11 Algebraic Structures and Coding Theory

- Introduction
- The Structure of Algebras
- Semigroups, Monoids and Groups
- Homomorphisms, Normal Subgroups and Congruence Relations
- Rings, Integral Domains and Fields
- Quotient and Product Algebras
- Coding Theory
- Polynomial Rings and Polynomial Codes

11.1 INTRODUCTION

Generally, to study a phenomenon or process of a real world, we construct a suitable mathematical model to represent it and study the properties of the model to understand the phenomenon. Often the mathematical structure of a model is presented implicitly. But in this chapter, we specify in detail some mathematical structures and develop a few basic properties of these structures, emphasizing those properties which are useful for the models under consideration. The mathematical structures are called algebras or algebraic structures. The structures mainly considered are semigroups, monoids, groups, rings and fields.

Semigroups are the simplest algebraic structures which satisfy the properties of closure and associativity. They are very important in the theory of sequential machines, formal languages and in certain applications relating to computer arithmetic.

A monoid in addition to being a semigroup also satisfies the identity property. Monoids are used in a number of application but most particularly in the area of syntactic analysis and formal languages.

Groups are monoids which also possess inverse property. The application of group theory is important in the design of fast adders and error-correcting codes.

Rings and fields are algebraic systems with two binary operations.

In this chapter, we also study some useful and important concepts like isomorphism and homomorphism. The concept of isomorphism shows that two algebraic systems which are isomorphic to one another are structurally indistinguishable and that 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.

Another important concept studied here is that of homomorphism and congruence classes.

We also study coding theory in this chapter. When bits are transmitted through a communications channel, it is quite possible that some bits are erroneously transmitted due to noise or some fluctuations. In order to avoid erroneous transmission of bits, sequence of bits are divided into blocks and each block is encoded into a larger binary string and transmitted. The decoding scheme is defined in such a way that if a small error occurs, the bits transferred erroneously are found out, corrected and the correct original block of strings recovered. Various ways of encoding and decoding are studied here. The use of algebraic structure group is made use of in some encoding schemes. This is studied in detail.

In the last section, rings whose elements are polynomials and their use in defining cyclic codes is discussed.

Scanned by CamScanner

11.2 THE STRUCTURE OF ALGEBRAS

In this section, we try to give a general introduction of an algebra which describes the concept and also we give some examples.

An algebra has the following components:

1. an underlying set S (sometimes it is called the carrier of the algebra)
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 $S^p \to S$. 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 1 Underlying set is the set of real numbers R. Operation is binary $+$. $+ (a, b) = a + b$. Constant is 0

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

Operation maps $R^2 \to R$.

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

Example 2 *Underlying set is the set of all strings over an alphabet Σ, denoted as Σ^*; operation is concatenation.*

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 $(\Sigma^*, \cdot, \lambda)$.

Example 3 $(S, \oplus, \odot, 0, 1)$

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

Two operations are defined:

$\oplus\ S^2 \to S$ – mod p addition

$a \oplus b = a + b$ if $a + b < p$
$a + b - p$ if $(a + b) \geq p$.

$\odot\ S^2 \to S$ – mod p multiplication

$a \odot b = ab \bmod p$.

Both are binary operators.

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

1 is another constant with the specific property that

$a \odot 1 = 1 \odot a = a$ for all $a \in S$.

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

Scanned by CamScanner

Usually we would like to specify a class of algebras possessing some common properties rather than a single algebra.

We define a signature or species of an algebra first. Two algebras are of the same signature (or of the same species) if they have the same number of operations and same number of constants and also the corresponding operations are of the same arity.

Example 4 *$(I, +, 0)$ and $(\Sigma^*, \cdot, \lambda)$ are of the same species.*

$(R, \cdot, 1)$ and $(I, -, 0)$ have the same signature.

They have one binary operation and one constant. The $-$ here is a binary operation.

It maps $I^2 \to I$. i.e.,

It maps (a, b) to $a - b$.

Similarly $\cdot$ is a multiplication operator mapping $R^2 \to R$.

It maps (a, b) into ab.

$a \cdot 1 = 1 \cdot a = a$ for all a in R

But $a - 0 \neq 0 - a$

$a - 0 = a$ for all a in I

But $0 - a = -a$

So they have different properties.

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

So we have to consider additional properties to define algebras of similar type. We define these properties and call them as axioms. Each axiom is an equation written in terms of the elements of the underlying set and the operations in the set. A set of axioms, together with a signature, specifies a class of algebras called a variety. Algebras which have the same signature and which obey the same set of axioms belong to the same variety. Examples are groups, rings, monoids, etc. Usually we explore and study results of algebras of particular varieties. The theorems are proved based on the axioms of the variety and the results hold for all algebras of the given variety.

Definition 1 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 $a, b, c, \varepsilon S$.

Example 5 *Consider the variety of algebras with an underlying set, one binary operation and one constant similar to $(I, +, \cdot)$ with the following axioms*

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

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

(iii) $x + 0 = x$

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

Example 6 *Consider the variety of algebras with the same signatures as $(R, +, \cdot, -, 0, 1)$ where $+$ and $\cdot$ 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) $x \cdot y = y \cdot x$

Scanned by CamScanner

(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 $(I, +, \cdot, -, 0, 1)$ and $(Q, +, \cdot, -, 0, 1)$ where Q is the set of rational numbers are of the same variety. But $(P(S), \cup, \cap, \bar{r}, \phi, S)$ where $\bar{r}$ denotes set complementation, is not of the same variety because axiom (vi) does not hold for this algebra.

Let us denote an algebra by (S, O, C) where S is the underlying set, O is the set of operations and C is the set of constants. ◀

Definition 2 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 an algebra with the same signature which is contained in A.

Definition 3 Let $A = (S, O, C)$ be an algebra with $O = \{o_1, o_2, \ldots, o_n\}$ and $C = \{c_1, c_2, \ldots, c_k\}$. Then $A' = (S', O', C')$ is a subalgebra of A if

(i) $S' \subset S$
(ii) Each o_i is same as o_i restricted to S'
(iii) $C' = C$

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. The largest possible subalgebra of A is A itself.

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.

Example 7 *Let E be the set of even integers and I the set of integers. Then $(E, +, 0)$ is a subalgebra of $(I, +, 0)$.* ◀

Example 8 Let $\cdot$ denote multiplication. Then $([0, 1], \cdot, 1)$ is a subalgebra of $(R, \cdot, 1)$ where R is the set of real numbers. ◀

Definition 4 Let $\square$ be a binary operation on a set T. An element $e \in S$ is an identity element (or unit element) for the operation $\square$ if for every $x \in T$

$$e \square x = x \square e = x.$$

An element $\mathbf{0} \in T$ is a zero for the operation $\square$, if for every $x \in T$,

$$\mathbf{0} \square x = x \square \mathbf{0} = \mathbf{0}.$$

Example 9 *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.* ◀

Scanned by CamScanner

Definition 5 Let $\square$ be a binary operation an the set T. An element e_ℓ is a left identity for the operation $\square$ if for every $x \in T$, $e_\ell \square x = x$.

An element $\mathbf{0}_\ell$ is a left zero for the operation $\square$ if for every $x \in T$

$$0_\ell \square x = 0_\ell.$$

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

Example 10

$\square$	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 $\{a, b, c, d\}$ be the underlying set. The binary operation is given by the above table.

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.

Theorem 1 Let $\square$ 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 $\mathbf{e}_\ell$ and $\mathbf{e}_r$ are left and right identities $\mathbf{e}_r = \mathbf{e}_\ell \square \mathbf{e}_r = \mathbf{e}_r$.

Theorem 2 Let $\square$ be a binary operation on a set T will left zero $\mathbf{0}_\ell$ and right zero $\mathbf{0}_r$. The $\mathbf{0}_\ell = \mathbf{0}_r$ and this element is a two-sided zero.

Proof: Since $\mathbf{0}_\ell$ is a left zero

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

Similarly $\mathbf{0}_\ell \cdot \mathbf{0}_r = \mathbf{0}_r$ as $\mathbf{0}_r$ is the right zero. Therefore $\mathbf{0}_\ell = \mathbf{0}_r$.

Corollary 1 A two-sided identity (or zero) for a binary operation is unique.

Proof: If possible let e_1 and e_2 be two identities.

Then $e_1 \square e_2 = e_1$ and also $e_1 \square e_2 = e_2$

Hence $e_1 = e_2$.

Similar proof can be given for zero element.

Scanned by CamScanner

Definition 6 Let $\square$ be a binary operation on T and e an identity element for the operation $\square$. If $x \square y = e$, then x is the left inverse of y and y is the right inverse of x with respect to the operation $\square$. If both $x \square y = e$ and $y \square x = e$, then x is the inverse of y (or a two-sided inverse of y) with respect to the operation $\square$.

Example 11 *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 12 *Let N_k be the first k natural numbers, where $k > 0$*

$$N_k = \{0, 1, 2, \ldots, k-1\}.$$

Define $\oplus$ as mod k addition, i.e., for every $x, y \in N_k$.

$$x \oplus y = x + y \text{ if } x + y < k$$
$$= x + y - k \text{ if } x + y \geq k$$

$\oplus$ 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 $k - x$. ◀

Theorem 3 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 $\square$. 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 $y \square x = e$.

Since z is the right inverse $x \square z = e$.

$$y = y \square e = y \square (x \square z) = (y \square x) \square z \text{ (associativity)}$$
$$= e \square z = z.$$

Exercises

1. Let $(A, \square)$ be an algebraic system where $\square$ is a binary operation such that, for any a and b in A, $a \square b = a$.
   a) Show that $\square$ is an associative operation
   b) Can $\square$ ever be a commutative operation?
2. Let N be the set of all natural numbers. For each of the following determine whether $*$ is an associative operation:
   a) $a * b = \max(a, b)$
   b) $a * b = \min(a, b+2)$
   c) $a * b = a + b + 3$
   d) $a * b = a + 2b$
   e) $a * b = \begin{cases} \min(a, b) & \text{if } \min(a, b) < 10 \\ \max(a, b) & \text{if } \min(a, b) \geq 10 \end{cases}$

11.3 SEMIGROUPS, MONOIDS AND GROUPS

Many specific algebraic varieties are useful in various applications in computer science and other areas. In this section we study about some properties of semigroups, monoids and groups.

Definition 1 Let A be an algebra with an underlying set T and $\square$ a binary operation on T. $(T, \square)$ is called a semigroup if the following two conditions are satisfied

1. T is closed with respect to $\square$
2. $\square$ is an associative operation.

Scanned by CamScanner

Example 1 *Let $(E, +)$ be a system.*

E is closed with respect to $+$ and

$+$ is an associative operation.

$\therefore (E, +)$ is a semigroup.

Example 2 *Consider* $(\Sigma^*$, concatenation$)$ *where* Σ *is an alphabet.*

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

Hence $(\Sigma^*$, concatenation$)$ is a semigroup.

Definition 2 Let $(T, \square)$ be an algebraic system, where $\square$ is a binary operation on T. $(T, \square)$ is called a monoid if the following conditions are satisfied.

1. T is closed with respect to $\square$.
2. $\square$ is an associative operation.
3. There exists an identity element $e \in T$ for the operation $\square$.

i.e., for any $x \in T$, $e \square x = x \square e = x$.

In the above examples both $(E, +)$ and $(\Sigma^*$, concatenation$)$ are monoids.
For $(E, +)$, 0 is the identity element.
For $(\Sigma^*$, concatenation$)$, λ, the empty word (sometimes also denoted as ε) is the identity element.

Definition 3 Let $(T, \square)$ be an algebraic system, where $\square$ is a binary operation on T. Then $(T, \square)$ is called a group if the following conditions are satisfied.

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

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

In the examples considered above $(E, +)$ is a group, with $-x$ as the inverse of x for every $x \in E$. $(\Sigma^*$, concatenation$)$ is not a group as inverse of a string x with respect to concatenation does not exist.

Example 3 *If* $Z_n = \{0, 1, \ldots, n-1\}$ *and* $\oplus$ *is mod n addition operation (addition modulo n), then we can easily check that* $(Z_n, \oplus)$ *is a group.*

Extra Examples

Example 4 *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* $\square$ *be the operation defined as* $r_{\theta_1} \square r_{\theta_2} = r_{\theta_1+\theta_2}$. *Then* $(R, \square)$ *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 $(A, \square)$ is called a commutative group or abelian group if $\square$ is a commutative operation. For example $(Z_n, \oplus)$ is a commutative group.

Scanned by CamScanner

A group $(A, \square)$ is said to be finite if A is a finite set, and infinite if A is an infinite set. The size of A is often referred to as the order of the group. If A is a finite set $\{a_1, \ldots, a_n\}$ with n elements and the binary operation of the group is denoted by $\square$, the effect of this operation on pairs of elements of A can be given by a $n \times n$ matrix as given in the table below.

$\square$	a_1	$\cdots$	a_n
a_1	c_{11}	$\cdots$	c_{1n}
$\cdots$		$\cdots$	
a_n	c_{n1}	$\cdots$	c_{nn}

$c_{ij} = a_i \square a_j$

Because of the property that each element has an inverse, two elements in a row cannot be the same. For suppose $c_{ij} = c_{ik}$, $a_i \square a_j = a_i \square a_k$

$$a_i^{-1} \square a_i \square a_j = a_i^{-1} \square a_i \square a_k$$
$$e \square a_j = e \square a_k$$
$$a_j = a_k$$

Similarly two elements in a column cannot be the same. Hence each row of the above table in a permutation of $a_1, \ldots, a_n$ and each column is also a permutation of $a_1, \ldots, a_n$.

If A has two elements $\{a, b\}$ with a as the identity element the table is of the form

$\square$	a	b
a	a	b
b	b	a

a is its own inverse; similarly b is also its own inverse.

If A has 3 elements $\{a, b, c\}$ with a as identity, the table has the form

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

a is its own inverse; b and c are inverses of each other. Note that these are abelian groups.

If A has 4 elements $\{a, b, c, d\}$ with a as identity, two possibilities exist;

$\square$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\square$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Scanned by CamScanner

Both are abelian groups. In the first case each element is its own inverse. In the second case, a and c are their own inverses and b and d are inverses of each other. (Interchange of two rows and corresponding columns does not give rise to another group).

Subgroups 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 $(I, +)$. If $R' = (r_0, r_{120}, r_{240})$, $(R', \square)$ is a subgroup of $(R, \square)$ considered earlier.

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'.

Theorem 1 Let $(T, \square)$ be a group and T' a subset of T. If T' is a finite set, then $(T', \square)$ is a subgroup of $(T, \square)$, if T' is closed under $\square$.

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 if T' is a finite set.

Proof: Already we noted that the associative property will hold for $\square$ on T'. It is given that T' is closed with respect to $\square$. Let a be an element of T'. Hence $a^2, a^3, a^4, \ldots$ are all in T'. Because T' is a finite set, by the pigeonhole principle for some i and j, $i < j$, $a^i = a^j$. i.e., $a^i = a^i \square a^{j-i}$.

Hence a^{j-i} is the identity of the operation $\square$ on T'. The identity is in T'. If $j-i > 1$. Also $a^{j-i} = a \square a^{j-i-1}$. Hence a^{j-i-1} is the inverse of a and is in T'. If $j - i = 1$, we have $a^i = a^i \square a$. Hence a must be the identity element and hence its own inverse. Thus we see that if T' is closed with respect to $\square$, the other properties of group follow and $(T', \square)$ is a group.

Generators for a Group Let $(T, \square)$ be an algebraic system where $\square$ 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 $a_i \square a_j$ for a_i, a_j in B. S_1 is called the set generated directly by S. Similarly, let S_2 denote the set generated directly by $S_1, \ldots$ and S_{i+1} denote the set directly generated by S_i. Let S^* denote the union of $S, S_1, S_2, \ldots$. The algebraic system $(S^*, \square)$ is called the subsystem generated by S, and an element is said to be generated by S if it is in S^*. Note that $\square$ is a closed operation on S^*. Thus for a group $(T, \square)$, if S^* is finite, then $(S^*, \square)$ is a subgroup. If $S^* = T$, S is called a generating set or a set of generators of the algebraic system $(T, \square)$. In the example of rotation of geometric figures, $\{60°\}$ is a generating set $\{120°, 180°\}$ is also a generating set.

A group that has a generating set consisting of a single element is known as a cyclic group. We considered two groups with 4 elements. The second one is a cyclic group with generating set $\{b\}$. $\{d\}$ is also a generating set for that group. The first one is not a cyclic group.

Let $(T, \square)$ be a cyclic group and $\{a\}$ a generating set of $(T, \square)$. Clearly elements of T can be expressed as $a, a^2, a^3, a^4, \ldots$ because of associating $a^i \square a^j = a^j \square a^i$ with a^{i+j}. Hence any cyclic group is a commutative group. Note that the group of four elements given in the left table (a) is commutative but not cyclic.

Let $G = (T, \square)$ be a group and let $a \in T$. a^m is defined as $a \square a \square \ldots \square a$ (m factors) $a^0 = e$ and $a^{-m} = (a^{-1})^m$ where a^{-1} is the inverse of a.

Lemma 1 If $G = (T, \square)$ is a group and $a \in T$, then

$$a^r \square a^s = a^{r+s} \qquad (a^r)^s = a^{rs}$$

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

Scanned by CamScanner

If r and s are negative integers,

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

$$\begin{aligned} a^r \square a^s &= a^{-m} \square a^{-n} = (a^{-1})^m \square (a^{-1})^n \\ &= (a^{-1})^{m+n} = a^{-(m+n)} \\ &= a^{(-m)+(-n)} = a^{r+s}. \end{aligned}$$

$$\begin{aligned} (a^r)^s &= (a^{-m})^{-n} = ((a^m)^{-1})^{-n} \\ &= (((a^m)^{-1})^{-1})^n \\ &= (a^m)^n = a^{mn} \\ &= a^{(-m)(-n)} = a^{rs}. \end{aligned}$$

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

Theorem 2 In any group $G = (T, \square)$, the powers of any fixed element $a \in T$ constitute a subgroup of G.

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

Theorem 3 Let $G = (T, \square)$ be a finite cyclic group generated by an element $a \in T$. 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 $a^m = e$ for some positive integer $m < n$. Since G is generated by a, any element of T can be written as a^k for some integer k. k can be written as $mq + r$, where q is some integer and $0 \le r < m$. This leads to

$$\begin{aligned} a^k &= a^{mq+r} = (a^{mq}) \square a^r = (a^m)^q \square a^r \\ &= (e)^q \square a^r = e \square a^r = a^r \end{aligned}$$

so that every element of T can be expressed as a^r for some r, $0 \le r < m$. This means that T has at most m distinct elements and the order of G is $m < n$. Thus we arrive at a contradiction. Hence $a^m = e$ for $m < n$ is not possible.

We also note that all the elements $a, a^2, \ldots, a^n$ are all distinct and $a^n = e$. This can be seen as follows. Suppose if possible let $a^i = a^j$, $i < j \le n$. This means $a^{j-i} = e$ where $j < n$, and this is a contradiction.

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 $\{x \square a \mid x \in H\}$.

The cosets of groups have some interesting properties. Let $(T, \square)$ be a group and $(H, \square)$ be a subgroup of $(T, \square)$. If H has r elements say, $a \square H$ also has r elements. Since any element of T cannot occur twice in a row or in a column of the group table, no two elements of $a \square H$ can be identical.

Theorem 4 Let $a \square H$ and $b \square H$ be two cosets of H. Then either $a \square H$ and $b \square H$ are disjoint or they are identical.

Scanned by CamScanner

Proof: Suppose $a \square H$ and $b \square H$ are not disjoint. Let c be a common element of both. i.e., there exist elements h_1 and h_2 in H such that $c = a \square h_1 = b \square h_2$ which means $a = b \square h_2 \square h_1^{-1}$. Let $x \in a \square H$. Then $x = a \square h_3$. i.e., $x = (b \square h_2 \square h_1^{-1}) \square h_3 = b \square (h_2 \square h_1^{-1} \square h_3)$. But $h_2 \square h_1^{-1} \square h_3$ is an element of H and hence $x = b \square h_4$ for $h_4 = h_2 \square h_1^{-1} \square h_3$. Therefore, $x \in b \square H$. Similarly if $y \in b \square H$, we can show $y \in a \square H$ too. Thus $a \square H$ and $b \square H$ are identical. So if they are not disjoint, they are identical.

Let $(T, \square)$ be a group and $(H, \square)$ be a subgroup of $(T, \square)$. Because $(T, \square)$ is a group, no two elements in a column or no two elements in a row of the group table are the same. Hence it follows that for any $a \in T$ and h_1 and h_2 in H, $a \square h_1 \neq a \square h_2$. It follows that the size of any coset of H is the same as that of H. H contains the identity of the group. Hence if we compute all the left cosets of H, we would have exhausted all the elements in T. Consequently, we can conclude that the left cosets of H form a partition of T, in which all blocks are of the same size. Thus the size of T is the product of the size of H and the number of distinct cosets of H. Hence we have the following theorem

Theorem 5 **(Lagrange's Theorem)** The order of any subgroup of a finite group divides the order of the group.

From the above theorem, we can conclude that 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 6 Any group of prime order is cyclic and any element other than the identity is a generator. It also follows that it is abelian.

Proof: Let $G = (T, \square)$ be a group of prime order and let $a \in T$ and $a \neq e$. The powers of a form a group. This should be G itself as G has no nontrivial subgroup and hence any element a is a generator of G and G is cyclic.

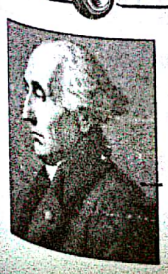
Isomorphisms and Automorphisms Let $(T, \square)$ be the algebraic system where $T = \{a, b, c\}$ and $(S, *)$ be an algebraic system with $S = \{\alpha, \beta, \gamma\}$. The tables for the operations are given below.

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

$*$	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	β

One can easily see the similarity between the two systems. In essence, they are the same, except for renaming of the elements and symbols used for operation. In this case we say that $(T, \square)$ is isomorphic to $(S, *)$. We say two systems $(T, \square)$ and $(S, *)$ are isomorphic if there is a bijection f from T to S such that for any a_1, a_2 in T

Links



JOSEPH LOUIS LAGRANGE Joseph Louis Lagrange was born in Italy on 25th January 1736. He lived part of his life in Prussia and part in France. He has contributed a lot to the areas of analysis, number theory, classical and celestial mechanics. He had served as the director of mathematics at the Prussian Academy of Sciences in Berlin for 20 years. Then he moved over to France and was a member of the French academy till his death in 1813. Napolean named Lagrange to the Legion of Honour and made him a count of the empire in 1808. His treatise on analytical mechanics published in 1788, was considered as the best treatment of classical mechanics in those days.

Scanned by CamScanner

$$f(a_1 \square a_2) = f(a_1) * f(a_2)$$

The function f is called an isomorphism from $(T, \square)$ to $(S, *)$. $(S, *)$ is called an isomorphic image of $(T, \square)$. In the above example f is a function such that

$$f(a) = \alpha$$
$$f(b) = \beta$$
$$f(c) = \gamma$$

Note that a function g defined as follows is also an isomorphism from $(T, \square)$ to $(S, *)$.

$$g(a) = \alpha$$
$$g(b) = \gamma$$
$$g(c) = \beta$$

An isomorphism from an algebraic system $(T, \square)$ to $(T, \square)$ is called an automorphism. For example, the function

$$f(a) = a$$
$$f(b) = c$$
$$f(c) = b$$

is an automorphism.

Example 5 *Let $G = (T, \square)$ be a group of order p where p is a prime. Any group of order p is isomorphic to G.*

We saw that for any integer n, $(Z_n, \oplus)$ is a group. Any group of order p is isomorphic to $(Z_p, \oplus)$. This can be seen as follows.

Let $G = (T, \square)$ be a group of prime order p. Then G is cyclic and elements of T are of the form $a, a^2, \ldots, a^p = e$, for any a in T which is not an identity. Define a mapping $\theta(a^i) = i$ for $1 \le i \le p$. Then θ is an isomorphism from $(T, \square)$ to $(Z_p, \oplus)$. This can be easily checked. Consequently, we can conclude that any group of order p is isomorphic to $(Z_p, \oplus)$. Let $G' = (T', \square')$ be another group of prime order. G' is isomorphic to $(Z_p, \oplus)$ and let θ' be the mapping defining the isomorphism. Define a mapping f from T' to T as follows: $f(x') = x$ if $\theta(x) = i$ and $\theta'(x') = i$, $1 \le i \le p$. It is straightforward to see that f is a bijection and hence G' is isomorphic to G. ◀

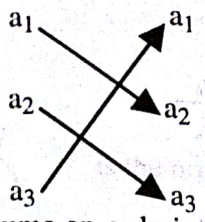
Extra Examples

Permutation Groups Let $S = \{a_1, a_2, a_3\}$ be a set and let p denote a permutation of S. i.e., p is a bijective mapping $p : S \to S$.

Suppose $p(a_1) = a_2$, $p(a_2) = a_3$, $p(a_3) = a_1$. This may be represented as $\begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$ or even as $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. The image of a_1 is a_2 and is written below it in this representation. p can also be represented as

Scanned by CamScanner

$\begin{pmatrix} a_1 & a_3 & a_2 \\ a_2 & a_1 & a_3 \end{pmatrix}$ or as



Generally we assume an ordering $a_1, a_2, \ldots$ among the elements and p is represented as $\begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$ rather than $\begin{pmatrix} a_1 & a_3 & a_2 \\ a_2 & a_1 & a_3 \end{pmatrix}$.

If p_1 and p_2 are permutations, $p_1 \circ p_2$ is a permutation, where $p_1 \circ p_2$ is the composition of functions.

Suppose $p_1 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$, $p_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}$

$$p_1 \circ p_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_3 & a_2 \end{pmatrix}$$

$$p_1 \circ p_2(a_1) = p_1(p_2(a_1)) = p_1(a_3) = a_1$$

$$p_1 \circ p_2(a_2) = p_1(p_2(a_2)) = p_1(a_2) = a_3$$

$$p_1 \circ p_2(a_3) = p_1(p_2(a_3)) = p_1(a_1) = a_2$$

If p_1, p_2, p_3 are permutations we can easily see that the associative property holds. $p_1 \circ (p_2 \circ p_3) = (p_1 \circ p_2) \circ p_3$, $\begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix}$ is the identity permutation.

If $P = \{p_1, p_2, \ldots\}$ is the set of all permutation of elements of a set $S = \{a_1, \ldots, a_n\}$, it is not difficult to see $(P, \circ)$ is a group. The order of this group is $n!$. If $S = \{a_1, a_2\}$ there are only two permutations $p_1 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$, $p_2 = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$ and the group table is

	p_1	p_2
p_1	p_1	p_2
p_1	p_2	p_1

If $S = \{a_1, a_2, a_3\}$, there are 6 permutations

$$p_1 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix} \quad p_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix} \quad p_3 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_3 & a_2 \end{pmatrix} \quad p_5 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} \quad p_6 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \end{pmatrix}$$

Scanned by CamScanner

and the group table is given by

	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_6	p_5	p_4	p_3
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_5	p_1	p_3	p_2
p_5	p_5	p_3	p_4	p_2	p_6	p_1
p_6	p_6	p_4	p_2	p_3	p_1	p_5

This is called a permutation group. A permutation group is a group made up of elements which are permutations of a set. Note that this is not a commutative group. The order of this group is 6. We say that the degree of a permutation group is the cardinality of the set on which the permutations are defined. The degree of the above group is 3. In general, the set S_n of all permutation of n elements is a permutation group $(S_n, \circ)$. This is called the symmetric group. The $(S_n, \circ)$ is of order $n!$ and degree n. Note that $(\{p_1, p_4\}, \circ)$ is a subgroup of $(S_3, \circ)$ and has order 2 but degree 3. The group $(S_4, \circ)$ is of order 24 and degree 4. Consider a set of permutations

$$p_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix} \qquad p_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_3 & a_4 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_4 & a_3 \end{pmatrix} \qquad p_4 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix}$$

They form a subgroup of $(S_4, \circ)$ with the following table.

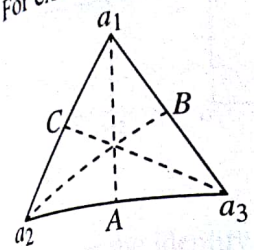
	p_1	p_2	p_3	p_4
p_1	p_1	p_2	p_3	p_4
p_2	p_2	p_1	p_4	p_3
p_3	p_3	p_4	p_1	p_2
p_4	p_4	p_3	p_2	p_1

This permutation group is of order 4 and degree 4. If $p\begin{pmatrix} a_1 & \cdots & a_n \\ a_1' & \cdots & a_n' \end{pmatrix}$ is a permutation, an element is invariant under the permutation if $p(a_i) = a_i$, i.e., $a_i' = a_i$. Sometimes it is of interest to count the number of invariant elements in a permutation. In the example considered above in p_1, the number of invariant elements in 4. In p_2, p_3 it is 2 and in p_4 it is 0.

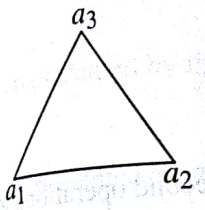
By considering the symmetries of regular polygons we obtain another class of groups. These are called dihedral groups. Let us consider the simplest regular polygon, the equilateral triangle. Let the vertices be named as a_1, a_2, a_3. Now consider all possible rotations and reflections of the triangle which leave the final position of the triangle unchanged from its original position except for the renaming of the vertices.

Scanned by CamScanner

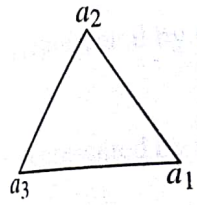
For example



is the original position

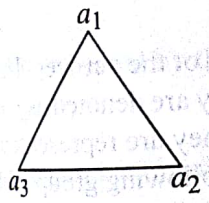


is obtained by rotating anticlockwise through 12°

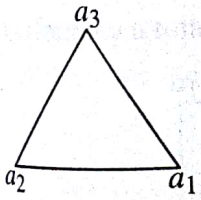


is obtained by rotating anticlockwise through 240°

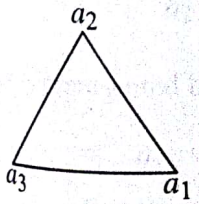
If we rotate through 360° we get the original triangle itself.



is obtained by reflecting about a_1A



is obtained by reflecting about a_2B

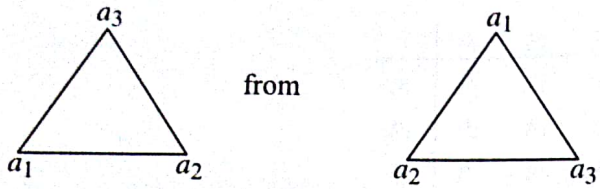


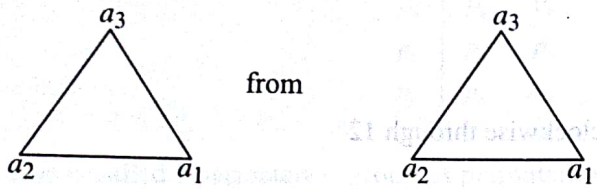
is obtained by reflecting about a_3C

We can easily see that these six variations of the triangle correspond to permutation p_1, p_5, p_6, p_4, p_3, p_2 respectively. This group of rotations and reflections of an equilateral triangle is called a dihedral group $(D_3, \Diamond)$ where the operation $\Diamond$ corresponds to performing one after another one of the two operations rotation and reflection.

Scanned by CamScanner

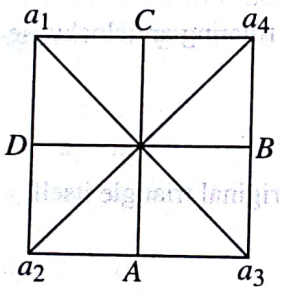
For example, if rotation through 120° is performed and then reflection about the vertical,





The first operation is represented by p_6 and the second by p_2 performing the first and second operations leads to a transformation represented by p_3 and we know $p_2 \cdot p_6 = p_3$.

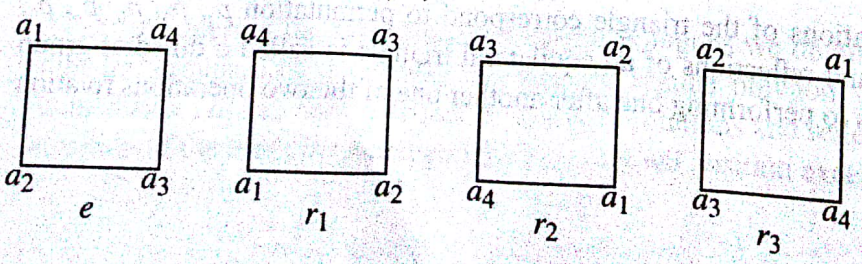
Consider the next size regular polygon which is a square.



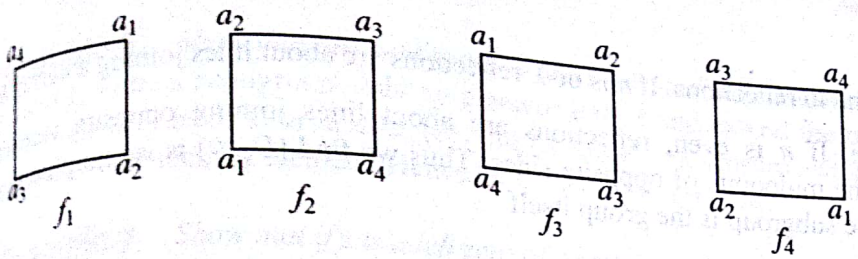
Rotation through 90°, 180°, 270° leave the square in the same position except renaming of the vertices. These are denoted as r_1, r_2, r_3. Reflection about AC and BD leave the square in position and they are denoted as f_1 and f_2 respectively. Reflections about $a_1\ a_3$ and $a_2\ a_4$ also keep the square in position and they are represented as f_3, f_4 respectively. Denoting by e the identity, these operations on the square give the following group table.

$\Diamond$	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
e	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
r_1	r_1	r_2	r_3	e	f_4	f_3	f_1	f_2
r_2	r_2	r_3	e	r_1	f_2	f_1	f_4	f_3
r_3	r_3	e	r_1	r_2	f_3	f_4	f_2	f_1
f_1	f_1	f_3	f_2	f_4	e	r_2	r_1	r_3
f_2	f_2	f_4	f_1	f_3	r_2	e	r_3	r_1
f_3	f_3	f_2	f_4	f_1	r_3	r_1	e	r_2
f_4	f_4	f_1	f_3	f_2	r_1	r_3	r_2	e

This is the dihedral group $(D_4, \Diamond)$



Scanned by CamScanner



e represents the identity permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}$

r_1 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$

r_2 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & . & a_2 \end{pmatrix}$

r_3 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}$

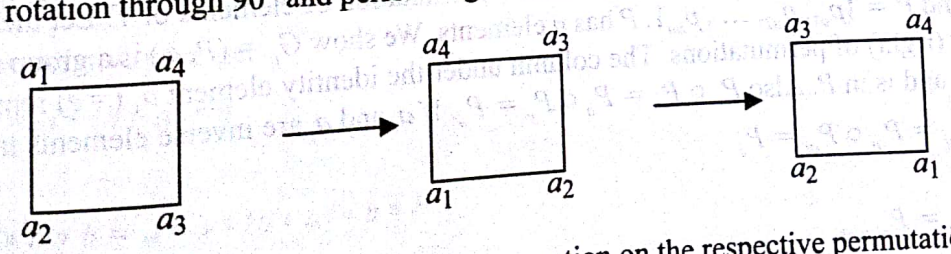
f_1 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$

f_2 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix}$

f_3 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_3 & a_2 \end{pmatrix}$

f_4 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_2 & a_1 & a_4 \end{pmatrix}$

Performing a rotation through 90° and performing reflection about vertical gives



This is represented by $r_1 \Diamond f_1 = f_4$. The corresponding operation on the respective permutation is

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_2 & a_1 & a_4 \end{pmatrix}$$

This dihedral group $(D_4, \Diamond)$ has 8 elements and $(S_4, \circ)$ has 24 elements. The permutations corresponding to the operations of rotation and reflection of a square form a subgroup of $(S_4, \circ)$. In general $(S_n, \circ)$ is of order $n!$ and degree n. $(D_n, \circ)$ is of order $2n$. n of them correspond to rotations through angles 0, $\underbrace{000...0}_{i-1}\ \underset{i}{1}\ \underbrace{000...0}_{2^{r-1}-i}$

Scanned by CamScanner

$360 \times \frac{(n-1)}{n}$. The other n correspond to reflections. If n is odd, reflections are about lines joining a vertex to the midpoint of the opposite side. If n is even, reflections are about lines joining opposite vertices (diagonals) or about lines joining the midpoints of opposite sides. Thus we find $(D_n, \Diamond)$ is isomorphic to a subgroup of $(S_n, \circ)$. When $n = 3$, the subgroup is the group itself.

Extra Examples

Even and Odd Permutations Let the elements be $\{1, \ldots, n\}$. A permutation $\{a_1, \ldots, a_n\}$ of $\{1, 2, \ldots, n\}$ is called even or odd according to the number of pairs (a_i, a_j) where $a_i > a_j$ and $i < j$ is even or odd.

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$ is an odd permutation.

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ is an even permutation.

The set of even permutations form a subgroup of $(S_n, \circ)$ called the alternating subgroup.

Extra Examples

Theorem 7 Every finite group of order n is isomorphic to a permutation group of degree n.

Proof: Let $G = (T, \square)$ be a group of order n, i.e., T consists of n elements and the group table is a $n \times n$ array. Let $T = \{a_1, \ldots, a_n\}$ and let $e = a_1$. Each row and each column in the table is a permutation of elements in T. For each $a \in T$, we denote by p_a the permutation given by the column under a in the table. Thus $p_a(b) = b \square a$ for all $b \in T$. Each column represents a permutation of elements of T. Let them be denoted as $p_{a1}, p_{a2}, \ldots, p_{an}$ and $P = \{p_{a1}, p_{a2}, \ldots, p_{an}\}$. P has n elements. We show $G_p = (P, \circ)$ is a group where $\circ$ denotes the composition (right) of permutations. The column under the identity element a_1 $(=e)$ represents the identity permutation and is in P. Also $P_e \circ P_a = P_a \circ P_e = P_a$. If a_i and a_j are inverse elements in G

$$P_{ai} \circ P_{aj} = P_{aj} \circ P_{ai} = P_e$$

and

$$P_{ai} \circ P_{aj} = P_{ai \square aj}$$

This can be seen as follows

$$\begin{aligned}(P_{ai} \circ P_{aj})(b) &= (b \square ai) \square aj \\ &= b \square (ai \square aj) \\ &= P_{ai \square aj}(b)\end{aligned}$$

Thus we find that $G_p = (P, \circ)$ is a group isomorphic to $G = (T, \square)$ where the isomorphism is defined by the bijective mapping $f: T \to P$ as $f(a) = P_a$ for all $a \in T$.

Scanned by CamScanner

Example 6 *Show that any semigroup S can be extended to a monoid by adjoining an identity element.*

Let $(A, *)$ be a semigroup. Add an element e to A and extend the operation $*$ to $A \cup \{e\}$ by defining $a * e = e * a = a$ for all a in $A \cup \{e\}$. For $(A \cup \{e\}, *)$, closure and associative properties hold and e by definition is the identity element. Hence $(A \cup \{e\}, *)$ is a monoid. ◀

Example 7 *Show that if z is a left zero of a semigroup $(S, *)$, then so are all its left multiples xz $(x \in S)$.*

Let z be a left zero for $(S, *)$

Then $zy = z$ for all y in S

$(xz)y = x(zy)$ (by associativity)

$= xz$ for any y in S

Hence (xz) is also a left zero. ◀

Example 8 a) *Show that if $a^2 = e$ for all a in a group $G = (A, *)$, then G is commutative.*

b) *Show that the same is true in any monoid.*

Let $G = (A, *)$ be a group with e as identity.

For any a in A, $a^2 = e$

$(a * a) * (b * b) = e * e = e$

$(a * b) * (a * b) = e$

Hence, using associativity we get

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

It follows

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

i.e., $e * (a * b) * e = e * (b * a) * e$

Hence $a * b = b * a$. Therefore G is commutative.

For a monoid

$(a * a) * (b * b) = e * e = e$

$(a * b) * (a * b) = e$

Hence, using associativity we get

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

It follows

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

i.e., $e * (a * b) * e = e * (b * a) * e$ ◀

Hence $a * b = b * a$. Therefore the monoid is commutative.

Example 9 *Let $(A, *)$ be a semi group*

Furthermore for every a and b in A

if $a \neq b$, then $a * b \neq b * a$

i.e., if $a * b = b * a$, then $b = a$.

a) *Show that for every a in A,*

$a * a = a$

Scanned by CamScanner

b) *Show that for every a, b in A*

$a * b * a = a$

c) *Show that for every a, b, c in A*

$a * b * c = a * c$

Solution

a) $a * (a * a) = (a * a) * a$

Hence $a = a * a$

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

$= a * b * a$

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

$= a * b * a$

as $a * a = a$ by part a

Hence $a * b * a = a$.

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

$= a * b * c$

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

$= a * b * c$

Hence $a * b * c = a * c$.

Exercises

1. Find the zeros of the semigroups $(P(x), \cap)$ and $(P(X), \cup)$ where X is any given set and $P(X)$ is its power set. Are these monoids? If so, what are the identities?
2. Let the alphabet $V = \{a, b\}$ and A be the set including λ of all sequences on V beginning with a. Show that $(A, \circ, A)$ is a monoid.
3. Let $S = \{a, b\}$. Show that the semigroup $(S^S, \circ)$ is not commutative, where S^S denotes the set of all functions $S \to S$.
4. Let Z_n denote the set of integers $\{0, 1, 2, \ldots, n-1\}$. Let $\odot$ be binary operation on Z_n such that $a \odot b =$ the remainder of ab divided by n
   a) Construct the table for the operation $\odot$ for $n = 7$.
   b) Show that $(Z_n, \odot)$ is a semigroup for any n.
5. Let $(A, *)$ be a semigroup. Let a be an element in A. Consider a binary operation $\square$ on A such that, for every x and y in A,

   $x \square y = x * a * y$

   Show that $\square$ is an associative operation.
6. An element $a \in S$, where $(S, *)$ is a semigroup, is called a left-cancellable element if for all $x, y \in S$, $a * x = a * y \to x = y$. Show that if a and b are left-cancellable, then $a * b$ is also left-cancellable.
7. Let $(A, \square)$ be a semigroup. Show that, for a, b, c in A, if $a \square c = c \square a$ and $b \square c = c \square b$, then $(a \square b) \square c = c \square (a \square b)$.
8. Let $(\{a, b\}, \square)$ be a semigroup where $a \square a = b$. Show that:
   a) $a \square b = b \square a$
   b) $b \square b = b$
9. Let $(A, \square)$ be a commutative semigroup. Show that if $a \square a = a$ and $b \square b = b$, then $(a \square b) \square (a \square b) = a \square b$.
10. Show that every finite semigroup has an idempotent.
11. Show that a semigroup with more than one idempotent cannot be a group. Give an example of a semigroup which is not a group.
12. Show that the set of all the invertible elements of a monoid form a group under the same operation as that of the monoid.
13. In a monoid, show that the set of left-invertibles (right-invertibles) form a submonoid.
14. Let $(A, \square)$ be a semigroup. Furthermore, let there be an element a in A such that for every x in A there exist u and v in A satisfying the relation

    $a \square u = v \square a = x$

    Show that there is an identity element in A.

Scanned by CamScanner

$a^{-1} \square b$ is in H, i.e., $a^{-1} \square b = h$ for some h in H or $b = a \square h$ for some h in H. So a and b are in the same coset of H.

Note that $a = a \square e$ and

$$b = a \square h, e \in H \text{ and so } a \text{ and } b \text{ are in the same coset } a \square H.$$

Thus we find that f corresponds to a partition of T into congruence classes induced by the normal subgroup $(H, \square)$.

Exercises

1. Show that if $g : A \to B$ is a homomorphism of an algebraic system $(A, *)$ onto $(B, \square)$ and $(A_1, *)$ is a subalgebra of $(A, *)$, then the image of A_1 under g is a subalgebra of $(B, \square)$.
2. Show that the intersection of any two congruence relations on a set is also a congruence relation.
3. Show that the composition of two congruence relations on a set is not necessarily a congruence relation.
4. If $f: S \to T$ is a homomorphism from $(S, *)$ to (T, Δ) and $g: T \to P$ is also a homomorphism from (T, Δ) to (P, ∇), then $g \circ f: S \to P$ is a homomorphism from $(S, *)$ to (P, ∇).
5. Let $g : S \to T$ be an isomorphism of semigroups $(S, *)$ and (T, Δ). Show that if z is a zero of S, then $g(z)$ must be a zero of (T, Δ).
6. Show that every monoid $(M, *, e)$ is isomorphic to a submonoid of $(M^M, \circ, \Delta)$ where Δ is the identity mapping of M and M^M is the set of all function from M to M.
7. Let f_1 and f_2 be homomorphisms from an algebraic system $(A, \blacklozenge)$ to another algebraic system $(B, *)$. Let g be a function from A to B such that

   $$g(a) = f_1(a) * f_2(a)$$

   for all a in A. Show that g is a homomorphism from $(A, \blacklozenge)$ to $(B, *)$ if $(B, *)$ is a commutative semigroup.
8. Let f and g be homomorphisms from a group $(G, \blacklozenge)$ to a group $(H, *)$. Show that $(C, \blacklozenge)$ is a subgroup of $(G, \blacklozenge)$, where

   $$C = \{x \in G \mid f(x) = g(x)\}$$
9. Most computers represent numbers with binary sequence of a fixed length. Only a finite set of numbers can be represented exactly, and "arithmetic overflow" occurs when the result of a computation is larger than any of the numbers which can be represented. Consider the following strategies for treating arithmetic overflow. For simplicity, we will treat only the natural numbers and the operation of addition. For each of the following functions f, determine whether f is a homomorphism from $(N, +, 0)$ to the specified algebra $(S, \oplus, 0)$ where S is the set of binary sequences of length k. In each case, the operation $\oplus$ is based on binary addition and is described by means of examples. In the illustrative examples given below, we use $k = 3$.

   a) The k bits represent the least significant digits of the k digit binary representation of each natural number. The operation $\oplus$ is the usual binary addition except that if overflow occurs, the leading digits are lost. Thus, $f(4) = 100$, $f(5) = 101$ and $f(9) = f(4+5) = 100 \oplus 101 = 001 = f(8n+1)$ for all $n \in N$.

   b) If $n < 2^k$, then $f(n)$ is the k digit binary representation of n. If $n \geq 2^k$, then $f(n)$ is represented by the k digit binary representation $2^k - 1$. Thus $f(4) = 100$, $f(5) = 101$ and $f(9) = f(4+5) = 100 \oplus 101 = 111 = f(x)$ for all $x \geq 7$.

   c) One bit is reserved for an indication that overflow has occurred. (We will use 0 for no overflow, 1 for overflow, and use the left most bit as the overflow indicator). For all numbers less than $2^{(k-1)}$, the numbers are represented in their $k - 1$ digit binary representation and the overflow bit is set to 0. If $n \geq 2^{(k-1)}$, then $f(n)$ consists of the digit 1 followed by the $k - 1$ least significant digits of the binary representation of n; e.g., if $k = 3$, then $f(12) = 100$. Thus $f(3) = 011$, $f(2) = 010$, and $f(3+2) = 011 \oplus 010 = 101 = f(4n+1)$ for all $n \in N$.

11.5 RINGS, INTEGRAL DOMAINS AND FIELDS

Semigroups, monoids and groups are algebraic systems with one binary operation. We now consider algebraic systems with two binary operations. Consider the set $S = \{a, b\}$ and two binary operations $\square$ and $*$ on S given by the following tables

Scanned by CamScanner

$\square$	a	b
a	a	b
b	b	a

$*$	a	b
a	a	a
b	a	b

$(S, \square)$ is a group and $(S, *)$ is a semigroup. Also for any α, β, γ in S,

$$\alpha * (\beta \square \gamma) = (\alpha * \beta) \square (\alpha * \gamma)$$
$$\text{and } (\beta \square \gamma) * \alpha = (\beta * \alpha) \square (\gamma * a)$$

In this case we say the operation $*$ is distributive the operation $\square$. In the above example note that

$$b \square (a * b) = b \square a = b$$
$$\text{and } (b \square a) * (b \square b) = b * a = a$$

Hence $\square$ is not distributive over $*$. Now we consider the definitions of rings, integral domains and fields.

For convenience we denote the two binary operation as $+$ and $\cdot$ respectively.

Definition 1 An algebraic system $(S, +, \cdot)$ is called a ring if the following conditions are satisfied

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

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

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

Let $\odot$ denote mod n multiplication

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

We have earlier seen that $(Z_n, \oplus)$ is an abelian group with 0 as identity and $n-i$ is the inverse of i. To see that $(Z_n, \odot)$ is a semigroup. We have to show that

1. Z_n is closed under.
2. $\odot$ is an associative operation.

It is easy to see that Z_n is closed under $\odot$. To see that $\odot$ is an associative operation, consider $a, b, c \in Z_n$.

$a \odot b =$ remainder when ab is divided by n

i.e., $ab = kn + \alpha$ where $a \odot b = \alpha$

$(a \odot b) \odot c = \alpha \odot c$

$=$ remainder when αc is divided by n

i.e., $\alpha c = \ell n + \beta \qquad \alpha \odot c = \beta \quad 0 \leq \beta < n$

$abc = (kn + \alpha)c = knc + \alpha c = knc + \ell n + \beta = n(kc + \ell) + \beta$

$\beta =$ remainder when abc is divided by n

$bc = k'n + \gamma$ where $b \odot c = \gamma$

Scanned by CamScanner

Let $a\gamma = \ell' n + \delta$ so that $a \odot (b \odot c) = \delta$ $0 \leq \delta < n$

$$\begin{aligned} abc &= a(k'n + \gamma) \\ &= ak'n + a\gamma \\ &= ak'n + \ell' n + \delta \\ &= n(ak' + \ell') + \delta \end{aligned}$$

Hence we note $\beta = \delta$

i.e., $(a \odot b) \odot c = a \odot (b \odot c)$

Hence $(Z_n, \odot)$ is a semigroup.

Let us now show that $\odot$ distributes over $\oplus$. This can also be checked easily.

i.e., $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, $0 \leq a, b, c < n$

L.H.S.: $b \oplus c = b + c$

or $b + c - n$

$a \odot (b \oplus c) = a(b + c) \bmod n$

or $a(b + c - n) \bmod n$

$= a(b + c) \bmod n$

$= (ab + ac) \bmod n$

$= ab \bmod n + ac \bmod n$

or $(ab \bmod n + ac \bmod n) - n$

R.H.S.: $a \odot b = ab \bmod n = r$ (say)

$a \odot c = ac \bmod n = s$ (say)

rhs $= (r + s) \bmod n$

$= r + s$

or $r + s - n$

$= (ab \bmod n + ac \bmod n)$

or $(ab \bmod n + ac \bmod n) - n$

◀

Hence lhs = rhs.

We shall hereafter call in this section the two operations + and · as addition and multiplication respectively. We shall refer to $a + b$ as the sum and $a \cdot b$ as the product of a and b. The identity of the group $(S, +)$ will be called the additive identity and denoted by 0. The inverse of an element a in this group will be called additive inverse and denoted by $-a$. $a - b$ denotes the sum of a and the additive inverse of b.

It should be noted that for any element a in a ring $(S, +, \cdot)$, $0 \cdot a = a.\ 0 = 0$.

This follows from the fact that

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

Hence $0 \cdot a = 0$. Similarly it can be seen that $a \cdot 0 = 0$.

Definition 2 Let $(S, +, \cdot)$ be an algebraic system with two binary operations. $<S, +, \cdot>$ is called an integral domain if

1. $(S, +)$ is an abelian group
2. The operation · is commutative. Furthermore, if $c \neq 0$ and $c \cdot a = c.\ b$, then $a = b$, where 0 is the additive identity.
3. The operation · is distributive over the operation +.

Scanned by CamScanner

Example 2 *Consider the set of integers I with the operation of addition and multiplication. (I, +) is a group. 0 is the identity of this group. −a is the inverse of a for any integer a. Property 2 is also satisfied if $c \cdot a = c \cdot b$ and $c \neq 0$, dividing by c we get $a = b$. Multiplication of integers is distributive over addition of integers. Hence it follows that (I, +, ·) is an integral domain.* ◀

Definition 3 Let $(S, +, \cdot)$ be an algebraic system with two binary operations. $<S, +, \cdot>$ is called a field if:

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

Example 3 *(Q, +, ·) and (R, +, ·) are fields where Q is the set of rational numbers and R is the set of real numbers. + and · are ordinary addition and multiplication respectively. 0 is the additive identity and 1 is the identity for multiplication. The properties can be easily checked. (C, +, ·) is a field where C is the set of complex numbers, + and · are addition and multiplication of complex numbers respectively. All the conditions can be checked. Here again 0 is the additive identity and 1 the identity for multiplication.*

Example 4 *The algebraic system $(Z_n, \oplus, \odot)$ is a field if and only if n is a prime. It is clear that both $\oplus$ and $\odot$ are commutative operations. We have seen that $(Z_n, \oplus)$ is a group for any n. We shall now show that $(Z_n - \{0\}, \odot)$ is a group if and only if n is a prime. If n is not a prime, $n = ab$ for some a, b in $Z_n - \{0\}$, i.e., $a \odot b = 0$. Since $\odot$ is not closed on the set $Z_n - \{0\}$, $(Z_n - \{0\}, \odot)$ cannot be a group. Consider the case when n is a prime. For any a and b in $Z_n - \{0\}$, $a \odot b$ is not equal to 0 and has a value in $Z_n - \{0\}$. So $Z_n - \{0\}$ is closed under $\odot$. It is straightforward to see $\odot$ is an associative operation and 1 is the identity for the operation. In a group table we have seen that no two elements of a row are equal and no two elements of a column are equal. In $(Z_n, \oplus, \odot)$ we can show that for distinct b and c in $Z_n - \{0\}$. $a \odot b \neq a \odot c$ and $b \odot a \neq c \odot a$.*

This is seen as follows:

Suppose $a \odot b = a \odot c$

$$ab = k_1 n + r$$
$$ac = k_2 n + r \qquad \text{for some } k_1, k_2, r$$

with $1 \leq r < n$. Assume $b > c$ and hence $k_1 > k_2$

$$ab - ac < (k_1 - k_2)\, n \tag{1}$$

Since both a and $b - c$ are less than n, (1) is impossible when n is a prime.

Thus it we have a group table with column heading $1, \ldots, n - 1$ and row headings $1, \ldots, n - 1$ for the operation $\odot$. Since all elements of a row are different, 1 occurs in each row and so for every a in $Z_n - \{0\}$ there is an element b in $Z_n - \{0\}$, such that $a \odot b = 1$. b is the inverse of a. Hence $(Z_n - \{0\}, \odot)$ is an abelian group. We have already seen $\odot$ is distributive over $\oplus$. So $(Z_n, \oplus, \odot)$ is a field when n is a prime. This is called as the field of integer modulo n.

Extra Examples

Scanned by CamScanner

Ring Homomorphisms and Ideals We have seen the definition of rings and fields in the previous section. Rings are of many types. Many rings are commutative in the sense that $a \cdot b = b \cdot a$. For all a in S where $(S, +, \cdot)$ is the ring, there exist noncommutative rings as well. Let $R = (S, +, \cdot)$ be a ring. Let $M_2(R)$ be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in S$. These two by two matrices under the operation of matrix addition and matrix multiplication form a noncommutative ring. This can be checked in a straightforward manner.

We also note that the additive identity 0 of any ring also serves as the 'zero' for multiplication. It should be noted that if $a, b \in S$ where $(S, +, \cdot)$ is a ring $(-a)$ and $(-b)$ are the additive inverses of a and b respectively, then $(-a)(-b) = ab$. This can be seen as follows

$$a + (-a) = 0$$

$$0 = 0 \cdot (-b) = (a + (-a)) \cdot (-b)$$
$$= a(-b) + (-a)(-b)$$

On the other hand

$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

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

Cancelling $a(-b)$ on both sides,

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

Definition 4 Let $\mathcal{R} = (A, +, \cdot)$ be a ring and $\mathcal{S} = (A', +, \cdot)$ be an algebraic system with $A' \leqslant A$. $\mathcal{S}$ is a subring of $\mathcal{R}$ if $\mathcal{S}$ is a ring by itself under $+$ and $\cdot$.

Definition 5 A homomorphism of a ring $(A, +, \cdot)$ to $(B, +', \cdot')$ is a surjective function $\theta : A \to B$ such that for any x and y in A

$$\theta(x + y) = \theta(x) +' \theta(y)$$
$$\theta(x \cdot y) = \theta(x) \cdot' \theta(y)$$

$(B, +', \cdot')$ is called the homomorphic image of $(A, +, \cdot)$.

Example 5 *Let us consider $\mathcal{R} = (I, +, \cdot)$ where I is the set of integers and $+$ and $\cdot$ are ordinary addition and multiplication. Consider the following ring $\mathcal{S}$ over {even, odd} and two operations $+'$ and $\cdot'$ defined by the following table*

$+'$	even	odd
even	even	odd
odd	odd	even

$\cdot'$	even	odd
even	even	even
odd	even	odd

$\mathcal{R}$ and $\mathcal{S}$ are rings.

Consider the mapping

$$\theta(n) = \begin{cases} \text{even} & \text{if } n \text{ is even} \\ \text{odd} & \text{if } n \text{ is odd.} \end{cases}$$

Scanned by CamScanner

Then $\theta(x + y) = \theta(x) +' \theta(y)$
$\theta(x \cdot y) = \theta(x) \cdot \theta(y)$

Hence θ is a homomorphism from R to S.

We can also look at homomorphism in another way. Let R be a congruence relation on A with respect to both the operations + and ·. That is, R is an equivalence relation on A and if a_1Ra_2 and b_1Rb_2, then $(a_1 + b_1)R(a_2 + b_2)$ and $(a_1 \cdot b_1)R(a_2 \cdot b_2)$. Let $B = \{c_1, \ldots, c_r\}$ be the set of congruence classes into which A is divided. We can define two binary operations $+'$ and $\cdot'$ on B such that $c_i +' c_j$ is equal to the congruence class to which $a_1 + a_2$ belongs to where $a_1 \in c_i$ and $a_2 \in c_j$. $c_i \cdot' c_j$ is equal to the congruence class to which $a_1 \cdot a_2$ belongs. It can be easily checked that $(B, +', \cdot')$ is a homomorphic image of $(A, +, \cdot)$.

We have seen earlier that exhausing all the normal subgroups of a group, we get all homomorphic images of that group. Now we explore the possibility of a similar result for rings.

Let $(A, +, \cdot)$ be a ring and $(H, +)$ be a subgroup of $(A, +)$. Let R denote the equivalence relation that H induces on A. Because of the commutative property of $(A, +)$, R is a congruence relation on A with respect to +. We want to find out under what condition R is also a congruence relation with respect to ·. Suppose aRb and cRd,

$$a = b + h_1$$
and $c = d + h_2$

for some h_1 and h_2 in H, because all left cosets of H exhaust A. It follows that

$$\begin{aligned} a \cdot c &= (b + h_1) \cdot (d + h_2) \\ &= (b \cdot d) + (b \cdot h_2) + (h_1 \cdot d) + (h_1 \cdot h_2) \end{aligned}$$

We note that if both $b \cdot h_2$ and $h_1 \cdot d$ are in H, then

$(b \cdot h_2) + (h_1 \cdot d) + (h_1 \cdot h_2)$ is also in H and we shall have $(a \cdot c)R(b \cdot d)$.

This observation motivates the definition of an ideal in a ring (somewhat similar concept like normal subgroups). Let $(A, +, \cdot)$ be a ring and H be a subset of A. H is said to be an ideal if the following two conditions are satisfied.

1. $(H, +)$ is a subgroup of $(A, +)$.
2. For any a in A and h in H, $a \cdot h$ and $h \cdot a$ are both in H. We can say that an element a is swallowed or absorbed into the ideal when multiplied by an element of the ideal.

From the discussion we had, it follows immediately that an ideal H of a ring $(A, +, \cdot)$ induces a congruence relation on A with respect to the operation + and ·.

On the other hand, can we say, every homomorphism corresponds to an ideal of the ring? Let f be a homomorphism from a ring $(A, +, \cdot)$ to $(B, +', \cdot')$. Let H be the set of elements of A that are mapped into additive identity of $(B, +', \cdot')$ under f. We see that $(H, +)$ is a normal subgroup of $(A, +)$. To show that $(H, +', \cdot')$ is an ideal. We note that for any a in A and h in H.

$$f(a \cdot h) = f(a) \cdot' f(h) = f(a) \cdot' 0 = 0$$

where 0 is the additive identity of $(B, +', \cdot')$. Thus $a.\ h$ is in H. In a similar manner we can show that $h \cdot a$ is in H. Hence H is an ideal.

Example 6 *Consider the ring over the set $\{0, 1, \ldots, 7\}$ with $\oplus$ mod 8 addition $\odot$ mod 8 multiplication. The tables for the operations are given below.*

Scanned by CamScanner

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\odot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

For this ring $\{0, 2, 4, 6\}$ is an ideal as $(\{0, 2, 4, 6\}, \oplus)$ is a normal subgroup of $(Z_8, \oplus)$. For any h in $\{0, 2, 4, 6\}$ and a in $\{0, 1, 2, 3, 4, 5, 6, 7\}$, $a \cdot h$ and $h \cdot a$ are in $\{0, 2, 4, 6\}$. The two congruence classes are $\{0, 2, 4, 6\}$ and $\{1, 3, 5, 7\}$ and if we denote them as J_1 and J_2 the homomorphic image is shown in the figure.

$+'$	J_1	J_2
J_1	J_1	J_2
J_2	J_2	J_1

$\cdot'$	J_1	J_2
J_1	J_1	J_1
J_2	J_1	J_2

$(\{0, 4\}, \oplus)$ is a subgroup of $(Z_8, \oplus)$. This is also an ideal as for any $h \in \{0, 4\}$ and $a \in \{0, \ldots, 7\}$, $a \cdot h$ and $h \cdot a$ are in $\{0, 4\}$. The corresponding congruence classes are $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$ and $\{3, 7\}$. Denoting them as C_1, C_2, C_3, C_4 respectively the homomorphic image is given below

$+'$	C_1	C_2	C_3	C_4
C_1	C_1	C_2	C_3	C_4
C_2	C_2	C_3	C_4	C_1
C_3	C_3	C_4	C_1	C_2
C_4	C_4	C_1	C_2	C_3

$\cdot'$	C_1	C_2	C_3	C_4
C_1	C_1	C_1	C_1	C_1
C_2	C_1	C_2	C_3	C_4
C_3	C_1	C_3	C_1	C_3
C_4	C_1	C_4	C_3	C_2

Exercises

1. Let $(T, *)$ be a subsemigroup of $(S, *)$. T is called a left ideal of S if $S * T \subseteq T$. Similarly define a right ideal. If T is both a left and right ideal, then it is called an ideal. Show that in $(I, \cdot)$, where I is the set of integers under multiplication $\cdot$, the set of multiples of an integer n is an ideal.
2. Let $(A, \blacklozenge)$ and $(B, *)$ be two algebraic systems and f be a homomorphism from $(A, \blacklozenge)$ to $(B, *)$.
   a) Show that, if $\blacklozenge$ is an associative operation, so is $*$.
   b) Show that, if e is an identity element in $(A, \blacklozenge)$, then $f(e)$ is an identity element n $(B, *)$.
   c) Show that, if b is an inverse of a in $(A, \blacklozenge)$, then $f(b)$ is an inverse of $f(a)$ in $(B, *)$.
   d) Show that a homomorphic image of a ring is a ring.
3. Let $(A, \blacklozenge, *)$ be an algebraic system, where
$$a \blacklozenge b = a$$
for all a, b in A and $*$ is an arbitrary binary operation. Show that $*$ distributes over $\blacklozenge$.
4. Let $(A, \blacklozenge, *)$ be an algebraic system with e_1 and e_2 being the identity elements with respect to the operations $\blacklozenge$ and $*$, respectively. Given that the operations $\blacklozenge$ and $*$ distribute over each other show that $x \blacklozenge x = x$ and $x * x = x$ for all x in A.
5. Let $(A, +, \cdot)$ be a ring such that $a \cdot a = a$ for all a in A.

Scanned by CamScanner