Permutations

Definition

A permutation of a set A is a bijection on A.

$S_A = \{\sigma : \sigma \text{ is a permutation of } A\}$

Lemma

Let A be a set. Composition of elements in S_A is associative.

Proof

Assume $\sigma, \tau, \gamma \in S_A$
Assume $x \in A$
$((\sigma\tau)\gamma)(x) = (\sigma\tau)(\gamma(x)) = \sigma(\tau(\gamma(x))) = \sigma((\tau\gamma)(x)) = (\sigma(\tau\gamma))(x)$

Lemma

Let A be a set. Composition of elements in S_A is closed.

Proof

Assume $\sigma, \tau \in S_A$

Assume $(\sigma\tau)(x) = (\sigma\tau)(y)$
Assume $\sigma(\tau(x)) = \sigma(\tau(y))$
But σ is a bijection and thus one-to-one
So $\tau(x) = \tau(y)$
But τ is a bijection and thus one-to-one
$x = y$
$\therefore$ $\sigma\tau$ is one-to-one.

Assume $y \in A$
σ is onto
So $\exists\, a \in A, \sigma(a) = y$
But τ is also onto so $\exists\, x \in A, \tau(x) = a$
$\sigma(\tau(x)) = y$
$(\sigma\tau)(x) = y$
$\therefore$ $\sigma\tau$ is onto.

$\therefore$ $\sigma\tau$ is a bijection and thus a permutation on S_A

$\therefore$ S_A is closed under the operation of composition.

Theorem

Let $A \neq \emptyset$. S_A is a group under the operation of composition.

Proof

Function composition is closed and associative (lemmas)
$\iota_A(x) = x$ is an identity permutation
$\sigma \in S_A \implies \sigma^{-1} \in S_A$, since σ is a bijection
$\therefore S_A$ is a group.

Definition

$[n] = \{1, 2, 3, \ldots, n\}$

$S_n = \{\sigma : \sigma \text{ is a permutation of } [n]\}$

Note that $|S_n| = n!$.

Permutations can be represented by $2 \times n$ matrices, where the top row contains $1, \ldots, n$ and the bottom row represents how the top row is permuted.

Example

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

Permutations can also be represented by a decomposition of cycles:

$$(abcd \cdots z) = \begin{pmatrix} a & b & c & \ldots & z \\ b & c & d & \ldots & a \end{pmatrix}$$

Elements that do not change are omitted.

The identity permutation is represented by $()$

Example

$S_3 = \{(123), (132), (213), (231), (312), (321)\}$

$|S_3| = 3! = 6$

Example

$$
\begin{array}{lll}
S_4: & () & 1 \\
& (ab) & \frac{4\cdot 3}{2} = 6 \\
& (abc) & \frac{4\cdot 3\cdot 2}{3} = 8 \\
& (abcd) & \frac{4\cdot 3\cdot 2\cdot 1}{4} = 6 \\
& (ab)(cd) & \frac{4\cdot 3}{2\cdot 2} = 3
\end{array}
$$

$|S_4| = 4! = 1 + 6 + 8 + 6 + 3 = 24$