X^X is the set of all maps (bijective) from X to X.

S(X) is also called the permutation group on X.

Note: $X \xrightarrow{f} X$, $X \xrightarrow{g} X$, $g \circ f : X \to X$.

We can show that $|S(X)| = |X|!$

↳ Cardinality of X

$\boxed{\text{Lecture 2-1}}$ Class No. 2

Examples of Monoids:

~~$(\mathbb{N}, +, \times)$~~, $(\mathbb{N}, +)$, $(\mathbb{N}^*, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}^*, \cdot)$

$(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ . . .

If X is the set, the power set of X is defined as

$P(X) = \{A \mid A \subseteq X\}$.

The power set P(X) is a monoid with the operation union. The only inverse is ϕ.

$M^X = \{x \in M \mid x$ is invertible, ie. $y \in M$, s.t $x \cdot y = y \cdot x = e\}$

M^X is a group.

Another example: $(P(X), \cap)$

~~non-empty~~

X is the identity element in monoid.

X^X = Maps(X, X) or $X^X = \{f : X \to X \text{ maps}\}$

$\circ$ = Composition is a binary operation

Identity map is the ~~identy~~ identity element

In general $(X^X, \circ)$ is not commutative for $|X| \geq 3$. However, it is associative

$(X^X)^\times = S(X) = \{$ set of invertible or bijective maps $\}$
$=$ permutation group on X.

If X is finite, $S(X)$ is also finite, &
$|S(X)| = |X|\,!$

<u>Product Monoid</u> $(M_i, *_i)$ $i \in I$ index set

By axiom of choice $\prod_{i \in M} M_i \neq \emptyset$

$x = (x_i)_{i \in I}$, $y = (y_i)_{i \in I}$, $x \times y = (x_i *_i y_i)_{i \in I}$

Identity : $e = (e_i)_{i \in I}$

Another example: $\prod_{i \in I} X = X^I$

$I = [a, b]$ $X = \mathbb{R}$, $\mathbb{R}^I$
i.e all real valued function defined on the interval $[a, b]$.

Special case for product monoid

$(M_i, *_i)$ family of monoids

$$\coprod_{i \in I} M_i = \left\{ x = (x_i)_{i \in I} \in \prod_{i \in I} M_i \;\middle|\; x_i = e_i \text{ for almost all } i \in I \right\}$$

$$\subseteq \prod_{i \in I} M_i$$

There exists a finite subset $J \subseteq I$, such that $\cancel{x_i \neq e_i}$, $\cancel{\forall}$ $x_i = e_i$ $\forall\ i \notin J$

$$\coprod_{i \in I} M_i = \prod_{i \in I} M_i \quad \text{if } I \text{ is finite}$$

$$\left(\coprod_{i \in I} M_i, *_i\right) \text{ is a monoid (sub-monoid)}$$

Special case:

$$M_i = M \quad \forall i,$$

$$M^{(I)} = \{ x : I \to M \mid x_i = e \text{ for almost all } i \in I \}$$

Definition of Cardinality:

Let X be a finite set, iff $\exists$ $n \in \mathbb{N}$, & a bijective map $\{(1, 2 \ldots n)\} \xrightarrow{\simeq} X$

~~There~~ There n is a unique $(\mathbb{Z})$ & is called the cardinality of X denoted by $|X|$.

$(M, *) \xrightarrow{f} (M', *')$ $\qquad f(x * y) = f(x) *' f(y)$ $\quad \forall\ x, y \in M$,

then f is called monoid homomorphism

f is automorphism if f is bijective.

Prime numbers: $(\mathbb{N}^*, \cdot)$. Let $a, b \in \mathbb{N}^*$.

a/b, (a divides b) if $b = ac$ for some $c \in \mathbb{N}^*$

a is irreducible (or prime for this case) if $a \neq e$ and the only divisor of a are e and a.

$\mathbb{P}$ is the set of all prime numbers.

$$\mathbb{P} = \{ 2, 3, 5, 7, 11, 13, \ldots \}$$