Algebraic Structures

An algebraic system is a triple $(A, O_1, O_2, \ldots O_n)$ where A is a non-empty set and $O_1, O_2, \ldots, O_n$ are finitary operations on A.

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

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

Nullary operation

$A^0 \to A$

Exercise

Realizing Nullary operations.

Examples

$(\mathbb{Z}, +)$, $(\mathbb{N}, +)$

$(\mathbb{R}, +)$, $(\mathbb{N}, -)$ ✗

$(\mathbb{Z}, -)$

$(\mathbb{N}, +, \cdot)$ ✓

$(\mathbb{Z}, +, \cdot, -)$ ✓ Be careful about $\cdot$

$(\mathbb{Q}, +)$ ✓

$(M_n(\mathbb{R}), +, \cdot)$ $\hookrightarrow ()^T$

$(M_{m\times n}(\mathbb{R}), +)$

All Relations of A.

$(R(A), \circ)$

↓ composition.

$(F(A), \circ)$ –

~~$(P(S), \cup)$~~ $(P(S), \cup, \cap, ^c)$

→ $(A, \circ)$ – 2

Associative property of $a \circ (b \circ c) = (a \circ b) \circ c$ $\forall a, b, c \in A$

Commutative property if $a \circ b = b \circ a$ $\forall a, b \in A$.

NT

Let (A, o) be an algebraic system with binary operation 'o'. Then, 'o' satisfies

i) associative

ii) commutative

iii) Idempotent (if $a \circ a = a \quad \forall \ a \in A$)

iv) If $\exists \ e \in A$ such that $e \circ a = a \circ e = a$ ($e \circ a = a$: left; $a \circ e = a$: right identity) $\forall \ a \in A$, then we say that e is an identity element.

v) For every $a \in A$, $\exists$ is a $b \in A$ s.t. $a \circ b = b \circ a = e$, (b: inverse) thus e is an identity. $b = a^{-1}$.

Left identity may exist, and right identity may not exist, ~~but do~~ & vice-versa, but if both exist, they are equal. ($e_r = e_r \circ e_l = e_l$)

Semi-group

(A, o) satisfies associative.

Monoid is

a semigroup with identity elt. (both left & right)

~~Group~~ is

a monoid in which every elt. has inverse.

$(\mathbb{C}, +)$

$(\mathbb{Z}, +)$

$(\mathbb{Q}, +)$

$(\mathbb{R}, +)$

NT

$X^* = X^* \setminus \{0\}$

$X = \mathbb{R}, \mathbb{Q}, \mathbb{C}$

They are groups. (w.r.t $\times$)

Any group satisfying a commutative property is called an abelian group.

S.G — Associative

↓

Monoid — id.

↓

G — inv.

↓

Ab. Group — com.

$n \in \mathbb{N}$

$\mathbb{Z}/\equiv_n = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(n-1)}\}$

$0 \equiv x \pmod{n}$

$\bar{a} +_n \bar{b} = \overline{a+b}$ } def^n

$\bar{a} \times_n \bar{b} = \overline{ab}$ } def^n $(\mathbb{Z}_n, +_n, \times_n)$

$f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, +_n$

f is well defined.

$a_1 \equiv a_2 \pmod{n}$ ✓

$b_1 \equiv b_2 \pmod{n}$ ✓

$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ ✓

$a_1 b_1 \equiv a_2 b_2 \pmod{n}$ ✓

$(x = y \Rightarrow f(x) = f(y))$

Addition

$\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n, \ (\bar{a} +_n \bar{b}) + \bar{c}$

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

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

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

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

* $\bar{0} \in \mathbb{Z}_n$, $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$
  identity

* $\bar{a} + \overline{-a} = \bar{0} = -\bar{a} + \bar{a} = 0 + \bar{a}$
  Inverse element.

For multiplication.
$\bar{1}$ is the identity.

* $(\mathbb{Z}_n, \times_n)$ is a commutative mod.

* $(\mathbb{Z}_n^*, \times_n)$ is a Abelian group.
  ↳ primes (without 0).

* Semi Group ✓
  Monoid ✓
  Group ✓
  Abelian group.

Distributive
→ $\circ$ distributes over $*$
does not imply $*$ distributes over $\circ$.

(But in a lattice,
$\oplus$ distributes over $*$,
$*$ distributes over $\oplus$.

Ring

An algebraic structure $(R, +, \cdot)$ with 2 binary operations is said to be a ring

if - $(R, +)$ is Abl group
- $(R, \cdot)$ is a semi-group
- distributive Law.
  ($\cdot$ over $+$)

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

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{Z}_n, +_n, \times_n)$

$(\mathbb{R}, +, \cdot)$

(A, o)

Semi-Group - Associative

Monoid = Semi group + identity.

Group = Monoid + Every elt. has inverse.

Ring = $\begin{cases} (R,+) \text{ Abl. group} \\ (R,\cdot) \text{ Semi group} \\ \text{Distributive laws.} \end{cases}$

Ring

+ $(R,\cdot)$ Monoid = Ring with unity.

Ring with unity in which every non-zero elt. has inverse. → Division ring

Field = Commutative division ring.

$R(+,\cdot)$

$\cdot$ is identity w.r.t. + is denoted by '0'.

Unity is denoted (+ Ring $(R,\cdot)$) by '1'.

The set of all non-singular matrices with real entries of order $n \times n$ is denoted by $GL_n(\mathbb{R})$.

$(GL_n(\mathbb{R}), \cdot)$.

★ Number Theory

Let X be a non-empty subset.
$M(X)$, the set of all mappings on X

$(M(X), \circ)$ where '$\circ$' is the composition of mappings.

$\forall f, g \in M(X), \quad fog \in M(X)$

$\forall f, g, h \in M(X), \quad fo(goh) = (fog)oh$

Note that $id : X \to X$ defined by
$id(x) = x \quad \forall x \in X$
satisfies $idof = fo id = f$
$\forall f \in M(X)$

Semi group ✓
Monoid ✓

★ S_X is the set of all bijections / permutations

$(S_X, \circ)$ is a group called Symmetric group or a permutation group.

if $|X| = n$, then $S_X = S_n$.
$|S_n| = n!$

S_1, S_2 are abelian.
S_3 onwards are non-abelian groups.

⊛ Cayley's table

* whenever G is a group. $(G, \cdot)$ $(G, +)$
arbitary Abelian
(just notation)

1. In a group, identity is unique.
$e = ee' = e'$
all in

2. Inverse of any G is unique.
If b and c are inverses of a
$ab = ba = e$
$ac = ca = e$

* Proof: $b = be$
$= b(ac) = (ba)c = ec = c$

Cor

$\forall a \in G$,

$(a^{-1})^{-1} = a$.

3) In a group, cancellation laws hold true.

$a, b, c \in G$,

$ab = ac \Rightarrow b = c$ (left)

$ba = ca \Rightarrow b = c$ (right)

$ab = ac$

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

$b = c$

Exercise

A finite semigroup is a group if & only if cancellation laws hold.

4) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$

$(b^{-1}a^{-1})(ab) = e$

Notation

For $n \in \mathbb{N}$,

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

$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{\text{notation}}$

$a^0 = e$

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

$\langle a \rangle \subseteq G$.

★ **Definition**

Order of a group is $|G|$. For $a \in G$, order of a, denoted by $|a|$ or $O(a)$, is the least +ve integer k such that $a^k = e$. If k does not exist, then $O(a) = \infty$

Examples

$(\mathbb{Z}, +)$ $\quad O(1) = \infty$

$O(n) = \infty \quad (n > 0)$ or $(n < 0)$

$O(0) = 1$

$O(e) = 1$

Examples

$(\mathbb{R}, +)$

(same as integer)

$(\mathbb{Q}^*, *)$ — Non-zero rational no.

$o(-1) = 2$

$o(1) = 1$

$(\mathbb{C}, *)$

n^{th} roots of unity;

Result

If G is finite, then $o(a) < \infty \ \forall\ a \in G$.

Contradiction

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

$a^j = a^2 \Rightarrow a^{j-2} = e$

So, every elt. is different - since the set is finite $a^k = e$ has to happen.

Remarks: If $o(a) = k$, and $a^n = e$, then $k \mid n$.

If $a^n = e$, then $o(a)$ divides n.

$n = qk + r, \quad 0 \leq r < k$

$e = a^n = a^{qk+r} = a^r \Rightarrow r > k \Rightarrow r$ has to be zero.

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

(then it repeats.

$|\langle a \rangle| = k$ (order)

* Let H be a ~~non-empty~~ subset of G.
H is said to be a subgroup of G if H is a group w.r.t the same operation of G.
In this case, we write $H < G$

$(\mathbb{Z}, +) < (\mathbb{Q}, +)$

$(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

trivial subgroup: $\{e\} \leq G$, ✓ (proper subgroup)
$G \leq G$ ✗

Date
Page

Result Let $H \subset G$ be a non-empty subset.

$H \leq G \iff \forall\, a, b \in H$

(i) $ab \in H$

(ii) $a^{-1} \in H$

or combine both the statements.

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

Take $b = a$, then,

$aa^{-1} \in H$

$\Rightarrow e \in H$

So, $ab^{-1} \in H$

take $a = e$,

$b^{-1} \in H$

Result

→ Let H be a ~~non~~ finite subset of G which is closed w.r.t. the opn on G.

Then, $H \leq G$.

For finite subsets, we don't have to check inverse.

So, for $a \in G$,

$$\langle a \rangle \leq G$$

Subgroup generated by a.

* Let $H \leq G$,

Define a relation on G by :

$$a \overset{\sim}{,} b \iff ab^{-1} \in H$$

Note that, $\sim$ is an equivalence relation on G.

For $a \in b$,

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

$$ab^{-1} = h$$
$$\Rightarrow b^{-1} = a^{-1}h$$
$$\Rightarrow \boxed{b = h^{-1}a}$$

$$[a] = \{b \mid \underset{\forall\, h \in H}{b = ha}\}$$

$$= Ha$$

$$= \{ha \mid h \in H\}$$

(Right coset)

For the equivalence relation,

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

$\sim_2$

$[a] = aH$ (left coset)

$G/_{\sim_2} = \{aH \mid a \in G\}$

$G/_{\sim_1} = \{Ha \mid a \in G\}$

These 2 sets are equipotent.

We can make a bijection

$Ha \longmapsto a^{-1}H$

$Ha = Hb \Rightarrow$

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

$\iff (a^{-1})^{-1} b^{-1} \in H$

$\iff a^{-1}H = b^{-1}H$

$\Rightarrow aH = bH$ is well defined and one one

Def: Let $H \leq G$, the cardinality of $G/_a$ left cosets and right cosets is called the index of H in G (denoted by $[H : G]$.

* $Ha, Hb, Hc, \ldots$ are of same size.
All cosets are of same size (sizeof H).
cardinality

Result:
Cardinality of $|G| = |H|\,[G : H]$

If G is finite, then
$|H| \mid |G| \quad \forall \; H \leq G$

(Lagrange's Th.)

→ **Coro:** For $a \in G$.

$o(a) \mid |G|$

(because $\langle a \rangle \leq G$)

→ Corollary: If $|G| = p$, prime $\forall a (\neq e)$, $o(a) = p$.

→ Hence, $\langle a \rangle = G \quad \forall a \neq e$

→ Defⁿ: A group G is said to be cyclic if $G = \langle a \rangle$ for some $a \in G$)

For example

$(\mathbb{Z}, +)$

$$\langle 1 \rangle = \{0, 1, 2, 3, \ldots \\ -1, -2, -3$$

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

$a^{-1} = +$ $a^0 = 0$ $a^1 = 1$

$a^{-2} = -2$ $a^2 = 2$

$\forall n$, $(\mathbb{Z}_n, +_n)$ is cyclic generated by 1.

* Remarks: Cyclic groups are abelian groups.

* Let G & H be 2 groups.

A mapping $f : G \to H$ is said to be a homomorphism if

$$f(ab) = f(a)\,f(b) \quad \forall a, b \in G.$$

(A, o_1, o_2), $(B, *_1, *_2)$

$f : A \to B$

$f(a\, o_1\, b) = f(a) *_2 f(b)$

$f(o_2(a, b, c)) = *_2(f(a), f(b), f(c))$

Note: operations need not be same

Remark: $\cong$ is an equivalence class of all groups. $\{G_1 \cong G_2 (f), G_2 \cong G_1, (f^{-1})$

$f: G_1 \to G_2$ a homo.

★ If f is one-one, $f \to$ monomorphism.

★ $f \to$ onto, $f \to$ epimorphism.

★ $f \to$ bijection, $f \to$ isomorphism.

We write, $G_1 \cong G_2$, G_1 is isomorphic to G_2

★ Homorphism from G to G is called endomorphism.

G_1 & G_2 be 2 groups.

$f: G_1 \to G_2$ is a homo.

if $f(xy) = f(x) \, f(y) \; \forall \; x, y \in G_1$

(operation can be anything.)

★ $id: G \to G$

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

it is homomorphism, endomorphism, iso, and epi.

★ $f: G_1 \to G_2$

$f(xy) = e \; \forall \; x \in G_1$,

homomorphic ✓

(a)

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

$g(x) = 2x$

$g(x+y) = 2(x+y)$

$g(x) + g(y) = 2x + 2y.$

homomorphism ✓

(if No operation is provided, take '+' as the operation)

* $n: \mathbb{Z} \to n\mathbb{Z}$

$h(K) = nK$

These are the only subgroups of $\mathbb{Z}$.

All the subgroups of $\mathbb{Z}$ are isomorphic to it.

Theorem:

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

Proof: Let G be a cyclic group generated by a.

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

If G is infinite,

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

$f(k) = a^k$

Date
Page

one-one

$a^{k_1} = a^{k_2} \Rightarrow a^{k_1 - k_2} = e \Rightarrow k_1 = k_2$

$f(k_1 + k_2) = a^{k_1 + k_2} = a^{k_1} a^{k_2} = f(k_1) \cdot f(k_2)$

homomorphism.

If G_1 is finite of order n,

$g : \mathbb{Z}_n \to G_1$

$g(\bar{k}) = a^k$

homomorphism

$g(\bar{k_1} + \bar{k_2}) = g(\overline{k_1 + k_2})$

$= a^{k_1 + k_2} = a^{k_1} a^{k_2} = g(\bar{k_1}) g(\bar{k_2})$

$g(\bar{k}) = a^k$

$\bar{k_1} = \bar{k_2} \iff n \mid k_1 - k_2$; if $a^t = e$, $o(a) \mid t$

$\iff a^{k_1 - k_2} = e$

$\iff a^{k_1} = a^{k_2}$

$g(\bar{k_1} +_n \bar{k_2}) = g(\overline{k_1 + k_2})$

$= a^{k_1 + k_2} = a^{k_1} a^{k_2}$

$= g(\bar{k_1})\, g(\bar{k_2})$

classmate
Date
Page

Q* Is $(\mathbb{Q}, +)$ is a cyclic group?

* Cayley's Theorem.

Every group is isomorphic to a subgroup of S_X. (a permutation group).

Remark : 1. $f(e_1) = e_2$

2. $f(a^{-1}) = (f(a))^{-1}$

$x, y \in \text{Im } f$

$\exists\ a, b \in G_1$, s.t. $(\Rightarrow)\ f(a) = x$, $f(b) = y$

Note : $ab^{-1} \in G_1$, s.t. $f(ab^{-1})$

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

Result: Every ~~cyclic~~ subgroup of a cyclic group is cyclic.

Let $H \leq \langle a \rangle$

Consider a non trivial subgroup

Note that $a^k, a^{-k} \in H$. Consider the set of all ~~non-negative~~ the exponents of a which are in H. By well-ordering let m be the least in the set

$$a^m \in H, \quad m > 0$$

Claim, $b = a^m$ generates H.

i.e., $H = \langle b \rangle$

Let $x \in H$

$x = a^n$ for some n.

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

$$a^r = a^{n-mq} = a^n (a^m)^{-q}$$

a^n: element of H; $(a^m)^{-q}$: element of H

$a^r \in H$ So, $r = 0$ ✓

Since $\mathbb{Z}$ is a cyclic group, all its subgroups would be cyclic.

$H \leq \mathbb{Z}$

$n\mathbb{Z} \leq \mathbb{Z}$ $\quad H = \langle k \rangle$

$= k\mathbb{Z}$

If $d \mid |G|$, then there need not exist $H \leq G$ of size d.

Result: Converse of Lagrange's Perrarchs theorem is true in case of cyclic group.

That is, if $d \mid |\langle a \rangle|$

then $\exists$ (!) $H \leq \langle a \rangle$

unique

with $|H| = d$.

let $|\langle a \rangle| = n$ and $d \mid n$.

let $K = n/d$

Set $b = a^k$.

Claim : $\langle b \rangle$ is of order d.

or $o(b) = d$.

$$b^d = (a^k)^d = (a^{n/d})^d = a^n = e$$

✓

In fact d is least s.t. $b^d = e$.

Now, let $H_1 \leq \langle a \rangle$

with $|H_1| = d$

Claim : $H = H_1$

(uniqueness).

★ $X = \{1\}$ $S_1 = \{id\}$

$X = \{1,2\}$ $S_2 = \{id, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$

$X = \{1,2,3\}$ $S_3 = \{id, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$

$$\sigma_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix}; \sigma_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \tau_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \tau_3 \begin{pmatrix} 123 \\ 213 \end{pmatrix}$$

$H_0 = \{e\}$ $\quad O(1)$

$H_1 = \{e, \tau_1\}$

$H_2 = \{e, \tau_2\}$ $\quad O(2)$

$H_3 = \{e, \tau_3\}$

$H_4 = \{e, \sigma_1, \sigma_2\}$ $\quad O(3)$

$H_5 = S_3$

★ NOTE: Sub-group ~~generated by~~ of prime order is cyclic.