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.

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

$a + 0 = a$ for all a 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

$a \odot b = ab$ mod 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 $(S, \oplus, \odot, 0, 1)$. ◀

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) $x \cdot y = y \cdot x$

(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 $0 \in T$ is a zero for the operation $\square$, if for every $x \in T$,

$$0 \square x = x \square 0 = 0.$$

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.* ◀

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 0_ℓ 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.

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.

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.*

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.

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	$\ldots$	a_n
a_1	c_{11}	$\ldots$	c_{1n}
$\ldots$		$\ldots$	
a_n	c_{n1}	$\ldots$	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

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, ... 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.

If r and s are negative integers,

$$r = -m \qquad s = -n, \qquad m, n > 0$$
$$a^r \square a^s = a^{-m} \square a^{-n} = (a^{-1})^m \square (a^{-1})^n$$
$$= (a^{-1})^{m+n} = a^{-(m+n)}$$
$$= a^{(-m)+(-n)} = a^{r+s}.$$
$$(a^r)^s = (a^{-m})^{-n} = ((a^m)^{-1})^{-n}$$
$$= (((a^m)^{-1})^{-1})^n$$
$$= (a^m)^n = a^{mn}$$
$$= a^{(-m)(-n)} = a^{rs}.$$

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

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

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.

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.

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

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.*

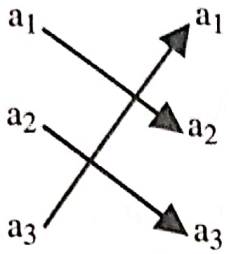
We saw that for any integer n, $(Z_n, \oplus)$ is a group. Any group of order p is isomorphic to $(Z_p, \oplus)$. This can be seen as follows.

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 $1 \leq i \leq p$. 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 $\theta'(x') = i$, $1 \leq i \leq p$. It is straightforward to see that f is a bijection and hence G' is isomorphic to G. ◀

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

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

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

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

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

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

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

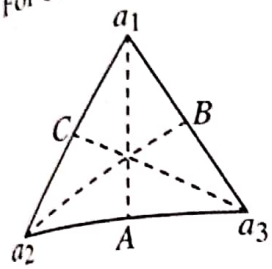
They form a subgroup of $(S_4, \circ)$ with the following table.

	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

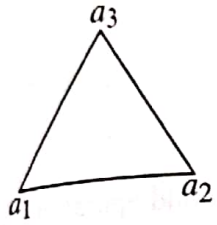
This permutation group is of order 4 and degree 4. If $p\begin{pmatrix} a_1 & \cdots & a_n \\ a_1' & \cdots & a_n' \end{pmatrix}$ is a permutation, an element is invariant under the permutation if $p(a_i) = a_i$, i.e., $a_i' = a_i$. Sometimes it is of interest to count the number of invariant elements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

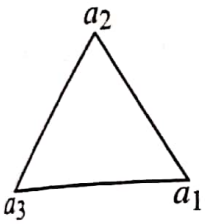
For example



is the original position

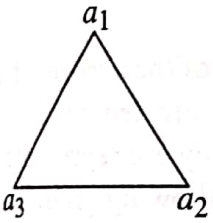


is obtained by rotating anticlockwise through 12°

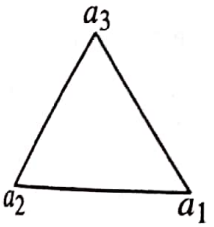


is obtained by rotating anticlockwise through 240°

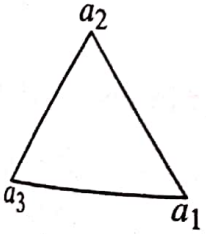
If we rotate through 360° we get the original triangle itself.



is obtained by reflecting about a_1A



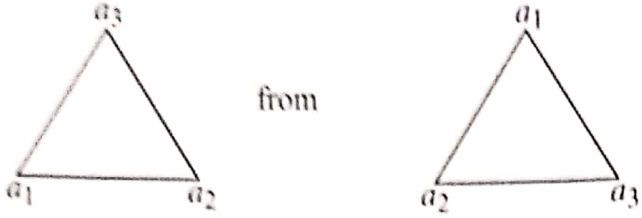
is obtained by reflecting about a_2B

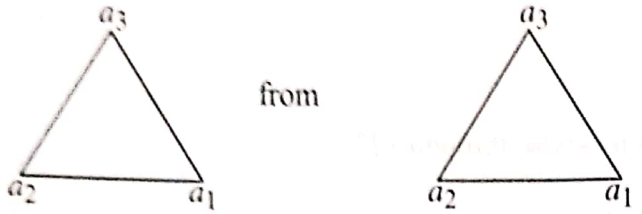


is obtained by reflecting about a_3C

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.

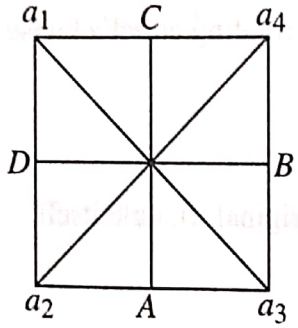
For example, if rotation through 120° is performed and then reflection about the vertical,





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 $p_2 \cdot p_6 = p_3$.

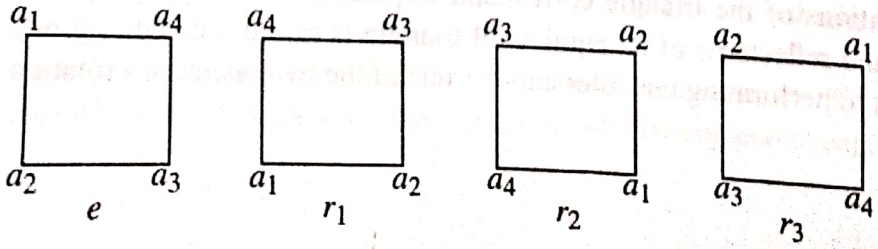
Consider the next size regular polygon which is a square.

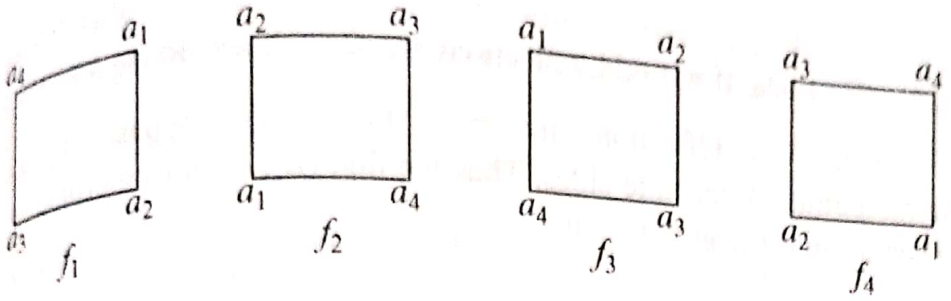


Rotation through 90°, 180°, 270° leave the square in the same position except renaming of the vertices. These are denoted as r_1, r_2, r_3. Reflection about AC and BD leave the square in position and they are denoted as f_1 and f_2 respectively. Reflections about $a_1\ a_3$ and $a_2\ a_4$ also keep the 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 $(D_4, \Diamond)$





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

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

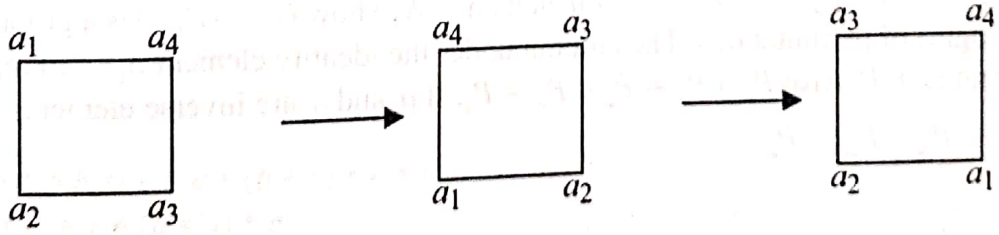
f_1 is represented by the permutation $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$

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 $r_1 \lozenge f_1 = f_4$. 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 $(D_4, \lozenge)$ 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 $0, \underbrace{000\ldots0}_{i-1}\ \underset{i}{1}\ \underbrace{000\ldots0}_{2^{r-1}-i}$

$360 \times \frac{(n-1)}{n}$ 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 $a \in T$.

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,*

$$a * a = a$$

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.

15. For $P = \{p_1, p_2, \ldots, p_5\}$ and $Q = \{q_1, q_2, \ldots, q_5\}$ explain why $(P, *)$ and $(Q, \square)$ are not groups. The operations $*$ and $\square$ are given in the following table:

$*$	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_3	p_4	p_5
p_2	p_2	p_1	p_4	p_2	p_3
p_3	p_3	p_5	p_1	p_2	p_4
p_4	p_4	p_3	p_5	p_1	p_2
p_5	p_5	p_4	p_2	p_3	p_4

$\square$	q_1	q_2	q_3	q_4	q_5
q_1	q_1	q_4	q_1	q_5	q_3	q_2
q_2	q_2	q_3	q_5	q_2	q_1	q_4
q_3	q_3	q_1	q_2	q_3	q_4	q_5
q_4	q_4	q_2	q_4	q_1	q_5	q_3
q_5	q_5	q_5	q_3	q_4	q_2	q_1

16. Consider a computer which uses words of k bits to represent nonnegative integers in binary notation. The only operation is addition. When overflow occurs, the high order bits are lost.
   a) What algebraic variety would be most appropriate to model addition in the machine? How big is the carrier?
   b) Suppose overflow causes the result to be set to the largest representable number. What algebraic variety would best model addition in this case?

17. a) Show that every group containing exactly two elements is isomorphic to $(Z_2, \oplus)$.
   b) Show that every group containing exactly three elements is isomorphic to $(Z_3, \oplus)$.
   c) How many nonisomorphic groups that contain exactly four elements are there?
   d) What can you say about a group with 5 elements?

18. Let $(A, \blacklozenge)$ and $(B, *)$ be two algebraic systems. The Cartesian product of $(A, \blacklozenge)$ and $(B, *)$ is an algebraic system $(A \times B, \square)$, where $\square$ is a binary operation such that for any (a_1, b_1) and (a_2, b_2) in $A \times B$

$$(a_1, b_1) \square (a_2, b_2) = (a_1 \blacklozenge a_2, b_1 * b_2)$$

Show that the Cartesian product of two groups is a group.

19. Let $(A, \cdot)$ be a group.
   a) Show that $(ab)^{-1} = b^{-1}a^{-1}$.
   b) Show that $(a_1a_2 \ldots a_{r-1}a_r)^{-1} = a_r^{-1}a_{r-1}^{-1} \ldots a_2^{-1}a_1^{-1}$
   c) Show that $(a^ib^j)^{-1} = b^{-j}a^{-i}$. [$b^{-j}$ denotes $(b^{-1})^j$ and a^{-i} denotes $(a^{-1})^i$.]

20. Let $(A, *)$ be a monoid such that for every x in A, $x * x = e$, where e is the identity element. Show that $(A, *)$ is an abelian group.

21. Let $(G, \blacklozenge)$ be a group and H be a nonempty subset of G. Show that $(H, \blacklozenge)$ is a subgroup if for any a and b in H, $a \blacklozenge b^{-1}$ is also in H.

22. Show that any subgroup of a cyclic group is cyclic.

23. Let $(H, \cdot)$ be a subgroup of a group $(G, \cdot)$. Let $N = \{x \mid x \in G, xHx^{-1} = H\}$. Show that $(N, \cdot)$ is a subgroup of $(G, \cdot)$.

24. Let $(H, \cdot)$ and $(K, \cdot)$ be subgroups of a group $(G, \cdot)$. Let $HK = \{h \cdot k \mid h \in H, k \in K\}$
   Show that $(HK, \cdot)$ is a subgroup of $(G, \cdot)$ if and only if $HK = KH$.

25. **a)** Let $(A, \blacklozenge)$ be a group. Show that $(A, \blacklozenge)$ is an abelian group if and only if $a^2 \blacklozenge b^2 = (a \blacklozenge b)^2$ for all a and b in A.
   b) For all $a, b \in A$, show that $(a \blacklozenge b)^n = a^n \blacklozenge b^n$.

26. Let $(A, \blacklozenge)$ be a group. Show that $(A, \blacklozenge)$ is an abelian group if $a^3 \blacklozenge b^3 = (a \blacklozenge b)^3$, $a^4 \blacklozenge b^4 = (a \blacklozenge b)^4$, and $a^5 \blacklozenge b^5 = (a \blacklozenge b)^5$, for all a and b in A.

27. Let $(G, \blacklozenge)$ be a group of even order. Let $(H, \blacklozenge)$ be a subgroup of $(G, \blacklozenge)$ where $|H| = |G|/2$. Show that $(H, \blacklozenge)$ is a normal subgroup.

28. Let $(H, \blacklozenge)$ be a subgroup of a group $(G, \blacklozenge)$. Show that $(H, \blacklozenge)$ is a normal subgroup if and only if $a \blacklozenge H \blacklozenge a^{-1} \subseteq H$ for every $a \in G$.

29. Let $(G, \blacklozenge)$ be a group. Let $H = \{a \mid a \in G \text{ and } a \blacklozenge b = b \blacklozenge a \text{ for all } b \in G\}$. Show that H is a normal subgroup.

30. **a)** Let $(H, \blacklozenge)$ and $(K, \blacklozenge)$ be subgroups of a group $(G, \blacklozenge)$. Show that $(H \cap K, \blacklozenge)$ is also a subgroup.
   b) Show that, if $(H, \blacklozenge)$ and $(K, \blacklozenge)$ are normal subgroups, then $(H \cap K, \blacklozenge)$ is also a normal subgroup.

31. Show that if every element in a group is its own inverse, then the group must be abelian.

32. Show that the set of all polynomials in x under the operation of addition is a group.

33. Show that the groups $(G, *)$ and (S, Δ) given by the following table are isomorphic.

$*$	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

Δ	q_1	q_2	q_3	q_4
q_1	q_3	q_4	q_1	q_2
q_2	q_4	q_3	q_2	q_1
q_3	q_1	q_2	q_3	q_4
q_4	q_2	q_1	q_4	q_3

34. Find the left cosets of $\{p_1, p_5, p_6\}$ in the group $(S, \Diamond)$ given in the following table

$\Diamond$	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_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

35. Show that if a group $(G, *)$ is of order n and $a \in G$ is such that $a^m = e$ for some integer $m \leq n$, then m must divide n.

36. Show that if a group $(G, *)$ is of even order, then there must be an element $a \in G$ such that $a \neq e$ and $a * a = e$.

37. If an abelian group has subgroups of orders m and n, then show that it has a subgroup whose order is the least common multiple of m and n.

38. Show that among the cosets determined by a subgroup S in a group $(G, *)$, only one of the cosets is a subgroup.

39. Let $P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$,

$P_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$, $P_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

Find $P_1 \circ P_2$, $P_2 \circ P_1$, $P_1 \circ P_1$, $P_1 \circ P_2 \circ P_3$.
Solve the equation $P_1 \circ x = P_2$.

40. Show that the set of permutations

$$\left\{\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}\right\}$$

Form a group. Draw the group table.

41. Show that (s_4, o) is generated by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

11.4 HOMOMORPHISMS, NORMAL SUBGROUPS AND CONGRUENCE RELATIONS

In the case of isomorphism, two algebraic systems are structurally similar and also have the same order if they are finite. Two algebras may be very similar, but they may not be of the same order even though their orders are finite. In order to study such structures we consider homomorphism, i.e., the function f defined in the case of homomorphism, need not be bijective, but other conditions will be satisfied.

The following figure explains the concept of homomorphism

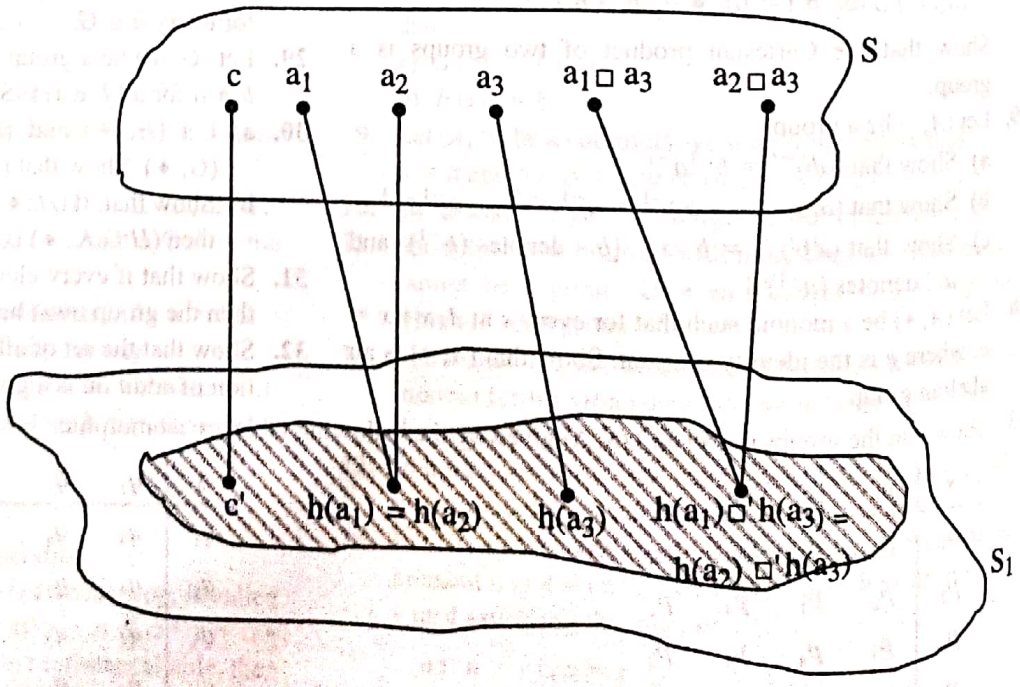


Figure 1 *Representation of a homomorphism*

Definition 1 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

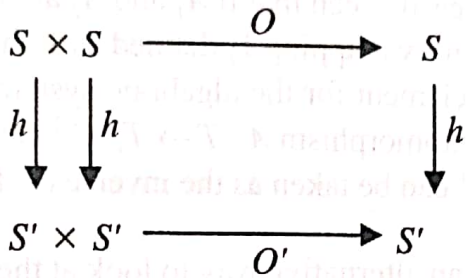
$h : S \to S'$

$h(a \square b) = h(a) \square' h(b)$

where $\square$ and $\square'$ are corresponding operations in A and A' respectively.

$h(c) = c'$, c and c' being corresponding constants.

Alternatively we can characterize a homomorphism from $A = (S, O, C)$ to $A' = (S', O', C')$ as a map h such that $h(c) = c'$ where c and c' are corresponding constants for the algebras and we have the following commuting diagram.



It should be noted that isomorphism is a particular case of homomorphism.

Example 1 *$f_k : I \to I$ where $f_k(x) = kx$ for an integer k is a homomorphism from* $(I, +, 0)$ to $(I, +, 0)$. ◀

Example 2 *Let Σ be a finite non empty alphabet, and let $|x|$ denote the length of a string $x \in \Sigma^*$. Then the function h defined by $h : \Sigma^* \to N$.*

$h(x) = |x|$ is a homomorphism from $(\Sigma^*$, concatenation, $\lambda)$ to $(N, +, 0)$.

Question: Under what conditions, the above-mentioned homomorphism is an isomorphism? ◀

Theorem 1 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 the homomorphic image of A under h.

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

1. $h(S) \subset S'$.
   This follows from the fact that $h : S \to S'$.
2. The constant k' is an element of $h(S)$. By definition of homomorphism $h(k) = k'$ and since $k \in S$, it follows that
   $k' = h(k) \in h(S)$.
3. The set $h(S)$ is closed under the operations O', i.e., if $a, b \in h(S)$, then $a \circ' b \in h(S)$. Suppose $a, b \in h(S)$. Then there exist elements x, y in S such that $h(x) = a$ and $h(y) = b$
   $h(x \circ y) = a \circ' b \in h(S)$

The homomorphic image of an algebra is of the same variety as A. If A is a semigroup, homomorphic image of A is a semigroup. If A is a monoid, homomorphic image of A is a monoid. If A is a group, homomorphic image of A is a group. This can be proved by verifying the conditions that have to be satisfied by that algebra.

A homomorphism is called a epimorphism if it is surjective and a monomorphism if it is injective. A homomorphism where the codomain and domain are the same is called an endomorphism. An isomorphism (homomorphism which is bijective) of an algebraic system with itself is called an automorphism.

Theorem 2 Let $S = (T, \square)$ be a semigroup. The automorphisms of S form a group called the automorphism group of S.

Proof: Let A be the set of automorphisms of S. Let $A_1, A_2 \in A$. The composition of A_1 and A_2 is defined as $A_1 * A_2 : A_1 * A_2 (x) = A_1 (A_2(x))$. It can be easily seen that if A_1 and A_2 are bijective $A_1 * A_2$ is bijective and hence $A_1 * A_2$ is an automorphism of S. The identity mapping 1_T defined as $1_T(x) = x$ for all $x \in T$ is an automorphism which can be considered as an identity element for the algebraic system $G = (A, *)$. The associative property of A under $*$ is also obvious. If A is an automorphism $A : T \to T$, A^{-1} can be defined as $A^{-1}(y) = x$ if $A(x) = y$. $A^{-1} : T \to T$ is hence a bijection and A^{-1} can be taken as the inverse of A. Hence $G = (A, *)$ forms a group.

Congruence Relations There is an alternative way to look at the notion of a homomorphism from one algebraic system to another. This is in terms of congruence relations.

A congruence relation is an equivalence relation defined on the carrier of an algebra such that the equivalence classes of the relation are "preserved" by the operations of the algebra. Recall that an equivalence relation is a relation which is reflexive, symmetric and transitive. An equivalence relation which is both right invariant and left invariant under the operations of the algebra is called a congruence relation.

Let us look at the example where ordered pairs of integers are associated with rational numbers. We define a fraction as an ordered pair of integers $< p, q >$ (written $\frac{p}{q}$) where $q \neq 0$, and let F be the set of all fractions. The binary operation of $+$, $-$ and $\cdot$ and unary $-$ can be defined on F. Using the corresponding operations on integers as follows

$$\left(\frac{p}{q}\right) + \left(\frac{r}{s}\right) = \frac{(ps + rq)}{(qs)}$$

$$\left(\frac{p}{q}\right) - \left(\frac{r}{s}\right) = \frac{(ps - rq)}{(qs)}$$

$$\left(\frac{p}{q}\right) \cdot \left(\frac{r}{s}\right) = \frac{(pr)}{(qs)}$$

$$-\left(\frac{p}{q}\right) = \frac{(-p)}{q}$$

When we consider fractions as pairs of integers $\frac{1}{2}$ and $\frac{2}{4}$ are not equal. They represent different pairs $<1, 2>$ and $<2, 4>$. However we would like to treat them as equal. This is done by establishing an equivalence relation $\sim$ over F as follows:

$$\frac{p}{q} \sim \frac{r}{s} \text{ iff } ps = rq.$$

Each equivalence class of F corresponds to a rational number. Thus we find $\frac{1}{3}, \frac{2}{6}, \frac{3}{9}, \frac{-1}{-3}, \frac{-3}{-9}$ all belong to one equivalence class.

If a and b are fractions in the same equivalence class $a + c$ and $b + c$ are in the same equivalence class for a fraction c. This can be seen as follows:

Suppose

$$a = \frac{p}{q} \quad b = \frac{r}{s} \quad c = \frac{t}{u}$$

$$a \sim b \quad \text{or} \quad ps = qr$$

$$a + c = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{uq}$$

$$b + c = \frac{r}{s} + \frac{t}{u} = \frac{ru + st}{us}$$

$$p = \frac{qr}{s}$$

Hence

$$\frac{pu + qt}{uq} = \frac{\frac{qr}{s}u + qt}{uq}$$

$$= \frac{ru + st}{su}$$

Hence $a + c \sim b + c$

Similarly $c + a \sim c + b$

$c - a \sim c - b$

$a - c \sim b - c$

$a.c \sim b.c$

$c \cdot a \sim b \cdot a$

$-a \sim -b$

The equivalence relation $\sim$ is right invariant and left invariant over the operations $+, -, \cdot$. We say that $\sim$ is a congruence relation with respect to $+, -, \cdot$ and unary $-$.

Let us consider an algebra with carrier T and binary operation $\square$. Let $\sim$ be an equivalence relation on $\sim$. Then $\sim$ is a congruence relation on T if and only if for all $a, b, c \in T$, if $a \sim b$, $a \square c \sim b \square c$ and $c \square a \sim b \square a$.

Informally we say that a relation $\sim$ on a set T is a congruence relation with respect to an operation $\square$ if $\sim$ is a congruence relation on the algebra, $(T, \square)$. A relation $\sim$ is a congruence relation on an algebra A with underlying set T if and only if $\sim$ is a congruence relation on T with respect to each of the operations of A.

Example 3 *Equality relation is a congruence relation on any algebra.*

For an arbitrary monoid $A = (S, \circ, 1)$ show that the equality and the universal relation $S \times S$ are both congruence relations on A.

Consider the equality relation

$a * b$ iff $a = b$

$a \cdot x = b \cdot x$ if $a = b$ for any a, b, x in A

Hence $a \cdot x \, R \, b \cdot x$

Similarly $x \cdot a \, R \, x \cdot b$

Hence R is both right invariant and left invariant. Equality is an equivalence relation and hence it is a congruence relation.

Each element of A is in one congruence class.

Consider the universality relation aRb for any $a, b \in A$.

Hence $a. x \, R \, b \cdot x$ and $x \cdot a \, R \, x \cdot b$

as $a \cdot x, b \cdot x, x \cdot a, x \cdot b$ are elements of A. All elements are in the same equivalence or congruence class and the operation is both left invariant and right invariant. ◀

Example 4 *Consider the set of integers together with the operation of multiplication. The equivalence relation ~ of "equivalence mod k" for some positive integer k is a congruence relation on the algebra* $(I, \cdot)$.

$x \sim y$ if and only if $x \equiv y \bmod k$

Now to show ~ is a congruence relation we have to show that for any $z \in I$,

$x \cdot z = y \cdot z$ and

$z \cdot x = z \cdot y$

$x = kn_1 + r$

$y = kn_2 + r \qquad 0 \le r < k, \qquad n_1, n_2 \in I$

$z \cdot x = z\,(kn_1 + r) = zkn_1 + zr$

$z \cdot y = z\,(kn_2 + r) = zkn_2 + zr$

Let $\quad zr = n_3 k + r' \qquad 0 \le r' < k$

Then $\quad z \cdot x = zk(n_1) + n_3 k + r' = k\,(2n_1 + n_3) + r'$

$z \cdot y = zk(n_2) + n_3 k + r' = k\,(2n_2 + n_3) + r'$

Hence $\quad z \cdot x \sim z \cdot y$

By commutativity of multiplication of integers $x \cdot z = y \cdot z$.

Thus ~ is a congruence relation over $(I, \cdot)$ ◀

Example 5 *Let I be the set of integers and* □ *binary operation on I such that*

$a \square b = \max(a, b)$

Consider ~ as equivalence relation 'mod 7'

i.e., $a \sim b$ if $a \equiv b \pmod 7$

Then ~ is not a congruence relation for □

$5 \sim 12$

$5 \square 8 = 8$

$12 \square 8 = 12$

$8 \not\equiv 12 \pmod 7$

$8 \neq 12$.

Hence it is not a congruence relation over $\square$.

◀

Theorem 3 The equivalence relation $\sim$ on a set T is a congruence relation with respect to the binary operation $\square$ if and only if whenever $a \sim b$ and $c \sim d$, we have $a \square c \sim b \square d$.

Proof: (a) (only if). Let $\sim$ be a congruence relation with respect to the binary operation $\square$. Suppose $a \sim b$ and $c \sim d$

$$a \square c \sim b \square c \text{ and } b \square c \sim b \square d$$

By transitivity of the equivalence relation $\sim$, we have $a \square c \sim b \square d$.

(b) (if) Suppose $\sim$ is an equivalence relation on T such that if $a \sim b$ and $c \sim d$, then $a \square c \sim b \square d$. We have to show $\sim$ is a congruence relation. We have $a \sim b$.

From $c \sim c$ we get $a \square c \sim b \square c$

and $c \square a \sim c \square b$. Hence $\square$ is a congruence relation.

A homomorphism h from an algebra A with carrier T to an algebra A' with carrier T' is a map from T to T', which preserves the operation of A. Any map induces a natural equivalence relation over its domain and hence homomorphism also induces an equivalence relation over the underlying set. $a \sim b$ if and only if $h(a) = h(b)$. We next show that the equivalence relation induced by h is in fact a congruence relation.

Theorem 4 Let $A = (T, \square)$ be an algebra with T as the underlying set and $\square$ a binary operation in T. Let h be a homomorphism from $A = (T, \square)$ to $A' = (T', \square')$. Then the equivalence relation induced by h is a congruence relation on the algebra A.

Proof: For $a, b \in T$, $a \sim b$ if and only if $h(a) = h(b)$. In order to show that this is a congruence relation, it is enough to show that whenever $a \sim b$ and $c \sim d$, $a \square c \sim b \square d$ for all $a, b, c, d \in T$.

If $a \sim b$ and $c \sim d$

$$h(a) = h(b) \text{ and } h(c) = h(d).$$

Hence $h(a) \square' h(c) = h(b) \square' h(d)$.

Since h is a homomorphism from $A = (T, \square)$ to $A' = (T, \square')$, $h(a \square c) = h(a) \square' h(c)$

$$h(b \square d) = h(b) \square' h(d) \text{ and it follows that}$$

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

Therefore $a \square c \sim b \square d$.

Thus $\sim$ is a congruence relation on T with respect to $\square$. i.e., $\sim$ is a congruence relation on the algebra A.

Example 6 *Consider the algebraic system given below as a description of the interaction of six different kind of particles $\{a, b, c, d, e, f\}$. Suppose a, b, c are positively charged particles; d and e are neutral particles and f is a negatively charged particle. If we let $\{+, 0, -\}$ to denote the three kinds of particles, the table in (b) shows how the three kinds of particles interact.*

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

(a)

□'	+	0	−
+	+	+	0
0	+	0	−
−	0	−	−

(b)

The homomorphism $h(a) = h(b) = h(c) = +$
$h(d) = h(e) = 0$
$h(f) = -$

maps the algebraic system in table (a) to the algebraic system given in table (b).

Normal Subgroups Let us now consider only groups. Given a group $G = (T, \square)$, what can we say about the homomorphic images of G? We have seen that a subgroup $H = (T', \square)$ of G induces a partition of T which is determined by the cosets of the subgroup. Each coset is a block of the partition. This partition on T induces an equivalence relation. Is this equivalence relation a congruence relation? The answer is 'no'. But putting an additional restriction on the subgroup H will make this equivalence relation a congruence relation.

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

G

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

H

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

H is a normal subgroup of G.

For example

$$e \square H = \{e \square a, e \square b, e \square c\} = \{e, d, f\}$$

$$H \square e = \{a \square e, b \square e, c \square e\} = \{e, f, d\}$$

We next show that the distinct left (right) cosets of a normal subgroup H are congruence classes of the underlying set of G. Let $a \square H$ and $b \square H$ be two cosets. We want to show that for all the elements a_1 in $a \square H$ and all the elements b_1 in $b \square H$, the elements $a_1 \square b_1$ are in one coset of H. Let

$a_1 = a \square h_1$
$b_1 = b \square h_2$ for some h_1 and h_2 in H.

We have $a_1 \square b_1 = (a \square h_1) \square (b \square h_2)$
$= (a \square h_1) \square (h_3 \square b)$ for some $h_3 \in H$
$= a \square h_1 \square h_3 \square b$
$= a \square h_4 \square b$ $h_4 = h_1 \square h_3 \in H$
$= a \square b \square h_5$ for some $h_5 \in H$

Thus $a_1 \square b_1$ is in the coset $(a \square b) \square H$.

For example, for the group $G = (\{a, b, c, d, e, f\}, \square)$ and the subgroup $H = (\{a, b, c\}, \square)$, the congruence classes are $\{a, b, c\}$ and $\{d, e, f\}$. Consequently we have the homomorphic image

$\square'$	$\{a, b, c\}$	$\{d, e, f\}$
$\{a, b, c\}$	$\{a, b, c\}$	$\{d, e, f\}$
$\{d, e, f\}$	$\{d, e, f\}$	$\{a, b, c\}$

Next we show that exhausting all normal subgroups of $(T, \square)$ would have exhausted all homomorphic images of $(T, \square)$.

Let f be a homomorphism from $(T, \square)$ to $(S, *)$. We want to show that f corresponds to a partition of T into congruence classes induced by a normal subgroup.

Let H be all the elements in T whose images under f are the identity of S, which we denote as e^*. This is called the kernel of the homomorphism.

We first show that $(H, \square)$ is a subgroup of $(T, \square)$.

1. Closure: To show $\square$ is closed on H.
   For any a and b in H, we have

$$f(a \square b) = f(a) * f(b) = e^* \cdot e^* = e^*$$

Hence $a \square b$ is in H.

2. We want to show that e, the identity of T is in H. For arbitrary element a in T, we have

$$f(a \square e) = f(a) * f(e) \text{ or}$$
$$f(a) = f(a) * f(e)$$

Since $(S, *)$ is a group, $f(e)$ must be the identity of $(S, *)$, i.e., e^*. Consequently e is in H.

3. We want to show that a^{-1} is in H for any element a in H.

Since $f(a \square a^{-1}) = f(a) * f(a^{-1})$

or $\quad f(e) = f(a) * f(a^{-1})$

or $\quad e^* = e^* * f(a^{-1})$

or $\quad f(a^{-1}) = e^*$. Hence a^{-1} is in H.

Next we show that $(H, \square)$ is a normal subgroup. For any a in T and h in H.

$$\begin{aligned} f(a \square h \square a^{-1}) &= f(a) * f(h) * f(a^{-1}) \\ &= f(a) * e^* * f(a^{-1}) \\ &= f(a) * f(a^{-1}) \\ &= f(a * a^{-1}) \\ &= f(e) \\ &= e^* \end{aligned}$$

Thus $a \square h \square a^{-1}$ is in H.

Let $a \square h \square a^{-1} = h_1$.

Then $a \square h = h_1 \square a$

for some h_1 in H. Hence every element of the right coset of H with respect to some element a is also in the left coset of H with respect to a.

Finally we show that if a and b are in the same coset of H, then $f(a) = f(b)$. Since b can be written as $b = a \square h$ for some h in H we have

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

Conversely, if $f(a) = f(b)$, a and b are in the same coset of H.

$$\begin{aligned} \text{Since } f(a^{-1} \square b) &= f(a^{-1}) * f(b) \\ &= f(a^{-1}) * f(a) \\ &= f(a^{-1} \square a) \\ &= f(e) \\ &= e^* \end{aligned}$$

$a^{-1} \square b$ 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

$b = a \square h$, $e \in H$ and so a and b 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