An algebraic system | structure if $(A; a_1, \dots, a_n)$ when A is a non empty set and $a_1, a_2, \dots, a_n$ are finitary operations.

Relation from A to B is a subset of $A \times B$.

n-ary relation on A is a subset of A^n.

n-ary operation on A is a function from A^n to A.

Eg- $(\{0,1\}, \wedge, \vee, \neg)$

→ Let (A, o) be algebra st with the binary op 'o'.

'o' is said to satisfy

(i) associative property, if $a o (b o c) = (a o b) o c \quad \forall a,b,c \in A$

$(\mathbb{Z}, -) \qquad (2-3)-5 \neq 2-(3-5)$

(ii) commutative property, if $a o b = b o a \quad \forall a,b \in A$

(iii) idempotent property, if $a o a = a \quad \forall a \in A$

(iv) If there is an element $e \in A$ such that ~~$e o A$~~ $e o a = a o e = a \quad \forall a \in A$, then e is called an identity element.

counter ex: $(\mathbb{N}, +)$

v) For every $a \in A$, $\exists\ b \in A$ st $a \circ b = b \circ a = e$, where e is identity.

In this case b is called inverse of a, denoted by a^{-1}.

Remark: A left identity may exist but not left identity or vice versa.

If both exist, they coincide.

$e_l = e_l \circ e_r = e_r$

$\therefore e_l = e_r$

$(\mathbb{Z}, -)$ 0 is e_r.

Semigroup

Semigroup is an algebraic system with one binary operation which is associative.

Monoid is a semigroup with identity element.

Group is a monoid in which every element has inverse.

Semigroup	associative
Monoid	semigroup + identity
Group	Monoid + inverse

→ Let $(A, \circ, *)$ be an algebraic structure with 2 binary operators.

Distributive property : $a * (b \circ c) = (a * b) \circ (a * c)$
(left distributive)

$(b \circ c) * a = (b * a) \circ (c * a)$
(right distributive)

Absorption property : $a * (a \circ b) = a \quad \forall\, a, b \in A$

→ $(A, \circ, *)$ semilattice

1. $(A, \circ)$ & $(A, *)$ are semigroups

2. Both operations are idempotent & commutative

In addition if it satisfies absorption laws wrt both operations.

$$a * (a \circ b) = a$$
$$a \circ (a * b) = a$$

Then, $(A, \circ, *)$ is called lattice.

→ If $*$ is distributive over $\circ$, then $\circ$ is also distributive over $*$.

→ commutative semigroup — semigroup + commutative

→ Abelian Group - Commutative + Group

→ Ring $(A, o, *)$

1. (A, o) Abelian group

2. $(A, *)$ Semigroup

3. $*$ is distributive over o.

Notation In additive systems $inv(a) = -a$.

→ Abelian group

$(\mathbb{Z}, +)$
$(\mathbb{Q}, +)$
$(\mathbb{R}, +)$
$(\mathbb{C}, +)$

$\times (\mathbb{Z}, \cdot)$ not a group
$(\mathbb{Q}^*, \cdot)$, when $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
$(\mathbb{R}^*, \cdot)$
$(\mathbb{C}^*, \cdot)$

→ Rings

$(\mathbb{Z}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$

→ Commutative Ring
If 2. is also commutative.

$(GL_n(\mathbb{R}), \cdot)$ is non abelian group
(General linear group)

The set of all non singular matrices of order $n \times n$.

→ commutative ring = ring + comm. wrt 2nd operation

→ Ring with unity / Ring with identity = ring + ($\cdot$ is monoid)
(1)

Definition In ring $(A, 0, *)$, the identity element with respect to '0' is called zero element, and is denoted by 0.

→ Division ring : Ring with unity + every non zero element has inverse

→ Field : commutative division ring

→ Division ring : - $(R, +)$ abelian group
- $(R^*, \cdot)$ group
- distributive laws

→ $n \in \mathbb{N}$

$\mathbb{Z}/\equiv_n = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

$\bar{a} +_n \bar{b} = \overline{a+b}$

Well defined $f : A \to B$

$a = b \Rightarrow f(a) = f(b) \quad \forall\ a, b \in A$

$g : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$u = y \Rightarrow g(u) = g(y)$

$(\alpha, \beta)\ (\gamma, \delta)$

$\alpha = \gamma \qquad \beta = \delta$

$\bar{a} = \bar{c}$

$a \equiv c \Rightarrow a + b \equiv c + d$

$b \equiv d$

→ $\bar{a} +_n (\bar{b} +_n \bar{c}) = (\bar{a} +_n \bar{b}) +_n \bar{c}$

$\bar{a} +_n (\overline{b+c}) = \overline{a + (b+c)}$

$= \overline{(a+b)+c}$

$= \overline{(a+b)} +_n \bar{c}$

$= (\bar{a} +_n \bar{b}) +_n \bar{c}$

$\bar{0}$ is identity element.

→ For $\bar{a} \in \mathbb{Z}_n$,

$\bar{a} + \overline{-a} = \overline{a + (-a)}$

$= \bar{0}$

Q. Is $(\mathbb{Z}_n, \times_n)$ Abelian group?

No, it is commutative monoid.

$(a, n) = 1 \iff \bar{a}$ has multiplicative inverse.

$(\mathbb{Z}_n^*, \times_n)$ is Abelian group $\iff n$ is a prime

→ $(\mathbb{Z}_n, +_n, \times_n)$ is a commutative ring with unity.

If n is prime then it is a field.

Functions

Let X be a non empty set.

$$M(X) = \{ f : X \to X \mid f \text{ is a function} \}$$

If $|X| = n \quad |M(X)| = n^n$

$(M(X), \circ)$ where $\circ$ is composition.

$$(f \circ g)(x) = f(g(x)) \quad \forall x \in X$$

$\circ$ is associative.

$id(x) = x \quad \forall x \in X$

is st

$$f \circ id = id \circ f = f$$

$(M(X), \circ)$ is a monoid.

Let S be a monoid.
$(M(S), \circ)$ is a monoid.

$S \hookrightarrow M(S)$

$a \in S$

$f_a : S \to S$

$f_a(x) = a \quad \forall\ x \in S$

$M(S)$ cannot be group.

$G(X) = \{f : X \to X \mid f \text{ is a bijection}\}$

$(G(X), \circ)$

Since $f \circ g$ is a bijection $\forall\ f, g \in G(X)$. we have,
$f \circ g \in G(X)$.

associative

id

$\forall\ f \in G(X),\ f^{-1} \in G(X)$

canonical example

Given f a bijection on X, define $f^{-1} : X \to X$

$f \circ f^{-1}(x) = f(f^{-1}(x))$

$f^{-1} = \{(b, a) \mid f(a) = b\}$

S_X is the symmetric group.

S_X is the set of all bijections on X.

→ Symmetric Group or Permutation group denoted by S_X is the set of all permutations on a non empty set X considered wrt composition of mappings.

$|X| = n$

$S_X = S_n$

$|S_n| = n!$

$|G| = n$

$n = 1 \qquad Z_1 = \{\bar{0}\}$

$G = \{a, b, c\}$

$\circ$	a	b	c
a			
b			
c			

Cayley's Table

$\circ$	a
a	a

There is only one group of one element.

	a	b
a	a	b
b	b	a

There is only one group of two elements.

a - identity

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

In a group,
$(a^{-1})^{-1} = a$

Statement:
Inverse of a in a group is unique

Let b & c be inverses of a.

$ba = e = ab$

$ca = e = ac$

$b = eb$

$= cab = c(ab) = ce$

$\Rightarrow b = c$

Q. There is only one group of 8 elements.

No. of groups - 4, 5

$(S_3, +)$ non commutative

$(\mathbb{Z}_6, +)$ commutative

1. Inverse of an element in a group is unique.

2. Identity element of a group is unique.

if e & e' are identities,

$$e = ee' = e'$$

3. Cancellation laws hold in a group.

$ab = ac \Rightarrow b = c$ Left cancellation

$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$

$\Rightarrow eb = ec$

$\Rightarrow b = c$

$ba = ca \Rightarrow b = c$ Right cancellation

Notation

For $n \in \mathbb{N}$

$a \in G$

$n \in \mathbb{Z}$

$a \in G$

$a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}$

$(a^{-1})^n = \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}}$

$a^0 = e$

Remark

For $a \in G$, $\{a^n \mid n \in \mathbb{Z}\} \subseteq G$.

Notation $\{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

(If it is an additive group, $a^n = na$)

Definition

Order of a group G is $|G|$. For $a \in G$, order of a, denoted by $|a|$ or $o(a)$, is the least positive integer (if exist) k such that $a^k = e$. If such k does not exist, we say $o(a)$ is infinite.

Remark $o(e) = 1$ in any group.

$(\mathbb{Z}, +)$

$o(1) = \infty$

For any $a \in \mathbb{Z}$ $(\neq 0)$, $o(a) = \infty$.

Remark

If $|G|$ is finite, $\forall\, a \in G$, $o(a)$ is finite.

Proof: Let $a \in G$ is of infinite order

$a^k = e$ $\forall\, k \in \mathbb{N}$

Note that $a, a^2, \cdots \in G$

Since G is finite $a^i = a^j$ for $i \neq j$

$\Rightarrow a^{j-i} = e$ Contradiction

Since $j - i \in \mathbb{N}$, contradiction to our assumption that $o(a) = \infty$.

→ Subgroup

Let H be a non empty subset of G, H is said to be a subgroup of G if H is also a group wrt the same operation of G. In which case we write, $H \leq G$.

$\{e\} \leq G$ $\quad$ $G \leq G$ $\quad$ Improper subgroups
Trivial group

$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ $\quad$ wrt $+$

$(\mathbb{Q}^*, \cdot) \leq (\mathbb{Q}, +)$
even though $\mathbb{Q}^* \subseteq \mathbb{Q}$

$A \subsetneq B$ $\quad$ A is a proper subset of B.

→ For $a \in G$,

$\langle a \rangle \leq G$

called the subgroup generated by a.

$k \in \mathbb{Z}$, $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} \leq \mathbb{Z}$

In integers, these are the only subgroups.

Result

$(\phi \neq) \quad H \subseteq G$

$H \leq G \Leftrightarrow \forall\, a, b \in H,\ ab \in H$
$\&\ a^{-1} \in H$

Or, $\Leftrightarrow \quad ab^{-1} \in H,\ \forall\, a, b \in H$

Proof: $\Rightarrow$ obvious

$\Leftarrow$ For $a \in H,\ a^{-1} \in H$ (By 2nd cond.)

$\Rightarrow aa^{-1} \in H$ (By 1st cond.)

$\Rightarrow e \in H$

→ Let H be a finite non empty subset of G such that $\forall\, a, b \in H,\ ab \in H$.

Then $H \leq G$. $\qquad a^{i-j} = e$

$a^k = e$

$a^{k+1} \neq a$

$a^{k-1} \cdot a = e$

~~Homomorphism~~

→ Let $H \leq G$

Define $\sim$ on G, ($\sim$: binary relation)

by $a \sim b \Leftrightarrow ab^{-1} \in H$

Note that $\sim$ is an equivalence relation.

$G/\sim$ is the partition wrt $\sim$.

$$[a] = \{b \mid ab^{-1} \in H\} = \{ha \mid h \in H\} = Ha$$

$ba^{-1} = h$ $\quad\quad$ $\because ab^{-1} \in H,\ (ab^{-1})^{-1} \in H$

$b = ha$ $\quad\quad$ $ba^{-1} \in H$

Each equivalence class, has exactly $|H|$ elements.

$h_1 a, h_2 a, \ldots h_n a$

$h_1 a = h_2 a \Rightarrow h_1 = h_2$

→ Note that $|[a]| = |Ha| = |H|$

→ Suppose G is finite, then $|H| \mid |G| \quad \forall\ H \leq G$ [for partition]

Lagrange's Theorem

→ Let $H \leq G$

For $a \in G$, $Ha = \{ha \mid h \in H\}$ is called the right coset of a wrt H.

$aH = \{ah \mid h \in H\}$ left coset of a.

Remark

The no. of left cosets = no. of right cosets

Definition

Let $H \leq G$, the no. of left cosets & no. of right cosets is called the index of H in G, $[G:H]$

$|G| < \infty$

Then $|H|\,[G:H] = |G|$

→ For $a \in G$, $\langle a \rangle \leq G$

$|\langle a \rangle| = o(a)$

If $o(a) = k$

$\langle a \rangle = \{e, a, a^2, \cdots, a^{k-1}\}$

Corollary

Let G be a finite group, $o(a) \mid |G| \quad \forall\, a \in G$.

→ Let $H \leq G$

The cardinality of the set of right (left) cosets is the index of H in G denoted by $[G:H]$.

$H \leq G$

$a \sim b \Leftrightarrow ab^{-1} \in H$

$[a] = Ha$

$a \sim b \Leftrightarrow a^{-1}b \in H$

$[a] = aH$

$Ha = Hb \Rightarrow aH = bH$

$\Rightarrow a \sim b$

$\Rightarrow ab^{-1} \in H$

$\Rightarrow ba^{-1} \in H \Rightarrow b^{-1}H = a^{-1}H$

$a^2 \in H \qquad aH = a^{-1}H$

$Ha = Hb \Rightarrow a^{-1}H = b^{-1}H$

→ $a \in G$

$o(a) = |\langle a \rangle| \mid |G|$

→ $a \in G$

If $a^n = e \neq$ then $o(a) \mid n$

Definition Homomorphism

Let ~~$(G_1, *_1)$~~ G_1 & G_2 be two groups

$(G_1, *_1), (G_2, *_2)$

$f : G_1 \longrightarrow G_2$ is homomorphism

if $f(a *_1 b) = f(a) *_2 f(b) \quad \forall \ a, b \in G_1$

$f(o(a_1, a_2, a_3)) = o'(f(a_1), f(a_2), f(a_3))$

Structure preserving mapping

On any group G,

$id : G \to G$ is homomorphism

$id(x) = x \quad \forall \ x \in G$

$id(xy) = xy = id(x)\, id(y)$

$f: G \to H$

$f(x) = e \quad \forall\, x \in G \qquad e \in H$

$f(xy) = e = f(x)\, f(y)$

$g: \mathbb{Z} \to \mathbb{Z}$

$g(x) = 2x \qquad x \in \mathbb{Z}$

$g(m+n) = 2(m+n)$

$= 2m + 2n$

$= g(m) + g(n)$

Isomorphism

A bijective homomorphism is called isomorphism.

$G_1 \cong G_2$ (G_1 isomorphic to G_2)

$\cong$ is an equivalence relation in class of all groups

Monomorphism

A one – one homomorphism is called monomorphism

Epimorphism

An onto homomorphism

Endomorphism

A homomorphism from a group to itself.

Definition

A group G is said to be cyclic if $G = \langle a \rangle$ for some $a \in G$.

$\mathbb{Z}$ is cyclic.

$(\mathbb{Z}_n, +_n)$ generator –

→ For $a \in G$, $o(a) \mid |G|$. Consequently, if $|G|$ is prime then G is cyclic.

$(e \neq) \; a \in G$

$o(a) = |G|$

$\langle a \rangle = G$

$(\mathbb{Z}_p, +)$ is cyclic.

$(\mathbb{Z}_n, +)$ is cyclic. $\forall \; n \in \mathbb{N}$

Theorem Every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some n.

Proof Let G be a cyclic group, say $G = \langle a \rangle$

If G is infinite,

$$f : \mathbb{Z} \to G$$

$$f(n) = a^n \quad \forall \; n \in \mathbb{Z}$$

& $f(m+n) = a^{m+n} = a^m a^n = f(m) f(n)$

Hence f is an isomorphism. Hence, $G \cong \mathbb{Z}$

If G is finite, say $|G| = n$

Define $f: \mathbb{Z}_n \to G$ by $f(\bar{k}) = a^k$

$\bar{k}_1 = \bar{k}_2 \Leftrightarrow n \mid k_1 - k_2 \Leftrightarrow a^{k_1 - k_2} = e \Leftrightarrow e^{k_1} = e^{k_2}$

$f(\bar{k}_1 + \bar{k}_2) = f(\overline{k_1 + k_2}) = a^{k_1 + k_2} = a^{k_1} a^{k_2} = f(\bar{k}_1) f(\bar{k}_2)$

$G \cong \mathbb{Z}_n$

Corollary Any two cyclic groups of same order are isomorphic.

$n = 1$ $\{e\}$

2 $\mathbb{Z}_2$

3 $\mathbb{Z}_3$

4 $\mathbb{Z}_4$ $G = \{e, a, b, c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$o(x) \neq 4 \quad x \in G$

$o(a) = 2$

$o(b) = 2$

$o(c) = 2$

G is not cyclic.

All groups for $n = 4$ are Abelian groups.

G is called Klein four group K_4.

Cayley's Theorem Every group is isomorphic to a permutation group or a subgroup of S_X.

$f : G \to H$ homo.

$\text{Im } f = \{y \mid \exists\ x \in G \text{ with } f(x) = y\} \leq H$

$e_2 \in \text{Im } f$

$f(e_1) - f(aa^{-1}) = f(a)\, f(a^{-1})$

$= f(a)\, f(a)^{-1} = e_2$

$f(e_1) = e_2$

Let $a, b \in \text{Im } f$

$\Rightarrow x, y \in G$ s.t. $f(x) = a \quad f(y) = b$

$f(xy^{-1}) = f(x)\, f(y^{-1})$

$= f(x)\, f(y)^{-1}$

$= ab^{-1}$

$ab^{-1} \in \text{Im } f$

Let G be a subgroup.

Consider the symmetric group S_G.

Given $a \in G$, define $f_a : G \to G$

$$f_a(x) = ax$$

$x = y \Leftrightarrow ax = ay$ $\therefore$ well defined & one-one

For $b \in G$, $a^{-1}b \in G$ s.t. $f_a(a^{-1}b) = a(a^{-1}b) = b$

Claim: $\psi : G \to S_G$

$\psi(a) = f_a$

is a monomorphism.

$\to$ Let $f : G_1 \to G_2$ be a homomorphism,

$$\ker f = \{a \in G_1 \mid f(a) = e_2\}$$

$\ker f \leq G_1$

$\ker f \neq \phi$, as $e_1 \in \ker f$

Let $a, b \in \ker f \Rightarrow \begin{cases} f(a) = e_2 \\ f(b) = e_2 \end{cases}$

$$f(ab^{-1}) = f(a)\, f(b^{-1}) = f(a)\, f(b)^{-1}$$

$$= e_2 e_2^{-1} = e_2$$

$\Rightarrow ab^{-1} \in \ker f$

→ Let G be a group,

$$Z(G) = \{a \in G \mid ab = ba \ \forall \ b \in G\}$$

is called centre of G.

Remark If G is abelian, $Z(G) = G$.

Remark $Z(G) \leq G$.

$e \in Z(G)$, so it is non empty.

→ Define $(Ha)(Hb) = Hab$

In general, it is not well defined.

Q. Find subgroups of S_3.

$$S_3 = \left\{ e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad \sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \right.$$

$$\left. \sigma_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \quad \tau_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \right.$$

$$\left. \tau_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \quad \tau_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \right\}$$

$H_0 = \{e\}$ $\quad H_1 = S_3$

$H_2 = \{e, \tau_1\}$ $\quad H_3 = \{e, \tau_2\}$ $\quad H_4 = \{e, \tau_3\}$

$\sigma_1^3 = e$ $\quad \sigma_1 \sigma_1^2 = e$

$\sigma_1 \sigma_1^2 = \sigma_2$

$H_5 = \{e_1, \sigma_1, \sigma_2\}$ $\quad H_6 = e_1$

Remark Converse of Lagrange's Theorem is not true in general.

Result Converse of Lagrange's Theorem is true in case of cyclic groups.

Let $G = \langle a \rangle$ of size n and $d \mid n$. Then $\exists!\ H \leq G$ st $|H| = d$.

Proof: $k = n/d$

$b = a^k$

$H = \langle b \rangle$

Claim : $|H| = d$

$b^d = e$

$b^d = (a^k)^d$

$= a^n$

$= e$

Such H is unique.

Suppose $|H_1| = |H_2| = d$

$a^k \qquad a^t$

$\Rightarrow k = t$

Result Every subgroup of a cyclic group is cyclic.

$H \leq G = \langle a \rangle$

If $H = \{e\}$, done.

Else, $H \neq \{e\}$

$a^k \in H$

$a^{-k} \in H$

consider the set of all the exponents of a in H.

By well ordering, let m be the least element in this set.

Claim: $H = \langle a^m \rangle$
$\quad\quad\quad\quad\quad\; \| \\ \quad\quad\quad\quad\quad\; c$

Let $x \in H$

$\Rightarrow x = a^n$ for some n

$n = mq + r \quad 0 \leq r < m$

$a^r = a^{n-mq}$

$= a^n (a^m)^{-q} \in H$

$\Rightarrow r = 0 \quad$ ($\because r < m$, but m is least)

$x = a^n = a^{mq} = (a^m)^q = c^q$

$H = \langle c \rangle$

All subgroups of $\mathbb{Z}$ are of the form $k\mathbb{Z}$.

$\therefore$ Subgroups of cyclic groups are cyclic.