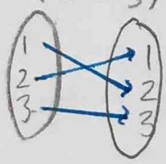
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$



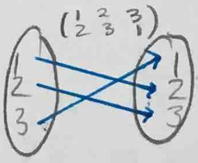
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$



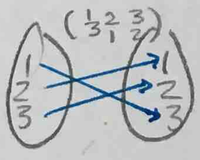
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$



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



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



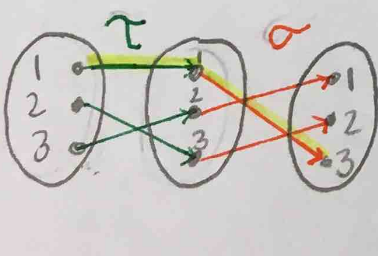
$$S_3 = \left\{\begin{matrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\end{matrix}\right\}$$

Note: In general, $|S_n| = n!$

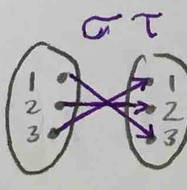
$|S_4| = 4! = 24$

Ex: $\sigma = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $\tau = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$

$\sigma\tau = \underleftarrow{\sigma \circ \tau}$



or



$\sigma\tau(1) = \sigma(\tau(1)) = \sigma(1) = 3$

$\sigma\tau(2) = \sigma(\tau(2)) = \sigma(3) = 2$

$\sigma\tau(3) = \sigma(\tau(3)) = \sigma(2) = 1$

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

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

$3 \longleftarrow 1 \longleftarrow 1$

$2 \longleftarrow 3 \longleftarrow 2$

$1 \longleftarrow 2 \longleftarrow 3$

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

$\uparrow$ has order 2

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

$\uparrow$ identity (i)

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

Ex: calculate the order of $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

$$\underbrace{\underbrace{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}$$

$$\underbrace{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}$$

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

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

that means $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ has order 3.

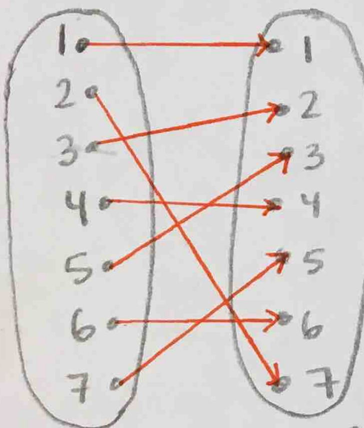
Notation: The notation $\sigma = (a_1, a_2, \dots, a_n)$ means the function that satisfies

$\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\dots$, $\sigma(a_{n-1}) = a_n$, and $\sigma(a_n) = a_1$

$\sigma(x) = x \quad \forall x$ that isn't one of the a_i

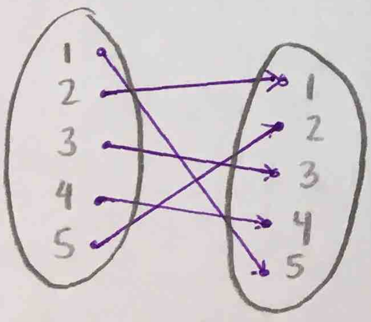
The function σ is called a cycle of length n.

Ex: In S_7 let $\sigma = (2, 7, 5, 3)$



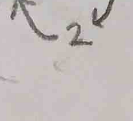
$\sigma = \begin{pmatrix}1&2&3&4&5&6&7\\1&7&2&4&3&6&5\end{pmatrix}$

Ex: Write $\beta = \begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix}$ in cycle notation



$\beta = (1, 5, 2)(3)(4)$

$\beta = (1, 5, 2) \qquad \beta = (2, 1, 5)$



$(1,5,2) = (2,1,5) = (5,2,1)$

$(1,5,2) \neq (1,2,5)$

10/19 P.2

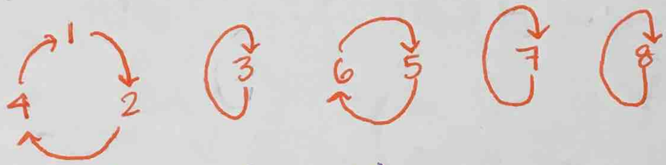
Def: Cycles are called disjoint if they don't share any common numbers.

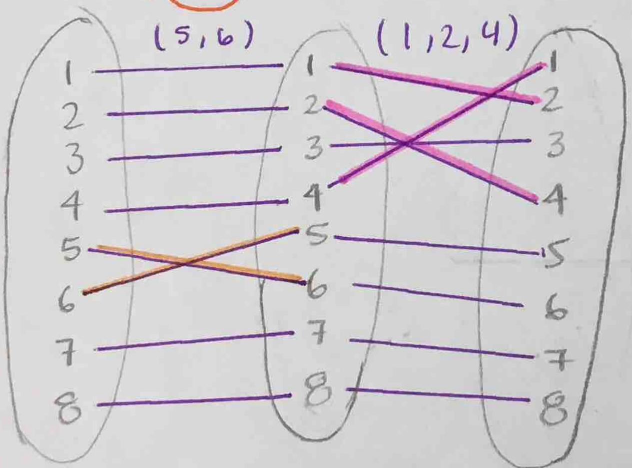
Ex:
- $(1,5,3)$ and $(2,4)$ are disjoint
- $(5,3)$ and $(2,5)$ are NOT disjoint since they share 5 in common.

Theorem: Any permutation in S_n can be written as the product of disjoint cycles.

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

$$\sigma = (1,2,4)(3)(5,6)(7)(8) = \boxed{(1,2,4)(5,6)}$$



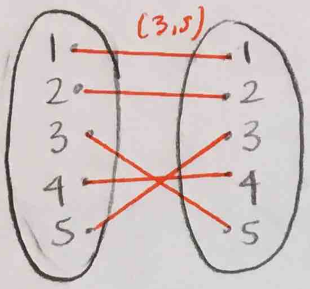


Ex: In S_9 what is $\sigma = (1,5,3)(2,7)(4,6)$ in the standard (non-cycle) notation.

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

Def A transposition is a cycle of length 2

Ex: $(3,5)$ in S_5



Theorem: Any permutation can be written as the product of transposition.

Technique

(1) Break the permutation into disjoint cycles

(2) Use the following on each cycle.

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

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

$$\sigma = \underline{(1,2,3)}\,\underline{(4,5,7,6,9)}$$

$$\underline{(1,3)(1,2)}\ \underline{(4,9)(4,6)(4,7)(4,5)}$$