Discrete Mathematics and Logic (UE17CS205)

Unit 5 - Algebraic Structures

Mr. Channa Bankapur ,Sangeeta V I
Department of CS&E, PES University

Algebraic Structures

- Algebraic structures are useful in defining mathematical models to study a phenomenon or a process of a real world.

- Some useful algebraic structures:
  - Semigroup
  - Monoids
  - Groups
  - Rings
  - Fields

Algebraic Structures

- **Semigroups** are simple algebraic structures which satisfy the properties of closure and associativity.
- Applications:
  - Sequential Machines
  - Formal Languages
  - Computer Arithmetic

- A **monoid** in addition to being a semigroup satisfies the identity property.
- Applications:
  - Syntactic Analysis
  - Formal Languages

Algebraic Structures

- **Groups** are monoids which also possess inverse property.
- Applications:
  - Public-key Cryptosystems
  - Error-correcting codes
  - Fast Adders
- **Rings** and **Fields** are algebraic systems with two binary operations.
- **Isomorphism** shows that two algebraic systems are structurally indistinguishable and the results of operations in one system can be obtained from those of the other by simply renaming the names of the elements and symbols for operations.
- **Homomorphism** and Congruence classes.

Algebraic Structures

An algebra has the following components:

1. An underlying **set S** (aka the carrier of the algebra)
2. **Operations** defined on the set S.
3. **Constants** of the algebra possessing specific properties.

An algebra is denoted by **(S, O, C)** where **S** is the underlying set, **O** is the set of operations and **C** is the set of constants.

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 $\mathbf{S^p} \rightarrow \mathbf{S}$, where **p** is called the "**arity**" of the operation.

Algebraic Structures

Example: Underlying set is the set of real numbers **R**.
Operation is binary **+**.
+ (a, b) = a + b.
Constant is **0**.

a + 0 = a for all **a** in **R**.
a + 0 = 0 + a

Operation maps $\mathbf{R^2} \rightarrow \mathbf{R}$.

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

Algebraic Structures

Example: Underlying set is the set of all strings over an alphabet $\mathbf{\Sigma}$, denoted as $\mathbf{\Sigma}^*$; operation is concatenation.

If $\mathbf{x} = a_1 a_2 \ldots a_n$

$\mathbf{y} = b_1 b_2 \ldots b_m$

$\mathbf{x \cdot y} = \mathbf{xy} = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m$

It maps $\mathbf{\Sigma}^* \times \mathbf{\Sigma}^* \rightarrow \mathbf{\Sigma}^*$ and is a binary operation.

The constant is $\boldsymbol{\lambda}$, the empty string with specific property $x \cdot \boldsymbol{\lambda} = \boldsymbol{\lambda} \cdot x = x$ for all x in $\mathbf{\Sigma}^*$.

The algebra can be specified as $(\mathbf{\Sigma}^*, \cdot, \boldsymbol{\lambda})$.

Algebraic Structures

Example: $(S, \oplus, \odot, 0, 1)$

Underlying set is the set of integers $S = \{0, 1, \ldots, p-1\}$ where **p** is a prime.

Operation $\oplus$: $S^2 \rightarrow S$ --- mod p addition

$a \oplus b = a+b \bmod p$

Operation $\odot$: $S^2 \rightarrow S$ --- mod p multiplication

$a \odot b = ab \bmod p$

0 is a constant and $a \oplus 0 = 0 \oplus a = a$ for all a in S.

1 is a constant and $a \odot 1 = 1 \odot a = a$ for all a in S.

The algebra can be specified as $(S, \oplus, \odot, 0, 1)$.

Signature (aka species) of an algebra

Two algebras are of the same signature if they have the same number of operations and same number of constants and also corresponding operations are of the same arity.

Example:
(I, +, 0) and ($\mathbf{\Sigma}^*$, ·, $\boldsymbol{\lambda}$).

Example:
(R, ·, 1) and (I, -, 0).
a·1 = 1·a = a for all a in R.
But, it's not the case that a-0 = 0-a = a for all a in I because a - 0 ≠ 0 - a for some a.

Two algebras can have the same signature but may have different properties.

Axioms and Varieties

- An **axiom** is an equation written in terms of the elements of the underlying set and the operation in the set.
- A **variety** is a class of algebras having a set of axioms, together with a signature.
- So algebras which have the same signature and which obey the same set of axioms belong to the same variety. Eg: Groups and Rings.
- The **theorems** are proved based on the axioms of the variety and the results hold for all the algebras of the given variety.

Commutative and Associative properties

Let S be a set and let # be a binary operation on S.
The operation #

1. is commutative over S, if a # b = b # a
2. is associative over S, if a # (b # c) = (a # b) # c

for a, b, c in S.

Variety

Example: Consider the variety of algebras with an underlying set, one binary operation and one constant similar to **(I, +, 0)** with the following axioms

1. $x + y = y + x$
2. $(x + y) + z = x + (y + z)$
3. $x + 0 = x$

Then **(R, +, 0)**, $(R, \cdot, 1)$, $(I, \cdot, 1)$, $(P(S), \cup, \boldsymbol{\phi})$, and $(P(S), \cap, S)$ satisfy these axioms and belong to the same variety. Any result proved for this variety will hold for all these algebras.

Closure property

Let S be a set and S′ a subset of S. Let # be a binary operation of S and ~ a unary operation. S′ is **closed** with respect to #, if for all a,b ∈ S′, a#b ∈ S′. S′ is **closed** with respect to ~, if for all a in S′, ~a ∈ S′.

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

Subalgebra

Let A = (S, O, C) be an algebra with
$O = \{o_1, o_2, \ldots, o_n\}$ and $C = \{c_1, c_2, \ldots, c_k\}$.
The **A' = (S', O', C')** is a subalgebra of A if

1. **S'** $\subset$ S
2. Each o_i is same as o_i restricted to **S'**
3. **C'** = C.

If **A'** is a subalgebra of A, then **A'** has the same signature as A and obeys the same set of axioms. Moreover, the underlying set **A'** is a subset of the set A and **A'** is closed under all operations of A.

Subalgebra

Example: Let **E** be the set of even integers and **I** the set of integers. Then **(E, +, 0)** is a subalgebra of **(I, +, 0)**.

Example: Let ▪ denote multiplication. Then **([0, 1], ▪, 1)** is a subalgebra of **(R, ▪, 1)** where **R** is the set of real numbers.

If the set of constants of **A** is closed under the operations of **A**, then the algebra with this underlying set is the smallest subalgebra of **A**.

Identity Element

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

An element **0 ∈ T** is a **zero** for the operation **#**, if for every **x ∈ T**,
0 # x = x # **0** = **0**

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.

Left and Right Identity Element

#	a	b	c	d
a	a	c	d	a
b	a	b	c	d
c	a	b	a	c
d	a	b	b	b

Let **#** be a binary operation on a set **T**. An element $\mathbf{e}_\ell$ is a left identity for the operation **#** if for every x ∈ T $\mathbf{e}_\ell$ # x = x. An element $\mathbf{0}_\ell$ is a left zero for the operation # if for every x ∈ T, $\mathbf{0}_\ell$ # x = **0.**

A right identity $\mathbf{e}_r$ and a right zero $\mathbf{0}_r$ can be defined in a similar manner.

Left and Right Identity Element

Theorem: Let # be a binary operation on a set T with left identity $\mathbf{e}_\ell$ and right identity $\mathbf{e}_r$. Then $\mathbf{e}_\ell = \mathbf{e}_r$ and this element is a two-sided identity.

Proof:

Since $\mathbf{e}_\ell$ # x = x,

$\mathbf{e}_\ell$ # $\mathbf{e}_r$ = $\mathbf{e}_r$

Since x # $\mathbf{e}_r$ = x,

$\mathbf{e}_\ell$ # $\mathbf{e}_r$ = $\mathbf{e}_\ell$

Therefore, $\mathbf{e}_r = \mathbf{e}_\ell$

Left and Right Zero

Theorem: Let # be a binary operation on a set T with left zero $\mathbf{0}_\ell$ and right zero $\mathbf{0}_r$. Then $\mathbf{0}_\ell = \mathbf{0}_r$ and this element is a two-sided zero.

Proof:

Since $\mathbf{0}_\ell$ # x = $\mathbf{0}_{\ell'}$

$\mathbf{0}_\ell$ # $\mathbf{0}_r$ = $\mathbf{0}_\ell$

Since x # $\mathbf{0}_r$ = $\mathbf{0}_{r'}$

$\mathbf{0}_\ell$ # $\mathbf{0}_r$ = $\mathbf{0}_r$

Therefore, $\mathbf{0}_r$ = $\mathbf{0}_\ell$

Two-sided identity and zero

Corollary: A two-sided identity (or zero) for a binary operation is unique.

Proof:
If possible let $\mathbf{e_1}$ and $\mathbf{e_2}$ be two identities.

Then $\mathbf{e_1} \# \mathbf{e_2} = \mathbf{e_1}$, and also $\mathbf{e_1} \# \mathbf{e_2} = \mathbf{e_2}$

Hence, $\mathbf{e_1} = \mathbf{e_2}$

Inverse of an element

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 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.

Example: Let $\mathbf{N_k}$ = {0,1,2, …, k-1} and $\oplus$ is **mod k** operation. $\oplus$ is an associative binary operation with identity **0**. Every element has an inverse. **0** is its own inverse. For other elements, the inverse of **x** is **k-x**.

Inverse of an element

Theorem: If an element has both a left inverse and a right inverse with respect to an associative operation, then left and right inverse elements are equal.

Proof: Let **e** be an identity element for the operation **#**. Let **x** be an element, **y** its left inverse and **z** its right inverse. Then we have to show **y = z.**

Since **y** is the left inverse **y**#x = e.
Since **z** is the right inverse x#**z** = e.

y = y#e = y#(x#z) = (y#x)#z = e#z = **z**.

Some specific algebraic varieties

- **Semigroups** are simple algebraic structures which satisfy the properties of **closure** and **associativity**.
  - Sequential Machines
  - Formal Languages
  - Computer Arithmetic
- A **monoid** in addition to being a semigroup satisfies the **identity** property.
  - Syntactic Analysis
  - Formal Languages
- **Groups** are monoids which also possess **inverse** property.
  - Public-key Cryptosystems
  - Error-correcting codes
  - Fast Adders

Semigroups

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** property.

Example: Let (E, +) be a system.
E is closed with respect to + and
+ is an associative operation.
Therefore, (E, +) is a semigroup.

Example: Consider (**Σ***, concat) where **Σ** is an alphabet.
Σ* is closed with respect to concatenation and concatenation is an associative operation.
Hence, (**Σ***, concat) is a semigroup.

Monoid

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 property.
3. There exists an identity element **e** ∈ T for the operation #.
   i.e., for any x ∈ T, **e** # x = x # **e** = x.

In the previous example of (E, +) being a semigroup, **0** is the identity element of the set.
Therefore, (E, +) is a monoid.

In the previous example of (**Σ***, concat) being a semigroup, **λ** is the identity element of the set.
Hence, (**Σ***, concat) is a monoid.

Groups

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

1. T is closed with respect to #
2. # is an associative property.
3. There exists an identity element e ∈ T for the operation #.
4. Each element **x** ∈ T has an inverse element $\mathbf{x^{-1}}$ ∈ T with respect to #
   i.e., x # $\mathbf{x^{-1}}$ = $\mathbf{x^{-1}}$ # x = e.

In the previous example of (E, +) being a monoid,
-x is the inverse of **x** for every x ∈ E.
Therefore, (E, +) is a group.

But, (**Σ***, concat) is **not** a group as the **inverse** of a string **x** with respect to concatenation does not exist.

Groups

Example: If $Z_n = \{0, 1, \ldots, n-1\}$ and $\oplus$ is **mod n addition** operation (addition modulo n), then $\mathbf{(Z_n, \oplus)}$ is a group.

Groups

Example: Let R = $\{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ where $\mathbf{r_\theta}$ denotes rotation of geometric figures drawn on a plane by θ degrees. Let # be the operation defined as $\mathbf{r_{\theta 1} \# r_{\theta 2} = r_{\theta 1 + \theta 2}}$. Then (R, #) is a group.

Abelian Groups

A group (A, #) is called an abelian (aka commutative) group if # is a commutative operation.

Example: $(Z_n, \oplus)$ is an abelian group.

Groups

A group **(A, #)** is said to be finite if **A** is a finite set, and infinite if **A** is an infinite set.

The size (aka cardinality) of **A** is the **order** the group.

If **A** is a finite set **{a_1, …, a_n}** with **n** elements and the binary operation of the group is denoted by **#**, the effect of this operation on pairs of elements of **A** can be given by a **nxn** matrix as given in the table below.

#	a_1	a_2	…	a_n
a_1	c_{11}	c_{12}	…	c_{1n}
a_2	c_{21}	c_{22}	…	c_{2n}
…	…	…	…	…
a_n	c_{n1}	c_{n2}	…	c_{nn}

where, $\mathbf{c_{ij} = a_i \# a_j}$

Groups

#	a_1	a_2	…	a_n
a_1	c_{11}	c_{12}	…	c_{1n}
a_2	c_{21}	c_{22}	…	c_{2n}
…	…	…	…	…
a_n	c_{n1}	c_{n2}	…	c_{nn}

#	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Two elements in a row (or a column) cannot be the same. Hence each row (and column) is a permutation of $a_1 \ldots a_n$.

Subgroups

Let G = (T, #) be a group and **T'** a subset of T.

G' = (T', #) is a subgroup of G if it satisfies the conditions of a group. In order to test whether **(T', #)** is a subgroup of (T, #), we have to check:

1. **T'** is closed with respect to #.
2. Associative property with respect to # on **T'**.
3. The identity element **e** of (T, #) should also be the identity for **(T', #)**. Hence **T'** should contain **e**.
4. For each element **a ∈ T'**, inverse of **a** also should be in **T'**.

Eg: (E, +) is a subgroup of (I, +).

(**R'**, #) is a subgroup of (R, #) where

R = $\{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ and **R'** = $\{r_0, r_{120}, r_{240}\}$.

Subgroups

Theorem: Let (T, #) be a group and **T'** a subset of T. If **T'** is a finite set, then (**T'**, #) is a subgroup of (T, #), if **T'** is closed under #.

What this result says is that it is enough to check the closure property alone as the other properties will be satisfied if the closure property is satisfied whenever **T'** is a finite set.

Proof: It is given that **T'** is **closed** with respect to #. **Associative** property will hold for # on **T'** whenever it holds for # on T because the operation is on a subset of elements.

Let **a** be an element of **T'**.
Hence $\mathbf{a^2, a^3, a^4, \ldots}$ are all in **T'**.
Because **T'** is a finite set, by the pigeonhole principle for some **i** and **j**, **i** < **j**, $\mathbf{a^i = a^j}$.
That is, $\mathbf{a^i = a^i \# a^{j-i}}$.
Hence $\mathbf{a^{j-i}}$ is the **identity** of the operation **#** on **T'**.
If **j-i = 1**, $\mathbf{a^i = a^i \# a}$ and hence **a** must the identity element and also its own inverse.
If **j-i > 1,** $\mathbf{a^{j-i} = a\#a^{j-i-1}}$ and hence $\mathbf{a^{j-i-1}}$ is the inverse of **a** and is in **T'**.
Thus we see that if **T'** is closed with respect to **#**, the other properties of the group follow and hence **(T',#)** is a group.

Generators for a Group

Let (T, #) be an algebraic system where # is a closed operation.

Let S = $\{a_1, a_2, \ldots\}$ be a subset of T.
Let S_1 denote the subset of T which contains S as well as all elements a_i # a_j for a_i, a_j in S.
S_1 is called the set generated directly by S.
Similarly, let S_2 denote the set generated directly S_1, … and S_{i+1} denote the set directly generated by S_i.
Let **S*** denote the union of S, S_1, S_2, ….
The algebraic system (**S***, #) is called the **subsystem generated by S**, and an element is said to be generated by S if it is in **S***.

Generators for a Group

- We can see that # is a **closed** operation on S*. Thus for a group (T, #), if S* is finite, then (S*, #) is a subgroup.
- If S* = T, S is called a **generating set** of the algebraic system (T, #). Eg: In (R, #) where R = {r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}}, both {r_{60}} and {r_{120}, r_{180}} are generating sets of (R, #).
- A group that has a generating set consisting of a **single element** is known as a **cyclic group**. (R, #) is a cyclic group because {r_{60}} is generating set.
- Let (T, #) be a cyclic group and {a} a generating set of (T, #). Elements of T can be expressed as **a, a^2, a^3, ...** because of associating $\mathbf{a^i \# a^j = a^j \# a^i}$ with $\mathbf{a^{i+j}}$. Hence any cyclic group is a **commutative group**.

Generators for a Group

Let G = (T, #) be a group and let **a** ∈ T. $\mathbf{a^m}$ is defined as a#a#…#a (**m** factors), $a^{\mathbf{0}} = e$ and $a^{\mathbf{-m}} = (a^{\mathbf{-1}})^{\mathbf{m}}$ where $a^{\mathbf{-1}}$ is the inverse of **a**.

Lemma: If G = (T, #) is a group and a ∈ T, then

$\mathbf{a^r \# a^s = a^{r+s}}$

$\mathbf{(a^r)^s = a^{rs}}$

For **r, s** ∈ N (the set of nonnegative integers) the result is obvious.

If **r** and **s** are **negative** integers,

r = **-m**, s = **-n**, m, n > 0

$a^r \# a^s =$

Lemma: If $G = (T, \#)$ is a group and $a \in T$, then
$a^r \# a^s = a^{r+s}$, $(a^r)^s = a^{rs}$

For $r, s \in N$ (the set of nonnegative integers) the result is obvious.

If r and s are negative integers,

$r = -m, s = -n, m, n > 0$

$$\mathbf{a^r \# a^s = a^{-m} \# a^{-n} = (a^{-1})^m \# (a^{-1})^n}$$
$$\mathbf{= (a^{-1})^{m+n} = a^{-(m+n)} = a^{(-m)+(-n)} = a^{r+s}}$$

$$\mathbf{(a^r)^s = (a^{-m})^{-n} = (((a^m)^{-1})^{-1})^n = (a^m)^n}$$
$$\mathbf{= a^{mn} = a^{(-m)(-n)} = a^{rs}}$$

The case where one of **r** and **s** is nonnegative and the other negative can similarly be proved.

Theorem: In any group **G = (T, #)**, the powers of any fixed element **a ∈ T** constitute a subgroup of **G**.

Proof: Consider **G' = (T', #)** where **T'** consists of all powers of an element **a**.
Closure under **#** is proved by previous lemma and associative property holds because all elements are of the form $\mathbf{a^m}$.
$\mathbf{a^0 = e}$ is the identity element and inverse of $\mathbf{a^r}$ is $\mathbf{a^{-r}}$.

Theorem: Let G = (T, #) be a finite cyclic group generated by an element **a** ∈ T. If G is of order **n**, i.e., **|T| = n**, then $a^n = e$, so that $T = \{a, a^2, a^3, \ldots, a^n = e\}$. Moreover **n** is the least positive integer for which $a^n = e$.

Proof: If possible let $\mathbf{a^m=e}$ for some +ve integer **m<n**. Since G is generated by **a**, any element of T can be written as $\mathbf{a^k}$ for some integer **k**. **k = mq+r**, where **q** is some integer and **0≤r<m**. This leads to

$$\mathbf{a^k = a^{mq+r} = (a^{mq})\#a^r = (a^m)^q\#a^r}$$
$$\mathbf{= e^q \# a^r = e \# a^r = a^r}$$

so that every element of T can be expressed as $\mathbf{a^r}$ for some **r**, 0≤r<m. This means that T has at most **m** distinct elements and the order of G is **m<n**. It is a contradiction. Hence $\mathbf{a^m=e}$ for m<n is not possible. HTP.

Cosets

Let (T, #) be an algebraic system, where # is a binary operation.

Let **a** ∈ T and **H ⊆ T**.

- The **left coset** of H with respect to **a**,
  - **a#H** = {a#x | x∈H}.
- Similarly, the **right coset** of H with respect to **a,**
  - **H#a** = {x#a | x∈H}.

Cosets of groups

Let (T,#) be a group and (H,#) be a subgroup of (T,#).

- For any element $a \in T$ and $h_1, h_2 \in H$, $a\#h_1 \neq a\#h_2$.
  - No two elements of a#H can be identical because any element of T cannot occur twice in a row.
- |a#H| = |H|
- **Theorem:** Let a#H and b#H be two cosets of H. Then either a#H and b#H are disjoint or they are identical.
- Since two left cosets are either identical or disjoint, the left cosets of **H** form a partition of **T**, in which all blocks are of the same size **|H|**.
- |T| = |H| * (number of distinct cosets of H).

Lagrange's Theorem

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

Let (S, #) is a group and (S`, #) is subgroup of (S, #).

|S| = k |S`|.

That is, the order of a subgroup divides the order of the group. If a group is of prime order, it cannot have nontrivial subgroups. Trivial subgroups are the entire group itself and the one having just the identity element alone.

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.

Isomorphisms and Automorphisms

Isomorphism: i) Two algebraic systems are structurally similar
ii) Orders are same if they are finite.

Consider the following algebraic systems (T, *) & (S, ▫).

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

▫	p	q	r
p	p	q	r
q	q	r	p
r	r	p	q

Two systems (T,*) , (S, ▫) are isomorphic if there is a bijection f from T to S such that for any $a_1, a_2 \in T, f \in (a_1 * a_2) = f(a_1) \,▫\, f(a_2)$

In the above example

$$f(a) = p, f(b) = q, f(c) = r$$

Function f is called an isomorphism from (T,*) , (S, ▫) . (S, ▫) is an isomorphic image of (T,*) .

An isomorphism from an algebraic system (T,*) to itself is called an automorphism.

Eg. $f(a) = a, f(b) = b, f(c) = c$

Example 1: Show that the multiplicative group G consisting of three cube roots of unity $1, \omega, \omega^2$ $1, \omega, \omega^2$ is isomorphic to the group G′ of residue classes (mod3) under addition of residue classes (mod3).

×	1	ω	ω^2
1	**1**	**ω**	**ω^2**
ω	**ω**	**ω^2**	**1**
ω^2	**ω^2**	**1**	**ω**

$+_3$	{0}	{1}	{2}
{0}	**{0}**	**{1}**	**{2}**
{1}	**{1}**	**{2}**	**{0}**
{2}	**{2}**	**{0}**	**{1}**

Mapping f of G onto G′defined by $f(1)=\{0\}$, $f(\omega)=\{1\}$, $f(\omega^2)=\{2\}$ is an isomorphism. Also:

$f(\omega\cdot\omega^2)=f(1)=\{0\}=\{1\}+\{2\}=f(\omega)+f(\omega^2)$

Permutation Groups

Let $S = \{a_1, \ldots, a_n\}$ be a set of n elements and
let p denote a permutation of S.
p is a bijective mapping $p: S \rightarrow S$.

If p_1 and p_2 are permutations, $\mathbf{p_1 \text{ o } p_2}$ is a permutation,
where $\mathbf{p_1 \text{ o } p_2}$ is the composition of functions.
Example: Suppose $p_1 = \langle a_2, a_3, a_1 \rangle$ and $p_2 = \langle a_3, a_2, a_1 \rangle$
$\mathbf{p_1 \text{ o } p_2} = \langle a_1, a_3, a_2 \rangle$

Associative property holds for the composition of permutations.
$p_1 \text{ o } (p_2 \text{ o } p_3) = (p_1 \text{ o } p_2) \text{ o } p_3$

$\langle a_1, a_2, \ldots, a_n \rangle$ is the identity permutation.

$\therefore$(P, o) is a group where $P=\{p_1, p_2, \ldots, p_{n!}\}$, $S=\{a_1, \ldots, a_n\}$

Homomorphisms

- Two algebraic systems are structurally similar.
- Orders of the two algebraic systems are not same.

So the function f is not bijection.

Definition: Let A=(S,O,C) be an algebra and A'=(S',O',C') be another algebra with the same signature and **h** be a function such that

h: S $\rightarrow$ S'

h(a # b) = h(a) **#'** h(b)

h(c) = c'

where # and **#'** are corresponding operators in A and **A'** respectively. **c** and **c'** being corresponding constants.

Isomorphism is a particular case of homomorphism.

Homomorphism

Example:

f_k: I→I where $f_k(x)$= kx for an integer k is a homomorphism from (I, +, 0) to (I,+,0).

Example:

f(x) = |x| is a homomorphism from (Σ^*, ·, λ) to (N, +, 0).

Theorem: Let h be a homomorphism from A=(S,O,C) to A'=(S',O',C'). Then (h(S),O',C') is a subalgebra of A', called homomorphic image of A under h.

Proof: To prove that (h(S),O',C') is a subalgebra, the following conditions must be satisfied.

i) $h(S) \subset S`$

ii) The constant k' is an element of h(S).

iii) The set h(S) is closed under the operations O`.

If A` is a

- semigroup, homomorphic image of A is also a semigroup.
- monoid, homomorphic image of A is also a monoid.
- group, homomorphic image of A is also a group.

Monomorphism: A homomorphism which is injective (one-to-one function).

Epimorphism: A homomorphism which is surjective (onto function).

Endomorphism: A homomorphism where codomain and domain are the same.

Isomorphism: A homomorphism which is bijective (one-to-one correspondence).

Congruence Relations

Alternate way to look at the notion of a homomorphism from one algebraic system to another.

A congruence relation is an equivalence relation defined on the carrier of an algebra that the equivalence classes of the relation are "preserved" by the operations of the algebra.

An equivalence relation which is both left invariant and right invariant under the operations of the algebra is called a congruence relation.

i.e. ~ is a congruent relation on T if and only if for all $a, b, c \in T, if\ a \sim b,\ \ a\#c \sim b\#c\ and\ \ c\#a \sim c\#b$

Example: Let F be a set of fractions. The binary operation +, -, . and the unary – can be defined on F.

Let F be the set of all fractions of the form p/q with ordered pairs <p, q>.
Binary operations +, - and ·, and unary - can be defined on F.

- (p/q) + (r/s) = (ps + rq) / (qs)
- (p/q) - (r/s) = (ps - rq) / (qs)
- (p/q) · (r/s) = (pr) / (qs)
- -(p/q) = (-p)/q

Ordered pairs <1, 2> and <2, 4> are different elements of F, but their value is same. An equivalence relation ~ can capture that.

- (p/q) ~ (r/s) iff ps = rq.

Example: Prove that equality relation is a congruence relation on any algebra.

Example: Consider the set of integers together with the operation of multiplication. Prove that the equivalence relation ~ of " equivalence mod k" for some positive integer k is a congruence relation on the algebra (I, ·).

Theorem:
The equivalence relation $\sim$ on a set T is a congruence relation with respect to the binary operation $\#$ if and only if whenever $a \sim b \ \ and \ c \sim d, we \ have \ a\#c \sim b\#d.$

Theorem :
Let $A = (T, \#)$ be an algebra with T as the underlying set and $\#$ a binary operation on T. Let h be a homomorphism from $A = (T, \#) to \ A' = (T', \#')$. Then the equivalence relation induced by h is a congruence relation on the algebra A.

Algebraic Systems with **one** binary operation

- Semigroups
- Monoids
- Groups

Algebraic Systems with **two** binary operation

- Rings
- Integral Domains
- Fields

Rings

Definition: An algebraic system $(S, +, .)$ is called a ring if the following conditions are satisfied

1. $(S, +)$ is an abelian group
2. $(S, .)$ is a semigroup
3. The operation . is distributive over +.

Eg. (I,+,*)

Example

$Let\ Z_n\ be\ the\ set\ of\ integers\ \{0,1,2,\ldots n-1\}.\ Let\ \oplus$ denote the binary operation of modn addition

i.e. , $a \oplus$b = $\begin{cases} a+b & if\ a+b<n \\ a+b-n & if\ a+b \geq n \end{cases}$

Let $\odot$ denote mod n multiplication.

$i.e.\ a \odot$b=the remainder of ab divided by n.

Integral Domains

Definition: Let $(S, +, .)$ be an abelian group with two binary operations. $< S, +, . >$ is called an integral domain if

1. $(S, +)$ is an abelian group
2. 2. The operation'.' is commutative. Further more, if $c \neq 0$ and $c.a = c.b,\ then\ a = b$, where 0 is the addiyive identity.
3. 3. The operation '.' is distributive over the opertaion '+'.

Eg. (I,+,*)

Fields

Definition: Let $(S, +, .)$ be an abelian group with two binary operations. $< S, +, . >$ is called a field if

1. $(S, +)$ is an abelian group
2. $(S - \{0\})$ is an abelian group,where 0 is the additive identity.
3. 3. The operation '.' is distributive over the operataion '+'.

Mathematicians are only dealing with the **structure of the reasoning** and they don't really care about what they are talking. They don't even need to know what they are talking about. Mathematicians prepare **abstract reasoning** that's ready to be used if you will only have a **set of axioms** about the real world.

- Richard Feynman

< End of
Algebraic Structures
/>