Recall that S_3 is the set of all permutations of $\{1, 2, 3\}$.

Example: With $\sigma, \tau \in S_3$ as shown below, their *composition* $\sigma \circ \tau$ is ...

$$\begin{array}{ccccc} \sigma & \circ & \tau & = & \varepsilon \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \circ & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & = & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \end{array}$$

- Here, ε is the identity element.
- Hence, $\sigma \circ \tau = \varepsilon$, and we also have $\tau \circ \sigma = \varepsilon$.
- Thus, σ and τ are inverses of each other (i.e., $\tau = \sigma^{-1}$ and $\sigma = \tau^{-1}$).

Discuss in your group: What does it mean that S_3 is a *group* under composition? What *group properties* are satisfied?

Definition: The set S_3 is a group under $\circ$ (composition) because...

1. S_3 is closed under $\circ$, i.e., if $\sigma, \tau \in S_3$, then $\sigma \circ \tau \in S_3$.

2. The operation $\circ$ is associative, i.e., $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$ for all $\sigma, \tau, \mu \in S_3$.

3. S_3 contains an identity element ε such that $\varepsilon \circ \alpha = \alpha$ and $\alpha \circ \varepsilon = \alpha$ for all $\alpha \in S_3$.

4. Each element $\sigma \in S_3$ has an inverse $\sigma^{-1} \in S_3$ such that $\sigma \circ \sigma^{-1} = \varepsilon$ and $\sigma^{-1} \circ \sigma = \varepsilon$.

Convention for notation:

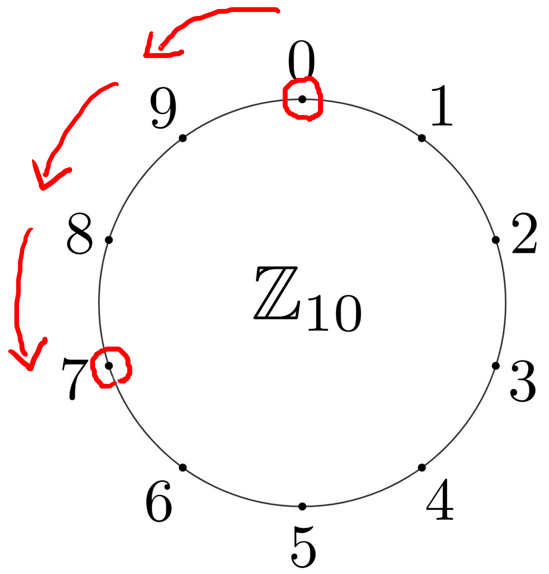
- With most groups, we'll employ the *multiplicative* notation.

  Example. In S_3, we can write $\sigma\tau$ instead of $\sigma \circ \tau$.

- But when we know that the operation is addition (e.g., the group $\mathbb{Z}$), we'll use the *additive* notation (e.g., $5 + 2 = 7$).

Additive groups

Examples of groups under *addition*: $\mathbb{Z}$, $\mathbb{Z}_{10}$, $\mathbb{Z}_7$.



In $\mathbb{Z}_{10}$: $3 + 7 = 0 \implies$ the *additive* inverse of 3 is 7

$$\implies -3 = 7$$

0 − 3

Remark: When the operation is addition, the (additive) inverse of x is denoted by $-x$, rather than by x^{-1}.

Problem #2: Are $\mathbb{Z}$, $\mathbb{Z}_{10}$, and $\mathbb{Z}_7$ also groups under multiplication?

Answer: No, since 0 does *not* have a multiplicative inverse.

~~$0 \cdot x = 1.$~~

Problem #4: In *any* group, we have $(ab)^{-1} = b^{-1}a^{-1}$.

1. *Algebraic* explanation:

We have $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a\,\varepsilon\,a^{-1} = \varepsilon$. Also $(b^{-1}a^{-1})(ab) = \varepsilon$.

Thus, the inverse of ab is $b^{-1}a^{-1}$, i.e., $(ab)^{-1} = b^{-1}a^{-1}$.

2. *Socks-shoes* explanation:

Let $a =$ putting on socks.

$b =$ putting on shoes.

How do you *undo* the product ab?

Remark: In a *commutative* group, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

Problem #5(a): What does σ^{-5} mean?

- $\sigma^5 = \sigma\,\sigma\,\sigma\,\sigma\,\sigma$.
- σ^{-1} = inverse of σ.
- σ^{-5} = ??

Elizabeth: σ^{-5} is the same as $(\sigma^{-1})^5$.

Anita: σ^{-5} equals $(\sigma^5)^{-1}$.

We have...

$$
\begin{aligned}
(\sigma^5)^{-1} &= (\sigma\,\sigma\,\sigma\,\sigma\,\sigma)^{-1} \\
&= \sigma^{-1}\,\sigma^{-1}\,\sigma^{-1}\,\sigma^{-1}\,\sigma^{-1} \qquad \longleftarrow \text{socks-shoes!} \\
&= (\sigma^{-1})^5
\end{aligned}
$$