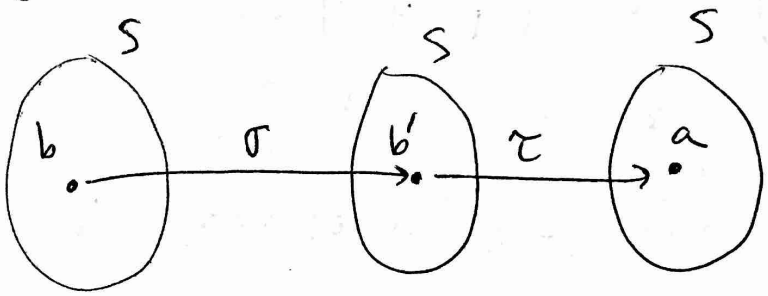
Lemma: Let S be a non-empty set and let σ, τ be two permutations of S, then $\sigma \circ \tau$ and $\tau \circ \sigma$ are both permutations of S.

pf: We must show that $\sigma \circ \tau$ is 1-1 and onto.

onto: Let $a \in S$. We must find $b \in S$, such that $(\sigma \circ \tau)(b) = a$.



Find b' s.t. $\tau(b') = a$ and b s.t. $\sigma(b) = b'$.

Then $(\tau \circ \sigma)(b) = \tau(\sigma(b)) = \tau(b') = a$.

1-1: Suppose $\exists\, b_1$ and b_2 such that

$$(\tau \circ \sigma)(b_1) = (\tau \circ \sigma)(b_2)$$

$$\tau(\sigma(b_1)) = \tau(\sigma(b_2))$$

Since τ is 1-1, $\sigma(b_1) = \sigma(b_2)$. Since σ is 1-1, $b_1 = b_2$.

Thm: Let A be a non-empty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication. That is $\langle S_A, \circ \rangle$ is a group.

pf:

(G1) The lemma shows that if $\sigma, \tau \in S_A$, then $\sigma \circ \tau \in S_A$.

(G2) Let $\sigma, \tau, \beta \in S_A$ and $a \in A$. Then,

$$[\sigma \circ (\tau \circ \beta)](a) = \sigma((\tau \circ \beta)(a)) = \sigma(\tau(\beta(a)))$$

$$[(\sigma \circ \tau) \circ \beta](a) = (\sigma \circ \tau)(\beta(a)) = \sigma(\tau(\beta(a)))$$

Therefore, $\sigma \circ (\tau \circ \beta) = (\sigma \circ \tau) \circ \beta$.

(G3) Let i be the permutation such that $i(a) = a$ for all $a \in A$. If $\sigma \in S_A$, then

$$(\sigma \circ i)(a) = \sigma(i(a)) = \sigma(a) \quad \text{and}$$

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

Therefore, $i \circ \sigma = \sigma \circ i \quad \forall \sigma \in S_A$.

(G4) Let $\sigma \in S_A$. Define $\sigma^{-1} \in S_A$ as follows:

$\sigma^{-1}(a) = a'$ where $\sigma(a') = a$ (σ^{-1} reverses σ's action)

(do a small example on the side).

(39) σ^{-1} is a bijection since σ is.

Also,

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

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

Therefore, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = i$.

---

ex: Let S_3 be the set of permutations of $A = \{1, 2, 3\}$.

Def: Let A be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the symmetric group on n letters, and is denoted by S_n.

Note $|S_n| = n!$