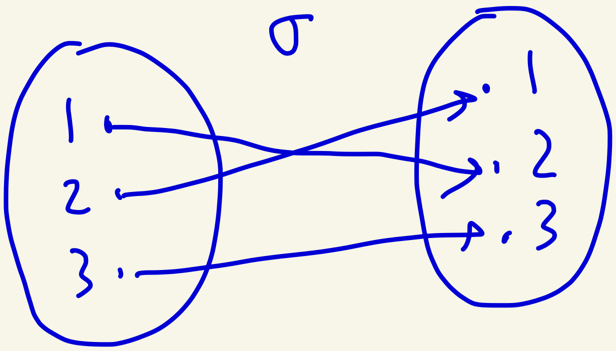
Math 4550

Topic 8 –

Symmetric group and Cayley's Theorem

Def: Let X be a non-empty set. A bijection $\sigma : X \to X$ is called a **permutation** of X

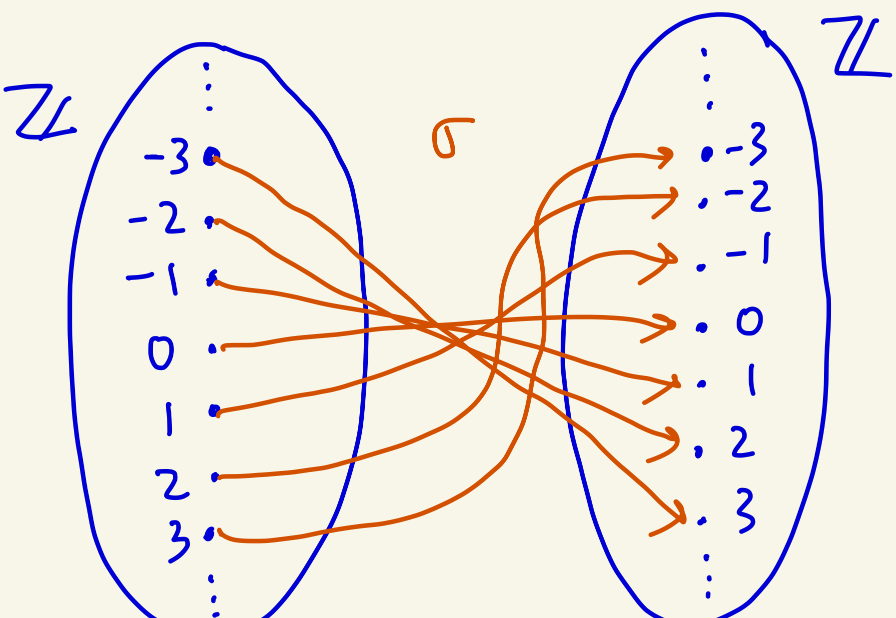
Ex: $X = \{1, 2, 3\}$



σ is a permutation of X

Ex: $X = \mathbb{Z}$, $\sigma : \mathbb{Z} \to \mathbb{Z}$, $\sigma(a) = -a$

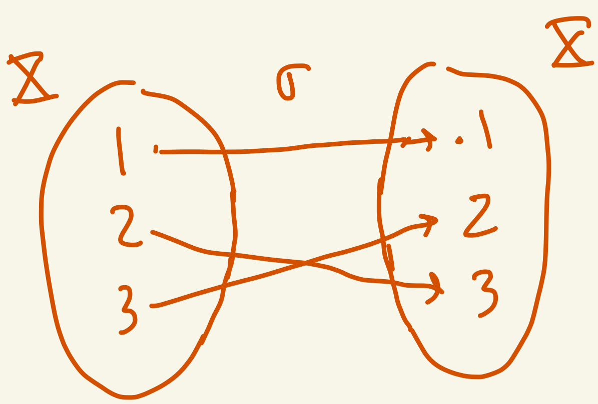
σ is a permutation of $\mathbb{Z}$.

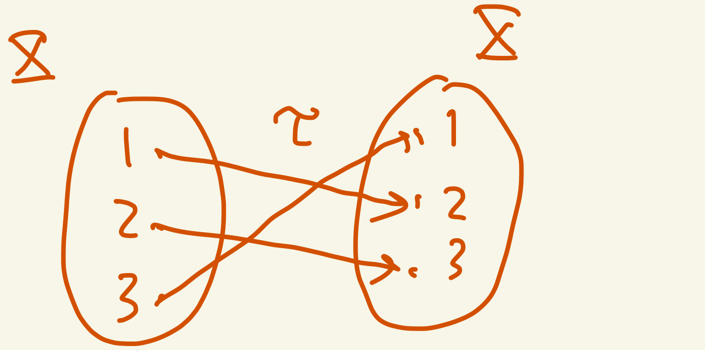


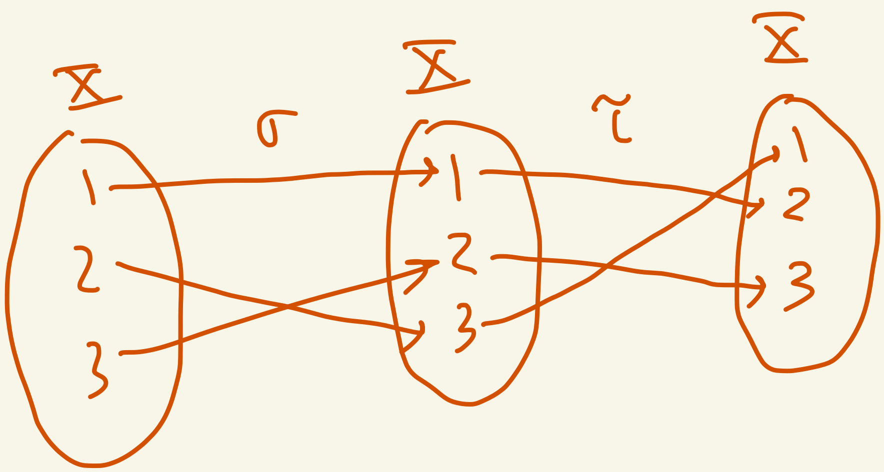
Def: Let X be a non-empty set.
Let S_X be the set of all permutations of X.
Given $\sigma, \tau \in S_X$ define the operation

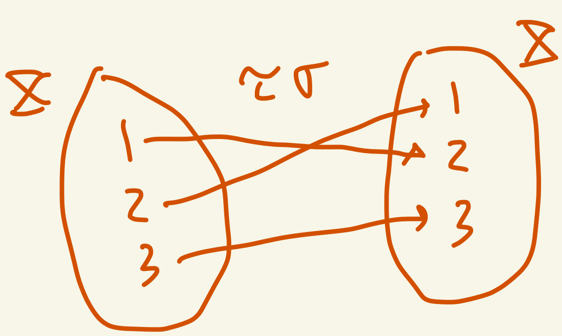
$$\sigma\tau = \sigma \circ \tau$$ ← (function composition)

Ex: $X = \{1, 2, 3\}$









Theorem: The above operation is well-defined.

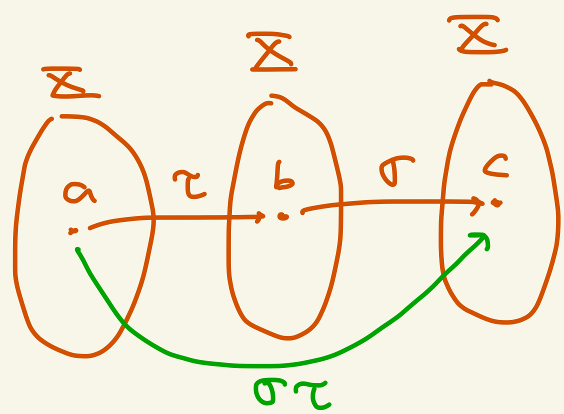
proof: Let X be a non-empty set.
Let $\sigma : X \to X$ and $\tau : X \to X$ be permutations.
We must show that $\sigma\tau$ is a permutation.

claim 1: $\sigma\tau$ is one-to-one

Suppose $\sigma\tau(a) = \sigma\tau(b)$ where $a, b \in X$.
Then $\sigma(\tau(a)) = \sigma(\tau(b))$
Since σ is one-to-one this implies that $\tau(a) = \tau(b)$.
Since τ is one-to-one this implies that $a = b$.
Hence $\sigma\tau$ is one-to-one.

claim 2: $\sigma\tau$ is onto.

Let $c \in X$.
Since σ is onto there exists $b \in X$ with $\sigma(b) = c$.
Since τ is onto there exists $a \in X$ with $\tau(a) = b$



Then,
$(\sigma\tau)(a) = \sigma(\tau(a) = \sigma(b) = c$.
Thus, $\sigma\tau$ is onto $\square$

<u>Theorem:</u> Let X be a non-empty set. Then, S_X is a group using function composition as the group operation.

<u>proof:</u>

① (closure) This was proven in the theorem above.

② (associativity). Let $\sigma, \tau, \gamma \in S_X$ and $a \in X$.

Then,

$$
\begin{aligned}
(\sigma(\tau\gamma))(a) &= \sigma((\tau\gamma)(a)) \\
&= \sigma(\tau(\gamma(a))) \\
&= (\sigma\tau)(\gamma(a)) \\
&= ((\sigma\tau)\gamma)(a)
\end{aligned}
$$

Thus, $\sigma(\tau\gamma) = (\sigma\tau)\gamma$.

③ (identity) Let $i : X \to X$ be defined as $i(x) = x$ for all $x \in X$.

Then $i \in S_X$.

HW: Show that i is 1-1 and onto

Given $\sigma \in S_X$ and $a \in X$ we have

$$(i\sigma)(a) = i(\sigma(a)) = \sigma(a)$$

$$(\sigma i)(a) = \sigma(i(a)) = \sigma(a)$$

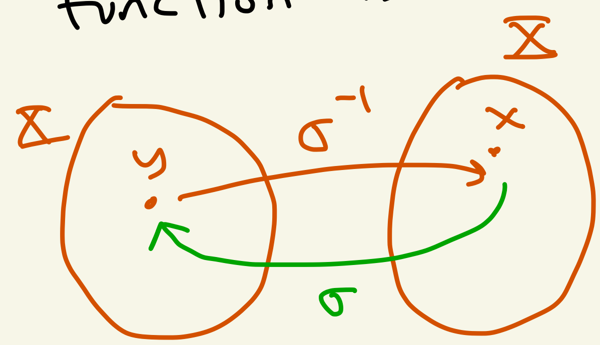
So, $i\sigma = \sigma = \sigma i$.

(4) (inverses)

Let $\sigma \in S_X$.

Define $\sigma^{-1} \in S_X$ by $\sigma^{-1}(y) = x$ iff $\sigma(x) = y$.

By Math 2450/3450 this function is well-defined.



Given $a \in X$ we have

$$(\sigma\sigma^{-1})(a) = \sigma(\sigma^{-1}(a)) = a$$

$$(\sigma^{-1}\sigma)(a) = \sigma^{-1}(\sigma(a)) = a.$$

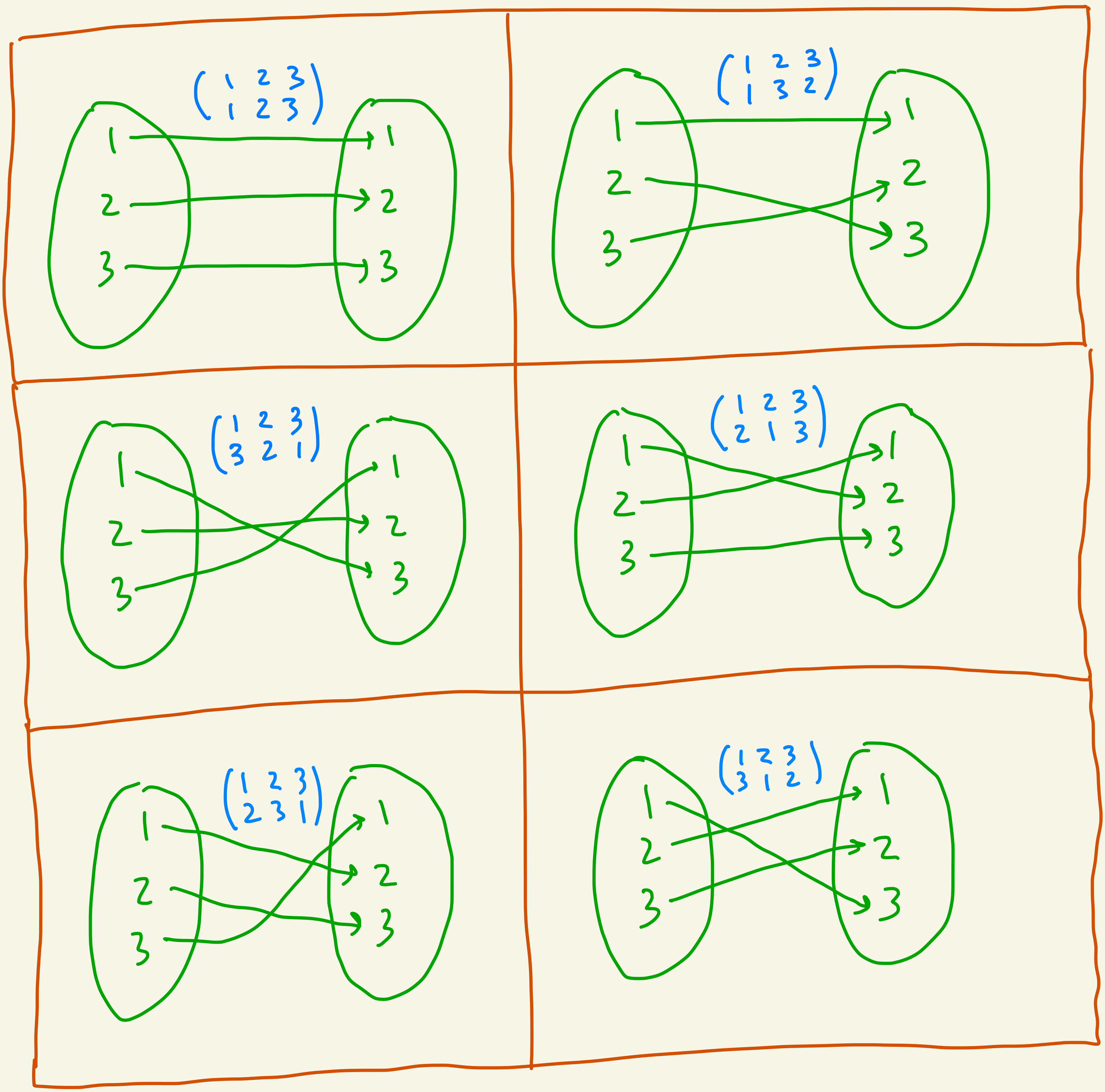
So, σ^{-1} is the inverse of σ in S_X.

$\blacksquare$

<u>Def:</u> For a non-empty set X we call S_X the <u>symmetric group on X</u>.

Def: If $X = \{1, 2, \ldots, n\}$ where $n \geq 1$ is an integer then we denote S_X by S_n.

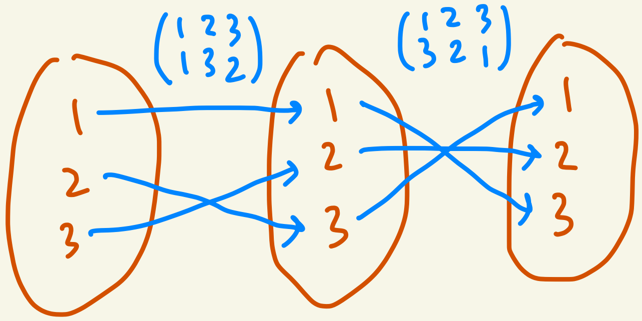
Ex: Let's calculate all the elements of S_3.



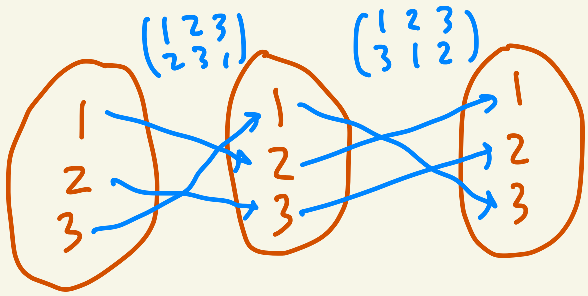
So,

$$S_3 = \left\{ \underbrace{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}_{i,\ \text{the identity}}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\}$$

Some example calculations are:



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



$$\underbrace{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}}_{\text{these are inverses}} = \underbrace{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}_{\text{identity}}$$

Theorem: (Cayley's Theorem)

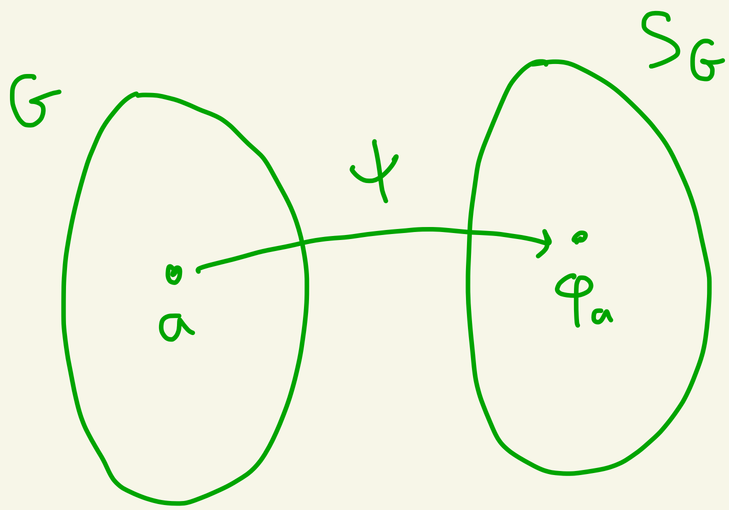
Every group is isomorphic to a subgroup of a symmetric group.

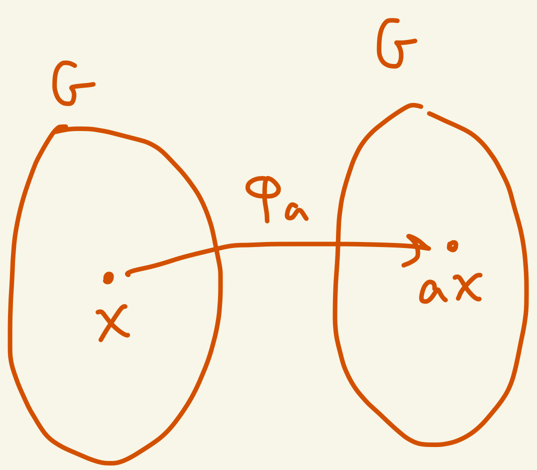
proof:

Let G be a group.

Define $\psi: G \to S_G$ by $\psi(a) = \varphi_a$

where $\varphi_a : G \to G$ by $\varphi_a(x) = ax$.





First let's show that Ψ is well-defined.

Let $a \in G$.

<u>Claim:</u> $\Psi(a) = \varphi_a$ is an element of S_G

<u>pf of claim:</u>

First we show φ_a is one-to-one.

Suppose $\varphi_a(x_1) = \varphi_a(x_2)$ where $x_1, x_2 \in G$.

Then, $ax_1 = ax_2$.

So, $a^{-1}ax_1 = a^{-1}ax_2$

Thus $x_1 = x_2$.

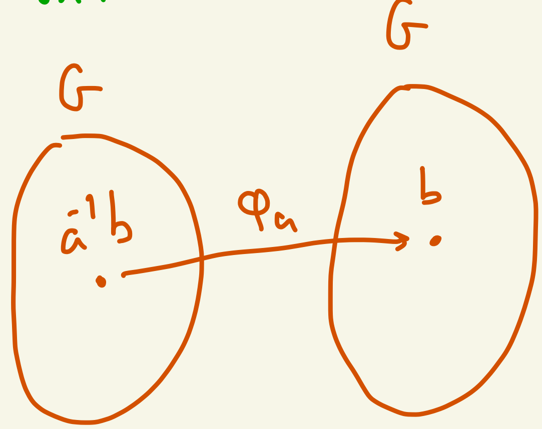
So, φ_a is one-to-one.

Second we show that φ_a is onto.

Let $b \in G$.

Then, $a^{-1}b \in G$ and

$$\varphi_a(a^{-1}b) = aa^{-1}b = b$$



Thus, φ_a is onto.

Claim: ψ is a homomorphism

proof of claim:

Let $a, b \in G$.

Given $x \in G$ we have

$$\varphi_{ab}(x) = (ab)x = a(bx)$$
$$= \varphi_a(bx) = \varphi_a(\varphi_b(x))$$
$$= (\varphi_a \varphi_b)(x)$$

Thus, $\varphi_{ab} = \varphi_a \varphi_b$

Therefore, $\psi(ab) = \varphi_{ab} = \varphi_a \varphi_b = \psi(a)\psi(b)$.

Claim: ψ is one-to-one

proof of claim:

Let $a, b \in G$.

Suppose $\psi(a) = \psi(b)$.

Then, $\varphi_a = \varphi_b$.

Let e be the identity of G.

Then,

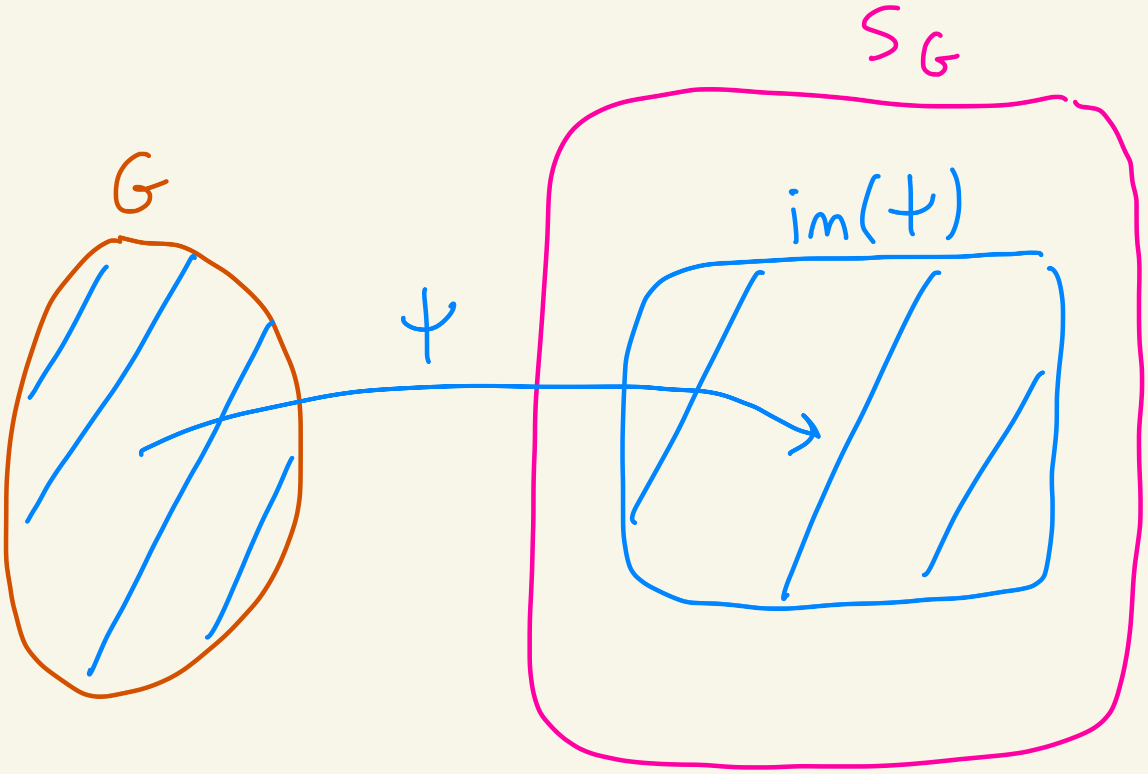
$$a = ae = \varphi_a(e) = \varphi_b(e) = be = b$$

$\boxed{\varphi_a = \varphi_b}$

So, $a = b$.

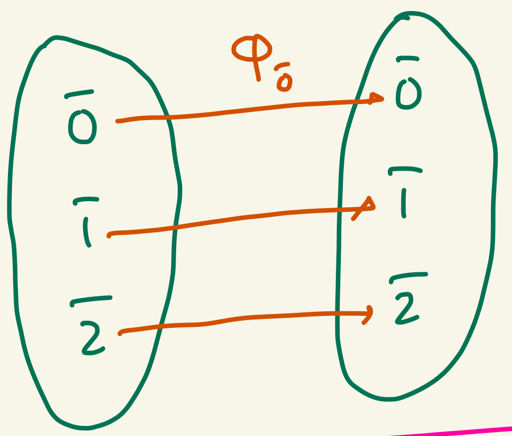
Thus, ψ is one-to-one.

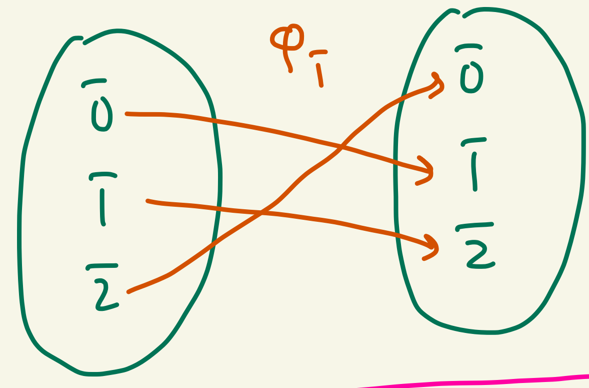
Summarizing the above we have that ψ is an isomorphism between G and the subgroup $\operatorname{im}(\psi) \leq S_G$.

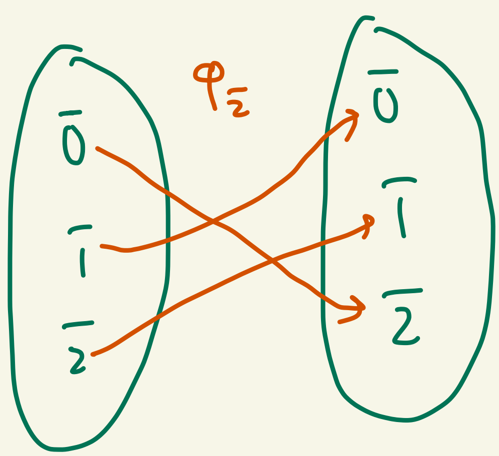


Ex: Consider $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

Then, $\varphi_{\bar{a}} : \mathbb{Z}_3 \to \mathbb{Z}_3$ is defined as $\varphi_{\bar{a}}(\bar{x}) = \bar{a} + \bar{x}$







Ex:

$\varphi_{\bar{0}}(\bar{2}) = \bar{0} + \bar{2} = \bar{2}$

$\varphi_{\bar{1}}(\bar{2}) = \bar{1} + \bar{2} = \bar{3} = \bar{0}$

$\varphi_{\bar{2}}(\bar{0}) = \bar{2} + \bar{0} = \bar{2}$