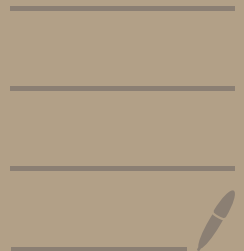


# Monoid

---



1.1

Def: Monoid 幺半群

$(S, *)$  is a monoid  $\Leftrightarrow$  this binary operation satisfies:

1) law of association

$$\forall x, y, z \in S, x*(y*z) = (x*y)*z$$

2) have Identity

$$\exists e \in S, \forall x \in S, e*x = x*e = x$$

In addition:

$(S, *)$  is commutative monoid  $\Leftrightarrow$  this operation satisfies:

law of commutation:

$$\forall x, y \in S, x*y = y*x$$

Prop. Identity of a monoid is unique.

Proof. assume  $e_1, e_2$  are Identities of monoid  $(S, \cdot)$

$$\text{then } e_1 = e_1 \cdot e_2 = e_2$$

Def.  $(T, \cdot)$  is a submonoid of  $(S, \cdot) \Leftrightarrow$

(i)  $T$  is closed under this operation

(ii)  $e \in T$

Def.  $f: S \rightarrow T$  is a map,  $(S, \cdot)$   $(T, *)$  are monoids

$f$  is a monoid homomorphism  $\Leftrightarrow$

$$\forall x, y \in S, f(xy) = f(x) * f(y) \quad \&$$

$$f(e) = e'$$

where  $e$  and  $e'$  are identities of  $S, T$

Example:  $f: (N, +) \rightarrow (S, \cdot)$  where  $(S, \cdot)$  is monoid

$$\text{suppose } f(n) = x^n, \quad f(0) = x^0 = e$$

$$\text{then } f(m+n) = x^{m+n} = x^m \cdot x^n = f(m) \cdot f(n)$$

Def.  $(S, \cdot)$  is a monoid,  $A \subset S$

$$\langle A \rangle = \bigcap \{ T \subset S : T \supset A, T \text{ is monoid} \}$$

Prop.  $(S, \cdot)$  is a monoid,  $A \subset S$ ,  $\langle A \rangle$  is a monoid  
therefore it's also the smallest submonoid that contain  $A$

Proof.

- (1) for all  $T$ ,  $e \in T \Rightarrow e \in \langle A \rangle$
- (2) for any  $x, y \in \langle A \rangle$ ,  $x, y \in T$ ,  $x \cdot y \in T$   
thus  $x \cdot y \in \langle A \rangle$

Def. suppose  $(S, \cdot)$   $(T, *)$  are monoids and  $f: S \rightarrow T$  a map  
 $f$  is monoid isomorphism  $\Leftrightarrow$

- (1)  $f$  is bijective
- (2)  $f$  is monoid homomorphism

Prop.  $f: (S, \cdot) \rightarrow (T, *)$  is a monoid isomorphism  $\Leftrightarrow$   
 $f^{-1}: (T, *) \rightarrow (S, \cdot)$  is a monoid isomorphism