$f: A \longrightarrow B$ $\quad g: B \longrightarrow A$

$g \circ f : A \to A \quad , \quad f \circ g : B \to B$

If f is invertible ($\equiv f$ is bijection) & g is the inverse, then $g \circ f = I_A$

, $f \circ g = I_B$

Conversely, suppose we have $g \circ f = I_A$ & $f \circ g = I_B$ then f is invertible

$b \in B$, then $g(b) \in A$, then $f(g(B)) = b$

1) so, f is onto

Suppose, $f(a) = f(b)$ apply g and get $a = b$

2) so, f is one-one

① If $f \circ g = I_B$, then f is onto

② If $g \circ f = I_A$, then f is one-one

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Composition of maps is associative

But $g \circ f = f \circ g$ is false

Suppose X is a non-empty set. A map $X \times X \to X$ is also called a binary operation on X.

Eg:- $\mathbb{N} \times \mathbb{N} \longmapsto \mathbb{N}$

① $(a, b) \longmapsto a + b$

② $(a, b) \longmapsto ab$

Binary operation is denoted by ab or $a+b$ or $a * b$ or $a.b$

Eg: $\{a, b, c\}$

	a	b	c
a	b	c	a
b	c	a	c
c	a	a	a

How many binary operations are there on $\{a,b,c\}$?

$(ab)c \overset{?}{=} a(bc)$

$$\begin{array}{ccc} (ab)c & & a(bc) \\ \| & & \| \\ cc & & ac \\ \| & & \| \\ a & & a \end{array}$$

$b(ac) = (bc)c$

$$\begin{array}{ccc} b(ac) & & (bc)c \\ \| & & \| \\ ba & \overset{NO}{—} & cc \\ \| & & \| \\ c & & a \end{array}$$

Q)

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$a(bc) \overset{?}{=} (ab)c$

$$\begin{array}{ccc} a(bc) & & (ab)c \\ \| & & \| \\ a \cdot a & & bc \\ \| & & \| \\ a & & a \end{array}$$

$c(ab) \overset{?}{=} (ca)b$

$$\begin{array}{ccc} c(ab) & & (ca)b \\ \| & & \| \\ cb & & cb \\ \| & & \| \\ a & & a \end{array}$$

This operation is commutative.

Are comm. operations associative?

Try to find one on $\{a, b, c\}$.

→ Suppose X is a set with a binary operation. Then an element $e \in X$ is called an identity element of X if $ex = xe = x \quad \forall x \in X$

Suppose e & e' are both identity then

$e = ee' = e'$

e' is an identity

e is an identity

So there is atmost one identity element in for a binary operation.

Composition is a binary operation on maps (A, A) non-commutative & associative.

Suppose e is the identity of a binary operation on a set X.

Let $x \in X$

Suppose $y \in X$ is such that $xy = yx = e$

then we say that y is an inverse of x

Suppose $z \in X$ such that $xz = zx = e$

$$xy = xz = yx = zx = e$$

Inverses are not unique

Groups

Def^n: Suppose G is a non-empty set together with a binary operation. Then G is a group if it satisfies the following properties:

1. Associativity, $(xy)z = x(yz) \quad \forall\, x, y, z \in G$
2. Existence of identity, there exist an element $e \in G$ such that

$$xe = ex = x \quad \forall\, x \in G$$

3. Existence of inverse: For $x \in G$ there exists $y \in G$ s.t.

$$xy = yx = e$$

Example:

1. $\mathbb{Z}$ with addition
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with addition
3. $\mathbb{Q}^{\times}, \mathbb{R}^{\times}, \mathbb{C}^{\times}$ with multiplication

(4) $\{0, 1\}$

	0	1
0	0	1
1	1	0

(5) $\{-1, 1\}$ with multiplication

(6) $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ with addition of congruence classes.

Notation: The inverse of x is normally denoted by x^{-1}. But if the operation is denoted by $+$ then the inverse of x is denoted by $-x$.

$z = ze = z(xy) = (zx)y = ey = y$

Associativity forces inverse of an element to be unique in a group

Suppose y & z are inverses of x

Cancellation law holds in G

$ab = ac \Rightarrow b = c$ & $ba = ca \Rightarrow b = c$

Let $S = \{1, 2, 3\}$

$S_3 \rightarrow G$ = the set of bijection from S to itself with composition of images

$x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$xy = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\quad yx = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

clearly $yx \neq xy$

The number of elements in $S_3 = 6$

S_3 is a non-commutative group.

The commutative groups are called abelian groups otherwise non-abelian.
A bijection of a set is also called permutation.

S_n = the group of permutation of a set of n elements with respect to composition of images

The size of $S_n = n!$

$\mu_n = \{\text{Roots of } x^n = 1\}$ wrt multiplication