

inputs outputs

Example. Let $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ be a function defined by

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

Then σ is a **permutation** of the set $\{1, 2, 3\}$,
i.e., it “shuffles” the numbers 1, 2, and 3.

Non-example. The function f is *not* a permutation of $\{1, 2, 3\}$:

$$f(1) = 2, f(2) = 1, f(3) = 1.$$

Let σ and τ be permutations of $\{1, 2, 3\}$ given by

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

We can **compose** σ and τ to obtain $\sigma \circ \tau$, which happens to be another permutation of $\{1, 2, 3\}$. Let's see...

- $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 1$
- $(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(1) = 3$
- $(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(3) = 2$ ☺

Note: This is just like composing symmetries.

Definition: Let S_3 be the set of all permutations of $\{1, 2, 3\}$.

Discuss in your group: Let $\sigma, \gamma, \varepsilon \in S_3$ where

- $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2$
- $\gamma(1) = 2, \gamma(2) = 3, \gamma(3) = 1$
- $\varepsilon(1) = 1, \varepsilon(2) = 2, \varepsilon(3) = 3$

Compute $\varepsilon \circ \sigma$ and $\sigma \circ \gamma$.
Notice anything?

Answer: We have $\sigma \circ \gamma = \varepsilon$, because...

- $(\sigma \circ \gamma)(1) = \sigma(\gamma(1)) = \sigma(2) = 1$
- $(\sigma \circ \gamma)(2) = \sigma(\gamma(2)) = \sigma(3) = 2$
- $(\sigma \circ \gamma)(3) = \sigma(\gamma(3)) = \sigma(1) = 3$

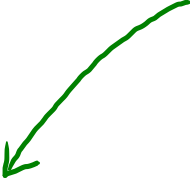
(Also, $\varepsilon \circ \sigma = \sigma$.)

Identity and Inverse

- The element $\varepsilon \in S_3$ defined by

$$\varepsilon(1) = 1, \quad \varepsilon(2) = 2, \quad \varepsilon(3) = 3$$

Analogous to
multiplying by 1
(or adding 0).



has the property $\varepsilon \circ \alpha = \alpha$ and $\alpha \circ \varepsilon = \alpha$ for all $\alpha \in S_3$.

We call ε the **identity permutation** in S_3 .

- We saw that $\sigma \circ \gamma = \varepsilon$ and $\gamma \circ \sigma = \varepsilon$. We say that σ and γ are **inverses** of each other, and we write $\gamma = \sigma^{-1}$ and $\sigma = \gamma^{-1}$.

Like $3 \cdot 5 = 1$ in U_7 .



Matrix notation: Consider again $\sigma \in S_3$ defined by

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

We can write σ in *matrix form* like this:

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

for S_3 , top row is always 1 2 3.

bottom row contains the corresponding outputs.

Problem #2: Let $\alpha, \beta, \chi \in S_n$. If $\alpha \circ \chi = \beta$, then $\chi = \alpha^{-1} \circ \beta$.

Proof: Assume $\alpha \circ \chi = \beta$.

Compose on the left by α^{-1} to get

$$\underbrace{\alpha^{-1} \circ (\alpha \circ \chi)} = \alpha^{-1} \circ \beta.$$

The left side of this equation becomes

$$\begin{aligned}\alpha^{-1} \circ (\alpha \circ \chi) &= (\alpha^{-1} \circ \alpha) \circ \chi && \text{(associative law)} \\ &= \varepsilon \circ \chi && (\alpha^{-1} \text{ is the inverse of } \alpha) \\ &= \chi && (\varepsilon \text{ is the identity})\end{aligned}$$

Thus, $\chi = \alpha^{-1} \circ \beta$.

Scrap:

$$\text{Solve } 5 \cdot x = 17.$$

$$\downarrow * \frac{1}{5}$$

$$\frac{1}{5} \cdot (5 \cdot x) = \frac{1}{5} \cdot 17$$

$$(\frac{1}{5} \cdot 5) \cdot x$$

$$1 \cdot x$$

$$x$$

$$\Rightarrow x = \frac{1}{5} \cdot 17$$