Binary composition

- $A \rightarrow$ a non-empty set.
- A binary composition on A is a mapping

$$\circ : A \times A \rightarrow A$$
$$(a, b) \rightarrow a \circ b$$

Examples $*, +, \cdot, \oplus, \odot$ (notations).

$(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, -)$

Example: $(\mathbb{Z}, \circ)$ defined by $a \circ b = a + 2b$, $a, b \in \mathbb{Z}$

e.g. $2 \circ 3 = 2 + 2 \cdot 3 = 8$

$3 \circ 0 = 3$

Example: $(\mathbb{Q}, *)$ defined by $a * b = \frac{1}{2}ab$.

e.g. $2 * 5 = 5$, $3 * 8 = 12$

closure property : $a \circ b \in A \quad \forall a, b \in A$.

A is closed under the binary composition $\circ$ defined on A

Example:

$\mathbb{N} \rightarrow$ closed under addition
$\rightarrow$ not closed under subtraction.

$a, b \in \mathbb{N} \Rightarrow a + b \in \mathbb{N}$

$a, b \in \mathbb{N} \not\Rightarrow a - b \in \mathbb{N}$ for some a, b, $a - b$ may not be a natural no.

Commutative $a \circ b = b \circ a \quad \forall a, b \in A$

associative $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in A$

Example: 1) $\mathbb{R}$ + Commutative, associative.

· Commutative, associative

– neither commutative, nor associative.

2) $S \to$ non-empty set

$P(S)$ $\cap$ Commutative, associative

$\cup$ Commutative, associative

Δ (Symmetric difference) Commutative, associative

3) $M_2(\mathbb{R}) \to 2 \times 2$ real matrices

$\circ \to$ matrix multiplication.

associative, but not commutative.

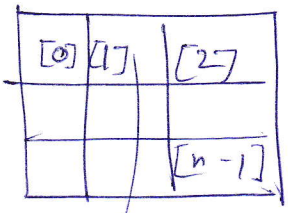
$\mathbb{Z}_n$ = classes of residues of integers modulo n

$= \{[0], [1], [2], \ldots, [n-1]\}$

$+$ $[a] + [b] = [a+b]$

$\cdot$ $[a] \cdot [b] = [ab]$

$\mathbb{Z}$



$a, b \in \mathbb{Z}$ in this class if $a - b$ is divisible by n

$a = qk_1 + l$

$b = qk_2 + l$

$a - b = n(k_1 + k$

Both $+$ & $\cdot$ are well defined

T.P.T. $[a]=[a'], [b]=[b'] \Rightarrow [a+b]=[a'+b']$ & $[ab]=[a'b']$

i.e. independent of the choice of representatives of the equivalence classes

$[a]=[a'] \Rightarrow a-a' = nk$ for some integer k

$[b]=[b'] \Rightarrow b-b' = np$ for some integer p.

$\therefore (a+b)-(a'+b') = (a-a')+(b-b') = n(k+p)$.

$\Rightarrow [a+b]=[a'+b']$.

Also $ab - a'b' = (a'+nk)(b'+np) - a'b'$

$= a'b' + nkb' + npa' + n^2kp - a'b'$

$= n(kb' + pa' + nkp)$.

$\Rightarrow [ab]=[a'b']$.

Example: $\mathbb{Z}_3 = \{[0], [1], [2]\}$

Composition table

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Groupoid Algebraic System $(G, \circ)$, closure property holds

- G non-empty set on which a binary composition $\circ$ is defined.

$a \circ b \in G \ \forall \ a, b \in G$.

- Some algebraic structure is imposed on G by $\circ$ and $(G, \circ)$ becomes an algebraic system

- $(G, \circ)$ is said to be a groupoid.

Example:
- $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$
- $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n, \cdot)$
- $(M_2(\mathbb{R}), +)$

- Commutative groupoid - if $\circ$ is commutative.
- identity element - an element $e \in G$ is said to be an identity element in the groupoid $(G, \circ)$ if $a \circ e = e \circ a = a \ \forall \ a \in G$.

Examples:
- $(\mathbb{Z}, +)$ commutative groupoid
- $(\mathbb{Z}, -)$ not commutative
- 0 is an identity element in $(\mathbb{Z}, +)$
- There is no identity element in $(\mathbb{Z}, -)$

- left identity - an element $e \in G$ is said to be a left identity if $e \circ a = a \ \forall \ a \in G$.
- right identity - an element $e \in G$ is said to be a right identity if $a \circ e = a \ \forall \ a \in G$.

Examples:
- 0 is a left as well as right identity in $(\mathbb{Z}, +)$
- 1 is a left as well as right identity in $(\mathbb{Z}, \cdot)$
- 0 is a right identity in $(\mathbb{Z}, -)$, but there is no left identity in the groupoid $(\mathbb{Z}, -)$

Uniqueness of identity

If a groupoid $(G, \circ)$ contains an identity element, then it is unique.

Proof:

$$e \circ a = a \circ e = a \quad \forall a \in G$$
$$f \circ a = a \circ f = a \quad \forall a \in G$$

if possible, let there be two identity elements e and f in $(G, \circ)$.

Now $e \circ f = f$ by the property of e
Also $e \circ f = e$ by the property of f
$\Rightarrow f = e$.

Equality of left and right identity

If a groupoid $(G, \circ)$ contains a left identity as well as a right identity, then they are equal & the equal element is the identity element in the groupoid.

Proof: $e \to$ a left identity, $f \to$ a right identity

$e \circ a = a \ \forall a \in G$, $a \circ f = a \ \forall a \in G$.

Then $e \circ f = f$ by the property of e
$e \circ f = e$ by the property of f
$\Rightarrow e = f$ & we get $e \circ a = a \circ e = a \ \forall a \in G$
$\Rightarrow e$ is the identity element of $(G, \circ)$ the groupoid.

Inverse

- $(G, \circ)$ groupoid with the identity element e.
- $a \in G$ is said to be invertible if $\exists\ a' \in G$ s.t. $a \circ a' = a' \circ a = e$.
- a' is said to be an inverse of a in the groupoid.

- **left inverse** : $a \in G$ is said to be a left invertible if $\exists\ b \in G$ s.t. $b \circ a = e$.
  - b is said to be a left inverse of a in the groupoid.
- **right inverse** : $a \in G$ is said to be right invertible if $\exists\ b \in G$ s.t. $a \circ b = e$
  - b is said to be a right inverse of a in the groupoid.

Example: $(\mathbb{Z}, \cdot)$, 1 is the identity element

$\exists\ x \in \mathbb{Z}$ s.t.

$-1 \in \mathbb{Z}$ is invertible as $x(-1) = (-1)x = 1$ (take $x = -1$)

$-2 \in \mathbb{Z}$ is neither left invertible nor left invertible as no element x in $\mathbb{Z}$ exists s.t.

$$x \cdot 2 = 2 \cdot x = 1$$

Example: $(\mathbb{Q}, \cdot)$, 1 is the identity element

$\exists x \in \mathbb{Q}$ s.t.

- $2 \in \mathbb{Q}$ is invertible as $x \cdot 2 = 2 \cdot x = 1$ (take $x = \frac{1}{2} \in \mathbb{Q}$)
- $0 \in \mathbb{Q}$ is not invertible.

- If e is just a left identity in the groupoid $(G,\circ)$, then an element $a \in G$ is said to be left $\circ$-e-invertible if $\exists$ an element $b \in G$ s.t. $b \circ a = e$ and a is said to be right e-invertible if $\exists$ an element $c \in G$ s.t. $a \circ c = e$.

- b is said to be a left e-inverse of a & c is said to be a right e-inverse of a.

- Similarly, if e is just a right identity, then a left e-inverse and a right e-inverse can be defined in a similar manner.

Example: $(\mathbb{Z}, -)$, 0 a right identity.

Any $a \in \mathbb{Z}$ has a left 0-inverse as well as a right 0-inverse.

$\exists\ b \in \mathbb{Z}$ s.t. $b - a = 0$

$b = a$ is a left 0-inverse of a

$\exists\ c \in \mathbb{Z}$ s.t. $a - c = 0$.

$c = a$ is a right 0-inverse of a.

Example: • Groupoid $(\mathbb{Z}, *)$,

• $*$ defined by $a * b = a + 2b$, $a, b \in \mathbb{Z}$.

• 0 is a right identity. $\quad a * 0 = a$.

• $3 \in \mathbb{Z}$ is left-0-invertible but no right 0-invertible

$\exists\ b \in \mathbb{Z}$ s.t. $b * 3 = 0$

i.e. $b + 6 = 0$

$b = -6 \in \mathbb{Z}$

$\exists\ c \in \mathbb{Z}$ s.t. $3 * c = 0$

i.e. $3 + 2c = 0$

$c = -\frac{3}{2} \notin \mathbb{Z}$.

Semigroup

A groupoid $(G, \circ)$ is said to be a semigroup

(i) $a \circ b \in G \quad \forall\ a, b \in G$

(ii) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall\ a, b, c \in G$

Commutative semigroup if $\circ$ is commutative

Examples
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ semigroups
- $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ semigroups
- $(\mathbb{Z}, -)$ is not a semigroup.

  $a - (b - c) \neq (a - b) - c$
- $(\mathbb{Z}_n, \cdot)$ Commutative semigroup.

Positive integral powers of $a \in G$, G is a semigroup

- $a^1 = a$, $a^2 = a \circ a$, $a^3 = a \circ a \circ a$, $\cdots$, $a^{n+1} = a^n \circ a$ $\forall n \in \mathbb{N}$ (ignoring parentheses)
- If $(S, \circ)$ is a semigroup. Then $a^{m+n} = a^m \circ a^n$.

  a^{m+n}: $a \circ a \circ \cdots \circ a$ ($m+n$ times)

  $a^m \circ a^n$: $(a \circ a \circ \cdots \circ a) \circ (a \circ a \circ \cdots \circ a)$ (m times, n times).

Monoid

A semigroup $(G, \circ)$ containing the identity element is said to be a monoid.

(i) $a \circ b \in G \quad \forall a, b \in G$

(ii) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$

(iii) $\exists$ an element $e \in G$ s.t. $a \circ e = e \circ a = a \quad \forall a \in G$.

Commutative monoid if $\circ$ is commutative.

Examples:

- $(\mathbb{Z}, +)$ monoid, $0 \rightarrow$ identity element
- $(\mathbb{Z}, \cdot)$ monoid, $1 \rightarrow$ identity element
- $(E, \cdot)$ semigroup, but not monoid, $E \rightarrow$ set of all even integers. $(2n) \cdot e = e \cdot (2n) = 2n$
- $(\mathbb{Z}_n, \cdot)$ monoid, $[1] \rightarrow$ identity element. $\rightarrow e = 1 \notin E$.
- $(M_2(R), \cdot)$ monoid, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow$ identity element. Not commutative.

Example 1: in next page

Uniqueness of inverse if exists

- In a monoid $(M, \circ)$, if an element a is invertible then it has a unique inverse.

proof: if not, let a' & a'' be two inverses of a

$\therefore a \circ a' = a' \circ a = e, \quad a \circ a'' = a'' \circ a = e$

$(a' \circ a) \circ a'' = a' \circ (a \circ a'')$ as monoid

$e \circ a'' = a' \circ e$

$a'' = a'$

Theorem In a monoid $(M, \circ)$, if an element a is left-invertible as well as right-invertible, then a is invertible.

Proof Let e be the identity element of M, b be a left-inverse & c be a right-inverse of a

Thus $b \circ a = e$ and $a \circ c = e$.

Now $b \circ (a \circ c) = (b \circ a) \circ c$ as $\circ$ is associative

$\Rightarrow b \circ e = e \circ c \Rightarrow b = c$

Thus $b \circ a = a \circ b = e \Rightarrow a$ is invertible.

Unit In a monoid $(M, \circ)$, an invertible element is said to be a unit.

Quasigroup

- A groupoid $(G, \circ)$ is said to be a quasigroup if for two elements $a, b \in G$, each of the equations $a \circ x = b$ and $y \circ a = b$ has a unique soln. in G.

Examples $(\mathbb{Z}, +)$ is a groupoid & $\left.\begin{matrix} a + x = b \\ y + a = b \end{matrix}\right\}$ $a, b \in \mathbb{Z}$

Each has soln. $(x = b - a,\ y = b - a)$ in $\mathbb{Z}$ respectively.

$\therefore (\mathbb{Z}, +)$ is a quasigroup.

$(\mathbb{Z}, \cdot)$ is a groupoid, but not a quasigroup.

Take $2, 3 \in \mathbb{Z}$

$2 \cdot x = 3$ has no soln in $\mathbb{Z}$

$a \cdot x = b$, $y \cdot a = b$ $\Big\}$ $a, b \in \mathbb{Z}$

soln of each need not be an element of $\mathbb{Z}$

$(\mathbb{Z}, -)$ is a quasigroup, but not a semigroup.

$(M_2(R), \cdot)$ is a groupoid, but not a quasigroup.

$AX = B$, $A, B \in M_2(R)$ has no soln. if A is singular

Example 1: Define a binary composition $\circ$ in $\mathbb{Z}$ by

$$\boxed{a \circ b = a + b - ab} \text{ for } a, b \in \mathbb{Z}.$$

Show that $(\mathbb{Z}, \circ)$ is a monoid.

Let $a, b, c \in \mathbb{Z}$.

Then $a \circ (b \circ c) = a \circ (b + c - bc)$

- closure ✓
- associativity ✓
- identity ✓

$= a + (b + c - bc) - a(b + c - bc)$

$= a + b + c - bc - ab - ca + abc$.

$(a \circ b) \circ c = (a + b - ab) \circ c$

$= (a + b - ab) + c - (a + b - ab)c$

$= a + b + c - ab - ac - bc + abc$.

Thus $\boxed{a \circ (b \circ c) = (a \circ b) \circ c}$.

To check if $\exists\, e \in G$ s.t. $a \circ e = e \circ a = a$ $\forall\, a \in G$.

$a \circ e = a + e - ae = a$, $e \circ a = e + a - ea = a$

$e(1 - a) = 0$, $e(1 - a) = 0 \Rightarrow \boxed{e = 0}$

Example: Let $(S, \circ)$ be a finite semigroup and $a \in S$. Prove that there exist positive integers m, n s.t.

$$a^{m+n} = a^m.$$

Exercise Deduce that a^{mn} is an idempotent element in the semigroup.

($x \in S$ idempotent element in S means $x \circ x = x$)

Soln $(S, \circ)$ semigroup.

$$\text{So } a \in S \Rightarrow a \circ a = a^2 \in S$$
$$a \circ (a \circ a) = a^3 \in S$$
$$\vdots$$

Since S finite, $\exists$ +ve integers $m \neq p$ $(p > m)$ s.t.

$$a^p = a^m.$$

Let $p = m + n$ $\therefore a^{m+n} = a^m$ for some +ve integers m, n.

Now $a^m = a^{m+n} \Rightarrow a^m \circ a^n = a^{m+n} \circ a^n$

$$\Rightarrow a^{m+n} = a^{m+2n}$$

$$a^{m+n} = a^{m+2n} \Rightarrow a^{m+n} \circ a^n = a^{m+2n} \circ a^n$$

$$\Rightarrow a^{m+2n} = a^{m+3n}$$

$$\vdots$$

$$a^m = a^{m+n} = a^{m+2n} = \cdots = a^{m+mn}$$

Again $a^{2m} = a^m \circ a^m = a^m \circ a^{m+mn} = a^{2m+mn}$

Similarly, $a^{3m} = a^{3m+mn}$, $a^{4m} = a^{4m+mn}$, $\cdots$, $a^{mn} = a^{mn+mn}$

$x = x \circ x$, $x = a^{mn}$ is a idempotent element.

Note. In a finite semigroup $(S, \circ)$, for each $a \in S$, a^n is an idempotent element.

Example: Let $(S, \circ)$ be a semigroup with the identity element e. (i.e. Monoid)
If each element of S is right-invertible, then prove that each element of S is also left-invertible.

Soln: $a \in S$ right-invertible, let a' be a right inverse of a.

$\therefore a \circ a' = e$.

Let a'' be a right-inverse of $a' \in S$
($\because$ each element of S is right invertible)

$\therefore a' \circ a'' = e$.

Claim: a' is a left-inverse of a.

proof of the claim

$$a' \circ a = (a' \circ a) \circ e = (a' \circ a) \circ (a' \circ a'')$$
$$= a' \circ (a \circ a') \circ a''$$
$$= a' \circ (e) \circ a''$$
$$= a' \circ a''$$
$$= e$$

$\Rightarrow$ a' is a left inverse of a & so a is left-invertible.

Group. A non empty set G is said to form a group with respect to a binary composition $\circ$, if

(i) G is closed under $\circ$

(ii) $\circ$ is associative

(iii) $\exists$ an element $e \in G$ s.t. $e \circ a = a \circ e = a \quad \forall a \in G$

(iv) for each element $a \in G$, $\exists$ an element $a' \in G$ s.t.

$$a' \circ a = a \circ a' = e.$$

The group is denoted by the symbol $(G, \circ)$.

- $e \rightarrow$ an identity element in the group. (unique, the identity)
- $a' \rightarrow$ an inverse of a. (unique, the inverse).

Commutative / abelian group (N. Abel) $\rightarrow$ $\circ$ commutative

uniqueness of e

e, e' $\quad a \circ e = e \circ a = a$ — (1)

$a \circ e' = e' \circ a = a$ — (2)

~~$(e \circ a) \circ e' = e \circ (a \circ e')$~~

~~$a e' =$~~ $\quad e' \circ e = e'$ by (1)

$e \circ e' = e$ by (2)

$e' \circ e$

$\Rightarrow e = e'$.

Note: e_G is used to denote the identity element of a gr $(G, \circ)$.

uniqueness of inverse of each element

$a \rightarrow a', a''$ two inverses of a if possible

(1) $\Rightarrow \begin{cases} a \circ a' = a' \circ a = e \\ a \circ a'' = a'' \circ a = e \end{cases}$ (e being the identity element)

Note: a^{-1} is used to denote the inverse of an element $a \in G$.

$a' \circ a) \circ a'' = a' \circ (a \circ a'')$ (∵ associative)

$e \circ a'' = a' \circ e$ (by (1))

$a'' = a'$ (∵ e is the identity element)

Cancellation laws $(G, \circ)$ be a group

- $a \circ b = a \circ c \Rightarrow b = c$ (left cancellation) $\forall a, b, c \in G$.
- $b \circ a = c \circ a \Rightarrow b = c$ (right cancellation).

proof $a \circ b = a \circ c$. $\quad a \in G \Rightarrow \bar{a}^1 \in G$.

$\bar{a}^1 \circ (a \circ b) = \bar{a}^1 \circ (a \circ c)$. (by closure)

$(\bar{a}^1 \circ a) \circ b = (\bar{a}^1 \circ a) \circ c$ (by associativity)

$e \circ b = e \circ c$ (by property of inverse)

$b = c$ (by as e is the identity element.)

Similarly, right cancellation.

Theorem $(G, \circ)$ group.

$a \circ x = b$ & $y \circ a = b$ each of the eqn. has a unique soln. in G.

proof claim $x = \bar{a} \circ b$ is a soln of $a \circ x = b$

proof of the claim $a \circ (\bar{a}^1 \circ b) = (a \circ \bar{a}^1) \circ b = e \circ b = b$.

uniqueness if two soln. x_1, x_2

$a \circ x_1 = b$, $a \circ x_2 = b$.

$\therefore a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2$ using left cancellation.

Similarly, $y = b \circ \bar{a}^1$ is a soln of $y \circ a = b$ & the soln. is unique.

Theorem $(G, \circ)$ group. Then $(a \circ b)^{-1} = \bar{b}^1 \circ \bar{a}^1$ $\forall a, b \in G$.

proof $a, b \in G \Rightarrow \bar{a}^1, \bar{b}^1, a \circ b, (a \circ b)^{-1} \in G$.

Now $(a \circ b) \circ (\bar{b}^1 \circ \bar{a}^1) = a \circ (b \circ \bar{b}^{-1}) \circ \bar{a}^1 = a \circ e \circ \bar{a}^1 = e$

Also $(\bar{b}^1 \circ \bar{a}^1) \circ (a \circ b) = \bar{b}^1 \circ (\bar{a}^1 \circ a) \circ b = \bar{b}^1 \circ e \circ b = e$

$\Rightarrow$ the result.

Examples

1. $(\mathbb{Z},+)$ abelian group, 0 is the identity element for $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ is the inverse
2. $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ each abelian group.
3. $(m\mathbb{Z},+)$ is abelian group, m being a positive integer.

$$2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \cdots\}.$$
$$3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$$

4. $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$ not group → 1 identity element
   - $(\mathbb{Z},\cdot)$: No element has inverse in $\mathbb{Z}$ except 1 & -1
   - $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$: inverse of 0 does not exist in each → all commutative monoid.
5. $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ → abelian groups
   ~~$\mathbb{Q}^* = \mathbb{Q} - \{0\}$~~
   ↓ excludes 0.
   e.g. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.
6. $M_2(\mathbb{R})$ → 2×2 matrices
   $+$ → matrix addition
   } Commutative group.
   identity element $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
   $-A$ is the inverse of A.
7. $(M_2(\mathbb{R}),\cdot)$ → not group
   → a monoid.
   } identity element $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
   No inverse for singular matrices in $M_2(\mathbb{R})$
   ↓ in $M_2(\mathbb{R})$

8. $S \rightarrow$ the set of all 2×2 non-singular matrices whose elements are real numbers.

$S \subseteq M_2(R)$.

$(S, \cdot) \rightarrow$ non-commutative group.

$\cdot \rightarrow$ matrix multiplication.

Notation

$GL(2,R) \rightarrow$ general linear group of degree 2 over R.

$\downarrow$

all 2×2 non-singular real matrices

Similarly, $GL(n,R) \rightarrow$ general linear group of degree n over R

$\downarrow$

all $n\times n$ non-singular real matrices.

(Proof skipped) done later

X Theorem Let $(G,\circ)$ be a semigroup s.t. for any two elements $a, b \in G$, each of the equn. $a\circ x = b$ and $y\circ a = b$ has a solution in G. Then $(G,\circ)$ is a group.

X

Theorem Let $(G,\circ)$ be a semigroup containing a finite number of elements in which both the cancellation laws hold. Then $(G,\circ)$ is a group.

Proof $a_1, a_2, \cdots, a_n \rightarrow$ all the (distinct) elements of G.

Then $a_1\circ a_1, a_1\circ a_2, \cdots, a_1\circ a_n \rightarrow$ all distinct — as $a_1, \cdots, a_n$ all distinct.

c.w. $a_1\circ a_i = a_1\circ a_j \Rightarrow a_i = a_j$

~~$\Rightarrow a_1\circ x =$~~ As G contains only n elements, $a_1\circ a_1, a_1\circ a_2, \cdots, a_1\circ a_n$ are all the elements of G.

$\Rightarrow a_1 \circ x = a_j$ has a soln. in G for $j = 1, 2, \cdots, n$

Since a_1 is arbitrary, the equn. $a \circ x = b$ has a soln. in G $\forall\, a, b \in G$.

Similarly, considering $a_1 \circ a_1, a_2 \circ a_1, \cdots, a_n \circ a_1$, we can proceed to prove that $y \circ a_1 = a_j$ has a soln. in G for $j = 1, 2, \cdots, n$.

Since a_1 is arbitrary, the equn. $y \circ a = b$ has a soln. in G $\forall\, a, b \in G$.

$\therefore$ By the previous theorem, $(G, \circ)$ is a group.

Note The theorem does not hold if G contains an infinite no. of elements.

e.g. $(\mathbb{N}, \cdot)$ is a semigroup in which cancellation laws hold. But $(\mathbb{N}, \cdot)$ is not a group.

Theorem Let G be a non-empty set satisfying the conditions:

(i) G is closed under a binary composition $\circ$

(ii) $\circ$ is associative

(iii) there exists an element e in G s.t. $e \circ a = a$ $\forall\, a \in G$ (e is a left identity)

(iv) for each element $a \in G$, there exists an element $a' \in G$ s.t. $a' \circ a = e$ (a' is a left inverse of a)

Then $(G, \circ)$ is a group.

i.e. $(G, \circ)$ semigroup where left-identity e exists & every element has a left inverse $\Rightarrow (G, \circ)$ is a group.

Proof:

Claim 1 $a \circ e = a$ $\forall\, a \in G$

Claim 2 $a \circ a' = e$

Let a'' be a left inverse of a' i.e. $a'' \circ a' = e$ by (iv)

Then $a' \circ a = e = a'' \circ a'$

Now $a \circ a' = e \circ (a \circ a')$

$= (a'' \circ a') \circ (a \circ a')$

$= a'' \circ (a' \circ a) \circ a'$

$= a'' (e) \circ a'$

$= a'' \circ a'$

$= e$ (proving claim) — ①

Also $a \circ e = a \circ (a' \circ a)$

$= (a \circ a') \circ a$

$= e \circ a$ (by ①)

$= a$ (by (iii)).

Theorem Let G be (i) closed under a binary composition $\circ$;

(ii) $\circ$ is associative

(iii) there exists an element e in G s.t. $a \circ e = e \ \forall a \in G$

& (iv) for each $a \in G$, there exists an element $a' \in G$

s.t. $a \circ a' = e$

Then $(G, \circ)$ is a group.

Note - A Semigroup $(G, \circ)$ in which there is a left identity e and every element a in G has a right e-inverse, may not be a group.

Example: $(Z, *)$ where $*$ is defined by $a * b = b, a, b \in Z$ → not group as no identity

- $*$ closed
- $*$ associative → $a * (b * c) = a * c = c$, $(a * b) * c = b * c = c$
- 0 → left identity → $0 * a = a \ \forall a \in Z$, no right identity
- $a * 0 = 0 \ \forall a \in Z$ → 0 is a right 0-inverse of every element $a \in Z$.

Theorem - $(G,\circ)$ Semigroup - for ~~each~~ any $a,b \in G$, each of the equn. $a\circ x = b$ & $y\circ a = b$ has a Soln. in G.

Then $(G,\circ)$ is a group.

proof:- $(G,\circ)$ Semigroup $\Rightarrow$ closed under $\circ$ & associativity hold

Existence of identity

Let e be a Soln. of $a\circ x = a$
& e' be a Soln. of $y\circ a = a$ $\Rightarrow$ $a\circ e = a$ — (1)
$e'\circ a = a$ — (2)

Now let c be any arbitrary element of G.

Let p be a Soln of $a\circ x = c$
and q be a Soln. of $y\circ a = c$ $\Rightarrow$ $a\circ p = c$ — (3)
$q\circ a = c$ — (4)

Now $c\circ e = (q\circ a)\circ e$
$= q\circ(a\circ e)$
$= q\circ(a)$ (using (1))
$= q\circ a = c$ (using (2))

As c is arbitrary element of G, we get

$$\boxed{a\circ e = a \ \forall\ a\in G.} \quad \text{— (A)}$$

Also $e'\circ c = e'\circ(a\circ p)$ (using (3))
$= (e'\circ a)\circ p$
$= a\circ p$ (using (4))
$= c$ using (3)

As c is arbitrary element of G, we get

$$\boxed{e'\circ a = a \quad \forall a\in G.} \quad \text{— (B)}.$$

~~Examples~~

1.

Theorem Let $(G,\circ)$ be a semigroup containing a finite no. of elements in which both the cancellation laws hold.

i.e. $a\circ b = a\circ c \Rightarrow b=c$ and

$b\circ a = c\circ a \Rightarrow b=c \quad \forall a,b,c \in G$.

Then $(G,\circ)$ is a group.

Proof Let $G=\{a_1, a_2, \ldots, a_n\}$.

Then $a_1\circ a_1, a_1\circ a_2, \ldots, a_1\circ a_n \in G$, all distinct because

$a_1\circ a_i = a_1\circ a_j \Rightarrow a_i = a_j$ by left cancellation law.

Since G contains only n elements, we have

$a_1\circ x = a_j$ has a sol^n. in G, for $j=1,2,\ldots,n$.

Since a_1 is arbitrary,

> the equ^n. $a\circ x = b$ has a sol^n. in G $\forall a,b\in G$.

Considering $a_2\circ a_1, a_2\circ a_2, \ldots, a_2\circ a_n$, we proceed with similar arguments & prove that ~~the equ^n.~~

> the equ^n. $y\circ a = b$ has a sol^n. in G $\forall a,b\in G$.

Thus $(G,\circ)$ is a semigroup in which each of the equ^n $a\circ x = b$ and $y\circ a = b$ has a sol^n. in G $\forall a,b\in G$.

Hence $(G,\circ)$ is a group.

Note: The theorem does not hold if G contains an infinite no. of elements.

e.g. $(\mathbb{N},\cdot)$ is a semigp. in which cancellation laws hold. But $(\mathbb{N},\cdot)$ is not a gp.

Alternative defn. of a group from the following theorem.

Theorem: Let G be a non-empty set satisfying the conditions –

(i) G is closed under a binary composition $\circ$

(ii) $\circ$ is associative

(iii) there exists an element $e \in G$ s.t. $e \circ a = a \ \forall \ a \in G$.

(iv) for each $a \in G$, $\exists$ an element $a' \in G$ s.t. $a' \circ a = e$.

(i.e. left identity e exists & left inverse of each element exists)

Then $(G, \circ)$ is a group.

Proof: It is sufficient to prove that e is the identity element & a' is the inverse of a.

Let a'' be a left e-inverse of a'.

Then $a'' \circ a' = e$ & $a' \circ a = e$

Also $a' \circ a = e$ (given).

Then $a' \circ a = e$ and $a'' \circ a' = e$

Now $a \circ a' = e \circ (a \circ a')$

$= (a'' \circ a') \circ (a \circ a')$

$= a'' \circ (a' \circ a) \circ a'$

$= a'' \circ e \circ a'$

$= a'' \circ a'$

$= e$.

Also $a \circ e = a \circ (a' \circ a) = (a \circ a') \circ a = e \circ a$

Thus $e \circ a = a \circ e = a$.

$\Rightarrow$ e is the identity element of G.

Also $a' \circ a = e = a \circ a'$

$\Rightarrow$ a' is the inverse of a in G.

Hence $(G, \circ)$ is a group

X Note- In an analogous manner, a group $(G, \circ)$ can be defined as a non-empty set G together with a binary composition $\circ$ satisfying the conditions -

(i) G is closed under $\circ$

(ii) $\circ$ is associative

(iii) there exists an element e in G s.t. $a \circ e = a \; \forall a \in G$

(iv) for each $a \in G$, there exists an element $a' \in G$ s.t. $a \circ a' = e$.

X Note. A semigr. $(G, \circ)$ in which there is a left identity e and every element $a \in G$ has a right e-inverse, may not be a group.

e.g. groupoid $(\mathbb{Z}, *)$ where $*$ is defined by

$$a * b = b \quad \text{for } a, b \in \mathbb{Z}.$$

- $*$ is associative since

$$a * (b * c) = c$$

and

$$(a * b) * c = c$$

- 0 is left identity, because $0 * a = a \quad \forall a \in \mathbb{Z}$
- There is no right identity.
- $a * 0 = 0$ for each $a \in \mathbb{Z}$

Therefore, 0 is a right 0-inverse of every element $a \in \mathbb{Z}$.

- But $(\mathbb{Z}, *)$ is not a group, since there is no identity element.

Example:

Let $(S, \circ)$ be a Semigroup with the identity element e. If for each $a \in S$, $\exists$ an element $a' \in S$ s.t. $a \circ a' = e$, prove that $(S, \circ)$ is a group.

Soln:

$$e \circ a = a \circ e = a \quad \forall\, a \in G.$$

~~a ∈ G~~

For $a \in S$ has a right inverse in S.

Let a'' be a right inverse of a' i.e. $a' \circ a'' = e$

Now $a' \circ a = (a' \circ a) \circ e$

$$= (a' \circ a) \circ (a' \circ a'')$$

$$= a' \circ (a \circ a') \circ a''$$

$$= a' \circ e \circ a''$$

$$= a' \circ a''$$

$$= e$$

Thus for each $a \in S$, $\exists\, a' \in S$ s.t.

$$a \circ a' = a' \circ a = e.$$

$\Rightarrow a'$ is the inverse of a.

Thus each element of S has an inverse in S.

Hence $(S, \circ)$ is a group.

Example: Let $(S,\circ)$ be a semigroup with a right identity element e.
If for every two distinct elements $a, b \in S$, there exists a unique $x \in S$ s.t. $a \circ x = b$, prove that $(S,\circ)$ is a group.

Soln As $(S,\circ)$ is a semigr. with a right identity e, we have $a \circ e = a \ \forall a \in S$.

for $a \neq e$, $\exists$ a unique $a' \in S$ s.t. $a \circ a' = e$

$\Rightarrow a$ has a right e-inverse in S.

Also $e \circ e = e \Rightarrow e$ has a right e-inverse.

Hence each element in S has a right e-inverse.

Thus $(S,\circ)$ is a semigr. with a right identity element e and each element in S has a right e-inverse.

Therefore, by previous Theorem, $(S,\circ)$ is a group.

Example: $(G,\circ)$ gr., $a \in G$.
Prove that $aG = G$ where $aG = \{a \circ g \mid g \in G\}$.

Soln. Let $p \in aG \Rightarrow p = a \circ g$ for some $g \in G$

$a \in G, g \in G \Rightarrow p = a \circ g \in G$.

So $\boxed{aG \subseteq G}$

Let $q \in G \Rightarrow \exists$ a unique $x \in G$ s.t. $a \circ x = q$

$q = a \circ x$ & $x \in G \Rightarrow q \in aG$

So $\boxed{G \subseteq aG}$

Example: $(G,\circ)$ gr., $a \in G$.

Define a mapping $f_a : G \to G$ by

$$f_a(x) = x \circ a, \quad x \in G.$$

Prove that f_a is a bijection.

Solⁿ. Let $x, y \in G$.

Then $f_a(x) = f_a(y) \Rightarrow x \circ a = y \circ a$

$\Rightarrow x = y$ by right-cancellation law.

$\therefore x \neq y \Rightarrow f_a(x) \neq f_a(y)$, proving f_a is injective.

- Let b be an arbitrary element in the codomain set G.

As $a \in G$, $b \in G$, $\exists$ a unique element $y \in G$ s.t. $y \circ a = b$.

$\Rightarrow y$ is a preimage of b, proving that f_a is surjective.

Hence f_a is a bijection.

Example: Let $(S,\circ)$ be a semigroup.

If for $x, y \in S$, $x^2 \circ y = y = y \circ x^2$, prove that $(S,\circ)$ is an abelian group.

Solⁿ. Let $p \in S$.

Then $p^2 = p \circ p \in S$ and $\forall a \in S$, $p^2 \circ a = a = a \circ p^2$

So p^2 is an identity element

If $q \in S$, then by similar argument, q^2 is an identity element.

Also by given condition,

$p^2 \circ q^2 = q^2 = q^2 \circ p^2$ and also $q^2 \circ p^2 = p^2 = p^2 \circ q^2$

$\Rightarrow p^2 = q^2$.

$\Rightarrow$ S has only one identity element.

Let e be the only identity element in S.

Then $\forall x \in S$, $x^2 \circ e = e = e \circ x^2$ by given condition.

$\Rightarrow x^2 = e$.

$\Rightarrow x^{-1} = x$.

Therefore, for each $x \in S$, $\exists\, x^{-1} \in S$.

Consequently, $(S, \circ)$ is a group.