Algebraic Structures

The Structure of Algebras

An algebra has the following components:

1. An underlying set S
2. Operations defined on this set.
3. Special elements of the underlying set possessing specific properties. These are called constants of the algebra.

- The underlying set could be something like the set of integers, real numbers or set of strings over an alphabet.
- An operation is a map from $S^p \rightarrow S$. p is called the 'arity' of the operation.
- For example if the underlying set is the set of real numbers, unary minus is a unary operator mapping x to –x.
- Addition is a binary operator mapping x and y into x + y.
- Algebras are specified by specifying the underlying set, operations on the set and the constants of the set in that order.

Example

The underlying set is the set of real numbers R and operation is binary +. Here +(a, b) = a + b.

Constant is 0.

$$a + 0 = a \text{ for all } a \text{ in } R$$
$$= 0 + a$$

The operation maps $R^2 \rightarrow R$.

This algebra can be specified as (R, +, 0).

Example

The underlying set is the set of all strings over an alphabet Σ, denoted on Σ*; the operation is concatenation.

$$\text{If } x = a_1 \ldots a_n$$
$$y = b_1 \ldots b_m$$
$$x \cdot y = xy = a_1 \ldots a_n b_1 \ldots b_m$$

It maps $\Sigma^* \times \Sigma^* \to \Sigma^*$ and is a binary operation.

The constant is λ, the empty string with specific property $x \cdot \lambda = \lambda \cdot x = x$ for all $x \in \Sigma^*$. This can be denoted as $(\Sigma^*, \cdot, \lambda)$.

Definition

Let S be a set and let $*$ be binary operation on S

1. The operation * is commutative over S, if $a * b = b * a$
2. The operation * is associative over S,

   if $a * (b * c) = (a * b) * c$, for $a, b, c \in S$.

- Two algebras of same signature or species if they have same number of operations and same number of constants.
- (I, +, 0), (Σ^*, ·, λ) are of the same species.

Example

Consider the variety of algebras with an underlying set, one binary operation and one constant similar to (I, +, ·) with the following axioms.

i. $x + y = y + x$

ii. $(x + y) + z = x + (y + z)$

iii. $x + 0 = x$

Then (R, +, 0), (P(S), ∪, ϕ), (P(S), ∩, S) and (I, ·, 1) satisfy these axioms and belong to the same variety. Any result proved for this variety will hold for all these algebras.

Example

Consider the variety of algebras with the same signatures as (R, +, ·, –, 0, 1) where + and · are binary operations of addition and multiplication respectively and – is a unary operator denoting unary minus. These operations satisfy the following axioms.

(i) $x + y = y + x$

(ii) $x \cdot y = y \cdot x$

(iii) $(x + y) + z = x + (y + z)$

(iv) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(v) $x \cdot (y + z) = x \cdot y + x \cdot z$

(vi) $x + (-x) = 0$

(vii) $x + 0 = x$

(viii) $x \cdot 1 = x$

Then (I, +, ·, –, 0, 1) and (Q, +, ·, –, 0, 1) where Q is the set of rational numbers are of the same variety. But (P(S), ∪, ∩, $\overline{\mathrm{r}}$, ϕ, S) where $\overline{\mathrm{r}}$ denotes set complementation, is not of the same variety because axiom (vi) does not hold for this algebra.

Definition

Let S be a set and S' a subset of S. Let $\square$ be a binary operation of S and Δ a unary operation. **S' is closed with respect to $\square$**, if for all $a, b \in S'$, $a \square b \in S'$. S' is closed with respect to Δ, if for all $a \in S'$, $\Delta a \in S'$.

If A is an algebra specified by (S, O, C), a subalgebra of A is A'= (S', O', C'), an algebra with the same signature which is contained in A.

e.g. (E,+,o) is subalgebra of (I,+,o)

Definition

Let □ be a binary operation on a set T. An element **e** ∈ S is an identity element (or unit element) for the operation □ if for every x ∈ T

$$\mathbf{e} \square x = x \square \mathbf{e} = x.$$

An element **o**∈T is a zero element for the operation □, if for every x∈T,

$$\mathbf{o} \square\ x = x \square \mathbf{o} = \mathbf{o}.$$

Example

Consider the set of integers. If addition is the operation, 0 is an identity element. If multiplication is the operation 1 is the identity element and 0 is the zero element.

Definition

Let □ be a binary operation an the set T. An element $\mathbf{e}_\ell$ is a left identity for the operation □ if for every $x \in T$, $\mathbf{e}_\ell \,\square\, x = x$.

An element $\mathbf{o}_\ell$ is a left zero for the operation □ if for every $x \in T$

$$\mathbf{o}_\ell \,\square\, x = \mathbf{o}_\ell.$$

A right identity and right zero can be defined in a similar manner.

Example

Let {a, b, c, d} be the underlying set. The binary operation is given by the below table.

□	a	b	c	d
a	a	c	d	a
b	a	b	c	d
c	a	b	a	c
d	a	b	b	b

The operation is not commutative as

$$a \square b = c$$
$$b \square a = a$$

and they are not equal

The operation is not associative as

$$a \square (b \square c) = a \square c = d$$
$$(a \square b) \square c = c \square c = a$$

and they are not equal. a is a right zero for the operation and b is a left identity.

Definition

Let □ be a binary operation on T and **e** an identity element for the operation □. If x □ y = **e**, then x is the left inverse of y and y is the right inverse of x with respect to the operation □. If both x □ y = **e** and y □ x = **e**, then x is the inverse of y (or a two-sided inverse of y) with respect to the operation □.

Example

The algebra (I, +, 0) has an identity 0 and for each x in I, –x is the inverse of x as x + (–x) = (–x) + x = 0.

Semigroups, Monoids and Groups

Definition

Let A be an algebra with an underlying set T and □ a binary operation on T.

(T, □) is called a semigroup if the following two conditions are satisfied

1. T is closed with respect to □.

2. □ is an associative operation.

Example

Let (E, +) be a system.

E is closed with respect to + and + is an associative operation.

∴ (E, +) is a semigroup.

Example

Consider (Σ^*, concatenation) where Σ is an alphabet.

Σ^* is closed with respect to concatenation and concatenation is an associative operation.

Hence (Σ^*, concatenation) is a semigroup.

- Find the zeros of the semigroups $(P(X), \cap)$ and $(P(X), \cup)$, where X is a set and $P(X)$ is its power set. Are these monoids?
- Soln

An element $\mathbf{o} \in T$ is a zero for the operation $\Box$, if for every $x \in T$,

$$\mathbf{o} \Box x = x \Box \mathbf{o} = \mathbf{o}.$$

The zero for $(P(X), \cap)$ is $\varnothing$

The zero for $(P(X), \cup)$ is X

An element $\mathbf{e} \in S$ is an identity element (or unit element) for the operation $\Box$ if for every $x \in T$

$$\mathbf{e} \Box x = x \Box \mathbf{e} = x.$$

The identity for $(P(X), \cap)$ is X

The identity for $(P(X), \cup)$ is $\varnothing$

Since identities exist, therefore also monoids.

Definition

Let (T, □) be an algebraic system, where □ is a binary operation on T. (T, □) is called a monoid if the following conditions are satisfied.

1. T is closed with respect to □.
2. □ is an associative operation.
3. There exists an identity element **e** ∈ T for the operation □.

i.e., for any x ∈ T, **e** □ x = x □ **e** = x.

In the above examples both (E, +) and (Σ^*, concatenation) are monoids.

For (E, +), 0 is the identity element.

For (Σ^*, concatenation), λ, the empty word (sometimes also denoted as ε) is the identity element.

Definition

Let (T, □) be an algebraic system, where □ is a binary operation on T. Then (T, □) is called a group if the following conditions are satisfied.

1. T is closed with respect to □

2. □ is an associative operation

3. There exists an identity element **e** ∈ T for the operation □

4. Each element x ∈ T has an inverse element x^{-1} ∈ T with respect to □. i.e.,

$$x \,\square\, x^{-1} = x^{-1} \,\square\, x = \mathbf{e}$$

In the examples considered above (E, +) is a group, with –x as the inverse of x for every x ∈ E. (Σ^*, concatenation) is not a group as inverse of a string x with respect to concatenation does not exist.

Examples

1. If Q is the set of rational numbers and + is an addition operation. Determine whether the algebraic system (Q,+) is a group.

   Closure and associativity of rational no's can easily be checked. 0 is the identity element and -a is the inverse of a which belongs to Q.

2. Let $R = \{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ where r_θ denotes rotation of geometric figures drawn on a plane by θ degrees. Let □ be the operation defined as $r_{\theta_1} □ r_{\theta_2} = r_{\theta_1} + r_{\theta_2}$.

Then (R, □) is a group. Closure and associativity can easily be checked. r_0 is the identity element and $r_{360-\theta}$ is the inverse of r_θ.

A group (T, □) is called a commutative group or abelian group if □ is a commutative operation. For example (Q, +) is a commutative group.

Let $G = (T, \square)$ be a group and T' a subset of T. $G' = (T', \square)$ is a subgroup of G if it satisfies the conditions of a group. For example $(E, +)$ is a subgroup of $(I, +)$.

In order to test whether $(T', \square)$ is a subgroup of $(T, \square)$, we have to check:

1. T' is closed with respect $\square$.
2. Associative property will hold and need not be checked.
3. The identity element **e** of $(T, \square)$ should also be the identity for $(T', \square)$. Hence T' should contain **e**.
4. For each element $a \in T'$, inverse of a also should be in T'.

Group

- Example: (I , $*$) where I is the set of integers and operation is defined as

$$a*b = a+b-2 \text{ for all } a,b \text{ in } I$$

Check if it is a group

i. $a \in I,\ b \in I \Rightarrow a+b-2 \in I$ so I is closed w.r.t.$*$

ii. $(a*b)*c = a*(b*c)$ (Associative)

$(a*b)*c = (a+b-2)*c = (a+b-2)+c-2 = a+b+c-4$

$a*(b*c) = a*(b+c-2) = a+(b+c-2)-2 = a+b+c-4$

Group Example

iii. Identity

$e*a = a$

$e+a-2 = a \Rightarrow e = 2 \in I$ for all a in I

iv. Inverse

If $a \in I$ then $b \in I$ will be the inverse of a if

$a*b = e = b*a$

$a+b-2 = 2 \Rightarrow b = -a+4 \in I$

- Is I an abelian group?

Cyclic Group

- A group is cyclic if every element is a power of some fixed element

$b = a^k$ for some a and every b in group

- **a** is said to be a generator of the group

Cyclic Groups

A *Cyclic Group* is a group which can be generated by one of its elements.

That is, for some *a* in **G**,
G={a^n | **n** is an element of **Z**}
Or, in addition notation,
G={*na* |*n* is an element of **Z**}

This element *a*
(which need not be unique) is called a *generator* of **G**.

Alternatively, we may write **G**=<*a*>.

***Examples**:*

(Z,.+) is generated by 1 or -1.

Z_n, the integers mod *n*
under modular addition,
is generated by 1
or by any element *k* in **Z_n**
which is relatively prime to *n*.

e.g. Let G={1,-1,i,-i} is a group with respect to the binary operation '×' .Then G is a cyclic group. Find the generators of a group G.

Ans. i and –i.

Cyclic Group

- Every cyclic group is an abelian group.
- If a finite group of order n contains an element of order n, the group must be cyclic.

RING

A ring is a mathematical system (R,+,.) consisting of a nonempty set R, with two binary operations denoted by (+) and (.) respectively, satisfying the following postulates.

R_1- (R,+) is an abelian group.

R_2- (R,.) is semi group.

R_3- Semi group operation (.) is distributive over the group operation(+).

a.(b+c) = a.b + a.c

EXAMPLE:(I,+,.),(R,+,.)

- If operation of multiplication is commutative, it forms a **commutative ring.**
- If multiplicative identity exists in a ring R, we call it **ring with unity or ring with unity element.**

i.e. If a.1= 1.a =a, then a is called a unit if a has a multiplicative inverse in R

- **Divisors of zero** – A ring (R,+,.) is said to have divisors of zero, if there exist non zero elements a, b ∈ R such that the product a.b=0. Thus a is called the left zero divisor, and b is called the right zero divisor.

INTEGRAL DOMAIN

The system (D,+,.) is an integral domain if

D_1- (D,+) is an abelian group.

D_2- (D,.) is commutative semi group with unity.

D_3- Multiplication operation is distributive over addition.

D_4- (D,+,.) is free of zero divisors.

OR

A commutative ring with unity without proper zero divisors is called an integral domain. i.e. if ab=0 implies a=0 or b=0

Ring with Zero Divisor

- If a and b are two non-zero elements of a ring R such that ab= o, then a and b are divisors of o.
- e.g.
- i) The ring of integers (z,+,.) is an integral domain since it is commutative ring with unity and for any two integers a,b, ab=o implies a=o or b=o(no zero divisors).
- ii) The ring of real numbers (R,+,.) is an integral domain.

FIELD

The system (F,+,.) is a field if,

F_1- (F,+) is an abelian group.

F_2- (F_0,.) is an abelian group.

F_3- Multiplication is distributive w.r.t addition.

OR

A commutative ring with unity is called a field if it contains multiplicative inverse of every non-zero element.

Ex. The systems (Q,+,.), (R,+,.), (C,+,.) are all fields.

- **Theorem : Every field is an integral domain. But every integral domain is not a field.**

Cosets and Lagrange’s Theorem

Let $(T, \square)$ be an algebraic system, where $\square$ is a binary operation. Let a be an element in T and H a subset of T. The left coset of H with respect to a, which is denoted by $a \square H$, is the set of elements $\{a \square x \mid x \in H\}$. Similarly, the right coset of H with respect to a is denoted as $H \square a$ and consists of elements $\{x \square a \mid x \in H\}$.

Theorem

(Lagrange's Theorem)

The order of any subgroup of a finite group divides the order of the group.

Theorem

Any group of prime order is cyclic and any element other than the identity is a generator. It also follows that it is abelian.

Normal Subgroups

Normal Subgroups

Let us now consider only groups. Given a group $G = (T, \square)$, We have seen that a subgroup $H = (T', \square)$ of G induces a partition of T which is determined by the cosets of the subgroup.

Each coset is a block of the partition.

Let H be a subgroup of G. H is said to be a normal subgroup if, for any element a in G, the left coset a □ H is equal to the right coset H □ a. It should be noted that if G is an abelian group, any subgroup of G is normal. Consider the following group G and its subgroup H.

G

□	a	b	c	d	e	f
a	a	b	c	d	c	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a

H

□	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

H is a normal subgroup of G.

For example

e □ H = {e □ a, e □ b, e □ c}
 = {e, d, f}

H □ e = {a □ e, b □ e, c □ e}
 = {e, f, d}