LOVELY
PROFESSIONAL
UNIVERSITY

ABSTRACT ALGEBRA I

Edited By
Richa Nandra

Printed by
EXCEL BOOKS PRIVATE LIMITED
A-45, Naraina, Phase-I,
New Delhi-110028
for
Lovely Professional University
Phagwara

SYLLABUS

Abstract Algebra I

Sr. No.	Content
1	Groups : Definition and examples, Quotient groups, Cyclic groups, Permutation groups and The alternating groups, Subgroups, normal subgroups and the commutator subgroup, Generating sets, Lagrange's Theorem and Cayley's theorem
2	Homomorphisms and Automorphisms, Direct products. External and internal direct products,
3	Structure of finite abelian groups, Conjugate elements and class equations of finite groups, Sylow's theorems and their simple applications.
4	Solvable groups,Jordan-Holder Theorem, Rings, Subrings, Ideals and their operations
5	Factor rings and Homomorphisms, Integral domains

CONTENT

Unit 1: Generating Sets

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Explain the operations on sets
- Define Cartesian products of sets
- Describe the equivalence classes
- Define different kinds of functions
- Explain the division algorithm and unique prime factorisation theorem

Introduction

In this unit, we will discuss some basic ideas concerning sets and functions. These concepts are elementary to the study of any branch of mathematics, in particular of algebra. In the unit, we discuss some basic number theory. The primary aim of this section is to assemble a few facts that will be required in the rest of the course. We also hope to give you a glimpse of the elegance of number theory. It is this sophistication that led the mathematician Gauss to call number theory the "queen of mathematics". Let us start explaining these concepts one-by-one.

Notes

1.1 Sets

You must have used the word 'set' off and on in your conversations to describe any collection. In mathematics, the term set is used to describe any well defined collection of objects, that is, every set should be so described that given any object it should be clear whether the given object belongs to the set or not.

For instance, the collection N of all natural numbers is well defined, and hence is a set. But the collection of all rich people is not a set, because there is no way of deciding whether a human being is rich or not.

If S is a set, an object a in the collection S is called an element of S. This fact is expressed in symbols as $a \in S$ (read as "a is in S" or "a belongs to S"). If a is not in S, we write $a \in S$. For example, $3 \in R$ the set of real numbers. But $\sqrt{-1} \notin R$.

A set with no element in it is called the **empty set,** and is denoted by the Greek letter ϕ (phi). For example, the set of all natural numbers less than 1 is ϕ.

There are usually two way of describing a non-empty set:

(1) Roster method, and (2) Set builder method.

Roster Method: In this method, we list all the elements of the set within braces. For instance, the collection of all positive divisors of 48 contains 1, 2, 3, 4, 6, 8, 12, 16, 24 and 48 as its elements. So this set may be written as (1, 2, 3,4, 6, 8, 12, 16, 24, 48).

In this description of a set, the following two conventions are followed:

Convention 1: The order in which the elements of the set are listed is not important.

Convention 2: No element is written more than once, that is, every element must be written exactly once.

For example, consider the set S of all integers between $1\frac{1}{2}$ and $4\frac{1}{4}$. Obviously, these integers are 2, 3 and 4. So we may write S = (2, 3, 4).

We may also write S = (3, 2, 4), but we must not write S = (2, 3, 2, 4). Why? Isn't this what Convention 2 says?

The roster method is sometimes used to list the elements of a large set also. In this case we may not want to list all the elements of the set. We list a few, enough to give an indication of the rest of the elements. For example, the set of integers lying between 0 and 100 is (0, 1, 2 ,........., 100), and the set of all integers is Z = (0, +1, ! 2, ... }.

Another method that we can use for describing a set is the Set Builder Method.

Set Builder Method: In this method we first try to find a property, which characterises the elements of the set, that is, a property P which all the elements of the set possess, and which no other objects possess. Then we describe the set as

{x | x has property P), or as

{x : x has property P).

This is to be read as "the set of all **x** such that **x** has property P"**.** For example, the set of all integers can also be written as

Z = {x | x is an integer}.

Some other sets that you may be familiar with are

Q, the set of rational numbers = $\left\{\frac{a}{b} \,\middle|\, \quad a, b \in Z, b \neq 0\right\}$

R, the set of real numbers

C, the set of complex numbers = (a+ib | a, b ● R). (Here $i = \sqrt{-1.}$)

Let us now see what subsets are.

Subsets: Consider the sets **A** = (1, 3, 4) and B = (1, 4). Here every element of B is also an element of A. In such a case, that is, when every element of a set B is an element of a set A, we say that B is a subset of A, and we write this as B $\subseteq$ A.

It is obvious that if **A** is any set, then every element of A is certainly an element of A. So, for every set A, A $\subseteq$ A.

Also, for any set A, $\phi \subseteq$ A.

Now consider the set S = (1, 3, 5, 15) and T = (2, 3, 5, 7}. Is S $\subseteq$ T? No, because not every element of S is in T; for example, 1 ● S but 1 $\notin$ T. In this case we say that S is not a subset of T, and denote it by S $\not\subseteq$ T.

Note that if B is not a subset of A, there must be an element of B which is not an element of A. In mathematical notation this can be written as '$\exists$ x $\in$ B such that x' $\notin$ A'.

We can now say that two sets A and B are equal (i.e., have precisely the same elements) if and only if A $\subseteq$ B and B $\subseteq$ A.

Let us now look at some operations on sets. We will briefly discuss the operations of union, intersection and complementation on sets.

Union: If A and B are subsets of a set S, we can collect the elements of both to get a new set. This set is called their union. Formally, we define the union of A and B to be the set of all those elements of S which are in A or in B. We denote the union of A and B by A $\cup$ B. Thus,

A $\cup$ B=(X $\in$ S | X $\in$ A or x $\in$ B).

For example, if A = {1, 2} and B = {4, 6, 7}, then A $\cup$ B = {1, 2, 4, 6, 7}.

Again, if A = {l, 2, 3, 4) and B = (2, 4, 6, 8), then A $\cup$ B = {l, 2, 3, 4, 6, 8). Observe that 2 and 4 are in both A and B, but when we write A $\cup$ B, we write these elements only once, in accordance with Convention 2 given earlier.

Can you see that, for any set A, A U A = A?

Now we will extend the definition of union to define the union of more than two sets.

If A_1, A_2, A_3, ...,A_k are k subsets of a set S, then their union $A_1 \cup A_2 \cup$ . ... $\cup A_k$ is the set of elements which belong to at least one of these sets. That is,

$A_1 \cup A_2 \cup$ .... $\cup A_k$ = {x $\in$ S | x $\in$ A_i for some i = 1, 2 ,......, k).

The expression $A_1 \cup A_2 \cup$ .... $\cup A_k$ is often abbreviated to $\bigcup_{i=1}^{k} A_i$.

Notes

If $\wp$ is a collection of subsets of a set **S,** then we can define the union of all members of $\wp$ by

$$\bigcup_{A \in \wp} A = (x \in S \mid X \forall A \text{ for some } A \in \wp).$$

Now let us look at another way of obtaining a new set from two or more given sets.

Intersection: If A and B are two subsets of a set S, we can collect the elements that are common to both A and B. We call this set the intersection of A, and B (denoted by $A \cap B$. So,

$$A \cap B = \{ x \in S \mid X \forall A \text{ and } x \in B \}.$$

Thus, if P = {1, 2, 3, 4} and Q = {2, 4, 6, 8}, then $P \cap Q$ = {2, 4},

Can you see that, for any set A, $A \cap A = A$?

Now suppose A = {1, 2) and B = (4, 6, 7). Then what is $A \cap B$? We observe that, in this case, A and B have no common elements, and so $A \cap B = \phi$, the empty set.

When the intersection of two sets is ϕ, we say that the two sets are disjoint (or mutually disjoint). For example, the sets (1, 4) and (0, 5, 7, 14) are disjoint.

The definition of intersection can be extended to any number of sets. Thus, the intersection of k subsets A_1, A_2 ,......, A_k of a set S is

$$A, \cap A_2 \cap \,......... \cap A, = \{ x \, E \, S \mid x \, E \, A_i \text{ for each } i = 1, 2, ..., k \}.$$

We can shorten the expression $A_1 \cap A_2 \cap .... \cap A_k$ to $\bigcap_{i=1}^{k} A_i$.

In general, if $\wp$ is a collection of subsets of a set S, then we can define the intersection of all the members of $\wp$ by

$$\bigcap_{A \in P} A = \{ X \in S \mid X \in A \cancel{\forall} A \in \wp \}$$ [$\cancel{\forall}$ denotes 'forever']

Apart from the operations of unions and intersections, there is another operation on sets, namely, the operation of taking differences.

Differences: Consider the sets A = { 1, 2, 3] and B = [2, 3, 4]. Now the set of all elements of A that are not in B is {1}. We call this set the **difference** A \ B. Similarly, the difference B \A is the set of elements of B that are not in A, that is, {4}.

Thus, for any two subsets A and B of a set S,

$$A \backslash B = \{ x \in S \mid x \in A \text{ and } x \notin B \}$$

When we are working with elements and subsets of a single set X, we say that the set X is the **universal set.** Suppose **X** is the universal set and $A \subseteq X$. Then the set of all elements of X which are not in A is called the **complement** of A and is denoted by A', A^C or **X** \ A.

Thus,

$$A^c = \{x \in X \mid x \notin A \}.$$

For example, if X = [a, b, p, q , r) and A = {a, p, q], then A^c = (b, r).

1.2 Cartesian Product

An interesting set that can be formed from two given sets is their Cartesian product, named after the French philosopher and mathematician Rene Descartes (1596 - 1650). He also invented the Cartesian co-ordinate system.

Notes

Let A and B be two sets. Consider the pair (a, b), in which the first element is from A and the second from B. Then (a, b) is called an ordered pair. In an ordered pair the order in which the two elements are written is important. Thus, (a, b) and (b,a) are different ordered pairs. Two ordered pairs (a, b) and (c, d) are called equal, or the same, if

$a = c$ and $b = d$.

Definition: The Cartesian product A x B, of the sets A and B, is the set of all possible ordered pairs (a, b), where $a \in A$, $b \in B$.

For example, if A = {l , 2 , 3} and B = (4, 6), then

$A \times B = \{ (1, 4), (1, 6), (2, 4), (2, 6), (3, 4), (3, 6) \}$.

Also note that

$B \times A = \{ (4, 1), (4, 2), (4, 3), (6, 1), (6, 2), (6, 3) \}$ and $A \text{ x } B \neq B \text{ x } A$.

Let us make some remarks about the Cartesian product here.

Remarks: (i) $A \text{ x } B = \Phi$ iff $A = \Phi$ or $B = \Phi$.

(ii) If A has m elements and B has n elements, then A x B has mn elements. B x A also has mn elements. But the elements of B x A need not be the same as the elements of **A** x B, as you have just seen.

We can also define the Cartesian product of more than two sets in a similar way. Thus, if A_1, A_2, A_3, ... A_n, are n sets, we can define their Cartesian product as

$A_1 \text{ x } A_2 \text{x} ....\text{x } A_n = \{ (a_1, a_2, ..., a_n) \mid a_1 \in A_1, ..., a_n$ ● $A_n\}$.

For example, if R is the set of all real numbers, then

$R \text{ x } R = \{ (a_1, a_2) \mid a_1 \in R, a_2 \in R \}$

$R \text{ x } R \text{ x } R = \{ (a_1, a_2, a_3) \mid a_i \in R$ for $i = 1, 2, 3$), and so on. It is customary to write R^2 for R x R and R^n for R x .... x R (n times).

Now, you know that every point in a plane has two coordinates, x and y. Also, every ordered pair (x, y) of real numbers defines the coordinates of a point in the plane. So, we can say that R^2 represents a plane. In fact, R^2 is the Cartesian product of the x-axis and the y-axis. In the same way R^3 represents three-dimensional space, and R^n represents n-dimensional space, for any $n \geq 1$. Note that R represents a line.

1.3 Relations

You are already familiar with the concept of a relationship between people. For example, a parent-child relationship exists between A and B if and only if A is a parent of B or B is a parent of A.

In mathematics, a relation R on a set S is a relationship between the elements of S. If $a \in S$ is related to $b \in S$ by means of this relation, we write a R b or $(a, b) \in R$. From the latter notation we see that $R \subseteq S \times S$. And this is exactly how we define a relation on a set.

Definition: A relation R on a set S is a subset of S × S.

For example, if N is the set of natural numbers and R is the relation 'is a multiple of', then 15 R 5, but not 5 R 15. That is, $(15, 5) \in R$ but $(5, 15) \notin R$. Here $R \subseteq N \times N$.

Again, if Q is the set of all rational numbers and R is the relation 'is greater than', then 3 R 2 (because 3 > 2).

Definition: A relation R defined on a set S is said to be

(i) **reflexive** if we have aRa, $\forall$ a $\in$ S.

(ii) **symmetric** if aRb $\Rightarrow$ bRa $\forall$ a, b $\in$ S.

(iii) **transitive** if aRb and bRc $\Rightarrow$ aRc $\forall$ a, b, c $\in$ S.

To get used to these concepts, consider the following examples.

Example: Consider the relation R on Z given by 'aRb if and only if a > b'. Determine whether R is reflexive, symmetric and transitive.

Solution: Since a > a is not true, aRa is not true. Hence, R is not reflexive.

If a > b, then certainly b > a is not true. That is, aRb does not imply bRa. Hence, R is not symmetric.

Since a > b and b > c implies a > c, we find that aRb, bRc implies aRc. Thus, R is transitive.

Example: Let S be a non-empty set. Let $\wp$(S) denote the set of all subsets of S, i.e., $\wp$(S) = (A | A $\subseteq$ S}. We call p (S) the power set of S.

Define the relation R on $\wp$(S) by

R= { (A,B) | A, B $\in$ $\wp$(S) and A $\subseteq$ B].

Check whether R is reflexive, symmetric or transitive.

Solution: Since A $\subseteq$ A $\forall$ A $\in$ $\wp$ (S), R is reflexive.

If A $\subseteq$ B, B need not be contained in A. (In fact, A $\subseteq$ B and B $\subseteq$ A $\Leftrightarrow$ A = B.) Thus, R is not symmetric.

If A $\subseteq$ B and B $\subseteq$ C, then A $\subseteq$ C $\forall$ A, B, C $\in$ $\wp$(S). Thus, R is transitive.

A very important property of an equivalence relation on a set S is that it divides S into a number of mutually disjoint subsets, that is, it **partitions** S. Let us see how this happens.

Let R be an equivalence relation on the set S. Let a $\in$ S. Then the set { b $\in$ S | aRb } is called the **equivalence class** of a in S. It is just the set of elements in S which are related to a. We denote it by [a].

This is

[1] = { n | 1 R n ; n $\in$ N }

= { n 1 n $\in$ N and 5 divides 1-n)

= { n I n $\in$ N and 5 divides n-1)

= { 1, 6, 11, 16, 21 .... }.

Similarly,

[2] = { n | n $\in$ N and 5 divides n–2 }

= { 2, 7, 12, 17, 22. .... },

[3] = { 3, 8, 13, 18, 23 .... },

[4] = { 4 , 9, 14 , 19, 24, ... },

[5] = { 5, 10, 15, 20, 25, ... },

Note that

(i) [1] and [6] are not disjoint. In fact, [1] = [6]. Similarly, [2] = [7], and so on.

(ii) **N** = [I] U [2] U [3] U [4] U [5], and the sets on the right hand side arc mutually disjoint.

We will prove these observations in general in the following theorem.

Theorem 1: Let R be an equivalence relation on a set S. For a ∈ S, let [a] denote the equivalence class of a. Then

(a) a ∈ [a],

(b) b ∈ [a] ⇔ [a] = [b],

(c) $S = \bigcup\limits_{a \in S} [a]$

(d) if a, b ∈ S, then [a] ∩ [b] = ϕ or [a] = [b].

Proof: (a) Since R is an equivalence relation, it is reflexive.

∴ aRa ∀ a ∈ S. ∴ a ∈ [a].

(b) Firstly, assume that b ∀ [a]. We will show that [a]■[b] and [b]■[a]. For this, let x ∈ [a]. Then xRa.

We also know that aRb. Thus, by transitivity of R, we have xRb, i.e., x ∈ [b]. ∴ [a] ⊆ [b]. We can similarly show that [b] ⊆ [a].

∴ [a] = [b].

Conversely, assume that [a] = [b]. Then b ∈ [b] = [a]. ∴ b ∈ [a].

(c) Since [a] ⊆ S ∀ a ∈ S, $\bigcup\limits_{a \in S} [a] \subseteq S$.

Conversely, let x ∈ S. Then x ∈ [x] by (a) above. [x] is one of the sets in the collection whose union is $\bigcup\limits_{a \in S} [a]$.

Hence, x ∈ $\bigcup\limits_{a \in S} [a]$. So, S ∈ $\bigcup\limits_{a \in S} [a]$.

Thus, S● $\bigcup\limits_{a \in S} [a]$ and $\bigcup\limits_{a \in S} [a] \subseteq S$, proving (c).

(d) Suppose [a] ∩ [b] ≠ ϕ. Let x ∈ [a] ∩ [b].

Then x ∈ [a] and x ∈ [b]

⇒ [x] = [a] and [x] = [b], by (b) above.

⇒ [a] = [b].

Note that, in Theorem 1, distinct sets on the right hand side of (c) are mutually disjoint because of (d). Therefore, (c) expresses S as a union of mutually disjoint subsets of S; that is, we have a partition of S into equivalence classes.

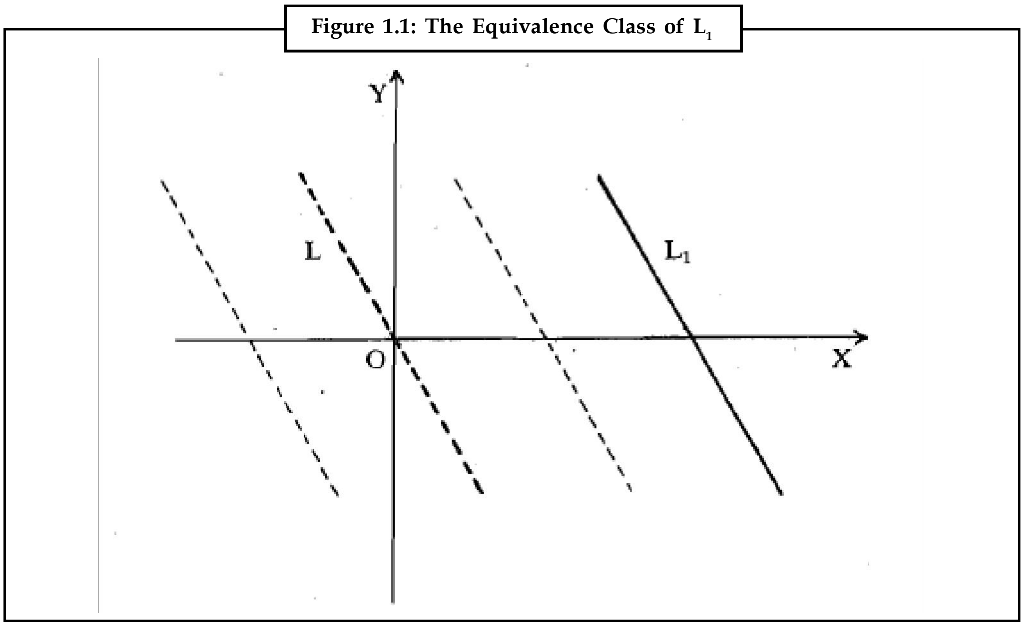
Let us look at some more examples of partitioning a set into equivalence classes.

Notes

Example: Let S be the set of straight lines in R × R. Consider the relation on S given by 'L$_1$ R L$_2$ iff L$_1$ = L$_2$ or L$_1$ is parallel to L$_2$. Show that R is an equivalence relation, What are the equivalence classes in S?

Solution: R is reflexive, symmetric and transitive. Thus, R is an equivalence relation. Now, take any line L$_1$ (see Figure 1.1).

Figure 1.1: The Equivalence Class of L$_1$



Let L be the line through (0, 0) and parallel to L$_1$. Then L ∈ [L$_1$]. Thus, [L] = [L,]. In this way the distinct lines through (0, 0) give distinct equivalence classes into which S is partitioned. Each equivalence class [L] consists of all the lines in the plane that are parallel to L.

In the next section we will briefly discuss a concept that you may be familiar with, namely, functions.

1.4 Functions

Recall that a function f from a non-empty set A to a non-empty set B is a rule which associates with every element of A exactly one element of B. This is written as f : A → B. If f associates with a ∈ A, the element b of B, we write f(a) = b. A is called the **domain** of f, and the set f(A) = { f(a) | a ∈ A] is called the **range** of f. The range of f is a subset of B.

i.e., f(A) ⊆ B. B is called the **codomain** of f.

Note that

(i) For each element of A, we associate some element of B.

(ii) For each element of A, we associate only one element of B.

(iii) Two or more elements of A could be associated with the same element of B.

For example, let A = { 1, 2, 3 }, B = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 }. Define f : A → B by f(1) = 1, f(2) = 4, f(3) = 9. Then f is a function with domain A and range {1, 4, 9}. In this case we can also write f(x) = x^2 for each x ● A or f : A → B : f(x) = x^2. We will often use this notation for defining any function.

If we define g : **A** → B by g(1) = 1, g(2) = 1, g(3) = 4, then g is also a function. The domain of g remains the same, namely, A. But the range of g is {1, 4}.

Remark: We can also consider a function f : A → B to be the subset { (a, f(a)) | a ∈ A } of A × B.

Now let us look at functions with special properties.

Definition: A function f : A → B is called One-one (or injective) if f associates different elements of A with different elements of B, i.e., if $a_1, a_2 \in A$ and al ≠ a,, then $f(a_l) \neq f(a_2)$. In other words, f is 1-1 if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

In the examples given above, the function f is one-one. The function g is not one-one because 1 and 2 are distinct elements of A, but g(1) = g(2).

Now consider another example of sets and functions.

Let A = (1, 2, 3), B = { p, q, r }. Let f : A → B be defined by f(1) = q, f(2) = r, f(3) = p. Then f is a function. Here the range of f = B = codomain of f. This is an example of an onto function, as you shall see.

Definition: A function f : A → B is called onto (or surjective) if the range of f is B, i.e., if, for each b ● B, there is an a ● A such that f(a) = b. In other words, f is onto if f(A) = B.

For another important example of a surjective function, consider two non-empty sets A and B. We define the function $\pi_1 : A \times B \to A : \pi_1((a, b)) = a$. π_1 is called the projection of A × B onto A. You can see that the range of π_1 is the whole of A. Therefore, π_1 is onto. Similarly, $\pi_2 : A \times B \to B : \pi_2$ ((a, b)) = b, the projection of A × B onto B, is a surjective function.

If a function is both one-one and onto, it is called bijective, or a bijection.

Consider the following example that you will use again and again.

Example: Let A be any set. The function $I_A : A \to A : I_A(a) = a$ is called the identity function on A. Show that I, is bijective.

Solution: For any a ∈ A, I_A (a) = a. Thus, the range of I_A is the whole of A. That is, I_A is onto.

I_A is also 1-1 because if $a_1, a_2 \in A$ such that $a_1 \neq a_2$, then $I_A (a_1) \neq I_A (a_2)$.

Thus, I_A is bijective.

If f : A → B is a bijection, then we also say that the sets A and B are equivalent. Any set which is equivalent to the set { 1, 2, 3 ,............, n}, for some n ∈ N, is called a finite set. A set that is not finite is called an infinite set.

Convention: The empty set ϕ is assumed to be finite.

Let us now see what the inverse image of a function is.

Definition: Let A and B be two sets and f : A → B be a function, Then, for any subset S of B, the inverse image of S under f is the set

$f^{-1}(S) = \{ a \in A \mid f(a) \in S \}$.

For example, $I_A^{-1}(A) = \{ a \in A \mid I_A(a) \in A \} = A$.

f–1({ 1, 2, 3 }) = { n ∈ N | f(n) ∈ { 1 , 2 , 3 } }

= { n ∈ N | n + 5 ∈ { 1,2,3 }}

= ϕ, the empty set.

We now give some nice theorems involving the inverse image of a function.

Theorem 2: Let f : A → B be a function. Then,

(a) for any subset S of B, $f(f^{-1}(S)) \subseteq S$.

(b) for any subset X of A, $X \subseteq f^{-1}(f(X))$.

Proof: We will prove (a) and you can prove (b). Let b $\forall$ $f(f^{-1}(S))$. Then, by definition, 3 a $\in f^{-1}(S)$ such that b = f(a). But a $\in f^{-1}(S) \Rightarrow f(a) \in S$. That is, b ∈ S.

Thus, $f(f^{-1}(S)) \subseteq S$.

Now let us look at the most important way of producing new functions from given ones.

1.4.1 Composition of Functions

If f : A → **B** and g : C → D are functions and if the range of f is a subset of C, there is a natural way of combining g and f to yield a new function h : A # D. Let us see how.

For each x ∈ A, h(x) is defined by the formula h(x) = g(f(x)).

Note that f(x) is in the range of f, so that f(x) ∈ C. Therefore, g(f(x)) is defined and is an element of D. This function h is called the **composition of** g **and f** and is written as g o f. The domain of g o f is A and its codomain is D. In most cases that we will be dealing with we will have B = C. Let us look at some examples.

Example: Let f : R → R and g : R → R be defined by $f(x) = x^2$ and g(x) = x + 1. What is g o f ? What is f o g ?

Solution: We observe that the range of f is a subset of R, the domain of g. Therefore, g o f is defined. By definition, $\forall$ x ∈ R, $g \text{ o } f(x) = g(f(x)) = f(x) + 1 = x^2 + 1$.

Now, let us find f o g. Again, it is easy to see that f o g is defined. $\forall$ x ∈ R,

$f \text{ o } g(x) = f(g(x)) = (g(x))^2 = (x + 1)^2$.

So f o g and g o f are both defined. But g o f ≠ f o g . (For example, g o f(1) ≠ f o g(l).)

Example: Let A = {1, 2, 3}, B = {p, q, r} and C = {x, y}. Let f : A → B be defined by f(1) = p, f(2) = p, f(3) = r. Let g : B → C be defined by g(p) = x, g(q) = y, g(r) = y. Determine if f o g and g o f can be defined.

Solution: For f o g to be defined, it is necessary that the range of g should be a subset of the domain of f. In this case the range of g is C and the domain of f is A. As C is not a subset of A, f o g cannot be defined.

Since the range of f, which is (p, r), is a subset of B, the domain of g, we see that g o f is defined. Also g o f : A → C is such that

g o f(l) = g(f(1)) = g(p) = x,

g o f(2) = g(f(2)) = g(p) = x,

g o f(3) = g(f(3)) = g(r) = y.

In this example note that g is surjective, and so is g o f.

We now come to a theorem which shows us that the identity function behaves like the number 1 ∈ R does for multiplication. That is, if we take the composition of any function f with **a** suitable identity function, we get the same function f.

Theorem 3: Let A be a set. For every function f : A → A, we have $f \text{ o } I_A = I_A \text{ o } f = f$.

Proof: Since both f and I_A are defined from A to A, both the compositions $f \text{ o } I_A$ and $I_A \text{ o } f$ are defined. Moreover, ∀ x ∈ A,

$f \text{ o } I_A(x) = f(I_A(x)) = f(x)$, so $f \text{ o } I_A = f$.

Also, ∀ X ∈ A, $I_A \text{ o } f(x) = I_A(f(x)) = f(x)$, so $I_A \text{ o } f = f$.

In the case of real numbers, you know that given any real number x + 0, ∃ y %0 such that xy = 1. y is called the inverse of x. Similarly, we can define an inverse function for a given function.

Definition: Let f : A → B be a given function. If there exists a function g : B → A such that f o g = I_B and g o f = I_A, then we say that g is the inverse of f, and we write $g = f^{-1}$.

For example, consider f : R → R defined by f(x) = x + 3. If we define g : R → R by g(x) = x – 3, then f o g(x) = f(g(x)) = g(x) + **3** = (x – 3) + 3 = x ∀ x ∈ R. Hence, f o g = I_R. You can also verify that g o f = I_R. So $g = f^{-1}$.

Note that in this example f adds 3 to x and g does the opposite – it subtracts 3 from x. Thus, the key to finding the inverse of a given function is : try to retrieve x from f(x).

For example, let f : R → R be defined by f(x) = 3x + 5. How can we retrieve x from 3x + 5? The answer is "first subtract 5 and then divide by 3"**.** So, we try g(x) = $(x) = \frac{x-5}{3}$. And we find

$$g \text{ o } f(x) = g(f(x)) = \frac{f(x)-5}{3} = \frac{(3x+5)-5}{3} = x.$$

$$\text{Also, } f \text{ o } g(x) = 3(g(x)) + 5 = 3\left[\frac{(x-5)}{3}\right] + 5 = x \ \forall \ x \in R.$$

Let's see if you've understood the process of extracting the inverse of a function,

Do all functions have an inverse? No, as the following example shows.

Example: Let f : R → R be the constant function given by f(x) = 1 ∀ x ∀R. What is the inverse of f ?

Solution: If f has an inverse g : R → R, we have f o g = I_R, i.e., ∀ x ∈ R, f o g(x) = x. Now take x = 5. We should have f o g (5) = 5, i.e., f(g(5)) = 5. But f(g(5)) = 1, since f(x) = 1 ∀ x. So we reach a contradiction. Therefore, f has no inverse.

In view of this example, we naturally ask for necessary and sufficient conditions for f to have an inverse. The answer is given by the following theorem.

Theorem 4: A function f ; A → B has an inverse if and only if f is bijective.

Proof: Firstly, suppose f is bijective. We shall define a function g : B → A and prove that $g = f^{-1}$.

Let b ∈ B. Since f is onto, there is some a ∀ A such that f(a) = b. Since f is one-one, there is only one such a ∈ A. We take this unique element a of A as g(b). That is, given b ∈ B, we define g(b) = a, where f(a) = b.

Note that, since f is onto, B = { f(a) | a ∈ A). Then, we are simply defining g : B → A by g(f(a)) = a. This automatically ensures that g o f = I_A.

Now, let b ∈ B and g(b) = a. Then f(a) = b, by definition of g. Therefore, f o g(b) = f(g(b)) = f(a) = b. Hence, f o g = I_B.

So, $f \circ g = I_B$ and $g \circ f = I_A$. This proves that $g = f^{-1}$.

Conversely, suppose f has an inverse and that $g = f^{-1}$. We must prove that f is one-one and onto.

Note g o f is 1 – 1 ⇒ f is 1 – 1

Suppose $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$.

$\Rightarrow g \circ f(a_1) = g \circ f(a_2)$

$\Rightarrow a_1 = a_2$, because $g \circ f = I_A$.

So, f is one-one.

Note g o f is onto ⇒ g is onto.

Next, given $b \in B$, we have $f \circ g = I_B$, So that $f \circ g(b) = I_B(b) = b$,

i.e., $f(g(b)) = b$. That is, f is onto.

Hence, the theorem is proved.

1.5 Some Number Theory

In this section we will spell out certain factorisation properties of integers that we will use throughout the course. For this we first need to present the principle of finite induction.

1.5.1 Principle of Induction

We will first state an axiom of the integers that we will often use implicitly, namely, the well-ordering principle. We start with a definition.

Definition: Let S be a non-empty subset of Z. An element $a \in S$ is called a least element (or a minimum element) of S if $a \leq b$ ∀ b ● S. For example, N has a least element, namely, 1. But Z has no least element. In fact, many subsets of Z, like 2Z, (-1, -2, -3, ...), etc., don't have least elements.

The following axiom tells us of some sets that have a least element.

Well-ordering Principle: Every non-empty subset of N has a least element.

You may be surprised to know that this principle is actually equivalent to the principle of finite induction, which we now state.

Theorem 5: Let $S \subseteq N$ such that

(i) $1 \in S$, and

(ii) whenever $k \in S$, then $k + 1 \in S$.

Then S = N.

This theorem is further equivalent to:

Theorem 6: Let $S \subseteq N$ such that

(i) $1 \in S$, and

(ii) if $m \in S \ \forall \ m < k$, then $k \in S$.

Then $S = N$

We will not prove the equivalence of the well-ordering principle and Theorems 5 and 6 in this course, since the proof is slightly technical.

Let us rewrite Theorems 5 and 6 in the forms that we will normally use.

Theorem 5: Let P(n) be a statement about a positive integer n such that

(i) P(1) is true, and

(ii) if P(k) is true for some $k \in N$, then P(k + l) is true.

Then, P(n) is true for all $n \in N$.

Theorem 6: Let P(n) be a statement about a positive integer n such that

(i) P(1) is me, and

(ii) if P(m) is true for all positive integers $m < k$, then P(k) is true.

Then P(n) is true for all $n \in N$.

The equivalent statements given above are very useful for proving a lot of results in algebra. As we go along, we will often use the principle of induction in whichever form is convenient. Let us look at an example.

Example: Prove that $1^3 + 2^3 + \ldots\ldots\ldots\ldots\ldots + n^3 = \frac{n^2(n+1)^2}{4}$ for every $n \in N$.

Solution: Let $S_n = 1^3 + \ldots\ldots\ldots\ldots + n^3$, and let P(n) be the statement that $S_n = \frac{n^2(n+1)^2}{4}$.

Since $S_1 = \frac{1^2 \times 2^2}{4}$, P(I) is true.

Now, suppose P(n – 1) is true, i.e., $S_{n-1} = \frac{(n-1)^2 n^2}{4}$

$$\text{Then, } S, = 1^3 + \ldots\ldots\ldots\ldots + (n-1)^3 + n^3$$

$$= S_{n-1} + n^3.$$

$$= \frac{(n-1)^2 n^2}{4} + n^3, \text{ since } P(n-1) \text{ is true.}$$

$$= \frac{n^2\left[(n-1)^2 + 4n\right]}{4}$$

$$= \frac{n^2(n-1)^2}{4}$$

Thus, P(n) is true.

Notes

Therefore, by the principle of induction, P(n) is true for all n in N.

Now, use the principle of induction to prove the following property of numbers that you must have used time and again.

1.5.2 Divisibility in Z

One of the fundamental ideas of number theory is the divisibility of integers.

Definition: Let a, b ∀, a %0. Then, we say that a divides b if there exists an integer c such that b = ac. We write this as a | b and say that a is a divisor (or factor) of b, or b is divisible by a, or b is a multiple of a.

If a does not divide b we write a × b.

We give some properties of divisibility of integers in the following exercise. You can prove them very easily.

We will now give a result, to prove **which** we use Theorem 5.

Theorem 7 (Division Algorithm): Let a, b ∈ Z, b > 0. Then there exist unique integers q, r such that a = qb + r, .where 0 5 r < b.

Proof: We will first prove that q and r exist. Then we will show that they are unique. To prove their existence, we will consider three different situations : a = 0, a > 0, a < 0.

Case 1 (a = 0): Take q = 0, r = 0. Then a = qb + r.

Case 2 (a > 0): Let **P(n)** be the statement that n = qb + r for some q, r ∈ Z, 0 ≤ r < b.

Now let us see if P(l) is true.

If b = l, we can take q = l, r = 0, and thus, 1 = 1.1 + 0.

If b ≠ l, then take q = 0, r = 1, i.e., 1 = 0.b + l.

So, P(1) is true.

Now suppose P(n – 1) is me, i.e., (n – 1) = $q_1b + r_1$ for some q_1, $r_1 \in Z$, $0 \le r_1 < b$. But then $r_1 \le b - 1$, i.e., $r_1 + 1 \le b$. Therefore,

$$n = \begin{cases} q_1 b + (r_1 + 1), \text{ if } (r_1 + 1) < b \\ (q_1 + 1)b + 0, \text{if } r_1 + 1 = b \end{cases}$$

This shows that P(n) is true. Hence, by Theorem 5, P(n) is true, for any n ∈ N. That is, for a > 0, a = qb + r, q, r ∈ Z, 0≤r < b.

Case 3 (a < 0): Here (-a) > 0. Therefore, by Case 2, we can write

(–a) = qb + r′, 0 ≤ r′ < b

$$\text{i.e., } a = \begin{cases} (-q)b, \text{ if } r' = 0 \\ (-q - 1)b + (b - r'), \text{ if } 0 < r' < b \end{cases}$$

This proves the existence of the integers q, r with the required properties.

Now let q′, r′ be in Z such that a = qb + r and a = q′b + r′, where 0 5 r, r′ < b. Then r – r′ = b(q′ – q). Thus, b | (r – r′). But | r – r′ | < b. Hence, r – r′ = 0, i.e., r = r′ and q = q′. So we have proved the uniqueness of q and r.

In the expression, a = qb + r, 0 &r < b, r is called the **remainder** obtained when a is divided by b.

Notes

Definition: Let a, b $\in$ Z. c $\in$ Z is called a **common divisor** of a and b if c | a and c | b. For example, 2 is a common divisor of 2 and 4. You know that 1 and –1 are common divisors of a and b, for any a, b $\in$ Z. Thus, a pair of integers do have more than one common divisor. This fact leads us to the following definition.

Definition: An integer d is said to be a greatest common divisor (g.c.d. in short) of two non-zero integers a and b if

(i) d | a and d | b, and

(ii) if c | a and c | b, then c | d.

Note that if d and d′ are two g.c.d s of a and b, then (ii) says that d | d′ and d′ | d. Thus, d = ±d′. But then only one of them is positive. This unique positive g.c.d. is denoted by (a, b).

We will now show that (a, b) exists for any non-zero integers a and b. You will also see how useful the well-ordering principle is.

Theorem 8: Any two non-zero integers a and b have a g.c.d., and (a, b) = ma+nb, for some m, n $\in$ Z.

Proof: Let S = {xa + yb | x, y $\in$ Z, (xa + yb) > 0).

Since $a^2 + b^2 > 0$, $a^2 + b^2 \in$ S, i.e., S $\neq$ 0. But then, by the well-ordering principle, S has a least element, say d = ma + nb for some m, n $\in$ Z. We show that d = (a, b).

Now d $\in$ S. Therefore, d > 0. So, by this division algorithm we can write

a = qd + r, $0 \leq r < d$. Thus,

r = a – qd = a – q(ma + nb) = (1 – qm)a + (–qn)b.

Now, if r $\neq$ 0, then r $\in$ S, which contradicts the minimality of d in S. Thus, r = 0, i.e., a = qd, i.e., d | a. We can similarly show that d | b. Thus, d is a common divisor of a and b.

Now, let c be an integer such that c | a and c | b.

Then a = a_1c, b = b_1c for some a_1, b_1 ● Z.

But then d = ma + nb = $ma_1c + nb_1c = (ma_1 + nb_1)c$. Thus, c | d, So we have shown that d is a g.c.d. In fact, it is the unique positive g.c.d. (a,b).

For example, the g.c.d. of 2 and 10 is 2 = 1.2 + 0.10, and the g.c.d, of 2 and 3 is 1 = (–1)2 + l(3).

Pairs of integers whose g.c.d. is 1 have a special name.

Definition: If (a,b) = 1, then the two integers a and b are said to be relatively prime (or coprime) to each other.

Using Theorem 8, we can say that a and b are coprime to each other iff there, exist m, n $\in$ Z such that 1 = ma + nb.

The next theorem shows us a nice property of relatively prime numbers.

Theorem 9: If a,b $\in$ Z; such that (a, b) = 1 and b | ac, then b | d.

Proof: We know that 3 m, n $\in$ **Z** such that 1 = ma + nb. Then c = c.1 = c(ma+nb) = mac + nbc.

Now, b | ac and b | bk. $\therefore$ b | (mac + nbc). Thus, b | c.

Let us now discuss prime factorisation.

Definition: A natural number p ($\neq$ 1) is called a prime if its only divisors are 1 and p. If a natural number n (%1) is not a prime, then it is called a composite number.

Notes

For example, 2 and 3 are prime numbers, while 4 is a composite number.

Note that, if p is a prime number and $a \in Z$ such that $p \times A$, then $(p,a) = 1$.

Now consider the number 50. We can write $50 = 2 \times 5 \times 5$ as a ,product of primes. In fact we can always express any natural number as a product of primes. This is what the unique prime factorisation theorem says.

Theorem 10 (Unique Prime Factorisation Theorem): Every integer $n > 1$ can be written as $n = p_1.p_2 .... p_n$, where $p_l, ... p_n$ are prime numbers. This representation is unique, except for the order in which the prime factors occur.

Proof: We will first prove the existence of such a factorisation. Let P(n) be the statement that n + l is a product of primes. P(1) is true, because 2 is a prime number itself.

Now let us assume that P(m) is true for all positive integers m < k. We want to show that P(k) is true. If (k+l) is a prime, P(k) is true. If k+l is not a prime, hen we can write $k + l = m, m_2$, where $1 < m, < k + l$ and $1 < m_2 < k + l$. But then $P(m_l - 1)$ and $P(m_2 - 1)$ are both true. Thus, $m_l = p_1p_2. .... p_r$, $m_2 = q_1q_2 ....q_s$, where $p_l,p_2, ...P_r, q_l, q_2, ...q_s$ are primes. Thus,

$k + 1 = p_l\ p_2 ... p_r\ q_1\ q_2 .... q_s$, i .e., P(k) is true. Hence, by Theorem 6, P(n) is true for every $n \in N$.

Now let us show that the factorisation is unique.

Let $n = p_l\ p_2 ... p, = q_1\ q_2 ... q_s$, where

$p_l, p_2, ...p_1. q_l, q_2, ..., q_s$ are primes. We will use induction on t.

If t = 1, then $p_1 = q_1, q_2 .... q_s$. But p_1 is a prime. Thus, its only factors are 1 and itself.

Thus, s = 1 and $p_1 = q_1$.

Now suppose t > 1 and the uniqueness holds for a product of t–1 primes. Now $p_1 \mid q_1q_2 ......q_s$ and hence, $p_1 \mid q_i$ for some i, By re-ordering $q_1 ....$ q, we can assume that $p_1 \mid q_1$. But both p_1 and q_1 are primes. Therefore, $p_1 = q_l$. But then $p_2 ..... p, = q_2 .... q,$. So, by induction, t–1 = s–1 and p_2 ,........ p_t are the same as $q_2. ......q,$, in some order.

Hence, we have proved the uniqueness of the factorisation.

The primes that occur in the factorisation of a number may be repeated, just as 5 is repeated in the factorisation $50 = 2 \times 5 \times 5$. By collecting the same primes together we can give the following corollary to Theorem 10.

Corollary: Any natural number n can be uniquely written as $n = p_l^{ml}\ p_2^{m2} .....P_r^{mr}$ where for i = 1, 2, ... r, each $m_i \in \mathbf{N}$ and each p_i is a prime with $1 < p_1 < p_2 < .... < p,$.

As an application of Theorem 10, we give the following important theorem, due to the ancient Greek mathematician Euclid.

Theorem 11: There are infinitely many primes.

Proof: Assume that the set P of prime numbers is finite, say

$P = \{ p_1, p_2, ... p_n\}$. Consider the natural number

$n = (p_1p_2 .... p_n) + 1$

Now, suppose some $p_i \mid n$. Then $p_i \mid (n - p_1p_2 .... p,)$, i.e., $p_i \mid 1$, a contradiction.

Therefore, no p_i divides n. But since n > 1, Theorem 10 says that n must have a prime factor. We reach a contradiction. Therefore, the set of primes must be infinite.

Self Assessment

1. Let A = {2, {4, 5}, 4}. Which statement is correct?

   (a) 5 is an element of A.

   (b) {5} is an element of A.

   (c) {4, 5} is an element of A.

   (d) {5} is a subset of A.

2. Which of these sets is finite?

   (a) {x | x is even}

   (b) {x | x < 5}

   (c) {1, 2, 3,...}

   (d) {1, 2, 3,...,999, 1000}

3. Which of these sets is not a null set?

   (a) A = {x | 6x = 24 and 3x = 1}

   (b) B = {x | x + 10 = 10}

   (c) C = {x | x is a man older than 200 years}

   (d) D = {x | x < x}

4. Let $D \subset E$. Suppose $a \in D$ and $b \notin E$. Which of the following statements must be true?

   (a) $c \in D$

   (b) $b \in D$

   (c) $a \in E$

   (d) $a \notin D$

5. Let A = {x | x is even}, B = {1, 2, 3... 99, 100}, C = {3, 5, 7, 9}, D = {101, 102} and E = {101, 103, 105}. Which of these sets can equal S if S A and S and B are disjoint?

   (a) A (b) B (c) C

   (d) D (e) E

6. Which statement best describes the Venn diagram below?

   (a) A = B

   (b) A and B are not comparable

   (c) $A \supset B$

   (d) $A \subset B$

7. Which set S does the power set 2^S = {∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}} come from?

   (a) {{1},{2},{3}}

   (b) {1, 2, 3}

   (c) {{1, 2}, {2, 3}, {1, 3}}

   (d) {{1, 2, 3}}

1.6 Summary

In this unit we have covered the following points:

- Some properties of sets and subsets.
- The union, intersection, difference and complements of sets.
- The Cartesian product of Sets.
- Relations in general, and equivalence relations in particular.
- The definition of a function, a 1-1 function, an unto function and a bijective function.
- The composition of functions.
- The well-ordering principle, which states that every subset of N has a least element.
- The principle of finite induction, which states that : If P(n) is a statement about some $n \in N$ such that

  (i) P(1) is true, and

  (ii) if P(k) is true for some $k \in N$, then P(k + l) is true,

  then P(n) is true for every $n \in N$.
- The principle of finite induction can also be stated as:

  If P(n) is a statement about some $n \in N$ such that

  (i) P(l) is true, and

  (ii) if P(m) is true for every positive integer m < k, then P(k) is true,

  then P(n) is true for every $n \in N$.

  Note that the well-ordering principle is equivalent to the principle of finite induction.
- Properties of divisibility in Z, like the division algorithm and unique prime factorisation.

1.7 Keywords

Empty Set: A set with no element in it is called the empty set, and is denoted by the Greek letter ϕ (phi). For example, the set of all natural numbers less than 1 is ϕ.

Roster Method: It is sometimes used to list the elements of a large set also. In this case we may not want to list all the elements of the set.

Union: If A and B are subsets of a set S, we can collect the elements of both to get a new set. This set is called their union.

1.8 Review Questions

1. Let C = {1, 2, 3, 4} and D = {1, 3, 5, 7, 9}. How many elements does the set $C \cup D$ contain? How many elements does the set $C \cap D$ contain?
2. Let U = {1, 2, 3... 8, 9}, B = {1, 3, 5, and 7} and C = {2, 3, 4, 5, 6}. How many elements does the set $(B \cap C)'$ contain? How many elements does the set $(C - B)'$ contain?
3. Let S = {a, b}. How many elements does the power set 2^S contain?
4. Let S = {1, 2, 3}. How many subsets does S contain?

5. Let a, b, c be non-zero integers. Then

   (a) $a \mid 0, \pm 1 \mid a, \pm a \mid a$.

   (b) $a \mid b \Rightarrow ac \mid bc$

   (c) $a \mid b$ and $b \mid c \Rightarrow a \mid c$

   (d) $a \mid b$ and $b \mid a \Leftrightarrow a = \pm b$

   (e) $c \mid a$ and $c \mid b \Rightarrow c \mid (ax + by) \ \forall x, y \in Z$.

6. If p is a prime and $p \mid ab$, then show that $p \mid a$ or $p \mid b$.

7. If p is a prime and $p \mid a_1a_2.....a_n$, then show that $p \mid a_i$ for some i = 1,....,n.

Answers: Self Assessment

1. A is consisted of elements: 3, {4, 5} and 8, so {4, 5} is an element of A

2. {1,2,3, ..., 1000} is finite, because it is consisted of final number of elements.

3. Set B is not an empty set because it contains one element. The only element of the set B is zero. B = {0}

4. $a \in E$ is true, because $a \in D$ and $D \subseteq E$ means that every element from D is contained in E.

5. The correct answer is E, because E consists of even numbers as elements and the intersection of sets S and B is a null set.

6. $A \supset B$ is the correct answer because A is a superset of B.

7. The correct answer is {1, 2, 3} because all subsets of {1, 2, 3} are ∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}.

1.9 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Richa Nandra, Lovely Professional University

Notes

Unit 2: Groups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the binary operations
- Explain the term abelian and non-abelian groups
- Describe the cancellation laws and laws of indices for various groups
- Discuss the properties of integers modulo n, permutations and complex numbers

Introduction

The theory of groups is one of the oldest branches of abstract algebra. It has many applications in mathematics and in the other sciences. Group theory has helped in developing physics, chemistry and computer science. Its own roots go back to the work of the eighteenth century mathematicians Lagrange, Ruffini and Galois.

In this unit, we will study about the group theory in detail. We surge fine groups and give some examples. After that we understand details of some properties of groups that the elements of a group satisfy. Let us discuss all these one by one.

2.1 Binary Operations

As you all know common operations of addition and multiplication in R, Q and C. All these operations are examples of binary operations. It can be defined as:

Definition: Let S be a non-empty set. Any function $* : S \times S \to S$ is called a binary operation on S.

So, a binary operation associates a unique element of S to every ordered pair of elements of S.

For a binary operation * on S and $(a, b) \in S \times S$, we denote $*(a, b)$ by $a*b$.

We will use symbols like +, –, ×, ⊕, o, * and A to denote binary operations.

Let us look at some examples.

(i) + and x are binary operations on Z. In fact, we have $+ (a, b) = a + b$ and $\times (a, b) = a \times b \; \forall \; a, b \in Z$. We will normally denote $a \times b$ by ab.

(ii) Let $\wp$ (S) be the set of all subsets of S. Then the operations $\bigcup$ and $\bigcap$ are binary operations on $\wp$ (S), since $A \bigcup B$ and $A \bigcap B$ are in $\wp$ (S) for all subsets A and B of S.

(iii) Let X be a non-empty set and F(X) be the family of all functions $f : X \to X$. Then the composition of functions is a binary operation on F(X), since $fog \in F(X) \; \forall \; f, g \in F(X)$.

After defining a non-empty set lets define properties of binary operations.

Definition: Let * be a binary operation on a set S. We say that

(i) * is closed on a subset T of S, if $a * b \in T \;\; \forall \;\; a, b \in T$

(ii) * is associative if, for all $a, b, c \in S$, $(a * b) * c = a * (b * c)$.

(iii) * is commutative if, for all $a, b \in S$, $a * b = b * a$.

For example, the operations of addition and multiplication on R are commutative as well as associative. But, subtraction is neither commutative nor associative on R. Why? Is $a - b = b - a$ or $(a - b) - c = a - (b - c)$ 4) $a, b, c \in R$? No, for example, $1 - 2$! $2 - 1$, and $(1 - 2) - 3 \neq 1 - (2 - 3)$. Also subtraction is not closed on $N \subseteq R$. because $1 \in N$. $2 \in N$ but $1 - 2 \notin N$.

Note A binary operation on S is always closed on S, but may not be closed on a subset of S.

Task For the following binary operations defined on R, determine whether they are commutative or associative. Are they closed on N?

(a) $x \oplus y = x + y - 5$

(b) $x * y = 2(x + y)$

(c) $x \,\Delta\, y = \dfrac{x - y}{2}$

for all $x, y \in R$.

Notes

As you are familiar with the equation such as $a(b + c) = ab + ac$ and $(b + c)a = bc + ba \ \forall\ a, b, c \in R$.

As this equation explains that multiplication distributes over addition in R. In general we can define this as.

Definition: If o and * are two binary operations on a set S, then we say that * is distributive over o if $\forall$ a, b, c $\in$ S, we have $a * (b \text{ o } c) = (a * b) \text{ o } (a * c)$ and $(b \text{ o } c) * a = (b * a) \text{ o } (c * a)$.

For example, let $a * b = \dfrac{a+b}{2} \ \forall\ a, b \in R$. Then $a(b \text{ a } c) = a\left(\dfrac{b+c}{2}\right) = \dfrac{ab+ac}{2} = ab * ac$, and $(b * c)a$

$$= \left(\frac{b+c}{2}\right)a = \frac{ba+ca}{2} = ba * ca \ \forall\ a, b, c \in R.$$

Hence, multiplication is distributive over *.

Let us now look deeper at some binary operations. You know that, for any $a \ \forall\ R$, $a + 0 = a$, $0 + a = a$ and $a + (–a) = (–a) + a = 0$. We say that 0 is the identity element for addition and (–a) is the negative or additive inverse of a.

Definition: Let *.be a binary operation on a set S. If there is an element $e \in S$ such that $\forall\ a \in S$, $a * e = a$ and $e * a = a$, then e is called an identity element for *.

For $a \in S$, we say that $b \in S$ is an inverse of a, if $a * b = e$ and $b * a = e$. In this case we usually write $b = a^{-1}$.

Let us first discuss the uniqueness of identity element for *, and uniqueness of the inverse of an element with respect to *, if it exists. After that we will discuss the examples related to identity elements.

Theorem 1: Let * be a binary operation on a set S. Then

(a) if * has an identity element, it must be unique.

(b) if * is associative and $s \in S$ has an inverse with respect to *, it must be unique.

Proof: (a) Suppose e and e′ are both identity elements for *.

Then $e = e * e'$, since e′ is an identity element.

$= e'$, since e is an identity element.

That is, $e = e'$. Hence, the identity element is unique.

(b) Suppose there exist $a, b \in S$ such that $s * a = e = a * s$ and $s * b = e = b * s$, e being the identity element for *, Then

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

$= (a * s) * b$, since * is associative.

$= e * b = b$.

That is, $a = b$.

Hence, the inverse of s is unique.

This uniqueness theorem allows us to say the identity element and the inverse, henceforth.

A binary operation may or may not have an identity element. For example, the operation of addition on N has no identity element.

Similarly, an element may not have an inverse with respect to a binary operation. For example, 2 ∀ Z has no inverse with respect to multiplication on Z, does it?

Now let us consider the following examples.

Example: If the binary operation # : R × R → R is defined by a ⊕ b = a + b – 1, prove that ⊕ has an identity. If x ∈ R, determine the inverse of x with respect to ⊕, if it exists.

Solution: We are looking for some e ∈ R such that a ⊕ e = a = e ⊕ a ∀ a ∈ R. So we want e ∈ R such that a + e – 1 = a ∀ a ∈ R. Obviously, e = 1 will satisfy this. Also, 1 ⊕ a= a ∀ a ∈ R. Hence, 1 is the identity element of ⊕.

For x ∈ R, if b is the inverse of x, we should have b ⊕ x = 1.

i.e., b + x – 1 = 1, i.e., b = 2 – x. Indeed, (2 – x) ⊕ x = (2 – x) + x – 1 = l.

Also, x ⊕ (2 – x) = x + 2 – x – 1 =l. So, x^{-1} = 2 – x.

Example: Let S be a non-empty set. Consider ℘ (S), the set of all subsets of S. Are ⋃ and ⋂ commutative or associative operations on ℘ (S)? Do identity elements and inverses of elements of ℘ (S) exist with respect to these operations?

Solution: Since A ⋃ B = B ⋃ A and A ⋂ B = B ⋂ A ∀ A, B ∈ ℘ (S), the operations of union and intersection are commutative. You can see that the empty set ϕ and the set S are the identities of the operations of union and intersection, respectively. Since S ≠ ϕ, there is no B ∈ ℘ (S) such that S ⋃ B = ϕ. In fact, for any A ∈ ℘ (S) such that A # IS, A does not have an inverse with respect to union. Similarly, any proper subset of S does not have an inverse with respect to intersection.

When the set S under consideration is small, we can represent the way a binary operation on S acts by a table.

2.1.1 Operation '.' Table

Let *S* be a finite set and * be a binary operation on S. We can represent the binary operation by a square table, called an operation table or a Cayley table. The Cayley table is named after the famous mathematician Arthur Cayley (1821-1895).

To write this table, we first list the elements of S vertically as well as horizontally, in the same order. Then we write a * b in the table at the intersection of the row headed by a and the column headed by b.

For example, if S = (–1, 0, 1) and the binary operation is multiplication, denoted by., then it can be represented by the following table.

.	–1	0	1
–1	(–1) . (–1) = 1	(–1) . 0 = 0	(–1) . 1 = –1
0	0 . (–1) = 0	0.0 = 0	0.1 = –1
1	1 . (–1) = –1	1.0 = 0	1.1 =1

Notes

Conversely, if we are given a table, we can define a binary operation on S. For example, we can define the operation * on *S* = {1, 2, 3} by the following table.

*	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

From this table we see that, for instance, 1 * 2 = 2 and 2 * 3 = 2.

Now 2 * 1 = 3 and 1 * 2 = 2. ∴ 2 * 1 ≠ 1 * 2. That is, * is not commutative.

Again, (2 * 1) * 3 = 3 * 3 = 1 and 2 * (1 * 3) = 2

∴ (2 * 1) * 3 ≠ 2 * (1 * 3). ∴ , * is not associative.

See how much information a mere table can give !

Now consider the following definition.

Definition: Let * be a binary operation on a non-empty set S and let a,, ...,a_{k+1}, ∈ S. We define the product a, * . ... .. * a_{k+1}, as follows:

If k = 1, a, * a_2 is a well defined element in S.

If a_1 * ..... * a, is defined, then

a, * .... . . * a_{k+l} = (a, * . ..... * a,) * a_{k+1}

We use this definition in the following result.

Theorem 2: Let a,, ... ,a_{m+n} be elements in a set S with an associative binary operation *. Then (a, * ..,...* a,) * (a,,, * ...... * a_{m+n}) = a_1 * ...... * a_{m+n}.

Proof: We use induction on n. That is, we will show that the statement is true for n = 1. Then, assuming that it is true for n – 1, we will prove it for n.

If n = 1, our definition above gives us

(a, ...* a,) * a,,, = a, *...... * a_{m+1}.

Now, assume that

(a, *.......* a,) * (a,,, ... a_{m+n-1}) = a, * .... a,,,,

Then

(a, * .... * a) * (a,,, ... a)

= (a_1 *.........* a,) * ((a_{m+1} * ..... * a_{m+n-1}) * a_{m+n})

= ((a, *......* a,,) * (a,,, *......* a,,,)) * a, since * is associative

= (a_1 .... a_{m+n-1}) * a_{m+n} by induction

= a, * .... a, by definition.

Hence, the result holds for all n.

We will use Theorem 2 quite often in this course, without explicitly referring to it.

Now that we have discussed binary operations let us talk about groups.

2.2 Group

After understanding the concept of binary operations. Let us start defining group.

Definition: Let G be a non-empty set and * be a binary operation on G. We say that the pair (G, *) is a **group** if

G 1) * is associative:′

G 2) G contains **an** identity element e for * , and

G 3) every element in G has **an** inverse in G with respect to *.

We will now give some examples of groups.

Example: Show that (Z, +) is a group, but (Z,.) is not.

Solution: + is an associative binary operation on Z. The identity element with respect to + is 0, and the inverse of any $n \in Z$ is $(-n)$. Thus, (Z, +) satisfies GI, G2 md G3. Therefore, it is a group.

Now, multiplication in Z is associative and $1 \in Z$ is the multiplicative identity. But does every element in Z have a multiplicative inverse? No. For instance, 0 and 2 have no inverses with respect to '.' Therefore, (Z,.) is not a group.

Note that (Z,.) is a semigroup since it satisfies GI. So, there exist semigroups that aren't groups!

Actually, to show that (G, *) is a group it is sufficient to show that * satisfies the following axioms.

G 1′) * is associative.

G 2′) $\exists\, e \in G$ such that $a * e = a \;\forall\; a \in G$.

G 3′) Given $a \in G$, 3 $b \in G$ such that $a * b = e$.

What we are saying is that the two sets of axioms are equivalent. The difference between them is the following:

In the first set we need to prove that e is a two-sided identity and that the inverse b of any $a \in G$ satisfies $a * b = e$ and $b * a = e$. In the second set we only need to prove that e is a one-sided identity and that the inverse b of any $a \in G$ only satisfies $a * b = e$.

In fact, these axioms are also equivalent to

G 1″) * is associative.

G 2") 3 $e \in G$ such that $i * a = a \;\forall\; a \in G$.

G 3") Given $a \in G$, 3 $b \in G$ such that $b * a = e$.

Clearly, if * satisfies GI, G2 and G3, then it also satisfies Gl′, G2' and G3'. The following theorem tells us that if * satisfies the second set of axioms, then it satisfies the first set too.

Theorem 3: Let (G, *) satisfy Gl′, G2′ and G3′. Then $e * a = a \;\forall\; a \in G$. Also, given $a \in G$, if $\exists\, b \in G$ such that $a * b = e$, then $b * a = e$. Thus, (G, *) satisfies G1, G2 and G3.

To prove this theorem, we need the following result.

Lemma 1: Let (G, *) satisfy Gl′, G2' and G3'. If $\exists\, a \in G$ such that $a * a = a$, then $a = e$.

Proof: By G3' we know that 3 $b \in G$ such that $a * b = e$.

Now (a * a) * b = a * b = e.

Also a * (a * b) = a * e = a. Therefore, by Gl′, a = e.

Now we will use this lemma to prove Theorem 3.

Proof of Theorem 3: G1 holds since G1 and G1' are the same axiom. We will next prove that G3 is true. Let a ∈ G. By G3' 3 b ∈ G such that a * b = e. We will show that

b * a = e. Now,

(b * a) * (b * a) = (b * (a * b)) * a = (b * e) * a = b * a .

Therefore, by Lemma 1, b * a = e. Therefore, G3 is true.

Now we will show that G2 holds. Let a ∈ G. Then by G2', for a ∈ G, a * e = a. Since G3 holds, ∃ b ∈ G such that a * b = b * a = e. Then

e * a = (a * b) * a = a * (b * a) = a * e = a .

That is, G2 also holds.

Thus, (G, *) satisfies G1, G2 and G3.

Example: Let G = { ±1, ± i }, i = $\sqrt{-1}.$ Let the binary operation be multiplication. Show that (G) is a group.

Solution: The table of the operation is

	1	–1	i	–i
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

This table shows us that a.l = a ∀ a ∈ G. Therefore, 1 is the identity element. It also shows us that (G) satisfies G3. Therefore, (G) is a group.

Note that $G = \{1, x, x^2, x^3\}$, where x = i.

2.2.1 Abelian Group

Definition: If (G, *) is a group, where ***G*** is a finite set consisting of n elements, then we say that (G, *) is a Finite group of order n. If G is an infinite set, then we say that (G,*) is an infinite group.

If * is a commutative binary operation we say that (G, *) is a commutative group, or an abelian group. Abelian groups are named after the gifted young Norwegian mathematician Niels Henrik Abel.

Now let us discuss an example of a non-commutative (or non-abelian) group. Before doing this example recall that an m x n matrix over a Set ***S*** is a rectangular arrangement of elements of S in m rows and n columns.

Note

If A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then ad-bc is called the determinant of A and is written as det A or |A|

Example: Let G be the set of all 2 x 2 matrices with non-zero determinant. That is,

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \; a, b, c, d \in r, ad - bc \neq 0 \right\}$$

Consider G with the usual matrix multiplication, i.e, for

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{and } p = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \text{in G, } A.P = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix}$$

Show that (G, ‘) is a group.

Solution: First we show that . is a binary operation, that is, A, P ∈ G ⇒ A.P ∈ G.

Now,

det (A.P) = det **A.** det P # 0. since det A ≠ 0, det P ≠ 0.

Hence, A.P ≠ G for all A, P in G.

Note det (AB) = (det A) (det B)

We also know that matrix multiplication is associative and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity.

Now, for A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G. the mamx

$$B = \begin{bmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{bmatrix} \text{is such that det } B = \frac{*}{ad - bc} \neq 0 \text{ and } AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, B = A^{-1}. (Note that we have used the axiom G3' here, and not G3.) This shows that the set of all 2 × 2 matrices over R with non-zero determinant forms a group under multiplication. Since

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \text{and}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$$

we see that this group is not commutative.

And now another example of an abelian group.

Example: Consider the set of all translations of R^2,

$$T = \{f_{a,b} : R^2 \to R^2 \mid f_{a,b}(x, y) = (x + a, y + b) \text{ for some fixed } a, b \in R\}$$

Note that each element $f_{a,b}$ in T is represented by a point (a, b) in R^2. Show that (T, o) is a group, where o denotes the composition of functions.

Solution: Let us see if o is a binary operation on T.

Now $f_{a,b}$ o $f_{c,d}$ (x , y) = $f_{a,b}$ (x + c, y + d) = (x + c + a, y + d + b)

= $f_{a+c,\ b+d}$ (x,y) for any (x, y) $\in R^2$.

$\therefore$ $f_{a,b}$ o$f_{c,d}$ = $f_{a+c,\ b+d}$ $\in$ T.

Thus, o is a binary operation on T.

Now, $f_{a,b}$ o $f_{0,0}$ = $f_{a,b}$ $\forall$ $f_{a,b}$ $\in$ T.

Therefore, $f_{0,0}$ is the identity element.

Also, $f_{a,b}$ o $f_{-a,\ -b}$ = $f_{0,0}$ $\forall$ $f_{a,b}$ $\in$ T.

Therefore, $f_{-a,'}$ is the inverse of $f_{a,b}$ $\in$ T.

Thus, (T, o) satisfies G1′, G2' and ***G3',*** and hence is a group.

Note that $f_{a,b}$ o $f_{c,d}$ = $f_{c,d}$ o $f_{a,b}$ $\forall$ $f_{a,b'}$ $f_{c,d}$ $\in$ T. Therefore, (T, o) is abelian.

2.3 Properties of Groups

Before understanding the properties of group lets first give notational conventions.

Convention: Let us, we will **denote a group** (G, *) **by** G, if there is no danger of confusion. We will also **denote a * b by ab,** for a, b $\in$ G, and say that we are multiplying a and b. The letter e will continue to denote the group identity.

Now let us discuss a simple theorem.

Theorem 4: Let G be a group. Then

(a) $(a^{-1})^{-1}$ = a for every a $\in$ G.

(b) $(ab)^{-1} = b^{-1} a^{-1}$ for all a, b $\in$ G.

Proof: (a) By the definition of inverse,

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

But, $a\, a^{-1} = a^{-1} a = e$ also, Thus, by Theorem 1 (b), $(a^{-1})^{-1}$ = a.

(b) For a, b $\in$ G, ab $\in$ G. Therefore, $(ab)^{-1}$ $\in$ G and is the unique element satisfying $(ab)\,(ab)^{-1} = (ab)^{-1}\,(ab) = e$.

However, $(ab)\,(b^{-1} a^{-1}) = ((ab)\, b^{-1})\, a^{-1}$

$= (a\,(b\, b^{-1})\, a^{-1})$

$= (a\, e)\, a^{-1}$

$= aa^{-1}$

$=e$

Similarly, $(b^{-1} a^{-1})\,(ab) = e$.

Thus, by uniqueness of the inverse we get $(ab)^{-1} = b^{-1} a^{-1}$.

Note that, for a group G, $(ab)^{-1} = a^{-1} b^{-1}$ $\forall$ a, b $\in$ G only if G is abelian.

You know that whenever ba = ca or ab = ac for a, b, c in R*, we can conclude that b = C. That is, we can cancel a. This fact is true for any group.

Theorem 5: For a, b, c in a group G,

(a) ab = ac $\Rightarrow$ b = c. (This is known as the left cancellation law.)

(b) ba = ca $\Rightarrow$ b = c. (This is known as the right cancellation law.)

Proof: We will prove (a) and leave you to prove (b).

(a) Let ab = ac. Multiplying both sides on the left hand side by $a^{-1} \forall$ G, we get

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

$\Rightarrow$ (a^{-1} a) b = (a^{-1} a) c

$\Rightarrow$ eb = ec, e being the identity element.

$\Rightarrow$ b = c.

Now let us prove another property of groups.

Theorem 6*:* For elements a. b in a group G, the equations ax = b and ya = b have unique solutions in G.

Proof: We will first show that these linear equations do have solulions in G, and then we will show that the solutions are unique.

For a, b $\in$ G, consider a^{-1} b $\in$ G. We find that a(a^{-1} b) = (aa^{-1}) b = eb = b. Thus, a^{-1} b satisfies the equation ax = b, i.e., ax = b has a solution in G.

But is this the only solution? Suppose x_1, x_2 are two solutions of ax = b in G. Then ax, = b = ax_2. By the left cancellation law, we get $x_1 = x_2$. Thus, a^{-1} b is the unique solution in G.

Similarly, using the right cancellation law, we can show that ba^{-1} is the unique solution of ya = b in G.

Now we will illustrate the property given in Theorem **6.**

Example: Consider $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in GL, (R)

Find the solution of AX = B.

Solution: From Theorem 6, we know that **X** = A^{-1} B. Now,

$$A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

$$\therefore \qquad A^{-1}B = \begin{bmatrix} 2 & -2 \\ -1 & 3 \end{bmatrix} = X.$$

In the next example we consider an important group.

Example: Let S be a non-empty set. Consider $\wp$ (S) with the binary operation of symmetric difference A, given by

A Δ B=(A\B) $\cup$ (B\A) $\forall$ A, B $\in$ $\wp$ (S).

Show that ($\wp$ (S), A) is an abelian group. What is the unique solution for the equation Y Δ A=B?

Solution: A is an associative binary operation. This can be seen by using the facts that A\B=A $\cap$ B^C, $(A \cap B)^C = A^C \cup B^C$, $(A \cup B)^C = A^C \cap B^C$

Notes

and that ⋃ and ⋂ are commutative and associative. A is also commutative since A A B = B Δ A ∀ A, B ∈ ℘ (S).

Also, ϕ is the identity element since A A ϕ = A ∀ A ∈ ℘ (S).

Further, any element is its own inverse, since A A A = ϕ ∀ A ∈ ℘ (S).

Thus, (℘ (S). A) is an abelian group.

For A, B in (℘ (S), A) we want to solve Y A A = B. But we know that A is its own inverse. So, by Theorem 6, Y = B A A^{-1} = B A A is the unique solution. What we have also proved is that (B A A) A A = B for any A, B in ℘ (S).

Definition: Let G be a group. For a ∈ G, we define

(i) $a^0 = e$.

(ii) $a^n = a^{n-1} . a$, if n > 0

(iii) $a^{-n} = (a^{-1})n$, if n > 0.

n is called the exponent (or index) of the integral power a^n of a.

Thus, by definition $a^1 = a$, $a^2 = a . a$, $a^3 = a^2 . a$, and so on.

Notes When the notation used for the binary operation is addition, a^n becomes na. For example, f a any a ∈ Z,

na = 0 if a = 0,

na = a + a+ ... +a (n times) if n > 0,

na = (–a) + (–a) + ... + (–a) (–n times) if n < 0.

Let us now prove some laws of indices for group elements.

Theorem 7: Let G be a group. For a ∀ G and m, n ∀ Z,

(a) $(a^n)^{-1} = a^{-n} = (a^{-1})^n$, (b) $a^m, a^n = a^{m+n}$, (c) $(a^m)^n = a^{mn}$

Proof: We prove (a) and (b), and leave the proof of (c) to you.

(a) If n = 0, clearly $(a^n)^{-1} = a^{-0} = (a^{-1})^n$.

Now suppose n > 0. Since $aa^{-1} = e$, We see that

$e = e^n = (aa^{-1})^n$

$= (aa^{-1}) (aa^{-1}) .... (aa^{-1})$ (n times)

$= a^n (a^{-1})^a$, since a and a^{-1} compute.

∴ $(a^n)^{-1} = (a^{-1})^n$.

Also, $(a^{-1})^n = a^{-n}$, by definition.

∴ $(a^n)^{-1} = (a^{-1})^a = a^{-a}$ when n > 0.

If n < 0, then (–n) > 0 and

$(a^n)^{-1} = [a^{-(n)}]^{-1}$

$= [(a^{-a})^{-1}\}^{-1}$, by the case n > 0

= ad

Also, $(a^{-1})^{n} = (a^{-l})^{-(-n)}$

$= [(a^{-1})^{-1}]^{-n}$, by the case n > 0

= a*.

So, in this case too,

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

(b) If m = 0 or n = 0, then $a^{m+n} = a^{m} . a^{n}$. Suppose m ≠ 0 and n ≠ 0.

Case 1 (m > 0 and n > 0): We prove the proposition by induction on n.

If n = 1, then $a^{m} . a = a^{m+1}$, by definition.

Now assume that $a^{m} . a^{n-1} = a^{m+n-1}$

Then, $a^{m} . a^{n} = a^{m}(a^{n-1} . a) = (a^{m} . a^{n-1}) a = a^{m+n-1} . a = a^{m+n}$. Thus, by the principle of induction, (a) holds for all m > 0 and n > 0.

Case 2 (m < 0 and n < 0): Then **(**-m) 0 and (-n) > 0. Thus, by Case 1, $a^{-n} . a^{-m} = a^{-(n+m)} = ad^{wn})$. Taking inverses of both the sides and using (a), we get,

$g^{m+n} = (a^{-n} . a^{-m})^{-1} = (a^{-m})^{-1} . (a^{-n})^{-1} = a^{m} . a^{n}$.

Case 3 (m > 0, n < 0 such that m + n ≥ 0): Then, by Case 1, $a^{m+n} . a^{-n} = a^{m}$. Multiplying both sides on the right by $a^{n} = (a^{-n})^{-1}$, we get $a^{m+n} = a^{m}. a^{n}$.

Case 4 (m > 0, n < 0 such that m+n < 0): By Case 2, $a^{-m}. a^{m+n}$= an. Multiplying both sides on the left by $a^{m} = (a^{-m})^{-1}$, we get $a^{m+n} = a^{m} . a^{n}$.

The cases when m < 0 and n > 0 are similar to Cases 3 and 4. Hence, $a^{wn} = a^{m} . a^{n}$ for all a ∈ G and m, n ∈ Z.

2.4 Different Types of Group

2.4.1 Integers Modulo n

Consider the set of integers, Z, and n ∈ N. Let us define the relation of congruence on Z by : a is congruent to b modulo n if n divides a-b. We write this as a ≡ b (mod n). For example, 4 ≡ 1 (mod 3), since 3 | (4-1).

Similarly, (-5) ≡ 2(mod 7) and 30 ≡ 0 (mod 6).

≡ is an equivalence relation, and hence partitions Z into disjoint equivalence classes called congruence classes modulo n. We denote the class containing r by $\bar{r}$.

Thus, $\bar{r}$ ={ m ∈ Z | m ≡ r (modn) }.

So an integer m belongs to $\bar{r}$ for some r, 0 ≤ r < n, iff n | (r-m), i.e., iff r–m = kn, for some k ∈ Z.

∴ $\bar{r}$ = { r + kn | k ∈ Z }

Now, if m ≥ n, then the division algorithm says that m = nq + r for some q, r ∈ Z, 0 ≤ r < n. That is, m ≡ r (mod n), for some r = 0, .,..., n-1. Therefore, all the congruence classes modulo n are $\bar{0}, \bar{1}, ..., \overline{n-1}$. Let $Z_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$. We define the operation + on Z_n by $\bar{a} + \bar{b} = \overline{a+b}$.

Notes

Is this operation well defined? To check this, we have to see that if $\bar{a}=\bar{b}=\bar{c}=\bar{d}$ in Z_n, then $\bar{a}+\bar{b}=\overline{c+d}$.

Now, a ≡ b (mod n) and c ≡ d (mod n). Hence, there exist integers k_1 and k_2 such that a – b = k_1n and c – d = k_2n. But then (a + c) – (b + d) = (a – b) + (c – d) = (k_1 + k_2)n.

$\therefore \quad \overline{a+c}=\overline{b+d}$.

Thus, + is a binary operation on Z.

For example, $\bar{2}+\bar{2}=\bar{0}$ in Z_4 since 2 + 2 = 4 and 4 ≡ 0(mod 4).

Now, let us show that (Z_n, +) is a commutative group.

(i) $\bar{a}+\bar{b}=\overline{a+b}=\overline{b+a}=\bar{b}+\bar{a}\ \forall\ \bar{a},\bar{b}\in Zn$, i.e.,

addition is commutative in Z

(ii) $\bar{a}+\left(\bar{b}+\bar{c}\right)=+\left(\overline{b+c}\right)=\overline{a+(b+c)}$

$=\overline{(a+b)+c}=(\overline{a+b})+\bar{c}=(\bar{a}+\bar{b})+\bar{c}\ \forall\ \bar{a},\bar{b},\bar{c}\in Z_n$,

i.e., addition is associative in **Z**,.

(iii) $\bar{a}+\bar{0}=\bar{a}=\bar{0}+\bar{a}\ \forall\ \bar{a}\in$ Z,, i.e., $\bar{0}$ is the identity for addition,

(iv) ~ or ; ∈ Z_n, $\exists\ \overline{n-Z_n}$ such that $\bar{a}+\overline{n-a}=n=0=\bar{n}-\overline{a+}\,a$.

Thus, every element $\bar{a}$ in Z_n has an inverse with respect to addition.

The properties (i) to (iv) show that (Z_n, +) is an abelian group.

Actually we can also define multiplication on $\mathbf{Z}_n$ by $\bar{a}\,.\,\bar{b}=\overline{ab}$. Then, $\bar{b}=\bar{b}\,\bar{a}\ \forall\ a,\bar{b}\in Z_n$. Also, $(\bar{a}\,\bar{b})\bar{c}=\bar{a}(\bar{b}\,\bar{c})\ \forall\ \bar{a},\bar{b},\bar{c}\in Z_n$. Thus, multiplication in Z_n is a commutative and associative binary operation.

Z, also has a multiplicative identity, namely, $\bar{1}$.

But (Z,, .) is not a group. This is because every element of Z_n, for example $\overline{Q}$, does not have a multiplicative inverse.

But, suppose we consider the non-zero elements of Z_n, that is, $\left(Z_n^*,.\right)$. Is this a group? For example, $Z_4^*=\left\{\bar{1},\bar{2},\bar{3}\right\}$ is not a group because* is not even a binary operation on Z_4^*, since $\bar{2}\,.\,\bar{2}=\bar{0}\in Z_4^*$. But $\left(Z_-^*,.\right)$ is an abelian group for any prime p.

2.4.2 The Symmetric Group

We will now discuss the symmetric group briefly. In Next Unit we will discuss this group in more detail.

Let X be a non-empty set. We have seen that the composition of functions defines a binary operation on the set F(X) of all functions from X to X. This binary operation is associative.

I_X, the identity map, is the identity in F(X).

Now consider the subset S(X) of F(X) given by

S(X) = {f $\in$ F(X) | f is bijective }.

So f $\in$ S(X) iff $f^{-1}: X \to X$ exists. Remember that f o f^{-1} = f^{-1} . o f = I_X. This also shows that $f^{-1} \in$ S(X).

Now, for all f, g in S(X),

(g o f) o (f^{-1} o g^{-1}) = I_X = (f^{-1} o g^{-1}) o (g o f), i.e., g o f $\in$ S(X).

Thus, o is a binary operation on S(X).

Let us check that (S(X), o) is a group.

(i) o is associative since (fog) o h = f o (g o h) $\forall$ f, g, h E S(X).

(ii) I_X is the identity element because f o I_X = I_X o f $\forall$ f $\in$ S(X).

(iii) f^{-1} is the inverse off, for any f $\in$ S(X).

Thus, (S(X), o) is a group. It is called the symmetric group on X.

If the set X is finite, say X = (1, 2, 3 ...... n), then we denote S(X) by S,, and each f $\in$ S, is called a permutation on n symbols.

Suppose we want to construct an element f in S_n. We can start by choosing f(1). Now, f(1) can be any one of the n symbols 1,2, ... n. Having chosen f(l), we can choose f(2) from the set { l,2 .... n } \ { f(l) }, i.e., in (n – 1) ways. This is because f is 1 – 1. Inductively, after choosing f(i), we can choose f(i + l) in (n – i) ways. Thus, f can be chosen in (1 × 2 × .... × n) = n ! ways, i.e., S_n contains n ! elements.

For our convenience, we represent f $\in$ S, by

$$\begin{pmatrix} 1 & 2 & .... & n \\ f(1) & f(2) & .... & f(n) \end{pmatrix}$$

For example, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ represents the function f : (1, 2. 3. 4) → {1. 2, 3. 4) : f (1) = **2,** f(2) = 4, f (3) = **3,** f (4) = 1. The elements in the top row can be placed in any order as long as the order of the elements in the bottom row is changed accordingly.

Thus, $\begin{pmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ also represents the same function f.

Definition: We say that f $\in S_n$ is a cycle of length r if there are x,, ..., x, in X = { 1, 2, ..., n) such that $f(x_i) = x_{i+1}$ for $1 \le i \le r - 1$, $f(x_r) = x_1$ and f(t) = t for t # x, ..., x,. In this case f is written as (x_1 .... x,).

For example, by f = (2 4 5 10) $\in S_{10}$, we mean f (2) = 4, f (4) = 5, f (5) = 10, f (10) = 2 and f (j) = j for j # 2, 4, 5, 10.

$$\text{i.e., } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$$

Notes

Note In the notation of a cycle, we don't mention the elements that are left fixed by the permutation. Similarly, the permutation $\begin{pmatrix} 2 & 5 \\ 5 & 3 \end{pmatrix}$ is the cycle (1 2 5 3 4) in S_5.

Now let us see how we calculate the composition of two permutations. Consider the following example in S_5.

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha\beta(1) & \alpha\beta(2) & \alpha\beta(3) & \alpha\beta(4) & \alpha\beta(5) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(5) & \alpha(3) & \alpha(4) & \alpha(1) & \alpha(2) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2 \quad 4).$$

since 1, 3 and 4 are left fixed.

And now let us talk of a group that you may be familiar with, without knowing that it is a group.

2.4.3 Complex Numbers

In this sub-section we will show that the set of complex numbers forms a group with respect to addition. Some of you may not be acquainted with some basic properties or complex numbers.

Consider the set C of all ordered pairs (x, y) of real numbers. i.e.. we take C = R × R. Define addition (+) and multiplication (.) in C as follows:

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and

$(x_1, Y_1) . (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$

for $(x_1 . y_1)$ and (x_2, y_2) in C.

This gives us an algebraic system (C, +, .) called the system of complex numbers. We must remember that two complex numbers (x_1, y_1) and (x_2, y_2) are equal iff $x_1 = x_2$ and $y_1 = y_2$.

You can verify that + and . are commutative and associative.

Moreover,

(i) (0, 0) is the additive identity.

(ii) for (x, y) in C, (–x, –y) is its additive inverse.

(iii) (1, 0) is the multiplicative identity.

(iv) if $(x, y) \neq (0, 0)$ in C, then either $x^2 > 0$ or $y^2 > 0$.

Hence, $x^2 + y^2 > 0$. Then

Notes

$$(x, y).\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$$

$$= \left(x\,.\frac{x}{x^2+y^2} - y\,.\frac{(-y)}{x^2+y^2}, x\,.\frac{-y}{x^2+y^2} + y\frac{x}{x^2+y^2}\right)$$

= (1, 0)

Thus, $\left(\frac{x}{x^2+y^2}, \quad \frac{-y}{x^2+y^2}\right)$ is the multiplicative inverse of (x, y) in C.

Thus, (C, +) is a group and (C*,.) is a group. (As usual, C* denotes the set of non-zero complex numbers.)

Now let us see what we have covered in this unit.

Self Assessment

1. For a binary operation * on S and (a, b) $\in$ S × S, we denote *(a, b) by ....

   (a) a * b (b) (a, b)*

   (c) ab* (d) ba*

2. Binary operations associates a .... of S to every ordered pair of elements of S.

   (a) same element (b) different element

   (c) unique element (d) single set element

3. Suppose their exist a, b $\in$ S such that S * a = e = a * s and S * b = e = b * s, e being the identity element for *, then

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

   (c) $a^{-1} = b$ (d) $a^2 = b$

4. For x $\in$ R, if b is inverse of x, the you should have $b \oplus x = 1$. Then x^{-1} is equal to

   (a) 2 – x (b) x – 2

   (c) 2^{-1} x (d) $2 + x^{-1}$

5. .... are named after the gifted young Norwegian mathematician Niels Henrik Abel.

   (a) Abelian group (b) Sub group

   (c) Normal group (d) Cyclic group

2.5 Summary

- Here we discussed various types of binary operations.
- Also defined and given examples of groups.
- We proved and used the cancellation laws and laws of indices for group elements.
- In this unit we discussed the group of integers modulo n, the symmetric group and the group of complex numbers.

Notes

2.6 Keywords

Binary Operation: A *binary operation* on S is always closed on S, but may not be closed on a subset of S.

Abelian Group: If (G, *) is a group, where G is a finite set consisting of n elements, then we say that (G, *) is a Finite group of order n. If G is an infinite set, then we say that (G,*) is an infinite group.

2.7 Review Questions

1. Obtain the identity element, if it exists, for the operations $\begin{Bmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{Bmatrix}$.

2. For $x \in R$, obtain x^{-1} (if it exists) for each of the operations $\begin{Bmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{Bmatrix}$.

3. Show that (Q, +) and (R, +) are groups.

4. Calculate (1 3) ° (1 2) in S3.

5. Write the inverse of the following in S_3:

   (a) (1 2)

   (b) (1 3 2)

   Show that $(1\ 2) \circ (1\ 3\ 2)^{-1} \neq (1\ 2)^{-1} \circ (1\ 3\ 2)^{-1}$. (This shows that in Theorem 4(b) we can't write (ab)-1 = $a^{-1}b^{-1}$.)

2.8 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 3: Subgroups

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define subgroups
- Explain the intersection, union and product of two subgroups
- Describe structure and properties of cyclic groups

Introduction

In the last unit, you have studied about the algebraic structures of integers, rational numbers, real numbers and complex numbers. You have got an idea that, not only is $Z \subseteq Q \subseteq R \subseteq C$, but the operations of addition and multiplication coincide in these sets. In the present unit, you will go through more examples of subsets of groups which are groups in their own right. Such structures are rightfully named subgroups. We will discuss some of their properties also. We will see some cases in which we obtain a group from a few elements of the group. In particular, we will study cases of groups that can be built up by a single element of the group.

3.1 Subgroups

In the previous unit, you have already read the concept of group. You also noted that group (Z+), (Q+) and (R+) are the member of a bigger group (C+) complex number. These all groups that contained in bigger group are not just subsets but groups.

All these are examples of subgroup. Lets define subgroup.

Definition: Let (G,*) be a group. A non-empty subset H of G is called a subgroup of G if

(i) $a * b \in H \ \forall \ a, b \in H$, i.e., * is a binary operation on H,

(ii) (H,*) is itself a group.

So, by definition, (Z,+) is a subgroup of (Q,+), (R,+) and (C,+).

Now, if (H,*) is a subgroup of (G,*), can the identity element in (H,*) be different from the identify element in (G,*)? Let us see. If h is the identity of (H,*), then, for any $a \in H$, $h * a = a * h = a$. However, $a \in H \subseteq G$. Thus, $a * e = e * a = a$, where e is the identity in G. Therefore, $h * a = e * a$.

By right cancellation in (G,*)w,e get h = e.

Thus, whenever (H, *) is a subgroup of (G,*), $e \in H$.

Remark 1: (H,*) is a subgroup of (G, *) if and only if

(i) $e \in H$,

(ii) $a, b \in H \Rightarrow a * b \in H$,

(iii) $a \in H \Rightarrow a^{-1} \in H$.

We would also like to make an important remark about notation here.

Remark 2: If (H,*) is a subgroup of (G,*), we shall just say that H is a subgroup of G, provided that there is no confusion about the binary operations. We will also denote this fact by $H \leq G$.

Now let us first discuss an important necessary and sufficient condition for a subset to be a subgroup.

Theorem 1: Let H be a **non-empty** subset of a group G. Then H is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: Firstly, let us assume that $H \leq G$. Then, by Remark l, $a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$.

Conversely, since $H \neq \phi$, $\exists\, a \in H$. But then, $aa^{-1} = e \in H$.

Again, for any $a \in H$, $ea^{-1} = a^{-1} \in H$.

Finally, if $a, b \in H$, then $a, b^{-1} \in H$. Thus, $a\,(b^{-1})^{-1} = ab \in H$, i.e.,

H is closed under the binary operation of the group.

Therefore, by Remark 1, H is a subgroup.

Note A subgroup of an abelian group is abelian.

Example: Consider the group **(C*.,)**. Show that

S = { z C | |z| = 1 } is a subgroup of C*.

Solution: $S \neq \phi$, since $1 \in S$. Also, for any $z_1, z_2 \in S$,

$$|z_1 z_2^{-1}| = |z_1|\ |z_2^{-1}| = |z_1| \frac{1}{|z_2|} = 1.$$

Hence, $z_1 z_2^{-1} \in S$. Therefore, by Theorem 1, $S \leq C^*$.

Example: Consider G = $M_{2\times 3}$ (C), the set of all 2 × 3 matrices over C. Check that (G,+) is an abelian group. Show that

$$S = \left\{ \begin{matrix} 0 & a & b \\ 0 & 0 & c \end{matrix} \;\middle|\; a, b, c \in C \right\} \text{ is a subgroup of G.}$$

Solution: We define addition on G By

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} p & q & r \\ s & t & u \end{bmatrix} = \begin{bmatrix} a+p & b+q & c+r \\ d+s & e+t & f+u \end{bmatrix}$$

You can see that + is a binary operation on G. 0 = $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is the additive identity and $\begin{bmatrix} -a & -c \\ -d & -f \end{bmatrix}$

is the inverse of $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \in$ G.

Since, a + b = b + a $\forall$ a, b $\in$ C, + is also abelian.

Therefore, (G,+) is an abelian group.

Now, since O $\in$ S, S $\neq \phi$. Also for

$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in S$, we see that

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \equiv S.$$

= S I G.

Example: Consider the set of all invertible 3 × 3 matrices over R, GL_3 (R). That is, A $\in$ GL_3(R) iff det (A) $\neq$ 0. Show that SL_3 (R) = (A $\in$ GL_3(R) | det(A) = I) is a subgroup of (GL_3(R),.).

Solution: The 3 × 3 identity matrix is in SL_3(R). Therefore, SL_3(R) $\neq \phi$.

Now, for A, B $\in$ SL_3(R),

det (AB^{-1}) = det (A) det(B^{-1}) = $\frac{1}{\det(B)} - 1,$ since det (A) = 1 and det (B) = I.

$\therefore$ $AB^{-1} \in SL_3(R)$

$\therefore$ SL_3(R) I GL_3(R).

Example: Any non-trivial subgroup of (Z, +) is of the form mZ, where m $\in$ N and mZ = { mt | t $\in$ Z) = { 0, ± m, ± 2m, ± 3m,.......).

Solution: We will first show that mZ is a subgroup of Z. Then we will show that if H is a subgroup of Z, H # {0}, then H = mZ, for some m $\in$ N.

Notes

Now, $0 \in mZ$. Therefore, $mZ \neq \phi$. Also, for mr, ms $\in$ mZ, mr-ms = m(r-s) $\in$ mZ.

Therefore, mZ is a subgroup of Z.

Note that m is the least **positive integer in mZ.**

Now, let $H \neq (0)$ be a subgroup of Z and S = { i | i > 0, i $\in$ H).

Since H # {0), there is a non-zero integer k in H. If k > 0, then k $\in$ S. If k < 0, then (-k) $\in$ S, since (–k) $\in$ H and (–k) > 0.

Hence, $S \neq \phi$.

Clearly, $S \subseteq N$. Thus, by the well-ordering principle S has a least element, say s. That is, s is the least positive integer that belongs to H.

Now $sZ \subseteq H$. Why? Well, consider any element st $\in$ sZ.

If t = 0, then st = 0 $\in$ H.

If t > 0, then st = s + s + ... + s (t times) $\in$ H.

If t < 0, then st = (–s) + (–s) + ...+ (–s) (–t times) $\in$ H.

Therefore, st $\in$ H $\forall$ t $\in$ Z. That is, $sZ \subseteq H$.

Now, let m $\in$ H. By the division algorithm m = ns + r for some n, r $\in$ Z, $0 \le r < s$. Thus, r = m – ns. But H is a subgroup of Z and m, ns $\in$ H. Thus, r $\in$ H. By minimality of s in S, we must have r = 0, i.e., m = ns. Thus, $H \subseteq sZ$.

So we have proved that H = sZ.

You know that the polar form of a non-zero complex number z $\in$ C is z = r (cos θ + i sine), where r = | z | and θ is an argument of z. Moreover, if θ_1, is an argument of z_1 and θ_2 that of z_2. then $\theta_1 + \theta_2$ is an argument of $z_1 z_2$. Using this we will try to find the nth roots of 1, where n $\in$ N.

If z = r (cos θ + i sin !) is an nth root of 1, then $z^n = 1$.

Thus, by De Moivre's theorem,

$1 = z^n = r^n (\cos n\theta + i \sin n\theta)$, that is,

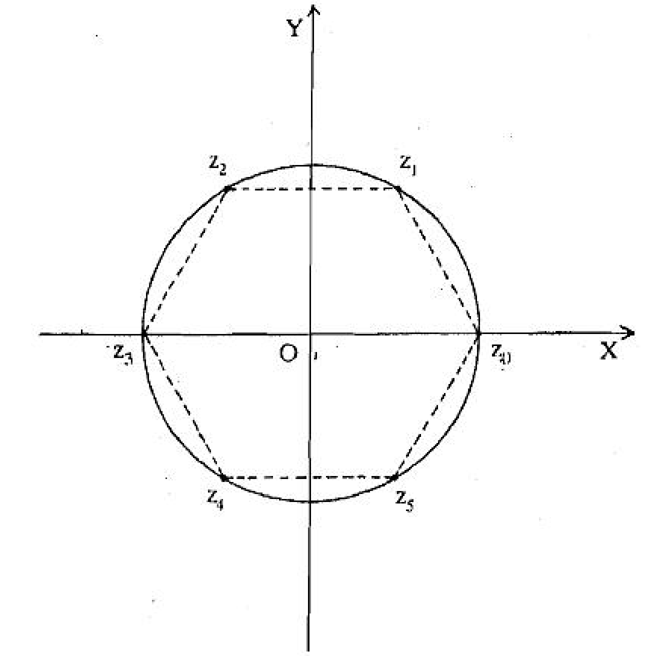
$\cos (0) + i \sin (0) = r^n (\cos n\theta + i \sin n\theta)$. .... (1)

Equating the modulus of both the sides of (1). we get $r^n = 1$, i.e., r =l.

On comparing the arguments of both sides of (1), we see that 0 + 2nk (k $\in$ Z) and nθ are arguments of the same complex number. Thus, nθ can take any one of the values 2πk, k $\in$ Z. Does this mean that as k ranges over Z and θ ranges over $\frac{2nk}{n}$ we get distinct nth roots of 1? Let us find out. Now, cos $\frac{2nk}{n}$ + i sin $\frac{2zk}{n}$ = $\cos\frac{2\pi m}{n} + i\sin\frac{2\pi m}{n}$ if and only if $\frac{2nk}{n} - \frac{2nm}{n} = 2nt$ for some t $\in$ Z. This will happen iff k = m + nt, i.e., $k \equiv m \pmod{n}$. Thus, corresponding to every $\bar{r}$ in Z, we get an nth root of unity, z = $\cos\frac{2\pi r}{n} + i\sin\frac{2\pi r}{n}, 0 \le r < n$; and these are all the nth roots of unity.

For example, If n = 6, we get the 6th roots of 1 as z_0, z_1, z_2, z_3, z_4 and z_5, where zj = $\cos\frac{2\pi j}{6} + i\sin\frac{2\pi j}{6}, j = 0,1,2,3,4,5.$ In Figure 3.1 you can see that all these lie on the unit circle (i.e., the circle of radius one with centre (0, 0)). They form the vertices of a regular hexagon.

Figure 3.1: 6th Roots of Unity



Now, let ω = $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then all the nth roots of 1 are 1, ω, ω^2, ...,ω^{n-1}, since

$\omega^j = \cos\frac{2\pi j}{n} + i\sin\frac{2\pi j}{n}$ for $0 \le j \le n-1$ (using De Moivre's theorem).

Note ω is the Greek letter omega.

Example: Show that $U_n \le (C', .)$.

Solution: Clearly, U, # 0. Now, let ω^1, $\omega^j \in$ U,.

Then, by the division algorithm, we can write i + j = qn + r for q, r ∈ Z, 0 ≤ r ≤ n – 1. But then $\omega^i . \omega^j = \omega^{i+j} = \omega^{qn+r} = (\omega^n)^q . \omega^r = \omega^r \in$ U,, since $\omega^n = 1$. Thus, U, is closed under multiplication.

Finally, if $\omega^i \in$ U,, then 0 ≤ n – i ≤ n – 1 and $\omega^i . \omega^{n-i} = \omega^n = 1$; i.e., ω^{n-i} is the inverse of o^i for all 1 ≤ i < n. Hence, U_n is a subgroup of C*.

Note that U_n, is a finite group of order n and is a subgroup of an infinite group, C*. So, for every natural number n we have a finite subgroup of order n of C*.

Before ending this we will introduce you to a subgroup that you will use off and on.

Definition: The centre of a group G, denoted by Z(G), is the set

z(G) = {G ∈ G | xg = gx ∀ x ∈ G}.

Thus, Z(G) is the set of those elements of G that commute with every element of G.

For example, if G is abelian, then Z(G) = G.

We will now show that $Z(G) \leq G$.

Theorem 2: The centre of any group G is a subgroup of G.

Proof: Since $e \in Z(G)$, $Z(G) \neq \phi$. Now,

$a \in Z(G) \Rightarrow ax = xa \ \forall \ x \in G$.

$\Rightarrow x = a^{-1} xa \ \forall \ x \in G$, pre-multiplying by a^{-1}.

$\Rightarrow xa^{-1} = a^{-1} x \ \forall \ x \in G$, post-multiplying by a^{-1}.

$\Rightarrow a^{-1} \in Z(G)$.

Also, for any $a, b \in Z(G)$ and for any $x \in G$, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x (ab)$.

$\therefore \quad ab \in Z(G)$.

Thus, Z(G) is subgroup of G.

3.2 Properties of Subgroups

After discussing the term subgroup let us start understanding the important properties of subgroup.

Theorem 3: Let G be a group, H be a subgroup of G and K be a subgroup of H. Then K is a subgroup of G.

Proof: Since $K \leq H$, $K \neq \phi$ and $ab^{-1} \in K \ \forall \ a, b \in K$. Therefore, $K \leq G$.

Let us discuss at subgroups of Z, in the context of Theorem 3.

Example: In earlier example we have seen that my subgroup of Z is of the form mZ for some $m \in N$. Let mZ and kZ be two subgroups of Z. Show that rnZ is a subgroup of kZ iff $k \mid m$.

Solution: We need to show that $mZ \subseteq kZ \Leftrightarrow k \mid m$. Now $mZ \subseteq kZ \Rightarrow m \in mZ \subseteq kZ \Rightarrow m \in kZ \Rightarrow m = kr$ for some $r \in Z \Rightarrow k \mid m$.

Conversely, suppose $k \mid m$.

Then, $m = kr$ for some $r \in Z$. Now consider any $n \in mZ$, and let $t \in Z$ such that $n = mt$.

Then $n = mt = (kr)\ t = k(rt) \in kZ$.

Hence, $mZ \subseteq kZ$.

Thus, $mZ \subseteq kZ$ iff $k \mid m$.

Theorem 4: If H and K are two subgroups of a group G, then $H \cap K$ is also a subgroup of G.

Proof: Since $e \in H$ and $e \in K$, where e is the identity of G, $e \in H \cap K$.

Thus, $H \cap K \neq \phi$.

Now, let $a, b \in H \cap K$. By Theorem 1 , it is enough to show that $ab^{-1} \in H \cap K$. Now, since $a, b \in H$, $ab^{-1} \in H$. Similarly, since $a, b \in K$, $ab^{-1} \in K$. Thus, $ab^{-1} \in H \cap K$.

Hence, $H \cap K$ is a subgroup of G.

Notes

The whole argument of Theorem 4 remains valid if we take a family of subgroups instead of just two subgroups. Hence, we have the following result.

Theorem 4 (a): If $\{H_i\}_{i \in 1}$ is a family of subgroups of a group G, then $\bigcup_{i \in 1} H_i$ H_i is also a subgroup of *G*.

Now question arises that does the union of two or more subgroup is again a subgroup. Lets see its true or not. Consider the, two subgroups 2Z and 3Z of Z. Let S = 2Z $\bigcup$ 32. Now, 3 $\in$ 32 $\subseteq$ S, 2 $\in$ 22 $\in$ S, but 1 = 3 – 2 is neither in 2Z nor in 3Z. Hence, S is not a subgroup of (Z, +). Thus, if A and B are subgroups of G, A $\bigcup$ B need not be a subgroup of G. But, if A $\in$ B, then A $\bigcup$ B = B is a subgroup of G. The next exercise says that this is the only situation in which A $\bigcup$ B is a subgroup of G.

Let us now see what we mean by the product of two subsets of a group G.

Definition: Let G be a group and A, B be non-empty subsets of G.

The product of A and B is the set AB = { ab | a $\in$ A, b $\in$ B).

For example, (2Z) (3Z) = { (2m) (3m) | m, n $\in$ Z)

= { 6mn | m, n $\in$ Z }

= 62.

In this example we find that the product of two subgroups is a subgroup. But is that always so? Consider the group

S_3 = {I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}, and its subgroups H = { I, (1 2) } and K = { I, (1 3)).

(Remember, (1 2) is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and (1 2 3) is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Now HK = {I × I , I × (1 3), (1 2) × I,(1 2) × (1 3)}

= { I, (1 3), (1 2), (1 3 2) }

HK is not a subgroup of G, since it is not even closed under composition. (Note that (1 3) $\circ$ (1 2) = (1 2 3) $\notin$ HK.)

So, when will the product of two subgroups be a subgroup? The following result answers this question.

Theorem 5: Let H and K be subgroups of a group G. Then HK is a subgroup of G if and only if HK = KH.

Proof: Firstly, assume that HK $\leq$ G. We will show that HK = KH; Let hk $\in$ HK. Then

$(hk)^{-1} = k^{-1} h^{-1} \in$ HK, since HK $\in$ G.

Therefore, $k^{-1} h^{-1} = h_1 k_1$ for some $h_i \in H$, $k_1 \in K$. But then $hk = (k^{-1} h^{-1})^{-1} = k_1^{-1} h_1^{-1} \in$ KH. Thus, HK $\subseteq$ KH.

Now, we will show that KH $\subseteq$ HK. Let kh $\in$ KH. Then $(kh)^{-1} = h^{-1} k^{-1} \in$ HK. But HK $\leq$ G. Therefore, $((kh)^{-1})^{-1} \in$ HK, that is, kh $\in$ HK. Thus, KH $\subseteq$ HK.

Hence, we have shown that HK = KH.

Conversely, assume that HK = KH. We have to prove that HK $\leq$ G. Since $e = e^2 \in$ HK, HK $\neq \phi$. Now, let a, b $\in$ HK. Then a = hk and b = $h_1 k_1$ for some h, $h_1 \in$ H and k, $k_1 \in$ K.

Then $ab^{-1} = (hk)\ (k_1^{-1}\ h_1^{-1}) = h\ [\ (kk_1^{-1})\ h_1^{-1}]$.

Now, $(kk_1^{-1})\ h_1^{-1} \in KH = HK$, Therefore, 3 $h_2k_2 \in HK$ such that $(kk_1^{-1})h_1^{-1} = h_2k_2$.

Then, $ab^{-1} = h(h_2k_2) = (hh_2)k_2 \in HK$.

Thus, by Theorem 1, $HK \leq G$.

The following result is a nice corollary to Theorem 5.

Corollary: If H and K are subgroups of an abelian group G, then HK is a subgroup of G.

3.3 Cyclic Groups

Let us understand the meaning of cyclic group.

Let G be any group and S a subset of G. Consider the family F of all subgroups of G that contain S, that is,

$F = \{\ H \mid H \leq G \text{ and } S \subseteq H\ \}$.

We claim that $F \neq \phi$. Why? Doesn't $G \in F$? Now, by Theorem 4'(a), $\bigcup_{H \in F} H$ is a subgroup of G.

Note that

(i) $S \subseteq \bigcup_{H \in F} H$.

(ii) $\bigcup_{H \in F} H$ is the smallest subgroup of G containing S. (Because if K is a subgroup of G containing S, then $K \in F$. Therefore, $\bigcup_{H \in F} H \subseteq K$.)

These observations lead us to the following definition.

Definition: If S is a subset of a group G, then the smallest subgroup of G containing S is called **the subgroup generated by the set S,** and is written as <S>.

Thus, $<S> = \bigcap\ \{\ H \mid H \leq G, S \subseteq H\ \}$.

If $S = \phi$, then $<S> = \{e\}$.

If <S> = G, then we say that G is **generated by the set S,** and that **S** is a **set of** generators of G.

If the set S is finite, we say that G is **finitely generated.**

We will give an alternative way of describing <S>. This definition is much easier to work with than the previous one.

Theorem 6: If S is a non-empty subset of a group G, then

$<S> = \left\{a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k} \mid a_i \in S \text{ for } 1 \leq i \leq k, n_1, \ldots, n_k \in Z\right\}$.

Proof: Let **A** = $\left\{a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k} \mid a_i \in S \text{ for } 1 \leq i \leq k, n_1, \ldots, n_k \in Z\right\}$.

Since $a_1, \ldots, a_k \in S \subseteq <S>$ and <S> is a subgroup of G, $a_1^{n_1} \in <S>$

$\forall\ i = 1, \ldots., k$. Therefore, $a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k} \in <S>$, i.e., $A \subseteq <S>$.

Now, let us see why <S> $\subseteq$ A. We will show that A is a subgroup containing S. Then, by the definition of <S>, it will follow that <S> $\subseteq$ A.

Since any a $\in$ S can be written as a = a^1, S $\subseteq$ A.

Since S $\neq \phi$, A $\neq \phi$.

Now let x, y $\in$ A. Then x = $a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k}$

y = $b_1^{m_1} b_2^{m_2} \ldots . b_r^{m_r}$ a_j , b_j $\in$ S for 1 $\leq$ i $\leq$ k, 1 $\leq$ j $\leq$ r.

Then $xy^{-1} = \left(a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k}\right)\left(b_1^{m_1} b_2^{m_2} \ldots . b_r^{m_r}\right)^{-1}$

$= \left(a_1^{n_1} a_2^{n_2} \ldots\ldots a_k^{n_k}\right)\left(b_1^{-m_1} \ldots . b_1^{m_1}\right) \in A.$

Thus, by Theorem 1, A is a subgroup of G. Thus, A is a subgroup of G containing S. And hence, <S> $\subseteq$ A.

This shows that <S> = A.

Note that, if (G, +) is a group generated by S, then any element of G is of the form n_1 a_1 + n_2 a_2 + ... + n_r a_r, where a_1, a_2,....., a, $\in$ S and n_1, n_2, ..., n_r, $\in$ Z.

For example, Z is generated by the set of odd integers S = { ± 1, f3, ± 5, ...). Let us see why. Let m $\in$ Z. Then m = 2^r_s where r $\geq$ 0 and s $\in$ S. Thus, m $\in$ <S>. And hence, <S> = Z.

Definition: A group G is called a **cyclic group** if G = < {a) > for some a E G. We usually write < {a) > as < a >.

Note that < a > = { a^n | n $\forall$ Z).

A subgroup H of a group G is called a **cyclic subgroup** if it is a cyclic group. Thus, < (12*)* > is a cyclic subgroup of S_3 and 22 = <2> is a cyclic subgroup of Z.

We would like to make the following remarks here.

Remark: (i) If K $\leq$ G and a $\in$ K, then < a > $\subseteq$ K. This is because < a > is the smallest subgroup of G containing a.

(ii) All the elements of < a > = { a^n | n $\in$ Z) may or may not be distinct. For example, take a = (12) $\in$ S_3.

Then < (1 2) > = { I, (1 2)), since $(1\ 2)^2$ = I, $(1\ 2)^3$ = (1 2), and so on.

We will now prove a nice property of cyclic groups.

Theorem 7: Every cyclic group is abelian.

Proof: Let G = < a > = { a^n | n $\in$ Z). Then, for any x, y in G, there exist m, n $\in$ Z such that x = a^m, y = a^n. But, then, xy = a^m. a^n a^{m+n} = a^{n+m} = a^n. a^m = yx. Thus, xy = yx for all x, y in G.

That is G is abelian.

Note Theorem 7 says that every cyclic group is abelian. But this does not mean that every abelian group is cyclic.

Notes

Example: Consider the set K_4 = {e, a, b, ab] and the binary operation on K_4 given by the table.

×	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

The table shows that (K_4, .) is a group.

This group is called the **Klein 4-group,** after the pioneering German group theorist Felix Klein.

Example: Show that $\mathbf{K_4}$ is an abelian but not cyclic.

Solution: From the table we can see that K_4 is an abelian. If it were cyclic, it would have to be generated by e, a, b or ab. Now, < e > = {e}. Also, $a^1 = a$, $a^2 = e$, $a'' = a$, and so on.

Therefore, < a > = { e, a }. Similarly, < b > = { e, b } and < ab > = { e, ab).

Therefore, K_4 can't be generated by e, a, b or ab.

Thus, K_4 is not cyclic.

Theorem 8: Any subgroup of a cyclic group is cyclic.

Proof: Let G = < x > be a cyclic group and H be a subgroup.

If H = {e}, then H = < e >, and hence, H is cyclic.

Suppose H ≠ {e}. Then 3 n ∈ Z such that $x^n \in H$, $n \neq 0$. Since H is a subgroup, $(x^n)^{-1} = x^{-n} \in H$. Therefore, there exists a positive integer m (i.e., n or -n) such that $x_m \in H$. Thus, the set S = {t ∈ N | $x^t \in H$) is not empty. By the well-ordering principle S has a least element, say k. We will show that H = < x^k >.

Now, <x^k > ⊆ H, since $x^k \in H$.

Conversely, let x^n be an arbitrary element in H. By the division algorithm n = mk + r where m, r ∈ Z, $0 \le r \le k - 1$. But then $x^r = x^{n-mk} = x^n \,.\, (x^k)^{-m} \in H$, since $x^n, x^k \in H$. But k is the least positive integer such that $x^k \in H$. Therefore, x^r can be in H only if r = 0. And then, n = mk and $x^n = (x^k)^m \in$ < x^k >. Thus, H ⊆ < x^k >. Hence, H = < x^k >, that is, H is cyclic.

Now, Theorem 8 says that every subgroup of a cyclic group is cyclic. But the converse is not true. That is, we can have groups whose proper subgroups are all cyclic, without the group being cyclic.

Consider the group S_3, of all permutations on 3 symbols. Its proper subgroups are

A = <I>

B = <(1 2)>

C = <(1 3)>

D = <(2 3)>

E = <(1 2 3)>.

As you can see, all these are cyclic. But, you know that S_3 itself is not cyclic.

Now we state a corollary to Theorem 8, in which we write down the important point made in the proof of Theorem 8.

Corollary: Let $H \neq \{e\}$ be a subgroup of $< a >$. Then $H = < a^n >$, where n is the least positive integer such that $a^n \in H$.

Self Assessment

1. Subgroup of an abelian group is ....

   (a) normal (b) abelian

   (c) cyclic (d) homomorphism

2. If H be a non-empty subset of a group G. Then H is a subgroup of G if a, b $\in$ H, then

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

   (c) $ab^{-1} \notin H$ (d) $a \notin H, b^{-1} \in H$

3. .... is a Greek letter omega.

   (a) ω (b) ϕ

   (c) θ (d) π

4. Let G be a group, H be subgroup of G and be subgroup of H then k is a .... of G.

   (a) normal group (b) cyclic group

   (c) abelian group (d) subgroup

5. Let H and k be subgroups of a group G. Then KH = HK then $(HK)^{-1}$ = ...

   (a) $k^{-1}, h^{-1} \in Hk$ (b) $h^k k^h \in Hk$

   (c) $x/h \in Hk$ (d) $H/k \in Hk$

3.4 Summary

In this unit we have covered the following points.

- Here we discussed the definition and examples of subgroups.
- The intersection of subgroups is a subgroup.
- The union of two subgroups H and K is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.
- The product of two subgroups H and K is a subgroup if md only if HK = KH.
- The definition of a generating set.
- A cyclic group is abelian, but the converse need not be true.
- Any subgroup of a cyclic group is cyclic, but the converse need not be true.

3.5 Keywords

Subgroup: Let (G,*) be a group. A non-empty subset H of G is called a subgroup of G if

(i) $a * b \in H \ \forall \ a, b \in H$, i.e., * is a binary operation on H,

(ii) (H,*) is itself a group.

Cyclic Groups: Let G be any group and S a subset of G. Consider the family F of all subgroups of G that contain S, that is, $F = \{ H \mid H \leq G \text{ and } S \subseteq H \}$.

3.6 Review Questions

1. Find all cyclic subgroups of $\mathbf{Z}_{24}^{\times}$.

2. In $\mathbf{Z}_{20}^{\times}$, find two subgroups of order 4, one that is cyclic and one that is not cyclic.

   (a) Find the cyclic subgroup of S_7 generated by the element (1, 2, 3)(5, 7). (b) Find a subgroup of S_7 that contains 12 elements. You do not have to list all of the elements if you can explain why there must be 12, and why they must form a subgroup.

3. In $G = \mathbf{Z}_{21}^{\times}$, show that

4. $H = \{ [x]_{21} \mid x \equiv 1 \pmod 3 \}$ and $K = \{ [x]_{21} \mid x\ 1 \pmod 7 \}$ are subgroups of G.

5. Let G be an abelian group, and let n be a fixed positive integer. Show that

   $$N = \{ g \text{ in } G \mid g = a^n \text{ for some } a \text{ in } G \} \text{ is a subgroup of G.}$$

6. Suppose that p is a prime number of the form $p = 2^n + 1$.

   (a) Show that in $Z_p^{\times}$ the order of $[2]_p$ is 2n.

   (b) Use part (a) to prove that n must be a power of 2.

7. In the multiplicative group $C^{\times}$ of complex numbers, find the order of the elements

   $$\alpha = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \text{ and } \beta = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.$$

8. Let K be the following subset of GL_2 (R).

   $$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| d = a, c = -2b, ad - bc \neq 0 \right\}$$

9. Show that K is a subgroup of GL_2 (R).

10. Compute the centralizer in GL_2 (R) of the matrix $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$.

11. Let G be the subgroup of GL_2 (R) defined by $G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\}$.

12. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Find the centralizers C(A) and C(B), and show that C(A) C(B) = Z(G), where Z(G) is the center of G.

Answers: Self Assessment

1. (b) 2. (a) 3. (a) 4. (d) 5. (a)

3.7 Further Readings

Notes

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Notes

Unit 4: Lagrange's Theorem

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the cosets of a subgroup
- Explain the partition a group into disjoint cosets of a subgroup
- Prove and explain Lagrange's theorem

Introduction

In the last unit, you have studied about the subgroup and different properties of subgroups. In this unit, you will learn the concept of cosets and also see how a subgroup can partition a group into equivalence classes. You can use cosets to prove a very useful result about the number of elements in a subgroup. In the present era, this elementary theorem is known as Lagrange's theorem, though Lagrange proved it for subgroups of S only. Let us understand these concepts with the help of examples and theorem.

4.1 Cosets

First of all we will discuss cosets. Cosets means the product of two subset of a particular group.

In a case when one of the subsets consists of single element only, we will go through a situation i.e.,

$$H(x) = \{hx \mid h \in H\}.$$

where H is a subgroup of G and $x \in G$, we will denote H{x} by Hx.

Definition: Let H be a subgroup of a group G, and let $x \in G$. We call the set

$Hx = \{hx \mid h \in H\}$

a right coset of H in G. The element x is a representative of Hx.

We can similarly define the left coset

$xH=\{xh \mid h \in H\}$.

Note that, if the group operation is +, then the right and left cosets of H in (G,+) represented by $x \in G$ are

$H + x = \{ h + x \mid h \in H\}$ and $x + H = \{ x + h \mid h \in H \}$, respectively.

Example: Show that H is a right as well as a left coset of a subgroup H in a group G.

Solution: Consider the right coset of H in G represented by e, the identity of G. Then

$He = \{ he \mid h \in H \} = (h \mid h \in H \} = H$.

Similarly, eH = H.

Thus, H is a right as well as left coset of H in G.

Example: What are the right cosets of 4Z in Z?

Solution: Now H = 4Z = { ......, -8, - 4, 0, 4, 8, 12, ... }

The right cosets of H are

H + 0 = H, using Example.

H+ 1 ={ ....., –11, –7, –3, 1, 5, 9, 13, ...)

H + 2 = { ....., –10, –6, –2, 2, 6, 10, 14, ...)

H + 3 = { ....., –9, –5, –1, 3, 7, 11, 15, ...)

H + 4 = { ....., –8, –4, 0, 4, 8, 12 ,.....) = H

Similarly, you can see that H + 5 = H + 1, H + 6 = H + 2, and so on.

You can also check that H – 1 = H + 3, H – 2 = H + 2, H – 3 = H + l, and so on.

Thus, the distinct right cosets are H, H + 1, H + 2 and H + 3.

In general, the distinct right cosets of H (= nZ) in Z are H, H + 1, ..., H + (n – 1). Similarly, the distinct left cosets of H (= nZ) in Z are H, 1 + H, 2 + H, ..., (n – 1) + H.

After understanding the concept of cosets. Let us discuss some basic and important properties of cosets.

Theorem 1: Let H be a subgroup of a group G and let $x, y \in G$.

Then

(a) $X \in HX$

(b) $Hx = H \Leftrightarrow x \in H$.

(c) $Hx = H \Leftrightarrow xy^{-1} \in H$.

Proof: (a) Since x = ex and $e \in H$, we find that $x \in Hx$.

(b) Firstly, let us assume that Hx = H. Then, since $x \in Hx$, $x \in H$.

Conversely, let us assume that $x \in H$. We will show that $Hx \subseteq H$ and $H \subseteq Hx$. Now any element of Hx is of the form hx, where $h \in H$. This is in H, since $h \in H$ and $x \in H$. Thus, $Hx \subseteq H$. Again, let $h \in H$. Then $h = (hx^{-l}) x \in Hx$, since $hx^{-1} \in H$.

$\therefore$ $H \subseteq HX$.

Notes

$\therefore$ H = Hx.

(c) $Hx = Hy \Rightarrow Hxy^{-1} = Hyy^{-1} = He = H \Rightarrow xy^{-1} \in H$, by (b)

Conversely, $xy^{-1} \in H \Rightarrow Hxy^{-1} = H = Hxy^{-1}y = Hy \Rightarrow Hx = Hy$.

Thus, we have proved (c).

The properties listed in Theorem 1 are not only true for right cosets.

Note Along the lines of the proof of Theorem 1, we can prove that if H is a subgroup of G and x, y $\in$ G, then

(a) $x \in xH$.

(b) $xH = H \Leftrightarrow x \in H$.

(c) $x H = yH \Leftrightarrow x^{-1}y \in H$.

Example: Let G = Sg = {I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)} and H be the cyclic subgroup of G generated by (1 2 3). Obtain the left cosets of H in G.

Solution: Two cosets are

H = { I, (1 2 3). (1 3 2)) and

(1 2)H = { (1 2), (1 2) × (1 2 3), (1 2) × (1 3 2))

= { (1 2) , (2 3), (1 3)}

For the other cosets you can apply Theorem 1 to see that

(1 2)H = (2 3)H = (1 3)H and

(1 2 3)H = H = (1 3 2)H.

Example: Consider the following set of 8, 2 × 2 matrices over C, Q, = (± I, ± A , ± B, ± C}, where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \text{and } i = \sqrt{-1}.$$

You can check that the following relations hold between the elements of Q_8:

$I_2 = I$, $A^2 = B^2 = C^2 = -I$,

AB = C = –BA, BC = A = –CB, CA = B = –AC.

Therefore, Q_8 is a non-abelian group under matrix multiplication.

Show that the subgroup H = < A > has only two distinct right cosets in Q_8.

Solution: $H = < A > = \{ I, A, A^2, A^3\} = \{I, A, -I, -A\}$,

since $A^4 = I$, $A^5 = A$, and so on.

Therefore, HB = {B, C, –B, –C} , using the relations given above.

Using Theorem 1 (b), we see that

H = HI = HA = H(–I) = H(–A).

Using Theorem 1 (c), we see that

HB = HC = H(–B) = H(–C).

Therefore, H has only two distinct right cosets in Q_8, H and HB.

We will now show that each group can be written as the union of disjoint cosets of any of its subgroups. For this, first we define a relation on the elements of G.

Definition: Let H be a subgroup of a group G. We define a relation '~' on G by x – y iff $x\ y^{-1} \in H$, where $x, y \in G$. Thus, from Theorem 1 we see that x – y iff Hx = Hy.

We will prove that this relation is an equivalence relation.

Theorem 2: Let H be a subgroup of a group G. Then the relation ~ defined by '$x \sim y$ iff $xy^{-1} \in H$' is an equivalence relation. The equivalence classes are the right cosets of H in G.

Proof: We need to prove that ~ is reflexive, symmetric and transitive.

Firstly, for any $x \in G$, $xx^{-1} = e \in H$. $\therefore$ $x \sim x$, that is, ~ is reflexive.

Secondly, if $x \sim y$ for any $x, y \in G$, then $xy^{-1} \in H$.

$\therefore$ $(xy^{-1})^{-1} = yx^{-1} \in H$. Thus, $y \sim x$. That is, ~ is symmetric.

Finally, if x, y, **z** $\in$ G such that $x \sim y$ and $y \sim z$, then $xy^{-1} \in H$ and $yz^{-1} \in H$.

$\therefore$ $(xy^{-1})\ (yz^{-1}) = x\ (y^{-1}y)z^{-1} = xz^{-1} \in H$. $\therefore$ $x \sim Z$.

That is , ~ is transitive.

Thus, ~ is an equivalence relation.

The equivalence class determined by $x \in G$ is

$[\ x\ l = \{\ y \in G \mid y \sim x\ \} = \{\ y \in G \mid xy^{-1} \in H\}$.

Now, we will show that [x] = Hx. So, let $y \in [X\}$. Then Hy = Hx, by Theorem 1. And since $y \in Hy$, $y \in Hx$.

Therefore, $[x] \subseteq Hx$.

Now, consider any element hx of Hx. Then $x(hx)^{-1} = xx^{-1}h^{-1} = h^{-1} \in H$.

Therefore, $hx \sim x$. That is, $hx \in [x]$. This is true for any $hx \in Hx$. Therefore, $Hx \subseteq [x]$.

Thus, we have shown that [x] = Hx.

Remark: If Hx and Hy are two right cosets of a subgroup H in G, then $W_x = W_y$ or $HX \cap HY = \phi$

Note that what Theorem 2 and the remark above say is that any subgroup H of a group G partitions G into disjoint right cosets.

On exactly the same lines as above we can state that:

(i) any two left cosets of H in G are identical or disjoint, and

(ii) G is the disjoint union of the distinct left cosets of H in G.

4.2 Lagrange's Theorem

To understand this theorem first we have to define the order of a finite group, after that we will show that the order of any subgroup divides the order of the group.

Notes

So let us start with a definition.

Definition: The order of a finite group G is the number of elements in G. It is denoted by o(G).

For example, $o(S_3) = 6$ and $o(A_3) = 3$. Remember, $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$!

You can also see that $o(Z_n) = n$. And, you know that $o(S_n) = n!$.

Now, let G be a finite group and H be a subgroup of G. We define a function f between the set of right cosets of H in G and the set of left cosets of H in G by

$f : \{ Hx \mid x \in G \} \to \{ yH \mid y \in G \} : f(Hx) = x^{-1}H.$

Definition: Let H be a subgroup of a finite group G. We call the number of distinct cosets of H in G the index of H in G, and denote it by $\mid G : H \mid$.

Thus, we see that $\mid S_3 : A_3 \mid = 2$.

Note that, if we take H = {e}, then $\mid G : \{e\} \mid = o(G)$, since $\{e\}g = \{g\}\ \forall\ g \in G$ and $\{e\}g \neq \{e\}g'$ if $g \neq g'$.

Now let us look at the order of subgroups. In last unit you saw that the orders of the subgroups of S_3 are 1, 2, 3 and 6. All these divide $o(S_3) = 6$. This fact is part of a fundamental theorem about finite groups. Its beginnings appeared in a paper in 1770, written by the famous French mathematician Lagrange. He proved the result for permutation groups only. The general result was probably proved by the famous mathematician Evariste Galois in 1830.

Theorem 3 (Lagrange): Let H be a subgroup of a finite group G. Then

$o(G) = o(H) \mid G : H \mid$. Thus, o(H) divides o(G) and $\mid G : H \mid$ divides o(G).

Proof: You know that we can write G as a union of disjoint right cosets of H in G. So, if $Hx_1, Hx_2, ..., H_x$, are all the distinct right cosets of H in G, we have

$G = Hx_1 \cup Hx_2 \cup ... \cup Hx_r$ ...(1)

and $\mid G : H \mid = r$.

We know that $\mid Hx_1 \mid = \mid Hx_2 \mid = ... = \mid Hx_r \mid = o(H)$.

Thus, the total number of elements in the union on the right hand side of (I) is

$o(H) + o(H) + ...+ o(H)$ (r times) $= r\ o(H)$.

Therefore, (1) says that $o(G) = r\ o(H)$

$$= o(H) \mid G : H \mid.$$

You will see the power of Lagrange's theorem when we get down to obtaining all the subgroups of a finite group.

For example, suppose we are asked to find all the subgroups of a group G of order 35. Then the only possible subgroups are those of order 1, 5, 7 and 35. So, for example, we don't need to waste time looking for subgroups of order 2 or 4.

In fact, we can prove quite a few nice results by using Lagrange's theorem. Let us prove some results about the order of an element.

Definition: Let G be a group and $g \in G$. Then the order of g is the order of the cyclic subgroup $< g >$, if $< g >$ is finite. We denote this finite number by o(g). If $< g >$ is an infinite subgroup of G, we say that g is of infinite order.

Now, let $g \in G$ have finite order. Then the set $\{e, g, g^2, ...\}$ is finite, since G is finite. Therefore, all the powers of g can't be distinct. Therefore, gr = gs for some r > s. Then $g^{r-s} = e$ and $r\text{-}s \in N$. Thus, the set $\{ t \in N \mid g^t = e \}$ is non-empty. So, by the well ordering principle it has a least element. Let n be the least positive integer such that $g^n = e$.

Then

$< g > = \{e, g, g^2, ..., g^{n-1}\}$.

Therefore, $o(g) = o(< g >) = n$.

That is, o(g) is the least positive integer n such that $g^n = e$.

Note If $g \in (G, +)$, then o(g) is the least positive integer n such that ng = e.

Now suppose $g \in G$ is of infinite order. Then, for m ≠ 11. $g^m \neq$ gn. (Because, if $g^m = g^n$, then $g^{m-n} = e$, which shows that < g > is a finite group.) We will use this fact while proving Theorem 5.

Theorem 4: Let G be a group and $g \in G$ be of order n. Then $g^m = e$ for some $m \in N$ iff $n \mid m$.

Proof: We will first show that gm = e ! n (m.F or this consider the set $S = \{ r \in Z \mid g^r = e \}$.

Now, $n \in S$. Also, if $a, b \in S$, then $g^a = e = g^b$. Hence, $g^{a-b} = ga\,(g^b)^{-1} = e$. Therefore, $a\text{-}b \in S$. Thus, $S \leq Z$.

Note So, from last unit, we see that S = nZ. Remember, n is the least positive integer in S!

Now if $g^m = e$ for some $m \in N$, then $m \in S = nZ$. Therefore, n / m.

Now let us show that $n \mid m \Rightarrow g^m = e$. Since $n \mid m$, m = nt for some t E Z. Then $g^m = g^{nt} = (g^n)^t = e^t = e$. Hence, the theorem is proved.

We will now use Theorem 4 to prove a result about the orders of elements in a cyclic group.

Theorem 5: Let G = < g > be a cyclic group.

(a) If g is of infinite order then gm is also of infinite order for every $m \in Z$.

(b) If o(g) = n, then

$$o(g^m) = \frac{n}{(n, m)}\ \forall\ m = 1, ..., n-1. \text{ ((n,m) is the g.c.d. of n and m.)}$$

Proof: (a) An element is of infinite order iff all its powers are distinct. We know that all the powers of g are distinct. We have to show that all the powers of g^m are distinct. If possible, let $(g^m)^t = (g^m)^w$, Then $g^{mt} = g^{mw}$, But then mt = mw, and hence, t = w. This shows that the powers of g^m are all distinct, and hence g^m is of infinite order.

(b) Since o(g) = n, G = {e, g, ... g^{n-1}) . < g^m >, being a subgroup of G, must be of finite order. Thus, g^m is of finite order. Let $o(g^m) = t$. We will show that $t = \frac{n}{(n, m)}$.

Now, $g^{mt} = (g^m)^t = e \Rightarrow n \mid tm$, by Theorem 4.

Let $d = (n, m)$. We can then write $n = n_1d$, $m = m_1d$, where $(m_1, n_1,) = 1$.

Then $n_1 = \frac{n}{d} = \frac{n}{(n, m)}$.

Now, $n \mid tm \Rightarrow n \mid tm_1d \Rightarrow n_1d \mid tm_1d \Rightarrow n \mid tm_1$.

But $(n, m_1) = 1$. Therefore, $n_1 \mid t$. ...... (1)

Also, $(g^m)^{n_1} = g^{m_1dn_1} = g^{m_1n} = (g^n)^{m_1} = e^{m_1} = e$.

Thus, by definition of o(gm) and Theorem 4, we have

$t \mid n_1$. ...... (2)

(1) and (2) show that

$$t = n_1 = \frac{n}{(n, m)}.$$

$$\text{i.e., } o(g^m) = \frac{n}{(n, m)}.$$

Using this result we know that $o\,(\bar{4})$ in Z_{12} is $\frac{12}{(12, 4)} = 3$.

Theorem 6: Every group of prime order is cyclic.

Proof: Let G be a group of prime order p. Since $p \neq 1$, $\exists\ a \in G$ such that $a \neq e$. Theorem 4, $o(a) \mid p$. Therefore, $o(a) = 1$ or $o(a) = p$. Since $a \neq e$, $o(a) \geq 2$.

Thus, $o(a) = p$, i.e., $o(< a >) = p$. So, $< a > \leq G$ such that $o(< a >) = b(G)$. Therefore, $< a > = G$, that is, G is cyclic.

Using Theorems 3 and 6, we can immediately say that all the proper subgroups of a group of order 35 are cyclic.

Now let us look at groups of composite order.

Theorem 7: If G is a finite group such that o(G) is neither 1 nor a prime, then G has nontrivial proper subgroups.

Proof: If G is not cyclic, then any $a \in G$, $a \neq e$, generates a proper non-trivial subgroup $< a >$.

Now, suppose G is cyclic, say $C = < x >$, where $o(x) = mn$ $(m, n \neq 1)$.

Then, $(x^m)^n = x^{mn} = e$. Thus, by Theorem 4, $o(x^m) \leq n < o(G)$.

Thus $<x^m>$ is a proper non-trivial subgroup of G.

We first define the Euler phi-function, named after the Swiss mathematician Leonard Euler (1707-1783).

Definition: We define the Euler phi-function $\phi : N \rightarrow N$ as follows :

$\phi(1) = I$, and

$\phi(n)$ = number of natural numbers $< n$ and relatively prime to n, for n 2 2.

Notes

For example, $\phi(2)$ = I and $\phi(6)$ = 2 (since the only positive integers < 6 and relatively prime to 6 are 1 and 5).

We will now prove a lemma, which will be needed to prove the theorem that follows it. This lemma also gives us examples of subgroups of Z,, for every n 2 2.

Lemma: Let G = $G = \{\bar{r} \in Z,| (r,n) = 1\}$, where n 2 2. Then (G,.) is a group, where $\bar{r}\,.\,\bar{s}$ = $\overline{rs}\ \forall\ \bar{r}, \bar{s} \in Zn$. Further, o(G) = ϕ (n).

Proof: We first check that G is closed under multiplication.

Now, $\bar{r}, \bar{s}\ \in G \Rightarrow (r, n) = 1$ and $(s, n) = 1 \Rightarrow (rs, n) = 1$.

$\Rightarrow\ \overline{rs} \in G$. Therefore, is a binary operation on G.

$\bar{1}\ \in$ G, and is the identity.

Now, for any $\bar{r}\ \in G$, (r, n) = 1.

$\Rightarrow$ ar + bn = 1 for some a, b $\in$ Z

$\Rightarrow$ n | ar – 1

$\Rightarrow$ ar $\equiv$ 1 (mod n),

$\Rightarrow\ \bar{a}\,\bar{r} = \bar{1}$.

$\Rightarrow\ \bar{a} = \bar{r}^{-1}$

Further, $\bar{a} \in G$, because if a and n have a common factor other than 1; then this factor will 'divide ar + bn = 1. But that is not possible.

Thus, every element in G has an inverse.

Therefore, (G, .) is a group.

In fact, it is the group of the elements of Z, that have multiplicative inverses.

Since G consists of all those $\bar{r}\ \in$ Z, such that r < n and (r, n) = I, o(G) = ϕ(n).

Lemma and Lagrange's theorem immediately give us the following result due to the mathematicians Euler and Pierre Fermat.

Theorem 8 (Euler-Fermat): Let a $\in$ N and n $\geq$ 2 such that (a,n) = 1.

Then,, $a^{\phi(n)} \equiv$ I (mod n).

Proof:

1. Leonhard Euler published a proof in 1789. Using modern terminology, one may prove the theorem as follows: the numbers a which are relatively prime to n form a group under multiplication mod n, the group G of (multiplicative) units of the ring Z/nZ. This group has ϕ(n) elements. The element a : = a (mod n) is a member of the group G, and the order o(a) of a (the least k > 0 such that a^k = 1) must have a multiple equal to the size of G. (The order of a is the size of the subgroup of G generated by a, and Lagrange's theorem states that the size of any subgroup of G divides the size of G.)

   Thus for some integer M > 0, M · o(a) = ϕ(n). Therefore, $a^{\phi(n)} = a^{o(a)\cdot M} = (a^{o(a)})^M = 1^M = 1$. This means that $a^{\phi(n)}$ = 1 (mod n).

Notes

2. Another direct proof: If a is coprime to n, then multiplication by a permutes the residue classes mod n that are co prime to n; in other words, (writing R for the set consisting of the $\phi(n)$ different such classes) the sets { x : x in R } and { ax : x in R } are equal; therefore, the two products over all of the elements in each set are equal. Hence, $P \equiv a^{\phi(n)}P$ (mod n) where P is the product over all of the elements in the first set. Since P is coprime to n, it follows that $a^{\phi(n)} \equiv 1$ (mod n).

Self Assessment

1. If H is a subgroup of a group G, and let $x \in G$ then $Hx = \{Hx \mid h \in H\}$. Thus Hx called as

   (a) Left coset of H is G (b) Right coset of H is G

   (c) Subgroup of G (d) Cyclic group of G

2. If H is ...., the alternating group on 3 symbols

   (a) A1 (b) A3

   (c) A4 (d) A5

3. Every group of prime order is ....

   (a) normal (b) cyclic

   (c) subgroup (d) abelian

4. Two left cosets of a .... are disjoint or identical

   (a) normal (b) cyclic

   (c) subgroup (d) abelian

5. $a^{f(n)} = 1$ (modn) where $a, n \in N$, $(a, n) = 1$ and

   (a) $n \geq 2$ (b) $n \leq 2$

   (c) $n = 2$ (d) $n \neq 2$

4.3 Summary

- The definition and examples of right and left cosets of a subgroup.
- Two left (right) cosets of a subgroup are disjoint or identical.
- Any subgroup partitions a group into disjoint left (or right) cosets of the subgroup.
- The definition of the order of a group and the order of an element of a group.
- The proof of Lagrange's theorem, which slates that if H is a subgroup of a finite group G, then $o(G) = o(H) \mid G : H \mid$. But, if $m \mid o(G)$, then G need not have a subgroup of order.
- The following consequences of Lagrange's theorem:
  - ❖ Every group of prime order is cyclic.
  - ❖ $a^{\phi(n)} = 1$ (mod n), where $a, n \in N$, $(a,n) = 1$ and $n \geq 2$.

4.4 Keywords

Coset: Let H be a subgroup of a group G, and let $x \in G$. We call the set $Hx = \{hx \mid h \in H\}$ a right coset of H in G.

Lagrange: Let H be a subgroup of a finite group G. Then $o(G) = o(H) \mid G : H \mid$. Thus, o(H) divides o(G) and $\mid G : H \mid$ divides o(G).

4.5 Review Questions

1. Obtain the left and right cosets of $H = < (1\ 2) >$ in S_3. Show that $Hx \neq xH$ for some $x \in S_3$.
2. Show that $K = \{I, -I\}$ is a subgroup of Q_8. Obtain all its right cosets in Q_8.
3. Let H be a subgroup of a group G. Show that there is a one-to-one correspondence between the elements of H and those of any right or left coset of H.

   (Hint: Show that the mapping $f : H \rightarrow Hx : f(h) = hx$ is a bijection.)
4. Write Z as a union of disjoint cosets of 5Z.
5. Check that f is a bijection.
6. What are the orders of

   (a) $(1\ 2) \in S_3$, (b) $I \in S_4$,

   (c) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in Q_8$, (d) $\overline{3} \in Z_4$

   (e) $1 \in R$?

Answers: Self Assessment

1. (b) 2. (b) 3. (d) 4. (c) 5. (a)

4.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 5: Normal Subgroups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the concept of normal subgroups
- Explain the Quotient group

Introduction

In earlier units, you have studied about the term subgroups and cosets. In this unit, we will discuss a special class of subgroups known as normal subgroups. You will also come to know about that the cosets of such a subgroup form a group with respect to a suitably defined operation. These groups are called quotient groups. After discussing these concepts, we will also discuss some examples related to this concept.

5.1 Normal Subgroups

In the last unit, you have studied about coset of a subgroup also introduced with a fact that left coset aH, not be same as the right coset Ha.

But this fact is true for certain subgroup for which Ha and aH represented by the same element coincide.

In group theory, these types of subgroup are very important and this type of a subgroup has a special name. This subgroup is referred to normal subgroup.

Definition: A subgroup N of a group G is called a normal subgroup of G if Nx = xN $\forall$ x $\in$ G, and we write this as N $\trianglelefteq$ G.

For example, any group G has two normal subgroups, namely, {e} and G itself. Can you see why? Well, {e}x = {x} = x{e}, for any x $\in$ G, and Gx = G = xG, for any x $\in$ G.

Let us consider an example.

Example: Show that every 'subgroup of Z is normal in Z.

Solution: As you know that if H is a subgroup of Z, then H = mZ, for some $m \in Z$. Now, for any $z \in Z$,

$H + z = \{ ..., - 3 m + z , - 2 m + z , - m + z , z , m + z , 2 m + z ,...\}$

$= \{ ..., z - 3m, z - 2m, z - m, z, z + m, z + 2m,\}$ {since + is commutative)

$= z + H.$

$\therefore \quad H \trianglelefteq Z.$

Above example is a special case of the fact that every subgroup of a commutative group is a normal subgroup.

Let us now prove a result that gives equivalent conditions for a subgroup to be normal.

Theorem 1: Let H be a subgroup of a group G. The following statements are equivalent.

(a) H is normal in G.

(b) $g^{-1}Hg \subseteq H \ \forall \ g \in G.$

(c) $g^{-1}Hg = H \ \forall \ g \in G.$

Proof: We will show that (a) ⇒ (b) ⇒ (c) ⇒ (a). This will show that the three statements are equivalent.

(a) ⇒ (b) : Since (a) is true, $Hg = gH \ \forall \ g$ E G. We want to prove (b). For this, consider

$g^{-1}Hg$ for g E G. Let $g^{-1}hg \in g^{-1}Hg$.

Since $hg \in Hg = gH$, 3 $h_1 \in H$ such that $hg = gh_1$.

$\therefore \ g^{-1}hg = g^{-1}gh_1 = h_1 \in H$

∴ (b) holds.

Note $g^{-1}Hg = \{g^{-1}hg \mid h \in H \}$

(b) ⇒ (c) : Now, we know that (b) holds, i.e., for $g \in G$, $g^{-1}Hg \subseteq H$. We want to show

that $H \subseteq g^{-1}Hg$. Let $h \in H$. Then

$h = ehe = (g^{-1}g) h (g^{-1}g)$

$= g^{-1} (ghg^{-1}) g$

$= g^{-1}\{ (g^{-1})^{-1} hg^{-1} \} g \in g^{-1}Hg$, since $(g^{-1})^{-1}hg^{-1} \in (g^{-1})^{-1} H(g^{-1}) \subseteq H$.

$\therefore \quad H \subseteq g^{-1}Hg.$

$\therefore \quad g^{-1}Hg = H \ \forall \ g \in G.$

(c) $\Rightarrow$ (a) : For any $g \in G$, we know that $g^{-1}Hg = H$.

$\therefore$ $g(g^{-1}Hg) = gH$, that a, $Hg = gH$.

$\therefore$ $H \trianglelefteq G$, that is, (a) holds.

Note Ha = Hb $\Leftrightarrow$ Hac = Hbc for any a, b, c $\in$ G.

We would like to make the following remark about Theorem 1.

Remark: Theorem 1 says that $H \trianglelefteq G \Leftrightarrow g^{-1}Hg = H \; \forall \; g \text{ e } G$. This does not mean that

$g\,hg = h \;\; \forall \;\; h \in H$ and $g \in G$.

For example, you have shown that $A_3 \trianglelefteq S_3$. Therefore, by Theorem 1,

$(1\ 2)^{-1}\ A_3(1\ 2) = A_3$. But, $(1\ 2)^{-1}(1\ 3\ 2)\ (1\ 2) \neq (1\ 3\ 2)$. In fact, it is (1 2 3).

Theorem 2: Every subgroup of a commutative group is normal.

Proof: Let G be an abelian group, and $H \leq G$. For any $g \in G$ and $h \in H$, $g^{-1}hg = (g^{-1}g)h = h$ E H.

$\therefore$ $g^{-1}Hg \subseteq H$. Thus, $H \trianglelefteq G$.

Theorem 2 says that if G is abelian, then all its subgroups are normal. Unfortunately, the converse of this is not true. That is, there are non-commutative groups whose subgroups are all normal. We will give you an example after doing Theorem 3. Let us first look at another example of a normal subgroup.

Example: Consider the Klein 4-group, K_4, given in table below. Show that both its subgroups < a > and < b > are normal.

×	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Solution: Consider the table of the operation given in table. Note that a and b are of order 2. Therefore, $a = a^{-1}$ and $b = b^{-1}$. Also note that ba = ab.

Now, let H = < a > = {e, a}. We will check that $H \trianglelefteq K_4$, that is, $g^{-1}hg \in H \;\; \forall \;\; g \in K_4$ and h E H.

Now, $g^{-1}eg = e$ E H $\forall$ g E K_4.

Further, $e^{-1}ae = a \in H$, $a^{-1}aa = a \in H$, $b^{-1}ab = bab = a \in H$ and $(ab)^{-1}\ a(ab)$

$= b^{-1}\ (a^{-1}aa)b = bab = a$ E H.

$\therefore$ $H \trianglelefteq K_4$.

By a similar proof we can show that < b > $\trianglelefteq$ K_4.

In above Example, both < a > and < b > are of index 2 in K_4. We have the following result about such subgroups.

Theorem 3: Every subgroup of a group G of index 2 is normal in G.

Proof: Let $N \leq G$ such that $| G : N | = 2$. Let the two right cosets of N be N and Nx, and the two left cosets be N and yN.

Now, $G = N \cup yN$, and $x \in G$. $\quad \therefore x \in N$ or $x \in yN$.

Since $N \cap Nx = \phi$, $x \notin N$. $\quad \therefore x \in yN, xN = yN$.

To show that $N \trianglelefteq G$, we need to show that $Nx = xN$.

Now, for any $n \in N$, $nx \in G = N \cup xN$. Therefore, $nx \in N$ or $nx \in xN$.

But $nx \notin N$, since $x \notin N$. $\quad \therefore nx \in xN$.

Thus, $Nx \subseteq xN$.

By a similar argument we can show that $xN \subseteq Nx$.

$\therefore \quad Nx = xN$, and $N \trianglelefteq G$.

We will use this theorem to show that, for any $n \geq 2$, the alternating group A, is a normal subgroup of S_n.

In fact, if you go back b, you can see that $A_4 \trianglelefteq S_4$, since Lagrange's theorem implies that

$$|S_4 : A_4| = \frac{o(S_4)}{o(A_4)} = \frac{4!}{12} = 2.$$

Consider the quaternion group Q_8, which we discussed earlier. It has the following 6 subgroups:

Ho = (I}, H_1 = {I, – I}, H_2 = (I, – I, A, – A), H_3 = {I, – I, B, – B},

H_4 = {I, – I, C, – C), $H_5 = Q_8$.

You know that H_0 and H_5 are normal in Q_8. Using Theorem 3, you can see that Hz, H_3 and H_4 are normal in Q_e.

By actual multiplication you can see that

$$g^{-1}H_1 g \subseteq H_1 \ \forall\, g \in Q_8. \quad \therefore \ H_1 \trianglelefteq Q_8.$$

Therefore, all the subgroups of Q_8 are normal.

But, you know that Q_8 is non-abelian (for instance, AB = – BA).

So far we have given examples of normal subgroups. Let us look at an example of a subgroup that isn't normal.

Example: Show that the subgroup < (1 2) > of S_3 is not normal.

Solution: We have to find $g \in S_3$ such that $g^{-1}(1\ 2)g \notin$ < (1 2) >.

Let us try g = (1 2 3).

Then, $g^{-1}(1\ 2)g = (3\ 2\ 1)\ (1\ 2)\ (1\ 2\ 3)$

$\qquad = (3\ 2\ 1)\ (2\ 3) = (1\ 3) \notin$ < (1 2)>

Notes

Therefore, < (1 2) > is not normal in S_3.

In earlier unit we proved that if H I G and K ≤ H, then K I G. That is, '≤' is a transitive relation. But '$\trianglelefteq$' is not a transitive relation. That is, if H $\trianglelefteq$ N and N $\trianglelefteq$ G, it is not necessary that H $\trianglelefteq$ G.

Theorem 4: Let H and K be normal subgroups of a group G. Then H $\cap$ K $\trianglelefteq$ G:

Proof: From Theorem 4 of Unit 3, you know that H $\cap$ K ≤ G. We have to show that

$g^{-1}xg \in H \cap K \;\forall\; x \in H \cap K$ and $g \in G$.

Now, let x EH $\cap$ K and g $\in$ G. Then x $\in$ H and H $\trianglelefteq$ G. $\therefore$ $g^{-1}xg \in H$.

Similarly, $g^{-1}xg \in K$. $\therefore$ $g^{-1}xg \in H \cap K$

Thus, H $\cap$ K $\trianglelefteq$ G.

Example: Let G be the group generated by

$\{ x, y \mid x^2 = e, y^4 = e, xy = y^{-1}x \}$

Let H = < x > and K = < y > .

Then show that K $\trianglelefteq$ G, H $\not\trianglelefteq$ G and G = HK.

Solution: Note that the elements of G are, of the form x^i $, where i = 0, 1 and j = 0, 1, 2, 3

$\therefore$ G = {e, x, xy, xy^2, xy^3, y , y^2, y^3}

$\therefore$ | G : K | = 2. Thus, by Theorem 3, K $\trianglelefteq$ G.

Note that we can't apply Theorem 2, since G is non-abelian (as $xy = y^{-1}x$ and $y \neq y^{-1}$).

Now let us see if H $\trianglelefteq$ G.

Consider $y^{-1}xy$. Now $y^{-1}xy = xy^2$, because $y^{-1}x = xy$.

If $xy^2 \in H$, then $xy^2 = e$ or $xy^2 = x$. (Remember o(x) = 2, so that $x^{-1} = x$.)

Now, $xy^2 = e \Rightarrow y^2 = x^{-1} = x$

$\Rightarrow y^3 = xy = y^{-1}x$

$\Rightarrow y^4 = x$

$\Rightarrow$ e = x, a contradiction.

Again $xy^2 = x \Rightarrow y^2 = e$, a contradiction..

$\therefore$ $Y^{-1}xy = xy^2 \notin H$, and hence, H $\not\trianglelefteq$ G.

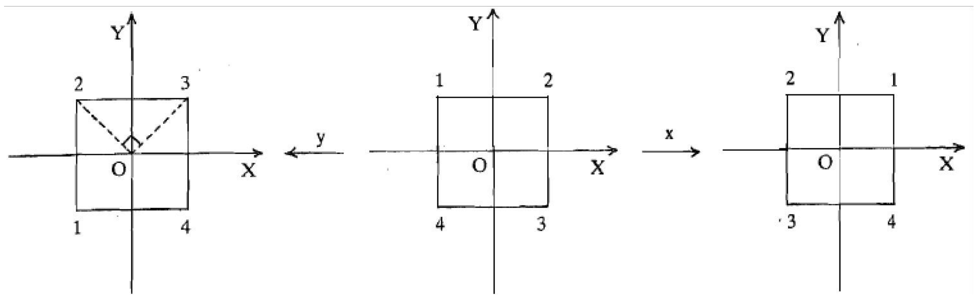
Finally, from the definition of G you see that G = HK.

The group G is of order 8 and is called the **dihedral group, D_8.** It is the group of symmetries of a square, that is, its elements represent the different ways in which two copies of a square can be placed so that one covers the other. A geometric interpretation of its generators is shown in figure 5.1.

Take y to be a rotation of the Euclidean plane about the origin through $\frac{\pi}{2}$, and x the reflection about the vertical axis.

Notes

Figure 5.1: Geometric Representation of the Generators of D_8



We can generalise D_8 to the dihedral group

$D_{2n} = < \{ x, y \mid x^2 = e, y^n = e, xy = y^{-1}x\} >$, for $n > 2$.

5.2 Quotient Groups

Here we will use a property of normal subgroups to create a new group. This group is analogous to the concept of quotient spaces given in the Linear Algebra course.

Let H be a normal subgroup of a group G. Then gH = Hg for every $g \in G$. Consider the collection of all cosets of H in G. (Note that since $H \underline{\Delta} G$, we need not write 'left coset' or 'right coset; simply 'coset' is enough.) We denote this set by G/H. Now, for $x, y \in H$, we have

$$\begin{aligned}(Hx)(Hy) &= H(xH)y, \text{ using associativity,}\\ &= HHxy, \text{ using normality of H,}\\ &= Hxy, \text{ since HH = H because H is a subgroup.}\end{aligned}$$

Now, we define the product of two cosets Hx and Hy and G/H by (Hx)(Hy) = Hxy for all x, y in G.

As this definition seems to depend on the way in which we represent a coset. Let us discuss this in detail. Suppose C_1 and C_2 are two cosets, say $C_1 = Hx$ and $C_2 = Hy$. Then $C_1C_2 = Hxy$. But C_1 and C_2 can be written in the form Hx and Hy in several ways. So, you may ask : Does C_1C_2 depend on the particular way of writing C_1 and C_2?

In other words, if $C_1 = Hx = Hx_1$ and $C_2 = Hy = Hy_1$, then is $C_1C_2 = Hxy$ or is $C_1C_2 = Hx_1y_1$? Actually, we will show you that $Hxy = Hx_1y_1$, that is, the product of cosets is well-defined.

Since $Hx = Hx_1$ and $Hy = Hy_1$, $xx_1^{-1} \in H$, $yy_1^{-1} \in H$.

$\therefore \quad (xy)(x_1 y_1)^{-1} = (xy)(y_1^{-1} x_1^{-1}) = x(yy_1^{-1})x_1^{-1}$

$= x(yy_1^{-1})x^{-1}(xx_1^{-1}) \in H$, since $xx_1 \in H$ and $H \underline{\Delta} G$

i.e:, $(xy)(x_1y_1)^{-1} \in H$.

$\therefore \quad Hxy = Hx_1y_1$.

So, we have shown you that multiplication is a well-defined binary operation on G/H.

We will now show that (G/H,.) is a group.

Theorem 5: Let H be a normal subgroup of a group G and G/H denote the set of all cosets of H in G. Then G/H becomes a group under multiplication defined by Hx . Hy = Hxy, $x, y \in G$. The coset H = He is the identity of G/H and the inverse of Hx is the coset Hx^{-1}

Notes

Proof: We have already observed that the product of two cosets is a coset.

This multiplication is also associative, since

$$\begin{aligned}((Hx)\,(Hy))\,(Hz) &= (Hxy)\,(Hz)\\ &= Hxyz, \text{ as the product in G is associative,}\\ &= Hx\,(yz)\\ &= (Hx)\,(\,Hyz)\\ &= (Hx)\,((Hy)\,(Hz)) \text{ for } x, y, z \in G.\end{aligned}$$

Now, if e is the identity of G, then Hx, He = Hxe = Hx and He. Hx = Hex = Hx for every $x \in G$. Thus, He = H is the identity element of G/H.

Also, for any $x \in G$, $Hx\,Hx^{-1} = Hx\,x^{-1} = He = Hx^{-1}x = Hx^{-1}.Hx$.

Thus, the inverse of Hx is Hx^{-1}.

So, we have proved that G/H, the set of all cosets of a normal subgroup H in G, forms a group with respect to the multiplication defined by Hx.Hy = Hxy. This group is called the quotient group (or factor group) of G by H.

Note that the order of the quotient group G/H is the index of H in G. Thus, by Lagrange's theorem you know that if G is a finite group, then

$$o(G/H) = \frac{o(G)}{o(H)}$$

Also note that if (G, +) is an abelian group and $H \leq G$, then $H \trianglelefteq G$. Further, the operation on G/H is defined by (H + x) + (H + y) = H + (x + y).

Let us look at a few examples of quotient groups.

Example: Obtain the group G/H, where $G = S_3$ and $H = A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

Solution: Firstly, note bat $A_3 \trianglelefteq S_3$, since $|S_3 : A_3| = 2$.

You know that G/H is a group of order 2 whose elements are H and (1 2) H.

Example: Show that the group Z/nZ is of order n.

Solution: The elements of Z/nZ are of the form a + nZ = {a + kn | k ∈ Z).

Thus, the elements of Z/nZ are precisely the congruence classes modulo n, that is, the elements of Z_n.

Thus, Z/nZ = $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

$\therefore$ o(Z/nZ) = n.

Note that addition in Z/nZ is given a + b = a + b

Definition: Let G be a group and $x, y \in G$. Then $x^{-1}y^{-1}xy$ is called the commutator of x and y. It is denoted by [x, y].

The subgroup of G generated by the set of all commutators is called the commutator subgroup of G. It is denoted by [G, G].

For example, if G is a commutative group, then

$x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e \;\forall\; x, y \in G.$ $\quad\therefore$ $[G, G] = \{e\}$.

Theorem 6: Let G be a group. Then [G, G] is a normal subgroup of G. Further, G/[G, G] is commutative.

Proof: We must show that, for any commutator $x^{-1}y^{-1}xy$ and for any $g \in G$, $g^{-1}(x^{-1}y\text{-}^{1}xy)g \in [G,G]$.

Now $g^{-1}(x^{-1}y\text{-}^{1}xy)g = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in [G, G]$.

$\therefore \quad [G, G] \trianglelefteq G$.

For the rest of the proof let us denote [G, G] by H, for convenience.

Now, for $x, y \in G$,

$HxHY = H y Hx \Leftrightarrow Hxy = Hyx \Leftrightarrow (xy)(yx)^{-1} \in H$

Thus, since $xy\,x^{-1}y^{-1} \in H \;\forall\; x, y \in G$, $HxHy = HyHx \;\forall\; x, y \in G$. That is, G/H is abelian.

Note We have defined the quotient group G/H only if $H \trianglelefteq G$. But if $H \trianglelefteq G$ we can still define G/H to be the set of all left (or right) cosets of H in G. But, in this case G/H will not be a group.

Remark: If H is a subgroup of G, then the product of cosets of H is defined only when $H \trianglelefteq G$. This is because, if $HxHy = Hxy \;\forall\; x, y \in G$, then, in particular,

$Hx^{-1}Hx = Hx^{-1}x = He = H \;\forall\; x \in G.$

Therefore, any $h \in H$, $x^{-1}hx = ex^{-1}hx \in Hx^{-1}Hx = H$.

That is, $X^{-1}Hx \subseteq H$ for any x E G.

$\therefore \quad H \trianglelefteq G.$

Self Assessment

1. Every subgroup of a .... group is a normal subgroup.

   (a) associative (b) large

   (c) cyclic (d) commutative

2. $g^{-1}Hg$ = ... if $h \in H$ where H is a subgroup of G.

   (a) $g^{-1}hg$ (b) $gh^{-1}g$

   (c) $gh^{-1}g^{-1}$ (d) ghg

3. The group of G is of order .... is called dihedral group.

   (a) 6 (b) 7

   (c) 8 (d) 9

4. Every group of index .... is normal.

   (a) 4 (b) 5

   (c) 3 (d) 2

Notes

5. If H and k are normal subgroup of group G, then so is H .... k.

   (a) $\cup$ (b) $\cap$

   (c) = (d) $\neq$

5.3 Summary

We discussed here:

- The definition and examples of a normal subgroup.
- Every subgroup of an abelian group is normal.
- Every subgroup of index 2 is normal.
- If H and K are normal subgroups of a group G, then so is H $\cap$ K.
- The product of two normal subgroups is a normal subgroup.
- If H $\trianglelefteq$ N and N $\trianglelefteq$ G, then H need not be normal in G.
- The definition and examples of it quotient group.
- If G is abelian, then every quotient group of G is abelian. The converse is not true.
- The quotient group corresponding to the commutator subgroup is commutative.
- The set of left (or right) cosets of H in G is a group if and only if H $\trianglelefteq$ G.

5.4 Keywords

Normal Subgroup: A subgroup N of a group G is called a normal subgroup of 6 if Nx = xN $\forall$ x $\in$ G, and we write this as N $\trianglelefteq$ 6.

Dihedral Group, D_8: It is the group of symmetries of a square, that is, its elements represent the different ways in which two copies of a square can be placed so that one covers the other.

Quotient Group: If $C_1 = Hx = Hx_1$ and $C_2 = Hy = Hy_1$, then is $C_1C_2 = Hxy$ or is $C_1C_2 = Hx_1y_1$? Actually, we will show you that $Hxy = Hx_1y_1$, that is, the product of cosets is well-defined.

5.5 Review Questions

1. Show that $A_3 \trianglelefteq S_3$.

2. Consider the subgroup $SL_2(R) = \{A \text{ E } GL_2(R) \mid \det(A) = 1\}$ of $GL_2(R)$. Using the facts that det (AB) = det (A) det (B) and $\det(A^{-1}) = \frac{1}{\det(A)}$, prove that $SL_2(R) \trianglelefteq GL_2(R)$.

3. Consider the group of all 2 × 2 diagonal matrices over R*, with respect to multiplication. How many of its subgroups are normal.

4. Show that Z(G), the centre of G, is normal in G. (Remember that $Z(G) = \{x \in G \mid xg = gx \ \forall\ g \in G\}$).

5. Show that <(2 3)> is not normal in S_3.

6. Prove that if $H \trianglelefteq G$ and $K \leq G$, then $HK \leq G$.

7. Prove that if $H \trianglelefteq G$, $K \trianglelefteq G$, then $HK \trianglelefteq G$.

Answers: Self Assessment

1. (d) 2. (a) 3. (c) 4. (d) 5. (b)

5.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Notes

Unit 6: Group Isomorphism

CONTENTS

Objectives

After studying this unit, you will be able to:

- Explain the concept of homomorphism
- Describe Isomorphism

Introduction

In the last unit, you have studied about the normal groups and the concept of quotient group. In this unit, we will discuss various properties of those functions between groups which preserve the algebraic structure of their domain groups. These functions are called group Homomorphisms. This term was introduced by the mathematician Klein in 1893. This concept is analogous to the concept of a vector space homomorphism, as you studied in the earlier unit. In this unit, you will also get an idea about a very important mathematical idea—isomorphism.

6.1 Homomorphisms

Let us start our study of functions from one group to another with an example.

Consider the groups (Z, f) and ({1, - 1},). If we define

$$f : Z \to \{1, -1\} \text{ by } f(n) = \begin{cases} 1, \text{ if n is even} \\ -1, \text{ if n is odd,} \end{cases}$$

then you can see that $f(a + b) = f(a).f(b) \ \forall\ a, b \in Z$. What we have just seen is an example of a homomorphism, a function that preserves the algebraic structure of its domain.

Definition: Let $(G_1, *_1)$ and $(G_2,*_2)$ be two groups. A mapping $f : G_1 - G_2$ is said to be a group homomorphism (or just a homomorphism), if

$f(x *_1 y) = f(x) *_2 f(y) \ \forall\ x, y \in G_1$.

Note that a homomorphism f from G_1 to G_2 carries the product $x *_1 y$ in G_1 to the product $f(x) *_2 f(y)$ in G_2.

Note The word 'homomorphism' is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

Let us define two sets related to a given homomorphism.

Definition: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups and $f : G_1 \rightarrow G_2$ be a homomorphism. Then we define

(i) the image of f to be the set

$\text{Im } f = \{f(x)\ 1\ x \in G_1\}$.

(ii) the kernel of f to be the set

$\text{Ker } f = \{x \in G_1 \mid f(x) = e_2\}$, where e_2 is the identity of G_2.

Note that $\text{Im } f \subseteq G_2$, and $\text{Ker } f = f^{-1} (\{e_2\} \subseteq G_1$.

Example: Consider the two groups (R, +) and (R*,.). Show that the map exp : (R, +) → (R*,.) : $\exp(r) = e^r$ is a group homomorphism. Also find Im exp and Ker exp.

Solution: For any $r_1, r_2 \in R$, we know that $e^{r_1 + r_2} = e^{r_1}.e^{r_2}$.

$:.\ \exp(r_1 + r_2) = \exp(r_1).\exp(r_2)$.

Hence, exp is a homomorphism from the additive group of real numbers to the multiplicative group of non-zero real numbers.

Now, $\text{Im exp} = \{\exp(r) \mid r \in R\} = \{e^r \mid r \in R\}$,

Also, $\text{Ker exp} = \{r \in R \mid e^r = 1\} = \{0\}$.

Note that examples takes the identity 0 of R to the identity 1 of R*. example also carries the additive inverse – r of r. to the multiplicative inverse of exp (r).

Example: Consider the groups (R, +) and (C, +) and define f : (C, +) → (R, +) by f(x + iy) = x, the real part of x + iy. Show that f is a homomorphism. What are Im f and Ker f?

Solution: Take any two elements a + ib and c + id in C. Then,

$f((a + ib) + (c + id)) = f((a + c) + i(b + d)) = a + c = f(a + ib) + f(c + id)$

Therefore, f is a group homomorphism.

$\text{Imf} = \{f(x + iy) \mid x, y \in R\} = \{x \mid x \in R) = R$.

So, f is a surjective function

$\text{Ker } f = \{x + iy \in C \mid f(x + iy) = 0\} = \{x + iy \in C \mid x = 0\}$

$= \{iy \mid y\ E\ R\}$, the set of purely imaginary numbers.

Note that f carries the additive identity of C to the additive identity of R and (– z) to – f(z), for any $z \in C$.

In Examples 1 and 2 we observed that the homomorphisms carried the identity to the identity and the inverse to the inverse. In fact, these observations can be proved for any group homomorphism.

Theorem 1: Let f ; $(G_1, *_1) \rightarrow (G_2, *_2)$ be a group homomorphism.

Then

(a) $f(e_1) = e_2$, where e_1 is the identity of G_1 and e_2 is the identity of G_2.

(b) $f(x^{-1}) = [f(x)]^{-1}$ for all x in G_1.

Proof: (a) Let $x \in G_1$. Then we have $e_1 * 1x = x$. Hence,

$f(x) = f(e_1 *_1 x) = f(e_1) *_2 f(x)$, since f is a homomorphism. But

$f(x) = e_2 *_2 f(x)$ in G_2.

Thus, $f(e_1) *_2 f(x)= e_2 *_2 f(x)$.

So, by the right cancellation law in G_2, $f(e_1) =e_2$.

(b) Now, for any $x \in G_1$, $f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2$.

Similarly, $f(x^{-1}) *_2 f(x) = e_2$.

Hence, $f(x^{-1}) = [f(x)]^{-1}\ \forall\ x\ E\ G_1$.

Note that the converse of Theorem 1 is false. That is, if $f : G_1 \rightarrow G_2$ is a function such that $f(e_1) = e_2$ and $[f(x)]^{-1} = f(x^{-1}) = f(x^{-1})\ \forall\ x \in G_1$, then f need not be a homomorphism. For example, consider $f : Z \rightarrow Z : f(0) = 0$ and ,

$$f(n) = \begin{cases} n+1 \ \forall \ n > 0 \\ n-1 \ \forall \ n < 0 \end{cases}$$

Since $f(l + 1) \neq f(1) + f(l)$, f is not a homomorphism. But $f(e_1) = e_2$ and $f(n) = - f(- n)\ \forall\ n \in Z$.

Let us look at a few more examples of homomorphisms now. We can get one important class of homomorphisms from quotient groups.

Example: Let $H \trianglelefteq G$. Consider the map $p : G \rightarrow G/H : p(x) = Hx$. Show that p is **a** homomorphism. Also show that p is onto. What is Ker p?

Solution: For $x, y \in G$, $p(xy) = Hxy = Hx\ Hy = p(x)\ p(y)$. Therefore, p is a homomorphism.

Now, Im p = { p(x) (x ∈ G} = (Hx | x ∈ G } = G/H. Therefore, p is onto.

Ker p = { x ∈ G | p(x) = H). (Remember, H is the identity of G/H.)

= (x ∈ G | H x = H }

= { x ∈ G | x ∈ H), by Theorem 1 of Unit 4.

= H.

In this example you can see that Ker p $\trianglelefteq$ G. You can also check that Theorem 1 is true here.

Example: Let H be a subgroup of a group G. Show that the map $i : H \rightarrow G$, $i(h) = h$ is a homomorphism. This function is called the inclusion map.

Solution: Since $i(h_1 h_2) = h_1 h_2 = i(h_1)i(h_2)$ $\forall$ $h_1, h_2 \in H$. i is a group homomorphism.

Let us briefly look at the inclusion map in the context of symmetric groups. Consider two natural numbers m and n, where m I n.

Then, we can consider $S_m \leq S_n$, where any $\sigma \in$ Sm, written as

$$\begin{pmatrix} 1 & 2 & .... & m \\ \sigma(1) & \sigma(2) & .... & \sigma(m) \end{pmatrix}, \text{ is considered to be the same as}$$

$$\begin{pmatrix} 1 & 2 & .... & m & m+1 & .... & n \\ \sigma(1) & \sigma(2) & .... & \sigma(m) & m+1 & .... & n \end{pmatrix} \in S_n, \text{ i.e., } \sigma(k) = k \text{ for } m + 1 \leq k \leq n.$$

Then we can define an inclusion map $i : S_m \to S_r$.

For example, under $i : S_3 \to S_4$, (1 2) goes to $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 4 \end{pmatrix}$.

We will now prove some results about homomorphisms. Henceforth, for convenience, we shall drop the notation for the binary operation, and write a * b as ab.

Now let us look at the composition of two homomorphisms. Is it a homomorphism? Let us see.'

Theorem 2: If $f : G_1 \to G_2$ and $g : G_2 \to G_3$ are two group homomorphisms, then the composite map $g . f : G_1 \to G_3$ is also a group homomorphism.

Proof: Let $x. y \in G_1$. Then

$g \text{ o } f(xy) = g(f(x : y))$

$= g(f(x)f(y)$, since f is a homomorphism.

$= g(f(x))\, g(f(g))$, since g is a homomorphism.

$= g \text{ o } f(x).g \text{ o } f(y)$.

Thus g, f is a homomorphism.

Theorem 3: Let $f : G_1 \to G_2$ be a group homomorphism. Then

(a) Ker f is a normal subgroup of G_1.

(b) Im f is a subgroup of G_2.

Proof: (a) Since $[(e_1) = e_2, e_1 \in \text{Ker } f$. $\therefore$ Ker f $\neq \phi$.

Now, if $x, y \in$ Ker f, then $f(x) = e_2$ and $f(y) = e_2$.

$\therefore$ $f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\, [f(y)]^{-1} = e_2$.

$xy^{-1} \in$ Ker f.

Therefore, by Theorem 1 of Unit 3, Ker f $\leq G_1$. Now, for any $y \in G_1$ and x E Ker f,

$f(y^{-1}xy) = f(y^{-1})\, f(x)f(y)$

$= [f(y)]^{-1}e_2f(y)$, since $f(x) = e_2$ and by Theorem 1

$= e_2$.

$\therefore$ Ker f $\trianglelefteq$ G_1.

(b) Im f ≠ ϕ, since $f(e_1)$ E Im f.

Now, let x_2, $y_2 \in$ Im f. Then $\exists x_1, y_1 \in G_1$ such that $f(x_1) = x_2$ and $f(y_1) = y_2$.

$\therefore \quad x_2y_2^{-1} = f(x_1)\, f(y_1^{-1}) = f(x_1y_1^{-1}) \in \text{Imf}.$

$\therefore \quad \text{Im } f \leq G_2.$

Using this result, we can immediately see that the set of purely imaginary numbers is a normal subgroup of C.

Consider $\phi : (R, +) \to (C^*,.)$ $\phi(x) = \cos x + i \sin x$. We have seen that $\phi(x + y) = \phi(x)\phi(y)$, that is, ϕ is a group homomorphism. Now $\phi(x) = 1$ iff $x = 2\pi n$ for some $n \in Z$. Thus, by Theorem 3, Ker ϕ = $(2\ \pi n \mid n \in Z)$ is a normal subgroup of (R. +). Note that this is cyclic, and 2n is a generator.

Similarly, Im ϕ is a subgroup of C*. This consists of all the complex numbers with absolute value 1, i.e., the complex numbers on the circle with radius 1 unit and centre (0, 0).

You may have noticed that sometimes the kernel of a homomorphism is {e} and sometimes it is a large subgroup. Does the size of the kernel indicate anything? We will prove that a homomorphism is 1 – 1 iff its kernel is {e}.

Theorem 4: Let $f : G_1 \to G_2$ be a group homomorphism. Then f is injective iff Ker f = $\{e_1\}$, where e_1 is the identity element of the group G_1.

Proof: Firstly, assume that f is injective. Let $x \in$ Ker f. Then $f(x) = e_2$, i.e., $f(x) = f(e_1)$. But f is 1 – 1. $\therefore$ $x = e_1$.

Thus, Kerf = $\{e_1\}$.

Conversely, suppose Ker f = $\{e_1]$. Let $x, y \in G_1$ such that

$f(x) = f(y)$. Then $f(xy^{-1}) = f(x)\, f(y^{-1})$

$= f(x)\, [f(y)]^{-1} = e_2.$

$\therefore \quad xy^{-1} \in$ Ker f = {e1}. $\qquad \therefore$ $xy^{-1} = e_1$ and $x = y$.

This shows that f is injective.

So, by using Theorem 4, we can immediately say that any inclusion $i : B \to G$ is 1-1, since Ker i = {e}.

Let us consider another example.

Example: Consider the group T of translations of R^2. We define a map $\phi : (R^2 +) \to (T, o)$ by 4 (a, b) = $f_{a,\, b}$. Show that ϕ is an onto homomorphism, which is also 1-1.

Solution: For (a, b), (c, d) in R*, we have seen that

$f_{a+c,h+d} = f_{a,b} \text{ o } f_{c.d}$

$\therefore \quad \phi((a, b) + (c, d)) = \phi(a, b) \text{ o } \phi(c, d).$

Thus, ϕ, is a homomorphism of groups.

Now, any element of T is -f(a, b). Therefore, ϕ is surjective. We now show that ϕ is also injective.

Let (R, b) $\in$ Ker ϕ. Then $\$(a, b) = f_{0,\, 0}$

i.e., $f_{a,\, b} = f_{0,0}$

$\therefore$ $f_{a,b}(0, 0) = f_{0,\, 0}\ (0, 0),$

i.e., (a, b) = (0, 0)

$\therefore$ Ker $\phi = \{1\ (0, 0)\}$

$\therefore$ ϕ is 1-1.

So we have proved that ! is a homomorphism, which is bijective.

And now let us look at a very useful property of a homomorphism that is surjective.

Theorem 5: Iff : $G_1 \to G_2$ is an onto group homomorphism and S is a subset that generates G_1, then f(S) generates G_2.

Proof: We know that

$G_1 = < S > = \{ x_1^{r_1} x_2^{r_2} ... x_m^{r_m} \mid m \in N, x_1 \in S, r_1 \in Z$ for all i). We will show that

$G_2 = < f(S) >$

Let $x \in G_2$, Since f is surjective, there exists $y \in G_1$ such that f(y) = x. Since $y \in G_1$, $y = x_1^{r_1} ... x_m^{r_m}$, for some $m \in N$, where xi $\in$ S and ri $\in$ Z, $\leq 1 \leq i \leq m$.

Thus, $x = f\ (y) = f\left(x_1^{r_1} ... x_m^{r_m}\right)$

$= (f(x_1))^{r_1} ... (f(x_m))^{r_m}$, since f is a homomorphism.

$\Rightarrow$ $x \in < f(S) >$. since $f(x_1) \in f(S)$ for every i = 1, 2, ..., r.

Thus $G_2 = < f(S) >$.

So far you have seen examples of various kinds of homomorphisms-injective, surjective and bijective. Let us now look at bijective homomorphism in particular.

6.2 Isomorphisms

Definition: Let G_1 and G_2 be two groups. A homomorphism f : $G_1 \to G_2$ is called an isomorphism if f is 1-1 and onto.

In this case we say that the group G_1 is isomorphic to the group G_2 or G_1 and G_2 are isomorphic. We denote this fact by $G_1 \approx G_2$.

An isomorphism of a group G onto itself is called an automorphism of G. For example, the identity' function IG : G $\to$ G : $I_G(x) = x$ is an automorphism.

Note The word 'isomorphisms' is derived from the Greek word 'ISOS' meaning 'equal'.

Let us look at another example of an isomorphism.

Example: Consider the set $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in R \right\}$.

Then G is a group with respect to matrix addition.

Show that $f : G \to C : f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$ is an isomorphism.

Notes

Solution: Let us first verify that f is a homomorphism. Now, for any two elements

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \text{and} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \text{in G,}$$

$$r\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = f\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} = (a+c)+i(b+d)$$

= (a + ib) + (c + id)

$$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$$

Therefore, f is a homomorphism.

$$\text{Now, Ker f = } f = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a+ib=0\right\} = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a+0, b=0\right\} = \left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right\}$$

Therefore, by Theorem 4, f is 1-1.

Finally, since Im f = C. f is surjective

Therefore, f is an isomorphism.

We would like to make an important remark now.

Remark: If G_1 and G_2 are isomorphic groups, they must have the same algebraic structure and satisfy the same algebraic properties. For example, any group isomorphic to a finite group must be finite and of the same order. Thus, two isomorphic groups are algebraically indistinguishable systems.

The following result is one of the consequences of isomorphic groups being algebraically alike

Theorem 6: If f : G → H is a group isomorphism and Y ∈ G, then $< x > \simeq < f(x) >$,

Therefore.

(i) if s is of finite order, then o(x) = o(f(s)).

(ii) if x is of infinite order, so is f(x).

Proof: If we restrict f to any subgroup K of G, we have the function f | K ; K → f(K), Since f is bijective, sc is its restriction f | k ; k ≃ f(K) for any subgroup K of G. In particular, for any x ∈ G, $< x > \simeq f(< x >) = < f(x) >$,

Now if x has finite order, then o(x) = o(< x >) = o(< f(x) >) = o(f(x)), proving (i)

To prove (ii) assume hat x is of infinite order. Then < x > is an infinite group.

Therefore, < f(x) > is an infinite group, and hence, f(x) is of infinite order. So, we have proved (ii).

Example: Show that (R*,.) is not isomorphic to (C*,.).

Solution: Suppose they are isomorphic, and f : C* — R* is an isomorphism. Then

o(i) = o(f(i)), by Theorem 6, Now o(i) = 4. ∴ o(f(i)) = 4.

However, the order of any real number different from ±1 is infinite: and o(1) = 1, o(–1) = 2.

So we reach a contradiction. Therefore, our supposition must be wrong. That is, R* and C* are not isomorphic.

You must have noticed that the definition of an isomorphism just says that the map is bijective, i.e., the inverse map exists. It does not tell us any properties of the inverse. The next result does so.

Theorem 7: If $f : G_1 \to G_2$ is an isomorphism of groups, then $f^{-1} : G_2 \to G_1$ is also an isomorphism.

Proof: You know that f^{-1} is bijective. So, we only need to show that f^{-1} is a homomorphism. Let a′, b′ $\in G_2$ and $a = f^{-1}(a')$, $b = f^{-1}(b')$. Then f(a)= a′ and f(b)= b′.

Therefore, f(ab) = f(a) f(b) = a′b′. On applying f^{-1}, we get

$f^{-1}(a'b') = ab = f^{-1}(a')\, f^{-1}(b')$, Thus,

$f^{-1}(a'b') = f^{-1}(a')\, f^{-1}(b')$ for all a′, b′ $\in G_2$.

Hence, f^{-1} is an isomorphism.

From Theorem 7 we can immediately say that

$\phi^{-1} : T \to R^2 : \phi^{-1}(f_{a,b,}) = (a, b)$ is an isomorphism.

Theorem 7 says that if $G_1 \simeq G_2$, then $G_2 \simeq G_1$. We will be using this result quite often.

6.3 Group Isomorphism

In abstract algebra, a group isomorphism is a function between two groups that sets up a one-to-one correspondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are called isomorphic. From the standpoint of group theory, isomorphic groups have the same properties and need not be distinguished.

Definition and Notation

Given two groups (G, *) and (H, ⊙), a group isomorphism from (G, *) to (H, ⊙) is a bijective group homomorphism from G to H. Spelled out, this means that a group isomorphism is a bijective function $f : G \to H$ such that for all u and v in G it holds that

$$f(u * v) = f(u) \odot f(v).$$

The two groups (G, *) and (H, ⊙) are isomorphic if an isomorphism exists. This is written:

$$(G, *) \cong (H, \odot)$$

Often shorter and more simple notations can be used. Often there is no ambiguity about the group operation, and it can be omitted:

$$G \cong H$$

Sometimes one can even simply write G = H. Whether such a notation is possible without confusion or ambiguity depends on context. For example, the equals sign is not very suitable when the groups are both subgroups of the same group.

Conversely, given a group (G, *), a set H, and a bijection $f : G \to H$, we can make H a group (H, ⊙) by defining

$$f(u) \odot f(v) = f(u * v).$$

If H = G and ⊙ = * then the bijection is an automorphism (q.v.)

Intuitively, group theorists view two isomorphic groups as follows: For every element g of a group G, there exists an element h of H such that h 'behaves in the same way' as g (operates with other elements of the group in the same way as g). For instance, if g generates G, then so does h. This implies in particular that G and H are in bijective correspondence. So the definition of an isomorphism is quite natural.

An isomorphism of groups may equivalently be defined as an invertible morphism in the category of groups, where invertible here means has a two-sided inverse.

Examples:

1. The group of all real numbers with addition, (ℝ, +), is isomorphic to the group of all positive real numbers with multiplication ($\mathbb{R}^+$, ×):

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

   via the isomorphism

   $$f(x) = e^x$$

   (see exponential function).

2. The group ℤ of integers (with addition) is a subgroup of ℝ, and the factor group ℝ/ℤ is isomorphic to the group S^1 of complex numbers of absolute value 1 (with multiplication):

   $$\mathbb{R}/\mathbb{Z} \cong S^1$$

   An isomorphism is given by

   $$f(x + \mathbb{Z}) = e^{2\pi x_1}$$

   for every x in ℝ.

3. The Klein four-group is isomorphic to the direct product of two copies of $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ (see modular arithmetic), and can therefore be written $\mathbb{Z}_2 \times \mathbb{Z}_2$. Another notation is Dih_2, because it is a dihedral group.

4. Generalizing this, for all odd n, Dih_{2n} is isomorphic with the direct product of Dih_n and Z_2.

5. If (G, *) is an infinite cyclic group, then (G, *) is isomorphic to the integers (with the addition operation). From an algebraic point of view, this means that the set of all integers (with the addition operation) is the 'only' infinite cyclic group.

Some groups can be proven to be isomorphic, relying on the axiom of choice, but the proof does not indicate how to construct a concrete isomorphism.

1. The group (ℝ, +) is isomorphic to the group (ℂ, +) of all complex numbers with addition.

2. The group ($\mathbb{C}^*$, ·) of non-zero complex numbers with multiplication as operation is isomorphic to the group S^1 mentioned above.

Properties

- The kernel of an isomorphism from (G, *) to (H, ⊙), is always $\{e_G\}$ where e_G is the identity of the group (G, *)

- If (G, *) is isomorphic to (H, ⊙), and if G is abelian then so is H.

- If (G, *) is a group that is isomorphic to (H, ⊙) [where f is the isomorphism], then if a belongs to G and has order n, then so does f(a).

Notes

- If (G, *) is a locally finite group that is isomorphic to (H, ⊙), then (H, ⊙) is also locally finite.
- We also go through that 'group properties' are always preserved by isomorphisms.

Cyclic Groups

All cyclic groups of a given order are isomorphic to ($\mathbb{Z}_n$, $+_n$).

Let G be a cyclic group and n be the order of G. G is then the group generated by < x > = {e,x,..., x^{n-1}}. We will show that

$$G \cong (\mathbb{Z}_n, +_n)$$

Define

$\phi : G \to \mathbb{Z}_n = \{0, 1,..., n - 1\}$, so that $\phi(x^a) = a$. Clearly, ϕ is bijective.

Then

$\phi(x^a . x^b) = \phi(x^{a+b}) = a + b = \phi(x^a) +_n \phi(x^b)$ which proves that $G \cong \mathbb{Z}_n$, +n.

Consequences

From the definition, it follows that any isomorphism f : G → H will map the identity element of G to the identity element of H,

$$f(e_G) = e_H$$

that it will map inverses to inverses,

$$f(u^{-1}) = [f(u)]^{-1}$$

and more generally, nth powers to nth powers,

$$f(u^n) = [f(u)]^n$$

for all u in G, and that the inverse map $f^{-1} : H \to G$ is also a group isomorphism.

The relation "being isomorphic" satisfies all the axioms of an equivalence relation. If f is an isomorphism between two groups G and H, then everything that is true about G that is only related to the group structure can be translated via f into a true ditto statement about H, and vice versa.

Self Assessment

1. Let H be a subgroup of a Group G. Then H → G, i(h) = h is a homomorphism. This function is called the ....

   (a) inclusion map (b) normal function

   (c) cyclic (d) abelian

2. gof (x, y) is equal to:

   (a) gof(x) . gof(y) (b) gof(x) + gof(y)

   (c) $gof(x^{-1}) . gof(y^{-1})$ (d) $gof(x) . gof(y^{-1})$

3. Let $f : G_1 \to G_2$ be a group homomorphism thus her f is a .... of G.

   (a) subgroup (b) normal

   (c) cyclic (d) abelian

Notes

6.4 Summary

We have discussed here:

- The definition and example of a group homomorphism.
- Let f : $G_1 \to G_2$ be a group homomorphism. Then $f(e_1) = e_2$,

  $[f(x)]^{-1} = f(x^{-1})$, Im f $\leq G_2$, Ker f $\underline{\Delta}$ G_1.
- A homomorphism is 1-1 iff its kernel is the trivial subgroup.
- The definition and examples of a group isomorphism.
- Two groups are isomorphic iff they have exactly the same algebraic structure.
- The composition of group homomorphisms (isomorphisms) is a group homomorphism (isomorphism).

6.5 Keywords

Homomorphism: Homomorphism is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

Inclusion Map: Let H be a subgroup of a group G. Show that the map i : H → G, i(h) = h is a homomorphism. This function is called the **inclusion map.**

6.6 Review Questions

1. Show that f : $(R^*,.) \to (R, 4)$: f(x) = inx, the natural logarithm of x, is a group homomorphism. Find Ker f and Im f also.
2. Is f : $(GL_3(R)_3,.) \to (w^*,.)$: f(A) = det(A) a homomorphism? If so, obtain Ker f and Im f.
3. Define the natural homomorphism p from S_3 to S_3/A_3. Does (1 2) E Ker p? Does (1 2) E Im p?
4. Let S = [z ∈ C | |z| = 1}.

   Define f : (R, +) → (S,.) L $f(x) = e^{Inx}$, where n is a fixed positive integer. Is f a homomorphism? If so find Ker f.

Answers: Self Assessment

1. (a) 2. (a) 3. (b)

6.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 7: Homomorphism Theorem

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss fundamental theorem of homomorphism
- Explain the concept of automorphism

Introduction

After understanding the concept of isomorphisms. Let us prove some result about the relationship between homomorphisms and quotient groups. The first result is the Fundamental Theorem of Homomorphism for groups. It is called 'fundamental' because a lot of group theory depends upon this result. This result is also called the first isomorphism theorem.

7.1 Fundamental Theorem of Homomorphism

Theorem 1 (Fundamental Theorem of Homomorphism): Let G_1 and G_2 be two groups and $f : G_1 \to G_2$ be a group homomorphism. Then

$G_1/\text{Ker } f \simeq \text{Im } f$.

In particular, if f is onto, then $G_1/\text{Ker } f \simeq G_2$.

Proof: Let Ker f = H. Note that $H \,\underline{\Delta}\, G_1$. Let us define the function

$\psi : G_1/H \to \text{Im } f : \psi\,(Hx) = f(x)$.

At first glance it seems that the definition of ψ depends on the coset representative. But we will show that if $x, y \in G_1$ such that $Hx = Hy$, then $\psi\,(Hx) = \psi\,(Hy)$. This will prove that ψ is a well-defined function.

Now, $Hx = Hy \Rightarrow xy^{-1} \in H = \text{Ker } f \Rightarrow f(xy^{-1}) = e_2$, the identity of G_2.

$\Rightarrow f(x)[f(y)]^{-1} = e^2 \Rightarrow f(x) = f(y)$.

$\Rightarrow \psi(Hx) = \psi(HY)$.

Therefore, y is a well-defined function,

Now, let us check that ψ is a homomorphism. For Hx, Hy $\in G_1/H$,

$$\begin{aligned} \psi(Hx)(Hy)) &= \psi(Hxy) \\ &= f(xy) \\ &= f(x)\, f(y), \text{ since f is a homomorphism.} \\ &= \psi(H)\ \psi(HY) \end{aligned}$$

Therefore, ψ is a group homomorphism.

Next, let us see whether ψ is bijective or not.

Now, $\psi(Hx) = \psi(Hy)$ for Hx, HY in G_1/H

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

$\Rightarrow f(x)\ [f(y)l^{-1} = e_2$

$\Rightarrow f(xy^1) = e_2$

$\Rightarrow xy^{-1} \in \text{Ker } f = H.$

$\Rightarrow Hx = Hy$

Thus, ψ, is 1-1.

Also, any element of Im f is $f(x) = \psi(Hx)$, where $x \in G_1$.

$\therefore$ Im ψ = Im f.

So, we have proved that ψ is bijective, and hence, an isomorphism. Thus, G1/Ker f = Im f.

Now, if f is surjective, Im f = G_2. Thus, in this case $G_1/\text{Ker } f \simeq G_2$.

The situation in Theorem 1 can be shown in the following diagram.

$$\begin{tikzcd} G_1 \arrow[rr, "f"] \arrow[dr, "p"'] & & \text{Im } f \leq G_2 \\ & G_1/\text{Ker } f \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

Here, p is the natural homomorphism.

The diagram says that if you first apply p, and then ψ, to the elements of G_1, it is the same as applying f to them. That is,

$\psi \circ p = f.$

Also, note that Theorem 1 says that two elements of G_1 have the same image under f iff they belong to the same coset of Ker f.

Let us look at a few examples.

One of the simplest situations we can consider is $I_G : G \rightarrow G$. On applying Theorem 1 here, we see that $G/\{e\} \simeq G$. We will be using this identification of G/{e) and G quite often.

Example: Prove that C/R ≃ R.

Solution: Define $f : C \to R : f(a + ib) = b$. Then f is a homomorphism, Ker f = R and Im f = R. Therefore, on applying Theorem 1 we see that $C/R \simeq R$.

Example: Consider $f : Z \to (\{1, - 1\},.) : f(n) = \begin{cases} 1, \text{if n is even} \\ -1, \text{if n is odd.} \end{cases}$

At the beginning, you saw that f is a homomorphism. Obtain Ker f and Im f. What does Theorem 1 say in this case?

Solution: Let Z_e and Z_o denote the set of even and odd integers, respectively. Then

Ker f = $\{n \in Z \mid f(n) = 1\} = Z,$

Im f = $\{f(n) \mid n \in Z) = \{1, -1\}$

Thus, by Theorem 1, $Z/Z, \simeq \{1, -1\}$.

This also tells us that $o(Z/Z_e) = 2$. The two cosets of Z_e in Z are Z_e and *.

$\therefore \quad \{Z_e, Z_o\} \simeq \{1, -1\}$.

Example: Show that $GL_2(R)/SL_2(R) \simeq R^*$, where $SL_2(R) = \{A \in GL_2(R) \mid \det(A) = 1\}$.,

Solution: We know that the function

$f : GL_2(R) \to R^* : f(A) = der(A)$ is a homomorphism. Now, Ker f = $SL_2(R)$.

Also, Im f = R^*, since any $r \in R^*$ can be written as $\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$.

Thus, using Theorem 1, $GL_2(R)/SL_2(R) \simeq R^*$.

Now-we will use the Fundamental Theorem of Homomorphism to prove a very important result which classifies all cyclic groups.

Theorem 2: Any cyclic group is isomorphic to (Z, +) or $(Z_n, +)$.

Proof: Let G = < x > be a cyclic group. Define

$f : Z \to G : f(n)=x^n$.

f is a homomorphism because

$f(n + m) = x^{n+m} = x^n . x^m = f(n) f(m)$.

Also note that Im f = G.

Now, we have two possibilities for Ker I $\to$ Ker f = {0) or Ker f $\neq$ {0}.

Case 1 (Ker f = {0)): In this case f is 1-1. Therefore, f is an isomorphism. Therefore, by Theorem 7 of unit 6, f-1 is an isomorphism. That is, $G \simeq (Z, +)$.

Case 2 (Ker f # {0)): Since Ker $f \leq Z$, we know that Ker f = nZ, for some $n \in N$. Therefore, by the Fundamental Theorem of Homomorphism, $Z/nZ \simeq G$.

$\therefore G = Z/nZ = (Z_n, +)$.

Over here note that since < x > = Z_n, o(x) = n. So, a finite cyclic group is isomorphic to Z_n, where n is the order of the group.

Theorem 3: If H and K are subgroups of a group G, with K normal in G, then $H/(H \cap K) \simeq (HK)/K$.

Proof: We must first verify that the quotient groups $H/(H \cap K)$ and $(HK)/K$ are well defined. You know that $H \cap K \trianglelefteq H$. You know that $HK \leq G$. Again, you know that $K \trianglelefteq HK$. Thus, the given quotient groups are meaningful.

Now, what we want to do is to find an onto homomorphism $f : H - (HK)/K$ with kernel $H \cap K$. Then we can apply the Fundamental Theorem of Homomorphism and get the result. We define $f : H \to (HK)/K : f(h) = hK$.

Now, for $x, y \in H$,

$f(xy) = xyK = (xK)(yK) = f(x) f(y)$.

Therefore, f is a homomorphism.

We will show that Im $f = (HK)/K$. Now, take any element $hK \in$ Im f. Since $h \in H$, $h \in HK$

$\therefore$ $hK \in (HK)/K$. $\therefore$ Im $f \subseteq (HK)/K$. On the other hand, any element of $(HK)/K$ is

$hkK = hK$, since $k \in K$.

$\therefore$ $hkK \in$ Im f. $(HK)/K \subseteq$ Im f.

$\therefore$ Im $f = (HK)/K$.

Finally, Ker $f = \{ h \in H \mid f(h) = K \} = \{ h \in H \; hK = K \}$

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

$= H \cap K$.

Thus, on applying the Fundamental Theorem, we get $H / (H \cap K) \simeq (HK) / K$

We would like to make a remark here.

Remark: If H and K are subgroups of (G.+), then Theorem 3 says that

$(H + K) / K \simeq H/H \cap K$.

Theorem 4: Let H and K be normal subgroups of a group G such that $K \subseteq H$. Then $(G/K)/(H/K) \simeq G/H$.

Proof: We will define a homomorphism from G/K onto G/H, whose kernel will turn out to be H/K.

Consider $f : G/K \to G/H : f(Kx) = Hx$. f is well-defined because $Kx = Ky$ tor $x, y \in G$

$\Rightarrow xy^{-1} \in K \subseteq H \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy \Rightarrow (Kx) = f(Ky)$

7.2 Automorphisms

Let us start discussing the concept of automorphism

Let G be a group. Consider

Aut $G = \{ f : G \to G \mid f \text{ is an isomorphism} \}$.

You have already seen that the identity map $I_G \in$ Aut G. You know that Aut G is closed under the binary operation of composition. Iff E Aut G, then $f^{-1} \in$ Aut G. We summarise this discussion in the following theorem.

An isomorphism from a group (G,*) to itself is called an Automorphisms of this group. Thus it is a bijection $f : G \to G$ such that

$f(u) * f(v) = f(u * v)$.

An automorphism always maps the identity to itself. The image under an automorphism of a conjugacy class is always a conjugacy class (the same or another). The image of an element has the same order as that element.

The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group G, denoted by Aut(G), forms itself a group, the automorphism group of G.

For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse this is the trivial automorphism, e.g. in the Klein four-group. For that group all permutations of the three non-identity elements are automorphisms, so the automorphism group is isomorphic to S_3 and Dih_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with corresponding changes in the other elements. The Automorphisms group is isomorphic to Z_{p-1}. For example, for n = 7, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 = 1$ (modulo 7), while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely.

The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these.

The automorphism group of $Z_2 \times Z_2 \times Z_2 = Dih_2 \times Z_2$ has order 168, as can be found as follows. All 7 non-identity elements play the same role, so we can choose which plays the role of (1,0,0). Any of the remaining 6 can be chosen to play the role of (0, 1, 0). This determines which corresponds to (1, 1, 0). For (0, 0, 1) we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphisms. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements. The lines connecting three points correspond to the group operation: a, b, and c on one line means a + b = c, a + c = b, and b + c = a. See also general linear group over finite fields.

For Abelian groups all automorphisms except the trivial one are called outer automorphisms.

Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer Automorphisms.

Theorem 5: Let G be a group. Then Aut G, the set of automorphisms of G, is a group.

Let us look at an example of Aut G.

Example: Show that Aut $Z \simeq Z_1$.

Solution: Let $f : Z \to Z$ be an automorphism. Let f(1) = n. We will show that n = 1

or – 1. Since f is onto and $1 \in Z$, $\exists\, m \in Z$such that f(m) = l, i.e., mf(l)=l, ie., m=l.

$\therefore$ n = 1 or n = –1.

Thus, there are only two elements in Aut Z, I and –I.

So Aut $Z = \langle -I \rangle \simeq Z_2$.

Now given an element of a group G. We will define an automorphism of G corresponding to it.

Consider a fixed element $g \in G$. Define

$f_g : G \to G : f_g(x) = gxg^{-1}$.

We will show that f_g is an automorphism of G.

(i) f, is a homomorphism : If x, y $\in$ G, then

$$f_g(xy) = g(xy)\ g^{-1}$$
$$= gx(e)\ yg^{-1}, \text{ where e is the identity of G.}$$
$$= gx(g^{-1}g)\ yg^{-1}$$
$$= (gxg^{-1})\ (gyg\text{-}^{1})$$
$$= f_g(x)\ f_g(dy).$$

(ii) f_g is 1-1 : For x, y $\in$ G, $f_g(x) = f_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y$, by the cancellation laws in G.

(iii) f_g is onto : If y $\in$ G, then

$$Y = (gg^{-1})y(gg^{-1})$$
$$= (g^{-1}yg)g^{-1}$$
$$= f_g(g^{-1}yg) \in \text{lm } f_g.$$

Thus, f, is an automorphism of G.

Definition: f_g is called an inner automorphism of G induced by the element g in G. The subset of Aut G consisting of all inner automorphism of G is denoted by Inn G.

For example, Let us compute $f_g(1)$. $f_g(l\ 3)$ and $f_g(1\ 2\ 3)$, where g = (1 2). Note that g^{-1} = (1 2) = g.

Now, f_g (1) = g a I o g^{-1} = I,

$f_g(l\ \ 3) = (1\ 2)\ (1\ 3)\ (1\ 2) = (2\ 3).$

$f_g(l\ 2\ 3) = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2).$

Theorem 6: Let G be a group. Then Inn G is a normal subgroup of Aut G. i

Proof: Inn G is non-empty, because $I_G = f_e \in$ Inn G, where e is the identity in G.

Now, let us see if f, o fh $\in$ Inn G for g, h $\in$ G.

For any x $\in$ G, $\quad f_g \,.\, f_n(x) = fg(hxh^{-1})$

$$= g(hxh^{-1})\ g^{-1}$$
$$= (gh)x\ (gh)^{-1}$$
$$= fgh(x)$$

Thus, $f_{gh} = f_g$ o f_h, i.e., Inn G is closed under composition. Also $f_e = I_G$ belongs to Inn G.

Now, for $f_g \in$ Inn G, 3 $fg^{-1} \in$ Inn G such that

f_g o $f_g^{-1} = f_{gg}^{-1} = f_e = I_G$. Similarly, $f_{g\text{-}1}$o $f_g = I_G$.

Thus, $f_g^{-1} = (f_g)^{-1}$. That is every element of Inn G has an inverse in Inn G.

This proves that Inn G is a subgroup of Aut G.

Now, to prove that Inn $\trianglelefteq$ Aut G, let $\phi \in$ Aut G and $f_g \in$ Inn G. Then, for any x $\in$ G

$\phi^{-1} \times f_g \times \phi(x) = \phi^{-1} \times f_g(\phi\ (x))$

$= \phi^{-1}\ (g\phi(x)g^{-1})$

$= \phi^{-1}\ (g)\ \phi^{-1}(\phi(x))\ \phi^{-1}(g^{-1})$

Notes

$= \phi^{-1}(g)\,x[\phi^{-1}(g)]^{-1}$

$= f_{\phi^{-1}(g)}(x)$. (Note that ϕ-1(g) ∈ G.)

$\therefore\ \phi^{-1} \circ f_g \circ \phi = f_{\phi^{-1}(g)} \in \text{Inn}\,G\ \forall\ \phi \in \text{Aut}\,G$ and $f_g \in \text{Inn}\,G$.

$\therefore$ Inn G $\trianglelefteq$ Aut G.

Now we will prove an interesting result which relates the cosets of the centre of a group G to lnn G. Recall that the centre of G, $Z(G) = \{ x \in G \mid xg = gx\ \forall\ g \in G \}$.

Theorem 7: Let G be a group. Then G/Z(G) ≃ Inn G.

Proof: As usual, we will use the powerful Fundamental Theorem of Homomorphism to prove this result.

We define $f : G \to \text{Aut}\,G : f(g) = f_g$.

Firstly, f is a homomorphism because for g, h ∈ G,

$f(gh) = f_{gh}$

$= I, \circ f_h$ (sec proof of Theorem 13)

$= [(g) \circ f(h)$.

Next, Im F = $(f_g, 1\ g \in G) =$ Inn G.

Finally, Ker $f = (g \in G \mid f, = I_G \}$

$= \{ g \in G\ [\ f_g(x) = x\ \forall\ x \in G \}$

$= \{ g \in G \mid gxg^{-1} = x\ \forall\ x \in G \}$

$= \{ g \in G \mid gx = xg\ \forall\ x \in G \}$

$= Z(G)$.

Therefore, by the Fundamental Theorem,

G/Z(G) ≃ Inn G.

Self Assessment

1. An isomorphism of a group G itself is called as an .... of G.

   (a) Homomorphism (b) automorphism

   (c) Herf (d) one-to-one function

2. The word isomorphisms is derived from Greek word ISOS meaning ....

   (a) equal (b) unequal

   (c) bijective (d) subjective

7.3 Summary

- The proof of the Fundamental Theorem of Homomorphism, which says that if $f : G_1 \to G_2$ is a group homomorphism, then $G_1/\text{Ker}\,f \simeq \text{Im}\,f$,

Notes

- Any infinite cyclic group is isomorphic to (Z, +). Any finite cyclic group of order n is isomorphic to (Z , +).
- Let G be a group, $H \leq G$, $K \trianglelefteq G$. Then $H/(H \cap K) \simeq HK)/K$.
- Let G be a group, $H \trianglelefteq G$, $K \trianglelefteq G$, $K \subseteq H$, Then $(G/K)/(H/K) \simeq G/H$.
- The set of automorphism of a group G, Aut G, is a group with respect to the composition of functions.
- Inn G $\trianglelefteq$ Aut G, for any group G.
- $G/Z(G) \simeq$ Inn G, for any group G.

7.4 Keywords

Group Homomorphism: Iff : $G_1 \to G_2$ and $g : G_2 \to G_3$ are two group homomorphisms, then the composite map $g \,.\, f : G_1 \to G_3$ is also a group homomorphism.

Isomorphisms: Let G_1 and G_2 be two groups. A homomorphism $f : G_1 \to G_2$ is called an isomorphism if f is 1-1 and onto.

7.5 Review Questions

1. Let G be a group and $H \trianglelefteq G$. Show that there exists a group G_1 and a homomorphism $f : G \to G_1$ such that Ker f = H.
2. Show that the homomorphic image of a cyclic group is cyclic i.e., if G is a cyclic group and $f : G \to G'$ is a homomorphism, then f(G) is cyclic.
3. Show that Z = nZ, for a fixed integer n,

   (Hint: Consider $f : (Z, +) \to (nZ, +) : f(k) = nk$)
4. Is $f : Z \to Z : f(x) = 0$ a homomorphism? An isomorphism?

Answers: Self Assessment

1. (b) 2. (a)

7.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Notes

Unit 8: Permutation Groups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the concept of permutation group
- Explain the symmetric group
- Describe the cyclic decomposition
- Prove and use Cayley's Theorem

Introduction

In earlier classes, you have studied about the symmetric group. As you have often seen in previous units, the symmetric groups S, as well as its subgroups, have provided us a lot of examples. The symmetric groups and their subgroups are called permutation groups. It was the study of permutation groups and groups of transformations that gave the foundation to group theory. In this unit, we will prove a result by the mathematician Cayley, which says that every group is isomorphic to permutations group. This result is what makes permutation groups so important.

8.1 Symmetric Group

In earlier units, you have studied that a permutation on n non-empty set X is a bijective function from X onto X. We denote the set of all permutations on X by S(X).

Suppose X is a finite set having n elements. For simplicity, we take these elements to be 1, 2, . . . , n. Then, we denote the set of all permutations on these n symbols by S_n.

We represent any $f \in S_n$ in n 2-line form as

$$f = \begin{pmatrix} 1 & 2 & .... & n \\ f(1) & f(2) & .... & f(n) \end{pmatrix}.$$

Now, there are n possibilities for f(l), namely, 1, 2, . . . , n. Once f(1) has been specified, there are (n – 1) possibilities for f(2), namely, {1, 2, . . . , n} \ {f(1)}. This is because f is 1-1. Thus, there are n(n – 1) choices for f(1) and f(2). Continuing in this manner, we see that there are n! different ways in which f can be defined. Therefore, S, has n! element.

Now, let us discuss at the algebraic structure of S(X), for any set X. The composition of permutations is a binary operation on S(X). To help you regain practice in computing the composition of permutations, consider an example.

Let f = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and g = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ be in S_4.

Then, to get fog we first apply g and then apply f.

$\therefore$ f o g(1) = f(g(1)) = f(4) = 3.

f o g (2) = f(g(2)) f(1) = 2.

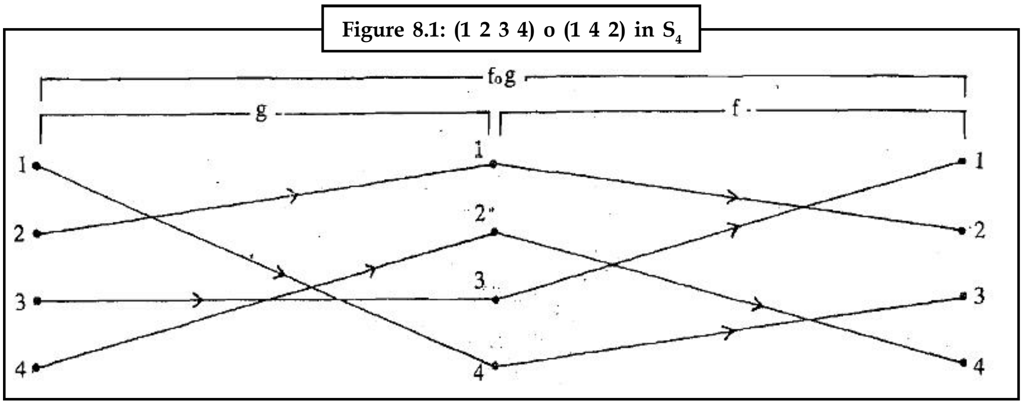
f o g (3) = f(g(3)) = f(3) = 1.

f o g (4) = f(g(4)) = f(2) = 4.

$$\therefore \quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

We show this process diagrammatically in Figure 8.1.

Figure 8.1: (1 2 3 4) o (1 4 2) in S_4



Now, let us go back to S(X), for any set k.

Theorem 1: Let X be a non-empty set. Then the system (S(X), 0) forms a group, called the symmetric group of X.

Thus, S_n is a group of order n!. We call S_n, the symmetric group of degree n. Note that if $f \in S_n$, then

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & .... & f(n) \\ 1 & 2 & .... & n \end{pmatrix}.$$

Notes

Remark: From now we will refer to the composition of permutations as multiplication of permutations. We will also drop the composition sign. Thus, we will write f o g as fg.

The two-line notation that we have used for a permutation is rather cumbersome. In the next section we will see how to use a shorter notation.

8.2 Cyclic Decomposition

Let us first discuss what a cycle is.

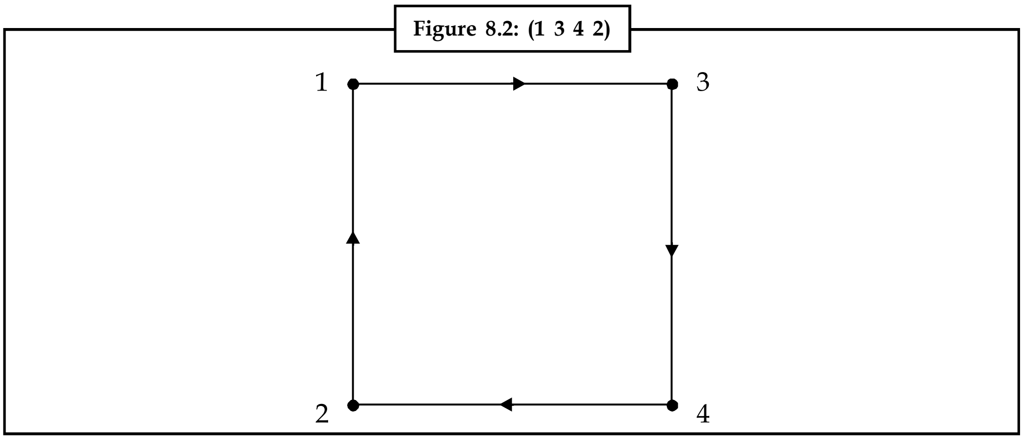
Consider the permutation f = $\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}$. Choose any one of the symbols say 1.

Now, we write down a left hand bracket followed by I :	(1
Since f maps 1 to 3, we write 3 after 1 :	(1 3
Since f maps 3 to 4, we write 4 after 3 :	(1 3 4
Since f maps 4 to 2, we write 2 after 4 :	(1 3 4 2
Since f maps 2 to 1 (the symbol we started with), we close the brackets after the symbol	(1 3 4 2)

Thus, we write f = (1 3 4 2). This means that f maps each symbol to the symbol on its right, except for the final symbol in the brackets, which is mapped to the first.

If we had chosen 3 as our starting symbol we would have obtained the expression (3 4 2 1) for f. However, this means exactly the same as (1 3 4 2), because both denote the permutation which we have represented diagrammatically in Figure 8.2.

Figure 8.2: (1 3 4 2)



Such a permutation is called a 4-cycle, or a cycle of length 4. Figure 8.2 can give you an indication as to why we give this name.

Let us give a definition now.

Definition: A permutation f ∈ S_n, is called an r-cycle (or cycle of length r) if there are r distinct integers i_1, i_2,, i_3, . . . , i_r lying between 1 and n such that

$f(i_1) = i_2$, $f(i_2) = i_3$, ... , $f(_{i,-1}) = i_r$, $f(i_r) = i_1$.

and $f(k) = k \ \forall \ k \notin \{i_1, i_2 , . . . , i_r)$.

Then, we write $f = (i_1 \, i_2 \, ... \, i_r)$.

Notes

In particular, 2-cycles are called transpositions. For example, the permutation f = (2 3) $\in S_3$ is a transposition. Here f(1) = 1, f(2) = 3 and f(3) = 2.

Later you will see that transpositions play a very important role in the theory of permutations.

Now consider any 1-cycle (i) in S,. It is simply the identity permutation $I = \begin{pmatrix} 1 & 2 & .... & n \\ 1 & 2 & .... & n \end{pmatrix}$, since it maps i to i and the other (n - 1) symbols to themselves.

Let us see some examples of cycles in S_3 (1 2 3) is the 3-cycle that takes 1 to 2, 2 to 3 and 3 to 1. There are also 3 transpositions in S_3, namely, (1 2), (1 3) and (2 3).

Now, can we express any permutation as a cycle? No. Consider the following example from S_5. Let g be the permutation defined by

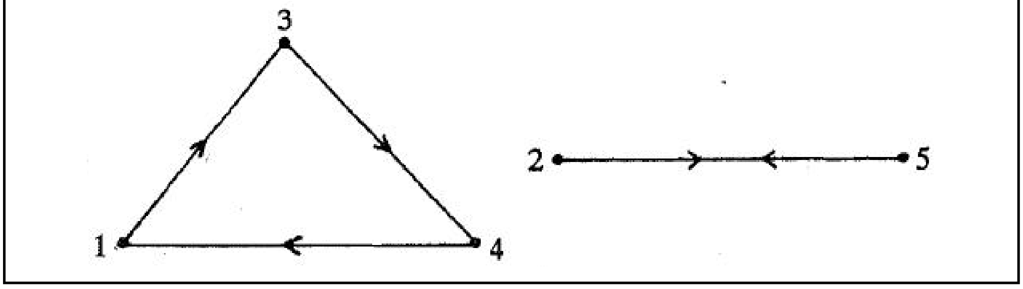
$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

If we start with the symbol 1 and apply the procedure for obtaining a cycle to g, we obtain (1 3 4) after three steps, Because, g maps 4 to 1, we close the brackets, even though we have not yet written down all the symbols. Now we simply choose another symbol that has not appeared so far, say 2, and start the procedure of writing a cycle again. Thus, we obtain another cycle (2 5). Now, all the symbols are exhausted.

$\therefore$ g = (1 3 4) (2 5).

We call this expression for g a product of a 3-cycle and a transposition. In Figure 8.3 we represent g by a diagram which shows the 3-cycle and the 2-cycle clearly.

Figure 8.3: (1 3 4) (2 5)



Because of the arbitrary choice of symbol at the beginning of each cycle, there are many ways of expressing g. For example,

g = (4 1 3) (2 5) = (2 5) (1 3 4) = (5 2) (3 4 1).

That is, we can write the product of the separate cycles in any order, and the choice of the starting element within each cycle is arbitrary.

So, you see that g can’t be written as a cycle; it is a product of disjoint cycles.

Definition: We call two cycle disjoint if they have no symbol in common. Thus, disjoint cycles move disjoint sets of elements, (Note that f ! S,, moves a symbol i if f(i) ≠ i. We say that f fixes i if f(i) = i.)

So, for example, the cycles (1 2) and (3 4) in S_4 are disjoint. But (1 2) and (1 4) are not disjoint, since they both move 1.

Notes

Note that if f and g are disjoint, then fg=-gf, since f and g move disjoint sets of symbols.

Now let us examine one more example. Let h be the permutation in S_5 defined by

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}.$$

Following our previous rules, we obtain

h = (1 4 5) (2) (3),

because each of the symbols 2 and 3 is left unchanged by h. By convention, we don't include the 1-cycles (2) and (3) in the expression for h unless we wish to emphasize them, since they just represent the identity permutation. Thus, we simply write h = (1 4 5).

The same process that we have just used is true for any cycle. That is, any r-cycle $(i_1\, i_2 \ldots\ldots i_r)$ can be written as $(i_1\, i_r)\, (i_1\, i_1) \ldots\ldots (i_1\, i_2)$, a product of transpositions.

Now we will use Theorem 2 to state a result which shows why transpositions are so important in the theory of permutations.

Theorem 2: Every permutation in S_n $(n \geq 2)$ can be written as a product of transpositions.

Proof: The proof is really very simple. By Theorem 1 every permutation, apart from I, is a product of disjoint cycles. Also, you have just seen that every cycle is a product of transpositions. Hence, every permutation, apart from I, is a product of transpositions.

Also, I = (1 2) (1 2). Thus, I is also a product of transpositions. So, the theorem is proved.

Let us see how Theorem 3 works in practice. This is the same as (1 4) (1 2) (1 3) (1 5).

Similarly, the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$

= (1 3 4) (2 6 5) = (1 4) (1 3) (2 5) (2 6).

The decomposition given in Theorem 3 leads us to a subgroup of S_n that we will now discuss.

8.3 Alternating Group

You have seen that a permutation in S_n can be written as a product of transpositions. But all such representations have one thing in common – if a permutation in S_n is the product of an odd number of transpositions in one such representation, then it will be a product of an odd number of transpositions in any such representation. Similarly, if $f \in S_n$ is a product of an even number of transpositions in one representation, then f is a product of an even number of transpositions in any such representation. To see this fact we need the concept of the signature or sign function.

Definition: The signature of $f \in S_n$, $(n \geq 2)$ is defined to be

$$\text{sign } f = \prod_{i,j=1} \frac{f(i) - f(i)}{j - i}$$

For example, for $f = (1\ 2\ 3) \in S_3$,

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

$$=\left(\frac{3-2}{1}\right)\left(\frac{1-2}{2}\right)\left(\frac{1-3}{1}\right)=1.$$

Similarly, iff = (1 2) ∈ S_3, then

$$\text{sign f} = \frac{f(2)-f(1)}{2-1}\cdot\frac{f(3)-f(1)}{3-1}\cdot\frac{f(3)-f(2)}{3-2}$$

$$=\left(\frac{1-2}{1}\right)\left(\frac{3-2}{2}\right)\left(\frac{3-1}{1}\right)=-1.$$

Henceforth, whenever we talk of sign f, we shall assume that f ∈ S_n for some n ≥ 2.

Theorem 3: Let f, g ∈ S,. Then sign (f o g) = (sign f) (sign g).

Proof: By definition,

$$\text{sign fog } = \prod_{\substack{i,j=1\\ i<j}}^{n}\frac{f(g(j))-f(g(i))}{j-i}$$

$$=\prod_{i,j}\frac{f(g(j))-f(g(i))}{g(j)-g(i)}.\prod_{i,j}\frac{g(j)-g(i)}{j-i}$$

Now, as i and j take all possible pairs of distinct values from 1 to n, so do g(i) and g(j), since g is a bijection.

$$\therefore \qquad \prod_{i<j}\frac{f(g(j))-f(g(i))}{g(j)-g(i)}=\text{sign f.}$$

∴ sign (fog) = (sign f) (sign g).

Now we will show that Im (sign) = (1, – 1}.

Theorem 4: (a) If t ∈ S, is a transposition, then sign t = – 1.

(b) sign f = 1 or - 1 ∀ f ∈ S,.

(c) Im (sign) = (1, –1).

Proof: (a) Let t = (p q), where p < q.

Now, only one factor of sign t involves both p and q, namely,

$$\frac{t\,(q)-t}{q-p}=\frac{p-1}{q-p}=1.$$

Every factor of sign t that doesn't contain p or q equals 1, since

$$\frac{t(i)-t(j)}{i-j}=\frac{i-j}{i-j}=1, \text{ if } i, j \neq p, q.$$

The remaining factors contain either p or q, but not both. These can be paired together to form one of the following products.

$$\frac{t(i)-t(p)}{i-p}\cdot\frac{t(i)-t(q)}{i-q}=\frac{i-q}{i-p}\cdot\frac{i-p}{i-q}=1, \text{ if } i>q,$$

Notes

$$\frac{t(i)-t(p)}{i-p}\,\frac{t(q)-t(i)}{q-i}=\frac{i-q}{i-p}\cdot\frac{p-i}{q-i}=1, \text{ if } q>i>p,$$

$$\frac{t(p)-t(i)}{p-i}\,\frac{t(q)-t(i)}{q-i}=\frac{q-i}{p-i}\cdot\frac{p-i}{q-i}=1, \text{ if } i>p,$$

Taking the values of all the factors of sign t, we see that sign t = –1.

(b) Let $f \in S$,. By Theorem 3 we know that $f = t_1,t_2 \dots t$, for some transpositions $t_1, \dots t_r$ in S_n.

$\therefore$ sign f = sign $(t_1 \, t_2 \dots t,)$

= (sign t_1) (sign t_2) . . . . . sign (t_r), by Theorem 3.

= $(-1)^r$, by (a) above.

$\therefore$ sign f = 1 or –1.

(c) We know that Im (sign) $\subseteq \{1, -1\}$.

We also know that sign t = –1, for any transposition t; and sign I = 1.

$\therefore \{1, -1\} \subseteq$ Im {sign}

$\therefore$ Im (sign) = {1, –1}.

Now, we are in a position to prove what we said at the beginning of this section.

Theorem 5: Let $f \in S$, and let

$f = t_1t_2 \dots t_r = t_1' \, t_2' \dots t_4'$

be two factorisations of f into a product of transpositions. Then either both r and s are even integers, or both are odd integers.

Proof: We apply the function sign: $S_n \to \{1, -1\}$ to $f = t_1t_2 \dots t_r$.

By Theorem 4 we see that

sign f = (sign t_1) (sign t_2) ...... (sign t_r) = (- 1)′.

$\therefore$ sign $(t_1' \, t_2' \dots t_s')$ = (–1) substituting $t_1' \, t_2' \dots$ ts′ for f.

that is, $(-1)^s = (-1)^r$.

This can only happen if both s and r are even, or both are odd.

So, we have shown that for $f \in S$, the number of factors occurring in any factorisation of f into transposition is always even or always odd. Therefore, the following definition is meaningful.

Definition: A permutation $f \in S_n$, is called even if it can be written as a product of an even sign number of transposition. f is called odd if it can be represented as a product of an odd number of transpositions.

For example, $(1\ 2) \in S_3$ is an odd permutation. In fact, any transposition is an odd permutation. On the other hand, any 3-cycle is an even permutation, since

(i j k) = (i k) (i j)

Now, we define an important subset of S_n, namely,

A, = (f $\in$ Sn, | f is even).

We'll show that A,, Δ S_n, and that $o(A_n) = \frac{n!}{2}$, for $n \geq 2$.

Theorem 6: The set A,, of even permutations in S,, forms a normal subgroup of S_n, of order $\frac{n!}{2}$.

Proof: Consider the signature function,

sign : $S_n \to (1, -1)$.

Note that (1, –1) is a group with respect to multiplication. Now, Im (sign) = (1, –1). Let us obtain Ker (sign).

Ker (sign) = $\{ f \in S_n \mid \text{sign } f = 1 \}$

$= (f \in S_n \mid f \text{ is even})$

= A.

$\therefore \quad A \trianglelefteq S_n$.

Further, by the Fundamental Theorem of Homomorphism

$S_n/A_n \simeq (1, -1)$.

$\therefore \quad o(S_n/A_n) = 2$, that is, $\frac{o(S_n)}{o(A_n)} = 2$.

$\therefore \quad o(An) = \frac{o(S_n)}{2} = \frac{n!}{2}$.

Note that this theorem says that the number of even permutations in S, equals the number of odd permutations in S,.

Theorem 6 leads us to the following definition.

Definition: A,, the group of even permutations in S_n, is called the alternating group of degree n.

Let us look at an example that you have already seen in previous units, A_3. Now, Theorem 6 says that $o(A_3) = \frac{3!}{2} = 3$. Since (1 2 3) = (1 3) (1 2), (1 2 3) $\in A_3$. Similarly,

(1 3 2) $\in A_3$. Of course, $I \in A_3$.

$\therefore A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2))$.

A fact that we have used in the example above is that an r-cycle is odd if r is even, and even if r is odd. This is because $(i_1 i_2 \ldots. i_r,) = (i_1\ i,)\ (i_1\ i_{r-1}) \ldots\ldots (i_1\ i_2)$, a product of (r – 1) transpositions.

Now, for a moment, let us go back to Unit 4 and Lagrange's theorem. This theorem says that the order of the subgroup of a finite group divides the order of the group. We also said that if n | o(G), then G need not have a subgroup of order n. Now that you know what A_4 looks like, we are in a position to illustrate this statement.

We will show that A_4 has no subgroup of order 6, even though 6 | o (A_4). Suppose such a subgroup H exists. Then o(H) = 6, o (A_4) = 12. $\therefore$ (A_4 : H | = 2. $\therefore$ H $\trianglelefteq$ A4 (see Theorem 3, Unit 5). Now, A_4/H is a group of order 2.

$(Hg)^2 = H \ \forall \ g \in A_4$. (Remember H is the identity of A_4/H.)

$\therefore \quad g^2 \in H \ \forall \ g \in A_4$.

Now, (1 2 3) E A_4. $\therefore$ (1 2 3)* = (1 3 2) $\in$ H.

Notes

Similarly, $(1\ 3\ 2)^2 = (1\ 2\ 3) \in H$. By the same reasoning (1 4 2), (1 2 4), (1 4 3), (1 3 4), (2 3 4), (2 4 3) are also distinct element of H. Of course, $I \in H$.

Thus, H contains at least 9 elements.

$\therefore$ $o(H) \geq 9$. This contradicts our assumption that $o(H) = 6$.

Therefore, A_4 has no subgroup of order 6.

We use A_4 to provide another example too. (See how useful A_4 is!) In earlier unit we'd said that if $H \trianglelefteq N$ and $N \trianglelefteq G$, then H need not be normal in 6. Well, here's the example.'

Consider the subset $V_4 = \{I, (1\ 2)\ (3\ 4), (1\ 4)\ (2\ 3), (1\ 3)\ (2\ 4))$ of A_4.

Now, let $H = \{I, (1\ 2)\ (3\ 4)\}$. Then H is a subgroup of index 2 in V_4. $\therefore$ H A V_4.

So, $H \trianglelefteq V_4$, $V_4 \trianglelefteq A_4$. But $H \ntrianglelefteq A_4$. Why? Well, $(1\ 2\ 3) \in A_4$ is such that

$(1\ 2\ 3)^{-1}\ (1\ 2)\ (3\ 4)\ (1\ 2\ 3) = (1\ 3)\ (2\ 4) \notin H$.

And now let us see why permutation groups are so important in group theory.

8.4 Cayley's Theorem

Most finite groups that first appeared in mathematics were groups of permutations. It was the English mathematician Clayley who first realised that every group has the algebraic structure of a subgroup of **S(X),** for some set X. In this section we will discuss Cayley's result and some of its applications.

Theorem 7 (Cayley): Any group G is isomorphic to a subgroup of the symmetric group S(G).

Proof: For $a \in G$, we define the left multiplication function

$f_a : G \rightarrow G : f_4(x) = ax$.

f_a is 1-1, since

$fa(x) = fa(y) \Rightarrow ax = ay \Rightarrow x = y\ x, y\ E\ G$.

fa is onto, since any x E G is **f,** (a – 'x).

:. $f_a \in S(G)\ \forall\ a \in G$.

(Note that S(G) is the symmetric group on the set G.)

Now we define a function $f : G \rightarrow S(G) : f(a) = fa$.

We will show that f is an injective homomorphism. For this we note that

$(f_{ao}, f_b)\ (x) = f_a(bx) = abx = f_{ab}\ (x)\ \forall\ a, b \in G$.

$\therefore$ $f(ab) = f_{ab} = f_a \text{ o } f_b = f(a) \text{ of } (b)\ \forall\ a, b \in G$.

That is, f is a homomorphism.

Now, $\text{Ker } f = (a \in G \mid fa = I_G)$

$= (a \in G \mid f_a(x)=x\ \forall\ x \in G \}$

$= (a \in G \mid a\,x = x\ \forall\ x \in G \}$

$= \{e\}$.

Thus, by the Fundamental Theorem of Homomorphism,

G/Ker f ≃ Im f ≤ S(G),

that is, G is isomorphic to a subgroup of S(G).

As an example of Cayley's theorem, we will show you that the Klein 4-group K_4 is isomorphic to the subgroup V_4 of S_4. The multiplication table for K_4 is

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Self Assessment

1. If .... is a group of order n!. Then we call S, the symmetric group of define n.

   (a) S^n (b) S_n

   (c) S_n^{-1} (d) Sn^{-1}

2. Every permutation is S_n (n ≥ ....) can be written as produce of transposition

   (a) n ≥ 2 (b) n ≥ 3

   (c) n ≥ 4 (d) n ≥ 5

3. If t ∈ S, is a transposition then sight = ...

   (a) –1 (b) 1

   (c) 0 (d) 2

4. Any group G is .... to a subgroup of the symmetric group S(G)

   (a) isomorphic (b) homomorphic

   (c) automorphic (d) surjective

5. Any group is isomorphic to a .... group.

   (a) normal group (b) subgroup

   (c) cyclic group (d) permutation group

8.5 Summary

- The symmetric group S(X), for any set X, and the group S,, in particular.
- The definitions and some properties of cycles and transpositions.
- Any non-identity permutation in S_n can be expressed as a disjoint product of cycles.
- Any permutation in S_n (n ≥ 2) can be written as a product of transpositions.
- The homomorphism sign : S_n — {1, – 1}, n ≥ 2.
- Odd and even permutations.
- A,, the set of even permutations in S,, is a normal subgroup of S_n of order $\frac{n!}{2}$, for
- Any group is isomorphic to a permutation group.

8.6 Keywords

Symmetric Group: Let X be a non-empty set. Then the system (S(Xj, 0) forms a group, called the symmetric group of X.

Permutation: A permutation f ∈ S, is called an r-cycle (or cycle of length r) if there are r distinct integers $i_1, i_2, i_3, \ldots, i_r$ lying between 1 and n.

8.7 Review Questions

1. Show that (S,, °) is a non-commutative group for $n \geq 3$.

   (Hint: Check the $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ don't commute.)

2. Write down 2 transpositions, 2 3-cycles and a 5-cycle in S_5.

3. Show that every permutation in S_n is a cyclic iff $n < 4$.

4. Iff = $(i_2\ i_2\ , \ldots i)$ ∈ S,, then show that $f^{-1} = (i_r\ i_{r-1} \ldots i_2 i_1)$.

5. Iff is an r-cycle, then show that o(f) = r, i.e., $f^r = I$ and $f^5 \neq I$, if $s < r$.

   (Hint: If $f = (i_1, i_2 \ldots i)$, then $f(i_1) = i_2$, $r^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_m$)

6. Express the following cycles as products of transpositions.

   (a) (1 3 5) (b) (5 3 1)

   (c) (2 4 5 3)

7. Write the permutation in E3(b) as a product of transpositions.

8. Show that (1 2 .... 10) = (1 2) (2 3) . . . (9 10).

9. Check that $(V_4, °)$ is a normal subgroup of A_4.

Answers: Self Assessment

1.	(b)	2.	(a)	3.	(a)
4.	(a)	5.	(d)		

8.8 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 9: Direct Products

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss direct product of groups
- State Sylow theorem
- Explain groups of order 1 to 10.

Introduction

In the last unit, we have studied about permutation group. This unit will provide you the information related to 15 finite groups and direct products. Let us understand all these one by one.

9.1 Direct Product of Groups

In this section, we will discuss a very important method of constructing new groups. We will first see how two groups can be combined to form a third group. Then we will see how two subgroups of a group can be combined to form another subgroup.

9.1.1 External Direct Product

In this sub-section we will construct a new group from two or more groups that we already have.

Let $(G_1, *_1)$ and $((G_2, *_2)$ be two groups. Consider their Cartesian product $G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$.

Notes

Can we define a binary operation on G by using the operations on G_1 and G_2? Let us try the method, namely, component-wise multiplication. That is, we define the operation * on G by $(a,b) * (c, d)=(a*_1 c, b*_2 d)$ $\forall$ $a, c \in G_1, b, d \in G_2$.

So, you have proved that $G = G_1 \times G_2$ is a group with respect to *. We call G the external direct product of $(G_1, *_1)$ and $(G_2, *_2)$.

For example, R^2 is the external direct product of R with itself.

Another example is the direct product (Z, +) × (R*, .) in which the operation is given by $(m, X) * (n, y) = (m + n, xy)$.

We can also define the external direct product of 3, 4 or more groups on the same lines.

Definition: Let $(G_1, *_1), (G_2, *_2), \ldots\ldots, (G_{,}, *_n)$ be n groups. Their external direct product is the group (G, *), where

$G = G_1 \times G_2 \ldots\ldots \times G_n$ and

Thus, R^n is the external direct product of n copies of R,

We would like to make a remark about notation now.

Remark: Henceforth, we will assume that all the operations $*, *_1, \ldots, *_n$ are multiplication, unless mentioned otherwise. Thus, the operation on

$G = G_1 \times G_2 \times \ldots\ldots \times G_n$ will be given by

$(a_1, \ldots\ldots, a) . (b_1, \ldots\ldots, b)$

$= (a_1b_1, a_2b_2, \ldots., a_ab_a,)$ $\forall$ $a_i, b_i \in G_i$.

Now, let G be the external direct product $G_1 \times G_2$. Consider the projection map

$T_1 : G_1 \times G_2 \to G_1 : !_1 : (x, y) = x$.

Then π_1 is a group homomorphism, since

$$\begin{aligned}\pi_1((a, b)(c, d)) &= \pi_1(ac, bd)\\ &= ac\\ &= \pi_1(a, b)\,\pi_1(c, d)\end{aligned}$$

π_1 is also onto, because any $x \in G_1$ is $!_1 (x, e_2)$

Now, let us look at Ker π_1.

$$\begin{aligned}\text{Ker } \pi_1 &= \{(x, y) \in G_1 \times G_2 \mid \pi_1(x, y) = e_1\}\\ &= \{(e_1, y) \mid y \in Gz\} = \{e_1\} \times G_2.\end{aligned}$$

$\therefore \{e\} \times G_2 \trianglelefteq G_1 \times G_2$.

Also, by the Fundamental Theorem of Homomorphism $(G_1 \times G_2)/(\{e_1\} \times Gz) \simeq G_1$.

We can similarly prove that $G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2$ and $(G_1 \times G_2)/(G_1 \times \{e_2\}) \simeq G_2$.

So, far we have seen the construction of $G_1 \times G_2$ from two groups G_1 and G_2. Now we will see under what conditions we can express a group as a direct product of its subgroups.

9.1.2 Internal Direct Product

Let us begin by recalling from Unit 5 that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. We are interested in the case when HK is the whole of G. We have the following definition.

Definition: Let H and K be normal subgroups of a group G. We call G the internal direct product of H and K if

$G = HK$ and $H \cap K = \{e\}$.

We write this fact as $G = H \times K$.

For example, let us consider the familiar Klein 4-group

$K_4 = \{e, a, b, ab\}$, where $a^2 = e$, $b^2 = e$ and $ab = ba$.

Let $H = <a>$ and $K = <b>$. Then $H \cap K = \{e)$. Also, $K_4 = HK$.

$\therefore \quad K_4 = H \times K$.

Note that $H \simeq Z_2$ and $K \simeq Z_2$ $\quad \therefore K_4 \simeq Z_2 \times Z_2$.

For another example, consider Z_{10}. It is the internal direct product of its subgroups $H = \{\bar{0}, \bar{5}\}$ and $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$. This is because

(i) $Z_{10} = H + K$, since any element of Z_{10} is the sum of an element of H and an element of K, and

(ii) $H \cap K = \{\bar{0}\}$.

Now, can an external direct product also be an internal direct product? What does it say? It says that the external product of $G_1 \times G_2$ is the internal product $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

We would like to make a remark here.

Remark: Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is isomorphic to the external direct product of H and K. Therefore, when we talk of an internal direct product of subgroups we can drop the word internal, and just say 'direct product of subgroups'.

Let us now extend the definition of the internal direct product of two subgroups to that of several subgroups.

Definition: A group G is the internal direct product of its normal subgroups $H_1, H_2, \ldots, H_n$ if

(i) $G = H_1 H_2 \ldots H_n$ and

(ii) $H_i \cap H_1 \ldots H_{i-1}, H_{i+1} \ldots H_n = \{e\} \ \forall \ i = 1, \ldots, n$.

For example, look at the group G generated by {a, b, c}, where $a^2 = e = b^2 = c^2$ and $ab = ba$, $ac = ca$, $bc = cb$. This is the internal direct product of $< a >$, $< b >$ and $< c >$. That is $G \simeq Z_2 \times Z_2 \times Z_2$.

Now, can every group be written as an internal direct product of two or more of its proper normal subgroups? Consider Z. Suppose $Z = H \times K$, where H, K are subgroups of Z.

You know that $H = < m >$ and $K = < n >$ for some $m, n \in Z$. Then $mn \in H \cap K$. But if $H \times K$ is a direct product, $H \cap K = \{0\}$. So, we reach a contradiction. Therefore, Z can't be written as an internal direct product of two subgroups.

By the same reasoning we can say that Z can't be expressed as $H_1 \times H_2 \times \ldots \times H_n$, where $Hi \leq Z$ $\forall \ i = 1, 2, \ldots, n$.

When a group is an internal direct product of its subgroups, it satisfies the following theorem.

Theorem 1: Let a group G be the internal direct product of its subgroups H and K. Then

(a) each $x \in G$ can be uniquely expressed as $x = hk$, where $h \in H$, $k \in K$; and

(b) $hk = kh \ \forall \ h \in H, k \in K$.

Proof: (a) We know that G = HK. Therefore, if $x \in G$, then x = hk, for some $h \in H$, $k \in K$. Now suppose $x = h_1k_1$ also, where $h_1 \in H$ and $k_1 \in K$. Then $hk = h_1k_1$.

$\therefore$ $h_1^{-1} h = k_1k^{-1}$. Now $h_1^{-1} h \in H$.

Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1} h \in K$. $\therefore$ $h_1^{-1} h \in H \cap K = \{e\}$.

$\therefore$ $h_1^{-1}h = e$, which implies that $h = h_1$.

Similarly, $k_1 k^{-1} = e$, So that $k_1 = k$.

Thus, the representation of x as the product of an element of H and an element of K is unique.

(b) The best way to show that two elements x and y commute is to show that their commutator $x^{-1}y^{-1} xy$ is identity. So, let $h \in H$ and $k \in K$ and consider h-'k-'hk. Since $K \trianglelefteq G$, $h^{-1}k^{-1} h \in K$.

$\therefore$ $h^{-1}k^{-1}hk \in K$.

By similar reasoning, $h^{-1}k^{-1}hk \in H$. $\therefore$ $h^{-1}k^{-1}hk \in H \cap K = \{e\}$.

$\therefore$ $h^{-1} k^{-1}hk = e$, that is, hk = kh.

Now let us look at the relationship between internal direct products and quotient groups.

Theorem 2: Let H and K be normal subgroups of a group G such that G = H × K. Then $G/H \simeq K$ and $G/K \simeq H$.

Proof: We will use Theorem 8 of Unit 6 to prove this result.

Now G = HK and $H \cap K = \{e\}$. Therefore,

$G/H = HK/H \simeq K/H \cap K = K/\{e) \simeq K$.

We can similarly prove that $G/K \simeq H$.

Theorem 3: Let G be a finite group and H and K be its subgroups such that G = H X K.

Then o(G) = o(H) o(K).

9.2 Sylow Theorems

In Unit 4 we proved Lagrange's theorem, which says that the order of a subgroup of a finite group divides the order of the group. We also said that if G is a finite cyclic group and m | o(G), then G has a subgroup of order. But if G is not cyclic, this statement need not be true, as you have seen in the previous unit. In this context, in 1845 the mathematician Cauchy proved the following useful result.

Theorem 4: If a prime p divides the order of a finite group G, then G contains an element of order p.

The proof of this result involves a knowledge of group theory that is beyond the scope of this course. Therefore, we omit it.

Theorem 5: If a prime p divides the order of a finite group G, then G contains a subgroup of order p.

Proof: Just take the cyclic subgroup generated by an element of order p. This element exists because of Theorem 4.

So, by Theorem 5 we know that any group of order 30 will have a subgroup of order 2, a subgroup of order 3 and a subgroup of order 5. In 1872 Ludwig Sylow, a Norwegian mathematician, proved a remarkable extension of Cauchy's result. This result, called the first Sylow theorem, has turned out to be the basis of finite group theory. Using this result we can say, for example, that any group of order 100 has subgroups of order 2, 4, 5 and 25.

Theorem 6 (First Sylow Theorem): Let G be a finite group such that o (G) = $p^n m$, where p is a prime, $n \geq 1$ and (p, m) = 1. Then G contains a subgroup of order pk $\forall$ k = 1, . . . , n.

We shall not prove this result or the next two Sylow theorems either. But, after stating all these results we shall show how useful they are.

The next theorem involves the concepts of conjugacy and Sylow p-subgroups which we now define.

Definition: Two subgroups H and K of a group G are conjugate in G if $\exists$ g $\in$ G such that K = $g^{-1}Hg$ and then K is called a conjugate of H in G.

Now we define Sylow p-subgroups.

Definition: Let G be a finite group and p be a prime such that p^n | o(G) but p^{n+1} o(G), for some n $\geq$ 1. Then a subgroup of G of order pn is called a Sylow p-subgroup of G.

So, if o(G) = $p^n m$, (p, m) = I, then a subgroup of G of order p″ is a Sylow p-subgroup. Theorem 6 says that this subgroup always exists. But, a group may have more than one Sylow p-subgroup. The next result tells us how two Sylow p-subgroups of a group are related.

Theorem 7 (Second Sylow Theorem): Let G be a group such that o(G) = $p^n m$, (p, m) = 1, p a prime. Then any two Sylow p-subgroups of G are conjugate in G.

And now let us see how many Sylow p-subgroups a group can have.

Theorem 8 (Third Sylow Theorem): Let G be a group of order $p^n m$, where (p, m) = 1 and p is a prime. Then n_p, the number of distinct Sylow p-subgroups of G, is given by $n_p = 1 + kp$ for some k $\geq$ 0. And further, n_p | o(G).

We would like to make a remark about the actual use of Theorem 8.

Remark: Theorem 8 says that $n_{p,} \equiv 1 \pmod{p}$. (n_p, pn) = 1. Also, since np | o(G), using Theorem 9 of Unit 1 we find that n_p | m. This fact helps us to cut down the possibilities for n,, as you will see in the following examples.

Example: Show that any group of order 15 is cyclic.

Solution: Let G be a group of order 15 = 3 × 5. Theorem 6 says that G has a Sylow 3-subgroup. Theorem 8 says that the number of such subgroups must divide 15 and must be congruent to l(mod 3). In fact, by Remark 3 the number of such subgroups must divide 5 and must be congruent to l(mod 3). Thus, the only possibility is 1. Therefore, G has a unique Sylow 3-subgroup, say H. Hence, by Theorem 7 we know that H $\underline{\Delta}$ G. Since H is of prime order, it is cyclic.

Similarly, we know that G has a subgroup of order 5. The total number of such subgroups is 1,6 or 11 and must divide 3. Thus, the only possibility is 1. So G has a unique subgroup of order 5, say K. Then K $\underline{\Delta}$ G and K is cyclic.

Now, let us look at H $\cap$ K. Let x $\in$ H $\cap$ K. Then x $\in$ H and x $\in$ K.

$\therefore$ o(x) | o(H) and o(x) | o(K) i.e., o(x) | 3 and o(x) | 5.

$\therefore$ o(x) = 1. $\therefore$ x = e. That is, H $\cap$ K = {e}. Also,

$\therefore$ G = HK.

So, G = H × K $\simeq$ Z_3 X Z_5 = Z_{15}, *Example:* Show that a group *G* of order 30 either has a normal subgroup of order 5 or a normal subgroup of order 3, i.e. G is not simple. A group G is called simple if its only normal subgroups.

Solution: Since 30 = 2 × 3 × 5, G has a Sylow 2-subgroup, a Sylow 3-subgroup and a Sylow 5-subgroup. The number of Sylow 5-subgroups is of the form 1 + 5k and divides 6. Therefore, it can be 1 or **6.** If it is 1, then the Sylow 5-subgroup is normal in G.

On the other hand, suppose the number of Sylow 5-subgroups is 6. Each of these subgroups are distinct cyclic groups of order 5, the only common element being e. Thus, together they contain 24 + 1 = 25 elements of the group. So, we are left with 5 elements of the group which are of order 2 or 3. Now, the number of Sylow 3-subgroups can be 1 or 10. We can't have 10 Sylow 3-subgroups, because we only have at most 5 elements of the group which are of order 3. So, if the group has 6 Sylow 5-groups then it has only 1 Sylow 3-subgroup.

Now let us use the powerful Sylow theorems to classify groups of order 1 to 10. In the process we will show you the algebraic structure of several types of finite groups.

9.3 Groups of Order 1 to 10

Here, we will apply the results of the above discussion to study some finite groups. In particular, we will list all the groups of order 1 to 10, up to isomorphism.

We start with proving a very useful result.

Theorem 9: Let G be a group such that o(G) = pq, where p, q are primes such that p > q and $q \nmid p - 1$. Then G is cyclic.

Proof: Let P be a Sylow p-subgroup and Q be a Sylow q-subgroup of G. Then o(P) = p and o(Q) = q. Now, any group of prime order is cyclic, so P = < x > and Q = < y > for some x, y ∈ G. By the third Sylow theorem, the number n_p of subgroups of order p can be 1 , 1+ p, 1 + 2p, . . . , and it must divide q. But p > q. Therefore, the only possibility for n_p is 1. Thus, there exists only one Sylow p-subgroup, i.e., P. Further, by Sylow's second theorem $P \trianglelefteq G$.

Again, the number of distinct Sylow q-subgroups of G is $n_{q'} = 1 + kq$ for some k, and n, | p. Since p is a prime, its only factors are 1 and p. ∴ n, = 1 or $n_q = p$. Now if 1 + kq = p, then q | p – 1. But we started by assuming that $9 \nmid p - 1$. So we reach a contradiction. Thus, $n_q = 1$ is the only possibility. Thus, the Sylow q-subgroup Q is normal in G.

Now we want to show that G = P × Q. For this, let us consider $P \cap Q$. The order of any element of $P \cap Q$ must divide p as well as q, and hence it must divide (p, q) = 1.

$P \cap Q = \{e\}$. ∴ o(PQ) = o(P) o(Q) = pq = o(G). ∴ G = PQ.

So we find that $G = P \times Q \simeq Z_p \times Z_p \simeq Z_{pq'}$

Therefore, G is cyclic of order pq.

Using Theorem 9, we can immediately say that any group of order 15 is cyclic. Similarly, if o(G) = 35, then G'is cyclic.

Now if q | p – 1, then does o(G) = pq imply that G is cyclic? Well, consider S_3. You know that $o(S_3)$ = 6 = 2.3, but S_3 is not cyclic. In fact, we have the following result.

Theorem 10: Let G be a group such that o(G) = 2p, where p is an odd prime, Then either G is cyclic or G is isomorphic to the dihedral group D_{2p} of order 2p.

(Recall that D_{2p} = < (x, y | $x^P = e = Y^2$ and $yx = x^{-1}y\}$ > .)

Proof: As in the proof of Theorem 9, there exists a subgroup P = < x > of order p with

P $\underline{\Delta}$ G and a subgroup Q = < y > of order 2, since p > 2. Since (2, p) = 1,

$P \cap Q = \{e\}$. $\therefore$ o(PQ) = o(G).

$\therefore$ G = PQ.

Now, two cases arise, namely, when Q $\underline{\Delta}$ G and when Q $\not\underline{\Delta}$ G.

If Q $\underline{\Delta}$ G, then G = P × Q. And then G = <xy>.

If Q is not normal in G, then G must be non-abelian.

(Remember that every subgroup of an abelian group is normal.)

$\therefore$ $xy \neq yx$. $\therefore$ $y^{-1}xy \neq x$.

Now, since P = < x > $\underline{\Delta}$ G, $y^{-1}xy \in P$. $\therefore$ $y^{-1}xy = x'$, for some r = 2 ,... . , p - 1.

Therefore, $y^{-2}xy^2 = y^{-1}(y^{-1}xy) = y^{-1}x^ry = (y^{-1}xy)^r = (x^r)^r = x^{r^2}$

$\Rightarrow x = x^{r^2}$, since o(y) = 2.

$\Rightarrow x^{r^{2-1}} = 6$.

But o(x) = p. Therefore, by Theorem 4 of Unit 4, p | $r^2 - 1$, i.e., p | (r – 1) (r + 1)

$\Rightarrow$ p | (r – 1) or p | (r + 1). But $2 \leq r \leq p - 1$. $\therefore$ p = r + l,

i.e., r = p – 1. So we see that

$y^{-1} xy = x^r =' x^{P-1} = x^{-1}$

So, G = PQ = < {x, y | $x^p = e$, $y^2 = e$, $y^{-1}xy = x^{-1}$ > , which is exactly the same algebraic structure as that of D_{2p}.

$\therefore$ G = D_{2p} = {e, x, x^2, ... , x^{P-1}, y, xy, x^2 y, ... , x^{P-1}y]

Example: What are the possible algebraic structures of a group of order 6?

Solution: Let G be a group of order 6. Then, by theorem 10, G ≃ Z_6 or G ≃ Ds. You must have already noted that $S_3 \simeq D_6$. So, if G is not cyclic, then G ≃ S_3.

Now, from Theorem 6 of Unit 4, we know that if o(G) is a prime, then G is cyclic. Thus, groups of orders 2, 3, 5 and 7 are cyclic. This fact allows us to classify all groups whose orders are 1, 2, 3, 5, 6, 7 or 10. What about the structure of groups of order 4 = 22 and 9 = 3^2? Such groups are covered by the following result.

Theorem 11: If G is a group of order p^2, p a prime, then G is abelian.

We will not prove this result, since its proof is beyond the scope of this course. But, using this theorem, we, can easily classify groups of order p^2.

Theorem 12: Let G be a group such that o(G) = p^2, where p is a prime. Then either G is cyclic or G = $Z_p \times Z_{p'}$, a direct product of two cyclic groups of order p.

Proof: Suppose G has an element a of order p^2. Then G = < a > .

On the other hand, suppose G has no element of order. Then, for any x E G, o(x) = I or o(x) = p.

Let $x \in G$, $x \neq e$ and $H = < x >$. Since $x \neq e$, $o(H) \neq 1$

$\therefore \quad o(H) = p$.

Therefore, $\exists\ y \in G$ such that $y \notin H$. Then, by the same reasoning, $K = < y >$ is of order p. Both H and K are normal in G, since G is abelian.

We want to show that $G = H \times K$. For this, consider $H \cap K$. Now $H \cap K \leq H$.

$\therefore$ $o(H \cap K) \mid o(H) = p$. $o(H \cap K) = 1$ or $o(H \cap K) = p$.

If $o(H \cap K) = p$, then $H \cap K = H$, and by similar reasoning, $H \cap K = K$. But then,

$H = K$. $\qquad \therefore\ y \in H$, a contradiction.

$o(H \cap K) = 1$, i.e., $H \cap K = \{e\}$.

So, $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$ and $o(HK) = p^2 = o(6)$.

$\therefore$ $G = H \times K \simeq Z_p \times Z_p$.

So far we have shown the algebraic structure of all groups of order 1 to 10, except groups of order 8. Now we will list the classification of groups of order 8.

If G is an abelian group of order 8, then

(i) $G \simeq Z_8$, the cyclic group or order 8, or

(ii) $G \simeq Z_4 \times Z_2$, or

(iii) $G \simeq Z_2 \times Z_2 \times Z_2$.

If G is a non-abelian group of order 8, then

(i) $G \simeq Q_8$, the quaternion group discussed in Unit 4, or

(ii) $G \simeq D_8$, the dihedral group discussed in Unit 5.

So, we have seen what the algebraic structure of any group of order 1, 2, ... , 10 must be. We have said that this classification is up to isomorphism. So, for example, any group of order 10 is isomorphic to Z_{10} or D_{10}. It need not be equal to either of them.

Self Assessment

1. Let a group G be the .... product of its subgroups H and k. Then $hk = kh\ \forall\ h \in H$, $k \in K$.

   (a) external (b) internal

   (c) finite (d) infinite

2. Let H and k be normal subgroups of a group G such that $G = H \times k$. Then $G/H \cong$ .... and $G/k \cong H$

   (a) k (b) H

   (c) H^{-1} (d) $k^{-1'}$

3. Let G .... be and H and k be its subgroup such that $G = H \times k$. Thus $O(G) = O(H)\ o(k)$.

   (a) external (b) internal

   (c) finite (d) infinite

Notes

4. If a prime p divides the order of a finite group G, then G contains an element of ....

   (a) P (b) G

   (c) Q (d) R

5. If a prime P divides the order of a finite group G, then G contains a .... of order P.

   (a) subgroup (b) normal

   (c) cycle (d) permutation

9.4 Summary

In this unit we have discussed the following points:

- The definition and examples of external direct products of groups.
- The definition and examples of internal direct products of normal subgroups.
- If (m, n) = 1, then $Z_m \times Z_n \simeq Z_{mn}$.
- o(H × K) = o(H) o(K).
- The statement and application of Sylow's theorems, which state that: Let G be a finite group of order $p^n m$, where p is a prime and $p \nmid m$. Then
  - ❖ G contains a subgroup of order p^k $\forall$ k = 1, ... , n;
  - ❖ any two Sylow p-subgroups are conjugate in G;
  - ❖ the number of distinct Sylow p-subgroups of G is congruent to 1 (mod p) and divides o(G) (in fact, it divides m).
- Let o(G) = pq, p a prime, p > q, $q \nmid p - 1$. Then G is cyclic.
- Let o(G) = p^2, p a prime. Then
  - ❖ G is abelian.
  - ❖ G is cyclic or $G \simeq Z_p \times Z_p$.
- The classification of groups of order 1 to 10, which we give in the following table.

O(G)	Algebraic Structure
1	{e}
2	Z_2
3	Z_3
4	Z_4 or $Z_2 \times Z_2$
5	Z_5
6	Z_6 or S_3
7	Z_7
8	Z_8 or $Z_4 \times Z_2$ or $Z_2 \times Z_2 \times Z_2$ (if G is abelian) Q_8 or D_8 (if G is non-abelian)
9	Z_9 or $Z_3 \times Z_3$
10	Z_{10} or D_{10}

Notes

9.5 Keywords

External Direct Product: Let $(G_1, *_1), (G_2, *_2), \ldots\ldots, (G_n, *_n)$ be n groups. Their ***external direct product*** is the group (G, *), where

$G = G_1 \times G_2 \ldots\ldots \times G_n$ and

Thus, R^n is the external direct product of n copies of R.

Internal Direct Product: Let H and K be normal subgroups of a group G. We call G the ***internal direct product*** of H and K if

$G = HK$ and $H \cap K = \{e\}$.

We write this fact as $G = H \times K$.

Sylow p-subgroup: Let G be a finite group and p be a prime such that $p^n \mid o(G)$ but $p^{n+1}\ o(G)$, for some $n \geq 1$. Then a subgroup of G of order p^n is called a ***Sylow p-subgroup*** of G.

9.6 Review Questions

1. Show that the binary operation * on G is associative. Find its identity element and the inverse of any element (x, y) in G.

2. Show that $G_1 \times G_2 = G_2 \times G_1$, for any two groups G_1 and G_2.

3. Show that $G_1 \times G_2$ is the product of its normal subgroup $H = G_1 \times \{e_2\}$ and $K = \{e_1\} \times G_2$. Also show that $(G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2) = \{(e_1, e_2)\}$.

4. Prove that $P(G_1 \times G_3) = Z(G_1) \times Z(G_2)$, where $Z(G_3)$ denotes the centre of G (see Theorem 2 of unit 3).

5. Let A and B be cyclic groups of order m and n, respectively, where (m, n) = 1. Prove that $A \times B$ is cyclic of order mn.

   (Hint: Define $f : Z \to Z_m \times Z_n : f(r) = (r + mZ, r + nZ)$). Then apply the Fundamental theorem of Homomorphism to show that $Z_m \times Z_n \cong Z_{mn}$.

6. Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that $G = H \times K$.

7. Use Theorem 2 to prove Theorem 3.

Answers: Self Assessment

1. (b) 2. (a) 3. (c) 4. (a) 5. (a)

9.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Notes

Unit 10: Finite Abelian Groups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define finite abelian group
- Explain the properties of finite abelian group
- Discuss the notation of finite abelian group

Introduction

A group for which the elements commute (i.e., AB = BA for all elements A and B) is called a finite abelian group. All cyclic groups are finite abelian, but a finite abelian group is not necessarily cyclic. All subgroups of a finite abelian group are normal. In a finite abelian group, each element is in a conjugacy class by itself, and the character table involves powers of a single element known as a group generator. In *Mathematica*, the function finite abelian group [{n_1, n_2 ...}] represents the direct product of the cyclic groups of degrees n_1 n_2 ...

10.1 Definition

A finite abelian group is a set, A, together with an operation "•" that combines any two elements a and b to form another element denoted a • b. The symbol "•" is a general placeholder for a concretely given operation. To qualify as a finite abelian group, the set and operation, (A, •), must satisfy five requirements known as the *finite abelian group axioms*:

Closure

For all a, b in A, the result of the operation a • b is also in A.

Associatively

For all a, b and c in A, the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity Element

There exists an element e in A, such that for all elements a in A, the equation $e \bullet a = a \bullet e = a$ holds.

Inverse Element

For each a in A, there exists an element b in A such that $a \bullet b = b \bullet a = e$, where e is the identity element.

Commutatively

For all a, b in A, $a \bullet b = b \bullet a$.

More compactly, a finite abelian group is a commutative group. A group in which the group operation is not commutative is called a "non-finite abelian group" or "non-commutative group".

You should notice that any field is a finite abelian group under addition. Furthermore, under multiplication, the set of non-zero elements of any field must also form a finite abelian group. Of course, in this case the two operations are not independent–they are connected by the distributive laws.

The definition of a finite abelian group is also useful in discussing vector spaces and modules. In fact, we can define a vector space to be a finite abelian group together with a scalar multiplication satisfying the relevant axioms. Using this definition of a vector space as a model, we can state the definition of a module in the following way.

10.2 Properties

Let us assume that, If n is a natural number and x is an element of a finite abelian group G written additively, then nx can be defined as x + x + ... + x (n summands) and (–n)x = –(nx). In this way, G becomes a module over the ring Z of integers. In fact, the modules over Z can be identified with the finite abelian groups.

Theorems about finite abelian groups can often be generalized to theorems about modules over an arbitrary principal ideal domain. A typical example is the classification of finitely generated finite abelian groups which is a specialization of the structure theorem for finitely generated modules over a principal ideal domain. In the case of finitely generated finite abelian groups, this theorem guarantees that a finite abelian group splits as a direct sum of a torsion group and a free finite abelian group. The former may be written as a direct sum of finitely many groups of the form Z/p^kZ for p prime, and the latter is a direct sum of finitely many copies of Z.

If f, g : G → H are two group homomorphisms between finite abelian groups, then their sum f + g, defined by (f + g)(x) = f(x) + g(x), is again a homomorphism. (This is not true if H is a non-finite abelian group.) The set Hom (G, H) of all group homomorphisms from G to H thus turns into a finite abelian group in its own right.

Somewhat kind to the dimension of vector spaces, every finite abelian group has a rank. It is defined as the cardinality of the largest set of linearly independent elements of the group. The integers and the rational numbers have rank one, as well as every subgroup of the rationals.

10.3 Notation

There are two main notational conventions for finite abelian groups: ‘+’ additive and ‘·’ multiplicative.

Convention	Operation	Identity	Powers	Inverse
Addition	$x + y$	0	nx	$-x$
Multiplication	$x * y$ or xy	e or 1	x^n	x^{-1}

Generally, the multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules. The additive notation may also be used to emphasize that a particular group is abelian, whenever both abelian and non-finite abelian groups are considered.

Multiplication Table

To verify that a finite group is abelian, a table (matrix) - known as a Cayley table - can be constructed in a similar fashion to a multiplication table. If the group is $G = \{g_1 = e, g_2, ..., g_n\}$ under the operation ”, the (i, j)’th entry of this table contains the product $g_i \cdot g_j$. The group is abelian if and only if this table is symmetric about the main diagonal.

This is true since if the group is abelian, then $g_i \cdot g_j = g_j \cdot g_i$. This implies that the (i, j)’th entry of the table equals the (j, i)’th entry, thus the table is symmetric about the main diagonal.

Examples:

1. For the integers and the operation addition “+”, denoted (**Z**,+), the operation + combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer n has an additive inverse, $-n$, and the addition operation is commutative since $m + n = n + m$ for any two integers m and n.

2. Every cyclic group G is abelian, because if x, y are in G, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Thus the integers, **Z**, form a finite abelian group under addition, as do the integers modulo n, **Z**/n**Z**.

3. Every ring is a finite abelian group with respect to its addition operation. In a commutative ring the invertible elements, or units, form an abelian multiplicative group. In particular, the real numbers are a finite abelian group under addition, and the non-zero real numbers are a finite abelian group under multiplication.

4. Every subgroup of a finite abelian group is normal, so each subgroup gives rise to a quotient group. Subgroups, quotients, and direct sums of finite abelian groups are again abelian.

In general, matrices, even invertible matrices, do not form a finite abelian group under multiplication because matrix multiplication is generally not commutative. However, some groups of matrices are finite abelian groups under matrix multiplication - one example is the group of 2 x 2 rotation matrices.

Example: Find all finite abelian groups of order 108 (up to isomorphism).

Notes

Solution: The prime factorization is 108 = $2^2 \cdot 3^3$. There are two possible groups of order 4: $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$. There are three possible groups of order 27: $\mathbf{Z}_{27}$, $\mathbf{Z}_9 \times \mathbf{Z}_3$, and $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$. This gives us the following possible groups:

$\mathbf{Z}_4 \times \mathbf{Z}_{27}$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{27}$

$\mathbf{Z}_4 \times \mathbf{Z}_9 \times \mathbf{Z}_3$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_3$

$\mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

Example: Let G and H be finite abelian groups, and assume that G × G is isomorphic to H × H. Prove that G is isomorphic to H.

Solution: Let p be a prime divisor of $|G|$, and let $q = p^m$ be the order of a cyclic component of G. If G has k such components, then G × G has 2k components of order q. An isomorphism between G × G and H × H must preserve these components, so it follows that H also has k cyclic components of order q. Since this is true for every such q, it follows that $G \cong H$

Example: Let G be a finite abelian group which has 8 elements of order 3, 18 elements of order 9, and no other elements besides the identity. Find (with proof) the decomposition of G as a direct product of cyclic groups.

Solution: We have $|G| = 27$. First, G is not cyclic since there is no element of order 27. Since there are elements of order 9, G must have Z_9 as a factor. To give a total of 27 elements, the only possibility is $G \cong Z_9 \times Z_3$.

Check: The elements 3 and 6 have order 3 in Z_9, while 1 and 2 have order 3 in Z_3. Thus, the following 8 elements have order 3 in the direct product: (3, 0), (6, 0), (3, 1), (6, 1), (3, 2), (6, 2), (0, 1), and (0, 2).

Example: Let G be a finite abelian group such that $|G| = 216$. If $|\, 6G \,| = 6$, determine G up to isomorphism.

Solution: We have 216 = $2^3 \cdot 3^3$, and $6G \cong Z_2 \times Z_3$ since it has order 6. Let H be the Sylow 2-subgroup of G, which must have 8 elements. Then multiplication by 3 defines an automorphism of H, so we only need to consider 2H. Since $2H \cong Z_2$, we know that there are elements not of order 2, and that H is not cyclic, since $2\,Z_8 \cong Z_4$. We conclude that $H \cong Z_4 \times Z_2$.

A similar argument shows that the Sylow 3-subgroup K of G, which has 27 elements, must be isomorphic to $Z_9 \times Z_3$.

Using the decomposition, we see that

$G \cong Z_4 \times Z_2 \times Z_9 \times Z_3$.

(If you prefer the form of the decomposition, you can also give the answer in the form $G \cong Z_{36} \times Z_6$.)

Example: Apply both structure theorems to give the two decompositions of the finite abelian group $Z^{\times}_{216}$

Solution: $Z^{\times}_{216} \cong Z^{\times}_{8} \times Z^{\times}_{27} \cong Z_2 \times Z_2 \times Z^{\times}_{27}$

Since 27 is a power of an odd prime, it follows that $Z_{27}^{\times}$ is cyclic. This can also be shown directly by guessing that 2 is a generator.

Since $Z_{27}^{\times}$ has order $3^3 - 3^2 = 18$, an element can only have order 1, 2, 3, 6, 9 or 18. We have

$2^2 = 4,$

$2^3 = 8,$

$2^6 \equiv 8^2 \equiv 10$, and

$2^9 \equiv 2^3 \cdot 2^6 \equiv 8 \cdot 10 \equiv -1,$

so it follows that 2 must be a generator.

We conclude that $Z_{216}^{\times} \cong Z_2 \times Z_2 \times Z_{18}$.

To give the first decomposition, states that any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. In this decomposition we need to split Z_{18} up into cyclic subgrops of prime power order, so we finally get the decomposition

$Z_{216}^{\times} \equiv Z_2 \times Z_2 \times Z_2 \times Z_9.$

On the other hand, the second decomposition, where any finite finite abelian group is written as a direct product of cyclic groups in which the orders any component is a divisor of the previous one. To do this we need to group together the largest prime powers that we can. In the first decomposition, we can combine Z_2 and Z_9 to get Z_{18} as the first component. We end up with

$Z_{216}^{\times} \equiv Z_{18} \times Z_2 \times Z_2$

as the second way of breaking $Z_{216}^{\times}$ up into a direct product of cyclic subgroups.

Example: Let G and H be finite abelian groups, and assume that they have the following property. For each positive integer m, G and H have the same number of elements of order m. Prove that G and H are isomorphic.

Solution: We give a proof by induction on the order of $|G|$. The statement is clearly true for groups of order 2 and 3, so suppose that G and H are given, and the statement holds for all groups of lower order. Let p be a prime divisor of $|G|$, and let G_p and H_p be the Sylow p-subgroups of G and H, respectively. Since the Sylow subgroups contain all elements of order a power of p, the induction hypothesis applies to G_p and H_p. If we can show that $G_p\ H_p$ for all p, then it will follow that G H, since G and H are direct products of their Sylow subgroups.

Let x be an element of G_p with maximal order $q = p^m$. Then $< x >$ is a direct factor of G_p, so there is a subgroup G′ with $G_p = < x > \times G'$. By the same argument we can write $H_p = < y > \times H'$, where y has the same order as x.

Now consider $< x^p > \times G'$ and $< y^p > \times H'$. To construct each of these subgroups we have removed elements of the form (x^k, g'), where x^k has order q and g′ is any element of G′. Because x has maximal order in a p-group, in each case the order of g′ is a divisor of q, and so (x^k, g') has order q since the order of an element in a direct product is the least common multiple of the orders of the components. Thus to construct each of these subgroups we have removed $(p^m - p^{m-1}) \cdot |G'|$ elements, each having order q. It follows from the hypothesis that we are left with the same number of elements of each order, and so the induction hypothesis implies that $< x^p > \times G'$ and $< y^p > \times H'$ are isomorphic. But then $G' \simeq H'$, and so $G_p \simeq H_p$, completing the proof.

Proposition: Every finite abelian group has a natural structure as a module over the ring Z.

As with vector spaces, one goal is to be able to express a finite abelian group in terms of simpler building blocks. For vector spaces we can use one-dimensional spaces as the building blocks; for finite abelian groups, it seems natural to use the simple finite abelian groups.

Recall that in an arbitrary group G, a subgroup $N \subseteq G$ is called a normal subgroup if $gxg^{-1} \in N$, for all $x \in N$ and all $g \in G$. Then G is said to be a simple group if its only normal subgroups are {1} and G. If the group A is abelian, then all subgroups are normal, and so A is simple iff its only subgroups are the trivial subgroup (0) and the improper subgroup A. The same definition is given for modules: a nonzero module M is a simple module if its only submodules are (0) and M. When you view a finite abelian group as a Z-module, then, of course, the two definitions coincide.

Note Any cyclic finite abelian group is isomorphic to Z or Z_n, for some n.

Outline of the Proof: Let A be a cyclic finite abelian group that is generated by the single element a. Define the group homomorphism $f : Z \to A$ by setting $f(n) = na$, for all $n \in Z$. Note that f maps Z onto A since $f(Z) = Za = A$. If f is one-to-one, then A is isomorphic to Z. If f is not one-to-one, we need to use the fundamental homomorphism theorem and the fact that every subgroup of Z is cyclic to show that A is isomorphic to Z_n, where n is the smallest positive integer such that $na = 0$.

Proposition: A finite abelian group is simple iff it is isomorphic to Z_p, for some prime number p.

Proof: First, let A be a finite abelian group isomorphic to Z_p, where p is a prime number. The isomorphism preserves the subgroup structure, so we only need to know that Z_p has no proper nontrivial subgroups. This follows from the general correspondence between subgroups of Z_n and divisors of n, since p is prime precisely when its only divisors are ±1 and ±p, which correspond to the subgroups Z_p and (0), respectively.

Conversely, suppose that A is a simple finite abelian group. Since A is nonzero, pick any nonzero element $a \in A$. Then the set $Za = \{na \mid n \in Z\}$ is a nonzero subgroup of A, so by assumption it must be equal to A. This shows that A is a cyclic group. Furthermore, A can't be infinite, since then it would be isomorphic to Z and would have infinitely many subgroups. We conclude that A is finite, and hence isomorphic to Z_n, for some n. Once again, the correspondence between subgroups of Z_n and divisors of n shows that if Z_n is simple, then n must be a prime number.

A module M is said to be semisimple if it can be expressed as a sum (possibly infinite) of simple submodules. Although the situation for finite abelian groups is more complicated than for vector spaces, it is natural to ask whether all finite abelian groups are semisimple.

Example: The group Z_4 is not a semisimple Z-module. First, Z_4 is not a simple group. Secondly, it cannot be written non-trivially as a direct sum of any subgroups, since its subgroups lie in a chain $Z_4 \supset 2Z_4 \supset (0)$, and no two proper nonzero subgroups intersect in (0).

Example: The group Z_6 is a semisimple Z-module. To see this, define $f : Z_6 \to Z_2 \oplus Z_3$ by setting $f(0) = (0, 0)$, $f(1) = (1, 1)$, $f(2) = (0, 2)$, $f(3) = (1, 0)$, $f(4) = (0, 1)$, $f(5) = (1, 2)$. You can check that this defines an isomorphism, showing that Z_6 is isomorphic to a direct sum of simple finite abelian groups.

The function defined in the example is a special case of a more general result that is usually referred to as the Chinese remainder theorem (this result is given more generally for rings. The proof of the next proposition makes use of the same function.

Proposition: If k = mn, where m and n are relatively prime integers, then Z_k is isomorphic to $Z_m \oplus Z_n$.

Outline of the Proof: Define $f : Z_k \rightarrow Z_m \oplus Z_n$ by $f([x]_k) = ([x]_m, [x]_n)$, for all $x \in Z$. Here I have been a bit more careful, by using $[x]_k$ to denote the congruence class of x, modulo k. It is not hard to show that f preserves addition. The sets Z_k and $Z_m \oplus Z_n$ are finite and have the same number of elements, so f is one-to-one iff it is onto, and therefore proving one of these conditions will give the other. (Actually, it isn't hard to see how to prove both conditions.) Showing that f is one-to-one depends on the fact that if x is an integer having both m and n as factors, then it must have mn as a factor since m and n are relatively prime. On the other hand, the usual statement of the Chinese remainder theorem is precisely the condition that f is an onto function.

Corollary: Any finite cyclic group is isomorphic to a direct sum of cyclic groups of prime power order.

The corollary depends on an important result in Z: every positive integer can be factored into a product of prime numbers. Grouping the primes together, the proof of the corollary uses induction on the number of distinct primes in the factorization.

This basic result has implications for all finite groups. The cyclic group Z_n also has a ring structure, and the isomorphism that proves the corollary is actually an isomorphism of rings, not just of finite abelian groups. To use this observation, suppose that A is a finite finite abelian group. Let n be the smallest positive integer such that na = 0 for all $a \in A$. (This number might be familiar to you in reference to a multiplicative group G, where it is called the exponent of the group, and is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.)

You can check that because na = 0 for all $a \in A$, we can actually give A the structure of a Z_n-module.

Next we can apply a general result that if a ring R can be written as a direct sum $R = I_1 \oplus \ldots \oplus I_n$ of two-sided ideals, then each I_j is a ring in its own right, and every left R-module M splits up into a direct sum $M_1 \oplus \ldots \oplus M_n$, where M_j is a module over I_j. Applying this to Z_n, we can write Z_n as a direct sum of rings of the form $Z_p{}^k$, where p is a prime, and then the group A breaks up into $A_1 \oplus \ldots \oplus A_n$, where each A_j is a p-group, for some prime p. (Recall that a group G is a p-group if every element of G has order p.) This argument proves the next lemma. (You can also prove it using Sylow subgroups, if you know about them.)

Every finite abelian group can be written as a direct sum of p-groups.

The decomposition into p-groups occurs in one and only one way. Then it is possible to prove that each of the p-groups splits up into cyclic groups of prime power order, and so we have the following fundamental structure theorem for finite abelian groups.

Theorem 1: Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order.

A proof of the fundamental structure theorem, let us first discuss some of the directions it suggests for module theory. First of all, the hope was to construct finite abelian groups out of ones of prime order, not prime power order. The only way to do this is to stack them on top of each other, instead of having a direct sum in which the simple groups are lined up one beside the other. To see what I mean by "stacking" the groups, think of Z_4 and its subgroups $Z_4 \supset 2Z_4 \supset (0)$. It might be better to picture them vertically.

$$\begin{tikzcd}
Z_4 \arrow[d, dash] \\
2Z_4 \arrow[d, dash] \\
(0)
\end{tikzcd}$$

The subgroup $2Z_4 = \{0, 2\} \cong Z2$ is simple, and so is the factor module $Z_4/2Z_4 \cong Z_2$. This having Z_2 stacked on top of Z_2, and the group is structured so tightly that you can't even find an isomorphism to rearrange the factors.

A module M is said to have a composition series of length n if there is a chain of submodules $M = M_0 \supset M_1 \supset . . . \supset M_n = (0)$ for which each factor module M_{i-1}/M_i is a simple module. Thus, we would say that Z_4 has a composition series of length 2. This gives a measurement that equals the dimension, in the case of a vector space. It is also true that the length of a cyclic group of order p^n is precisely n. It can be shown that if M has a composition series of length n, then every other composition series also has length n, so this is an invariant of the module. Furthermore, the same simple modules show up in both series, with the same multiplicity.

The idea of a composition series is related to two other conditions on modules. A module is said to satisfy the ascending chain condition, or ACC, if it has no infinite chain of ascending submodules; it is said to satisfy the descending chain condition, or DCC, if it has no infinite chain of descending submodules. Modules satisfying these conditions are called Noetherian or Artinian, respectively. A module has finite length iff it satisfies both the ACC and DCC. As an example to keep in mind, let's look at the ring of integers, which has ACC but not DCC. Since $mZ \subseteq nZ$ iff $n \mid m$, generators get smaller as you go up in Z, and larger as you go down. Any set of positive integers has a smallest element, so we can't have any infinite ascending chains, but, for example, we can construct the infinite descending chain $2Z \supset 4Z \supset 8Z$ ... .

The cyclic groups of prime power order play a crucial role in the structure of finite abelian groups precisely because they cannot be split up any further. A module M can be expressed as a direct sum of two submodules M_1 and M_2 iff $M_1 \cap M_2 = (0)$ and $M_1 + M_2 = M$. In the case of a cyclic group of prime power order, the subgroups form a descending chain, and so any two nonzero subgroups have a nonzero intersection. A module is called indecomposable if it cannot be written as a direct sum of two nonzero submodules. With this terminology, the cyclic groups of prime power order are precisely the indecomposable finite abelian groups. The major results in this direction are (the Krull-Schmidt theorem), which show that any module with finite length can be written as a direct sum of indecomposable submodules, and this decomposition is unique up to isomorphism and the order of the summands.

After this rather lengthy preview, or review, as the case may be, it is time to move on to study general rings and modules. The next results present a proof of the structure theorem for finite abelian groups, but you should feel free to skip them.

Lemma: Let A be a finite abelian p-group.

(a) Let $a \in A$ be an element of maximal order, and let $b + Za$ be any coset of A/Za. Then there exists $d \in A$ such that $d + Za = b + Za$ and $Zd \cap Za = (0)$.

(b) Let $a \in A$ be an element of maximal order. Then there exists a subgroup B with $A \cong Za \oplus B$.

Proof: (a) The outline of part (a) is to let s be the smallest positive integer such that $sb \in Za$. Then we solve the equation $sb = sx$ for elements $x \in Za$ and let $d = b - x$.

Using o(x) for the order of an element x, let s be the order of b + Za in the factor group G/Za. Then sb $\in$ Za, and we can write sb = (qt)a for some exponent qt such that t = p^β for some β and p $\not|$ q. Then qa is a generator for Za, since q is relatively prime to o(a). Since s is a divisor of the order of b, we have o(b)/s = o(sb) = o((qt)a) = o(a)/t, or simply, o(b) $\cdot$ t = o(a) $\cdot$ s. All of these are powers of p, and so o(b) $\leq$ o(a) implies that s | t, say t = ms. Then x = (qm)a is a solution of the equation sb = sx. If d = b – x, then d + Za = b + Za and so sd = sb – sx = sb – sb = 0. Therefore, Zd $\cap$ Za = (0), since nd $\in$ Za implies n(b – x) = nb – nx $\in$ Za. Thus, nb $\in$ Za implies n(b + Za) = Za in G/Za, so s | n and nd = 0.

(b) The outline of this part is to factor out Za and use induction to decompose A/Za into a direct sum of cyclic groups. Then part (a) can be used to choose the right preimages of the generators of A/Za to generate the complement B of Za.

We use induction on the order of A. If | A | is prime, then A is cyclic and there is nothing to prove. Consequently, we may assume that the statement of the lemma holds for all groups of order less than | A | = p^α. If A is cyclic, then we are done. If not, let Za be a maximal cyclic subgroup, and use the induction hypothesis repeatedly to write A/Za as a direct sum $B_1 \oplus B_2 \oplus \ldots \oplus B_n$ of cyclic subgroups.

We next use part (a) to choose, for each i, a coset a_i + Za that corresponds to a generator of A_i such that $Za_i \cap Za = (0)$. We claim that A $\cong$ Za $\oplus$ B for the smallest subgroup B = $Za_1 + Za_2 + \cdots + Za_n$ that contains $a_1, a_2, \ldots, a_n$.

First, if x $\in$ $Z_a \cap (Za_1 + \cdots + Za_n)$, then x = $m_1a_1 + \cdots + m_na_n$ $\in$ Za for some coefficients $m_1, \ldots, m_n$. Thus x + Za = $(m_1a_1 + \cdots + m_na_n)$ + Za = Za, and since A/Za is a direct sum, this implies that m_ia_i + Za = Za for each i. But then m_ia_i $\in$ Za, and so m_ia_i = 0 since $Za_i \cap Za = (0)$. Thus x = 0.

Next, given x $\in$ A, express the coset x + Za as $(m_1a_1 + \cdots + m_na_n)$ + Za for coefficients $m_1, \ldots, m_n$. Then x $\in$ xZa, and so x = ma + $m_1a_1 + \cdots + m_na_n$ for some m.

Thus, we have shown that Za $\cap$ B = (0) and A = Za + B, so A $\cong$ Za $\oplus$ B.

Theorem 2 (Fundamental Theorem of Finite Abelian Groups): Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order. Any two such decompositions have the same number of factors of each order.

Proof: We first decompose any finite abelian group A into a direct sum of p-groups, and then we can use the previous lemma to write each of these groups as a direct sum of cyclic subgroups.

Uniqueness is shown by induction on |A|. It is enough to prove the uniqueness for a given p-group. Suppose that

$$Z_p\alpha_1 \oplus Z_p\alpha_2 \oplus \cdots \oplus Z_p\alpha_n = Z_p\beta_1 \oplus Z_p\beta_2 \oplus \cdots \oplus Z_p\beta_m$$

where $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$ and $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_m$. Consider the subgroups in which each element has been multiplied by p. By induction, $\alpha_1 - 1 = \beta_1 - 1, \ldots$, which gives $\alpha_1 = \beta_1, \ldots$, with the possible exception of the α_i's and β_j's that equal 1. But the groups have the same order, and this determines that each has the same number of factors isomorphic to Z_p. This completes the proof.

Self Assessment

1. A .... is a set, A together with an operations ".". That combines any two elements a and b to form another element denoted a.b.

   (a) cyclic (b) permutation

   (c) abelian (d) normal

2. In a finite abelian group, each element is in a conjugacy class by itself and the character table involve powers of a single element known as a ....

   (a) group generator (b) group connector

   (c) group and subgroup (d) normal group element

3. In mathematica, the function finite abelian group {n_1, n_2, ... } represents .... product of the cyclic group of degree n_1n_2 ....

   (a) direct (b) indirect

   (c) single (d) external

4. In commutative ring .... the elements, or unit, from an abelian multiplication groups.

   (a) inversible (b) vertible

   (c) direct (d) finite

5. Every subgroup of a finite abelian group is normal, so each subgroup gives rest to a .... group.

   (a) cyclic (b) permutation

   (c) quotient (d) multiplicative

10.4 Summary

- A finite abelian group is a set, *A*, together with an operation "•" that combines any two elements *a* and *b* to form another element denoted *a* • *b*. The symbol "•" is a general placeholder for a concretely given operation. To qualify as a finite abelian group, the set and operation, (*A*, •), must satisfy five requirements known as the *finite Abelian group axioms.*
- Generally, the multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules. The additive notation may also be used to emphasize that a particular group is abelian, whenever both abelian and non-finite abelian groups are considered.
- For the integers and the operation addition "+", denoted (**Z**,+), the operation + combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer *n* has an additive inverse, "*n*, and the addition operation is commutative since $m + n = n + m$ for any two integers *m* and *n*.
- Every cyclic group *G* is abelian, because if *x*, *y* are in *G*, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Thus the integers, **Z**, form a finite abelian group under addition, as do the integers modulo *n*, **Z**/*n***Z**.

10.5 Keywords

Finite Abelian Group: A finite abelian group is a set, *A*, together with an operation "•" that combines any two elements *a* and *b* to form another element denoted *a* • *b*.

Multiplication: The multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules.

Cyclic Group: Every cyclic group *G* is abelian, because if *x*, *y* are in *G*, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$.

10.6 Review Questions

1. Compute all possible finite abelian groups of order n. What is the largest n for which it will work?
2. Find all finite abelian group of order less than or equal to 40 up to isomorphism.
3. Find all finite abelian groups of order 200 to 720 up to isomorphism.
4. Show that the infinite direct product $G = Z_2 \times Z_2 \times \ldots$ is not finitely generated.
5. Let G be a finite abelian group of order m. If n divides m, prove that G has a subgroup of order n.

Answers: Self Assessment

1. (c) 2. (a) 3. (a) 4. (a) 5. (c)

10.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 11: Conjugate Elements

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define conjugate subgroup
- Discuss conjugacy class of an element

Introduction

In the last unit, you have studied about finite abelian group. If G is a group and X is an arbitrary set, a group action of an element $g \in G$ and $x \in X$ is a product, g^x giving in x many problem in algebra may best be attached in group actions. In this unit, you will get the information related to conjugate elements.

11.1 Conjugate Subgroup

Definition: Let G be a group, and let x, y be elements of G. Then y is said to be a **conjugate** of x if there exists an element a in G such that $y = axa^{-1}$.

If H and K are subgroups of G, then K is said to be a **conjugate subgroup of H** if there exists an element a in G such that $K = aHa^{-1}$.

Proposition 1:

(a) Conjugacy of elements defines an equivalence relation on any group G.

(b) Conjugacy of subgroups defines an equivalence relation on the set of all subgroups of G.

Definition: Let G be a group. For any element x in G, the set

$$\{ a \text{ in } G \mid axa^{-1} = x \}$$

is called the **centralizer** of x in G, denoted by C(x).

For any subgroup H of G, the set

$$\{ a \text{ in } G \mid aHa^{-1} = H \}$$

is called the **normalizer** of H in G, denoted by N(H).

Proposition 2: Let G be a group and let x be an element of G. Then C(x) is a subgroup of G.

Proposition 3: Let x be an element of the group G. Then the elements of the conjugacy class of x are in one-to-one correspondence with the left cosets of the centralizer C(x) of x in G.

Example: Two permutations are conjugate in S_n if and only if they have the same shape (i.e., the same number of disjoint cycles, of the same lengths). Thus, in particular, cycles of the same length are always conjugate.

Theorem 1: [Conjugacy class Equation] Let G be a finite group. Then

$$| G | = | Z(G) | + \Sigma[g : C(x)]$$

where the sum ranges over one element x from each nontrivial conjugacy class.

Definition: A group of order p^n, with p a prime number and $n \geq 1$, is called a **p-group.**

Theorem 2: [Burnside] Let p be a prime number. The center of any p-group is nontrivial.

Corollary 1: Any group of order p^2 (where p is prime) is abelian.

Theorem 3: [Cauchy] If G is a finite group and p is a prime divisor of the order of G, then G contains an element of order p.

Example: Prove that if the center of the group G has index n, then every conjugacy class of G has at most n elements.

Solution: The conjugacy class of an element a in G has [G : C(a)] elements. Since the center Z(G) is contained in C(a), we have $[G : C(a)] \leq [G : Z(G)] = n$. (In fact, [G : C(a)] must be a divisor of n.)

Example: Find all finite groups that have exactly two conjugacy classes.

Solution: Suppose that $|G| = n$. The identity element forms one conjugacy class, so the second conjugacy class must have n-1 elements. But the number of elements in any conjugacy class is a divisor of $|G|$, so the only way that n-1 is a divisor of n is if n = 2.

Example: Let G = D_{12}, given by generators a, b with $|a|=6$, $|b|=2$, and $ba=a^{-1}b$. Let H = { 1, a^3, b, a^3b }. Find the normalizer of H in G and find the subgroups of G that are conjugate to H.

Solution: The normalizer of H is a subgroup containing H, so since H has index 3, either N_G (H) = H or N_G (H) = G. Choose any element not in H to do the first conjugation.

$$aHa^{-1} = \{ 1, a(a^3)a^5, aba^5, a(a^3b)a^5 \} = \{ 1, a^3, a^2b, a^5b \}$$

This computation shows that a is not in the normalizer, so N_G (H) = H. Conjugating by any element in the same left coset aH = { a, a^4, ab, a^4b } will give the same subgroup. Therefore, it makes sense to choose a^2 to do the next computation.

$$a^2Ha^{-2} = \{ 1, a^3, a^2ba^4, a^2(a^3b)a^4 \} = \{ 1, a^3, a^4b, ab \}$$

Comment: It is interesting to note that an earlier problem shows that b, a^2b, and a^4b form one conjugacy class, while ab, a^3b, and a^5 b form a second conjugacy class. In the above computations, notice how the orbits of individual elements combine to give the orbit of a subgroup.

Example: Write out the class equation for the dihedral group D_n. Note that you will need two cases: when n is even, and when n is odd.

Solution: When n is odd the center is trivial and elements of the form a^i b are all conjugate. Elements of the form a^i are conjugate in pairs; $a^m \neq a^{-m}$ since $a^{2m} \neq 1$. We can write the class equation in the following form:

$$|G| = 1 + ((n-1)/2) \cdot 2 + n$$

When n is even, the center has two elements. (The element $a^{n/2}$ is conjugate to itself since it is equal to $a^{-n/2}$. This shows that $Z(G) = \{1, a^{n/2}\}$.) Therefore, elements of the form a^i b split into two conjugacy classes. In this case the class equation has the following form:

$$|G| = 2 + ((n-2)/2) \cdot 2 + 2 \cdot (n/2)$$

Example: Show that for all n ≥ 4, the centralizer of the element (1,2)(3,4) in S_n has order $8 \cdot (n-4)!$. Determine the elements in the centralizer of ((1,2)(3,4)).

Solution: The conjugates of a = (1,2)(3,4) in S_n are the permutations of the form (a,b) (c,d). The number of ways to construct such a permutation is

$$n(n-1)/2 \cdot (n-2)(n-3)/2 \cdot 1/2,$$

and dividing this into n! gives the order $8 \cdot (n-4)!$ of the centralizer.

We first compute the centralizer of a in S_4. The elements (1, 2) and (3, 4) clearly commute with (1, 2) (3, 4). Note that a is the square of b = (1, 3, 2, 4); it follows that the centralizer contains < b >, so b^3 = (1, 4, 2, 3) also belongs. Computing products of these elements shows that we must include (1, 3)(2, 4) and (1, 4)(2, 3), and this gives the required total of 8 elements.

To find the centralizer of a in S_n, any of the elements listed above can be multiplied by any permutation disjoint from (1, 2)(3, 4). This produces the required total $|C(a)| = 8 \cdot (n-4)!$.

Self Assessment

1. Let G be a group and let x be an elements of the G. Then L(x) is a .... of G.

   (a) Normal subgroup (b) Cyclic subgroup

   (c) Subgroup (d) Permutation group

2. Any group of order p^2 is ....

   (a) permutation (b) abelian

   (c) cyclic (d) finite

3. If G is a .... group and P is a prime divisor of the order of G, then G contains an element of order P.

   (a) direct (b) external

   (c) internal (d) finite

4. Let P be a prime number. The center of any P-group is ....

   (a) trivial (b) non-trivial

   (c) finite (d) infinite

5. A group of order p^n, with P is a prime number and n .... is called a p-group.

   (a) $a = 1$ (b) $b > 1$

   (c) $c < 1$ (d) $d \geq 1$

Notes

11.2 Summary

- Let G be a group, and let x,y be elements of G. Then y is said to be a **conjugate** of x if there exists an element a in G such that y = axa^{-1}.
- If H and K are subgroups of G, then K is said to be a **conjugate subgroup of H** if there exists an element a in G such that K = aHa^{-1}.
- Conjugacy of elements defines an equivalence relation on any group G.
- Conjugacy of subgroups defines an equivalence relation on the set of all subgroups of G.
- Let G be a group. For any element x in G, the set

  $$\{ a \text{ in } G \mid axa^{-1} = x \}$$

  is called the **centralizer** of x in G, denoted by C(x).

  For any subgroup H of G, the set

  $$\{ a \text{ in } G \mid aHa^{-1} = H \}$$

  is called the **normalizer** of H in G, denoted by N(H).
- Let G be a group and let x be an element of G. Then C(x) is a subgroup of G.
- Let x be an element of the group G. Then the elements of the conjugacy class of x are in one-to-one correspondence with the left cosets of the centralizer C(x) of x in G.

11.3 Keywords

Conjugate Element: If H and K are subgroups of G, then K is said to be a ***conjugate subgroup*** of H if there exists an element a in G such that K = aHa^{-1}.

Centralizer: Let G be a group. For any element x in G, the set

$$\{ a \text{ in } G \mid axa^{-1} = x \}$$

is called the ***centralizer*** of x in G, denoted by C(x).

11.4 Review Questions

1. Compute the G-equivalence classes of X for each of the G-sets X = {1, –2, 24, 5, 6} and G = {(1), (1, 2) (3, 4, 5) ; (1 2) (3 4 5), (1 2) (3 8 4)} for each x ∈ X verify $|G| = |O_x| \; |G_x|$.
2. Write the class equation for S5 and for $|G_x|$
3. Let P be prime. Show that the number of different abelian groups of order P^n is the same as the number of conjugacy class in S_n.
4. Let a ∈ G, show that for any g ∈ G, $gc(a)g^{-1} = c(gag^{-1})$.
5. Let $|G| = p^n$ and suppose that $|Z(G)| = p^{n-1}$ for p prime. Prove that G is abelian.
6. Let G be a group with order p^n, where p is prime and X a finite G-set. If $X_G = \{x \in X : gx = x$ for all $g \in G\}$ is the set of elements in X fixed by the group actions, then prove that $|X| = |X_G| \; (\text{mod}_p)$.

Answers: Self Assessment

1. (c) 2. (b) 3. (d) 4. (b) 5. (d)

11.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 12: Sylow's Theorems

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss Sylow's Theorem
- Describe examples of Sylow's Theorem

Introduction

We already know that the converse of Lagrange's Theorem is false. If G is a group of order m and n divides m, then G does not necessarily possess a subgroup of order n. For example, A_4 has order 12 but does not possess a subgroup of order 6. However, the Sylow Theorems do provide a partial converse for Lagrange's Theorem: in certain cases they guarantee us subgroups of specific orders. These theorems yield a powerful set of tools for the classification of all finite non-abelian groups.

12.1 The Sylow Theorems

We will use the idea of group actions to prove the Sylow Theorems. Recall for a moment what it means for G to act on itself by conjugation and how conjugacy classes are distributed in the group according to the class equation. A group G acts on itself by conjugation via the map $(g, x) \to gxg^{-1}$. Let $x_1,...,x_k$ be representatives from each of the distinct conjugacy classes of G that consist of more than one element. Then the class equation can be written as

$$|G| = |Z(G)| + [G : C(x_1)] + ... + [G : C(x_k)],$$

where $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$ is the center of G and $C(x_i) = \{g \in G : gx_i = x_ig\}$ is the centralizer subgroup of x_i.

We now begin our investigation of the Sylow Theorems by examining subgroups of order p, where p is prime. A group G is a p-group if every element in G has as its order a power of p, where p is a prime number. A subgroup of a group G is a p-subgroup if it is a p-group.

12.1.1 A Proof of Sylow's Theorems

In this handout, we give proofs of the three Sylow theorems which are slightly different from the ones in the book. Recall the following lemma:

Lemma: Let p be a prime number, and let G be a p-group (a finite group of order p^k for some $k \geq 1$) acting on a finite set S. Then the number of fixed points of the action is congruent to $|S|$ modulo p.

We make the following definition: if G has order $p^k m$ with $p \nmid m$, a Sylow p-subgroup of G is a subgroup of order p^k.

Theorem (Sylow's First Theorem): If G is a finite group of order $n = p^k m$ with p prime and $p \nmid m$, then G has a subgroup of order p^k. In other words, if $Syl_p(G)$ denotes the set of Sylow p-subgroups of G, then $Syl_p(G) \neq \emptyset$.

Proof. The proof is by induction on $|G|$, the base case $|G| = 1$ being trivial. If there exists a proper subgroup H of G such that $p \nmid [G : H]$, then a Sylow p-subgroup of H is also a a Sylow p-subgroup of G and we're finished by induction. So without loss of generality, we may assume that $p \mid [G : H]$ whenever $H < G$. From the class equation, it follows that $p \mid |Z_G|$. By Cauchy's theorem, there exists a subgroup $N \leq Z_G$ of order p, which is necessarily normal in G. Let $\overline{G}$ = G/N, so $|\overline{G}| = p^{k-1}m$. By induction, $\overline{G}$ has a subgroup $\overline{P}$ of order p^{k-1}. Let P be the subgroup of G containing N which corresponds to $\overline{P}$ by the first isomorphism theorem. Then

$$|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k,$$

so that P is a Sylow p-subgroup of G as desired.

Theorem (Sylow's Second Theorem): If G is a finite group and p is a prime number, then all Sylow p-subgroups of G are conjugate to one another.

Proof: We show more precisely that if H is any subgroup of G of p-power order and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H \leq xPx^{-1}$. (This implies the theorem, since if $H \in Syl_p(G)$ then $|H| = |P| = |xPx^{-1}|$, which implies that $H = xPx^{-1}$, so that H is conjugate to P.) Note that H acts on G/P (the set of left cosets of P in G) by left multiplication. Let Fix denote the elements of G/P fixed by this action. Then $|Fix| \equiv |G/P| \pmod{p}$ by the Lemma. Since $p \nmid m = |G/P|$, $|Fix| \neq 0$, and thus Fix $\neq \emptyset$;. Let xP be a left coset fixed by the action. Then

$$hxP = xP \,\forall\, h \in H \Rightarrow x^{-1}Hx \leq P,$$

so that $H \leq xPx^{-1}$ as desired.

Theorem (Sylow's Third Theorem): If G is a finite group and p is a prime number, let $n_p = |Syl_p(G)|$. Then $n_p \mid |G|$ and $n_p \equiv 1 \pmod{p}$.

Proof: We consider the action of G on Sylp(G) by conjugation. By the second Sylow theorem, this action is transitive, so there is just one orbit. Hence n_p, which is the size of this orbit, divides $|G|$.

To prove the congruence $n_p \equiv 1 \pmod{p}$, we fix a Sylow p-subgroup $P \in Syl_p(G)$ and consider the action of P on $Syl_p(G)$ by conjugation. Let Fix denote the set of fixed points of this action. Note that $Q \in Fix \Leftrightarrow P \leq N_G(Q)$, and in particular $P \in Fix$. If $Q \in Fix$, then $P, Q \leq N_G(Q)$ are both Sylow p-subgroups of $N_G(Q)$, so they are conjugate in $N_G(Q)$ (again by the second Sylow theorem). But Q is a normal subgroup of $N_G(Q)$, so P = Q. Thus Fix = {P}, and in particular $|Fix| = 1$. By the Lemma, $np \equiv 1 \pmod{p}$ as desired.

Notes

The more precise fact established in our proof of Sylow's Second Theorem yields the following useful result:

Corollary: If G is a finite group and p is a prime number, then any subgroup of G of p-power order is contained in some Sylow p-subgroup.

Since G acts transitively by conjugation on $\text{Syl}_p(G)$, and the stabilizer of $P \in \text{Syl}_p(G)$ is $N_G(P)$, we deduce that np = $[G : N_G(P)]$ for any $P \in \text{Syl}_p(G)$.

Therefore:

Corollary: If G is a finite group and p is a prime number, let n_p be the number of Sylow p-subgroups of G. Then the following are equivalent:

1. np = 1.
2. Every Sylow p-subgroup of G is normal.
3. Some Sylow p-subgroup of G is normal.

Example: By direct computation, find the number of Sylow 3-subgroups and the number of Sylow 5-subgroups of the symmetric group S_5. Check that your calculations are consistent with the Sylow theorems.

Solution: In S_5 there are (5 ·4 ·3) / 3 = 20 three cycles. These will split up into 10 subgroups of order 3. This number is congruent to 1 mod 3, and is a divisor of 5 ·4 ·2.

There are (5!) / 5 = 24 five cycles. These will split up into 6 subgroups of order 5. This number is congruent to 1 mod 5, and is a divisor of 4 ·3 ·2.

Example: How many elements of order 7 are there in a simple group of order 168?

Solution: First, 168 = $2^3 \cdot 3 \cdot 7$. The number of Sylow 7-subgroups must be congruent to 1 mod 7 and must be a divisor of 24. The only possibilities are 1 and 8. If there is no proper normal subgroup, then the number must be 8. The subgroups all have the identity in common, leaving 8 ·6 = 48 elements of order 7.

Example: Prove that a group of order 48 must have a normal subgroup of order 8 or 16.

Solution: The number of Sylow 2-subgroups is 1 or 3. In the first case there is a normal subgroup of order 16. In the second case, let G act by conjugation on the Sylow 2-subgroups. This produces a homomorphism from G into S_3. Because of the action, the image cannot consist of just 2 elements. On the other hand, since no Sylow 2-subgroup is normal, the kernel cannot have 16 elements. The only possibility is that the homomorphism maps G onto S_3, and so the kernel is a normal subgroup of order 48 / 6 = 8.

Example: Let G be a group of order 340. Prove that G has a normal cyclic subgroup of order 85 and an abelian subgroup of order 4.

Solution: First, 340 = $2^2 \cdot 5 \cdot 17$. There exists a Sylow 2-subgroup of order 4, and it must be abelian. No divisor of 68 = $2^2 \cdot 17$ is congruent to 1 mod 5, so the Sylow 5-subgroup is normal. Similarly, then Sylow 17-subgroup is normal. These subgroups have trivial intersection, so their product is a direct product, and hence must be cyclic of order 85 = 5 · 17. The product of two normal subgroups is again normal, so this produces the required normal subgroup of order 85.

Example: Show that there is no simple group of order 200.

Solution: Since $200 = 2^3 \cdot 5^2$, the number of Sylow 5-subgroups is congruent to 1 mod 5 and a divisor of 8. Thus there is only one Sylow 5-subgroup, and it is a proper nontrivial normal subgroup.

Example: Show that a group of order 108 has a normal subgroup of order 9 or 27.

Solution: Let S be a Sylow 3-subgroup of G. Then [G:S] = 4, since $|G| = 2^2\,3^3$, so we can let G act by multiplication on the cosets of S. This defines a homomorphism $\mu : G \to S_4$, so it follows that $|\mu(G)|$ is a divisor of 12, since it must be a common divisor of 108 and 24. Thus $|\ker(\mu)| \geq 9$, and it follows that $\ker(\mu) \subseteq S$, so $|\ker(\mu)|$ must be a divisor of 27. It follows that $|\ker(\mu)| = 9$ or $|\ker(\mu)| = 27$.

Example: If p is a prime number, find all Sylow p-subgroups of the symmetric group S_p.

Solution: Since $|S_p| = p!$, and p is a prime number, the highest power of p that divides $|S_p|$ is p. Therefore, the Sylow p-subgroups are precisely the cyclic subgroups of order p, each generated by a p-cycle. There are (p-1)! = p! / p ways to construct a p-cycle $(a_1, \ldots, a_p)$. The subgroup generated by a given p-cycle will contain the identity and the p-1 powers of the cycle. Two different such subgroups intersect in the identity, since they are of prime order, so the total number of subgroups of order p in S_p is (p-2)! = (p-1)! / (p-1).

Example: Prove that if G is a group of order 56, then G has a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.

Solution: The number of Sylow 7-subgroups is either 1 or 8. Eight Sylow 7-subgroups would yield 48 elements of order 7, and so the remaining 8 elements would constitute the (unique) Sylow 2-subgroup.

Example: Prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G.

Solution: Suppose that N contains the Sylow p-subgroup P. Then since N is normal it also contains all of the conjugates of P. But this means that N contains all of the Sylow p-subgroups of G, since they are all conjugate. We conclude that N and G have the same number of Sylow p-subgroups.

Example: Prove that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Solution: The notation $n_p(G)$ will be used for the number of Sylow p-subgroups of G. Since $105 = 3 \cdot 5 \cdot 7$, we have $n_3(G) = 1$ or 7, $n_5(G) = 1$ or 21, and $n_7(G) = 1$ or 15 for the numbers of Sylow subgroups. Let P be a Sylow 5-subgroup and let Q be a Sylow 7-subgroup. At least one of these subgroups must be normal, since otherwise we would have $21 \cdot 4$ elements of order 5 and $15 \cdot 6$ elements of order 7. Therefore, PQ is a subgroup, and it must be normal since its index is the smallest prime divisor of $|G|$, so we can apply the result in the previous problem. Since PQ is normal and contains a Sylow 5-subgroup, we can reduce to the number 35 when considering the number of Sylow 5-subgroups, and thus $n_5(G) = n_5(PQ) = 1$. Similarly, since PQ is normal and contains a Sylow 7-subgroup, we have $n_7(G) = n_7(PQ) = 1$.

Self Assessment

1. A group G is a p-group of every element in G has its order a power of ....

   (a) g (b) p

   (c) g-1 (d) p-1

2. If G is a finite group. Then G is p-group of and only if |G| = ...

   (a) p^{-p} (b) p^p

   (c) p^n (d) p^n

3. Let P be a Sylow p-subgroups of a .... G and let x have as its order a power of p. If $x^{-1}p(x) = p$. Then $x \in p$.

   (a) indirect (b) infinite

   (c) finite (d) direct

4. A subgroup of a group G is a p- .... if it is a p-group.

   (a) subgroup (b) normal group

   (c) infinite group (d) cyclic group

5. How many elements of order 7 are there is a simple group of order 168.

   (a) 7 (b) 8

   (c) 9 (d) 48

12.2 Summary

- Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.
- **(First Sylow Theorem)** Let G be a finite group and p a prime such that p^r divides |G|. Then G contains a subgroup of order p^r.
- Let P be a Sylow p-subgroup of a finite group G and let x have as its order a power of p. If $x^{-1}Px = P$. Then $x \in P$.
- Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.
- **(Second Sylow Theorem)** Let G be a finite group and p a prime dividing |G|. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.

12.3 Keywords

Cauchy: Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.

First Sylow Theorem: Let G be a finite group and p a prime such that p^r divides |G|. Then G contains a subgroup of order p^r.

12.4 Review Questions

1. What are the order of all Sylow p-subgroups where G has order 18, 24, 54 and 80?
2. Find all the Sylow 3-subgroups of S_4 and show that they are all conjugate.
3. Show that every group of order 45 has a normal subgroup of order 9.
4. Let H be a Sylow p-subgroup of G. Prove that H ps the only Sylow p-subgroup of G contained in N(H).
5. Prove that no group of order 96 is simple.
6. If H is normal subgroup of a finite group G and $|H| = p^k$ for some prime p, show that H is a contained in every Sylow p-subgroup of G.

Answers: Self Assessment

1. (b) 2. (c) 3. (c) 4. (a) 5. (d)

12.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 13: Solvable Groups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the solvable groups
- Describe examples of solvable group

Introduction

In the earlier unit, you have studied about the conjugate elements and Sylow's Theorem. This unit will equip you with more information related to solvable group.

13.1 Solvable Group

Definition: The group G is said to be **solvable** if there exists a finite chain of subgroups $G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n$ such that

(i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, ... ,n,

(ii) N_{i-1} / N_i is abelian for i = 1, 2, ..., n, and

(iii) $N_n = \{e\}$.

Proposition: A finite group G is solvable if and only if there exists a finite chain of subgroups $G = N_0 \supseteq N_1 \supseteq ... N_n$ such that

(i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, . . ., n,

(ii) N_{i-1} / N_i is cyclic of prime order for i = 1, 2, . . ., n, and

(iii) $N_n = \{e\}$.

Theorem 1: Let p be a prime number. Any finite p-group is solvable.

Definition: Let G be a group. An element g in G is called a **commutator** if

$$g = aba^{-1}b^{-1}$$

for elements a, b in G.

The smallest subgroup that contains all commutators of G is called the **commutator subgroup** or **derived subgroup** of G, and is denoted by G′.

Proposition: Let G be a group with commutator subgroup G′.

(a) The subgroup G′ is normal in G, and the factor group G/G′ is abelian.

(b) If N is any normal subgroup of G, then the factor group G/N is abelian if and only if $G' \subseteq N$.

Definition: Let G be a group. The subgroup (G′)′ is called the **second derived subgroup** of G. We define $G^{(k)}$ inductively as $(G^{(k-1)})'$, and call it the *k* **th derived subgroup.**

Theorem 2: A group G is solvable if and only if $G^{(n)} = \{e\}$ for some positive integer n.

Corollary: Let G be a group.

(a) If G is solvable, then so is any subgroup or homomorphic image of G.

(b) If N is a normal subgroup of G such that both N and G/N are solvable, then G is solvable.

Definition: Let G be a group. A chain of subgroups $G = N_0 \supseteq N_1 \supseteq ... \supseteq N_n$ such that

(i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, . . . ,n,

(ii) N_{i-1} / N_i is simple for i = 1, 2, . . . ,n, and

(iii) $N_n = \{e\}$

is called a **composition series** for G.

The factor groups N_{i-1} / N_i are called the **composition factors** determined by the series.

Theorem 3: [Jordan-Hölder] Any two composition series for a finite group have the same length. Furthermore, there exists a one-to-one correspondence between composition factors of the two composition series under which corresponding composition factors are isomorphic.

Example: Let p be a prime and let G be a non-abelian group of order p^3. Show that the center Z(G) of G equals the commutator subgroup G′ of G.

Solution: Since G is non-abelian, we have $|Z(G)| = p$. (The center is nontrivial, and if $|Z(G)| = p^2$, then G/Z(G) is cyclic, the text implies that G is abelian.) On the other hand, any group of order p^2 is abelian, so G/Z(G) is abelian, which implies that G′ Z(G). Since G is nonabelian, G′ {e}, and therefore G′ = Z(G).

Example: Prove that D_n is solvable for all n.

One approach is to compute the commutator subgroup of D_n, using the standard description

$$D_n = \{ a^i b^j \mid 0 \leq i < n, 0 \leq j < 2, o(a) = n, o(b) = 2, ba = a^{-1}b \}$$

We must find all elements of the form $xyx^{-1}y^{-1}$, for x,y in D_n. We consider the cases $x = a^i$ or $x = a^ib$ and $y = a^j$ or $y = a^jb$.

Case 1: If $x = a^i$ and $y = a^j$, the commutator is trivial.

Case 2: If $x = a^i$ and $y = a^jb$, then $xyx^{-1}y^{-1} = a^ia^jba^{-i}a^jb = a^ia^ja^iba^jb = a^ia^ja^ia^{-j}b^2 = a^{2i}$, and thus each even power of a is a commutator.

Case 3: If $x = a^jb$ and $y = a^i$, we get the inverse of the element in Case 2.

Case 4: If $x = a^ib$ and $y = a^jb$, then

$xyx^{-1}y^{-1} = a^iba^jba^iba^jb$, and so we get

$xyx^{-1}y^{-1} = a^ia^{-j}b^2a^ia^{-j}b^2 = a^{2(i-j)}$, and again we get even powers of a.

Thus the commutator subgroup D_n' is either < a > (if n is odd) or $< a^2 >$ (if n is even). In either case, the commutator subgroup is abelian, so $D_n'' = \{e\}$.

Example: Prove that any group of order 588 is solvable, given that any group of order 12 is solvable.

We have $588 = 2^2 \cdot 3 \cdot 7^2$. Let S be the Sylow 7-subgroup. It must be normal, since 1 is the only divisor of 12 that is 1 mod 7. By assumption, G / S is solvable since | G / S | = 12. Furthermore, S is solvable since it is a p-group. Since both S and G / S are solvable, it follows from Corollary that G is solvable.

Example: Let G be a group of order $780=2^2 \cdot 3 \cdot 5 \cdot 13$. Assume that G is not solvable. What are the composition factors of G? (Assume that the only nonabelian simple group of order 60 is A_5.)

The Sylow 13-subgroup N is normal, since 1 is the only divisor of 60 that is 1 mod 13. Using the fact that the smallest simple nonabelian group has order 60, we see that the factor G/N must be simple, since otherwise each composition factor would be abelian and G would be solvable. Thus the composition factors are Z_{13} and A_5.

Theorem-[Jordan-Hölder] Any two composition series for a finite group have the same length. Furthermore, there exists a one-to-one correspondence between composition factors of the two composition series under which corresponding composition factors are isomorphic.

Let |G| = N. We first prove existence, using induction on N. If N = 1 (or, more generally, if G is simple) the result is clear. Now suppose G is not simple. Choose a maximal proper normal subgroup G1 of G. Then G1 has a Jordan-Hölder decomposition by induction, which produces a Jordan-Hölder decomposition for G.

To prove uniqueness, we use induction on the length n of the decomposition series. If n=1 then G is simple and we are done. For n > 1, suppose that

$$G \supset G1 \supset G2 \supset Gn = \{1\}$$

and

$$G \supset G1 \supset G2 \supset Gm=1$$

are two decompositions of G . If G1 = G1 then we're done (apply the induction hypothesis to G1), so assume G1/G1 . Set $H : = G1 \cap G1$ and choose a decomposition series $H \supset H_1 \supset Hk = \{1\}$ for H. By the second isomorphism theorem, G1/H=G1G1/G1=G/G1 (the last equality is because G1G1 is a normal subgroup of G properly containing G1). In particular, H is a normal subgroup of G1 with simple quotient. But then

$$G1 \supset G2 \supset ... \supset Gn$$

and

$$G1 \supset H \supset ... \supset Hk$$

are two decomposition series for G1, and hence have the same simple quotients by the induction hypothesis; likewise for the G1 series. Therefore, n=m. Moreover, since G/G1=G1/H and G/G1=G1/H (by the second isomorphism theorem), we have now accounted for all of the simple quotients, and shown that they are the same.

Self Assessment

1. Let P be a prime number. Any .... p-group is solvable

   (a) infinite (b) direct

   (c) finite (d) indirect

2. The smallest subgroup that contains all commutations of G is called as ....

   (a) commutator subgroup (b) normal subgroup

   (c) generator subgroup (d) cyclic subgroup

3. If x = a^i and y = ..., the commutator is trivial

   (a) a^j (b) a^{-1}

   (c) a^{-j} (d) y^{-1}

4. Let G be a group the subgroup is called the .... of G.

   (a) normal subgroup (b) second derived subgroup

   (c) composition series (d) cyclic series

13.2 Summary

- The group G is said to be **solvable** if there exists a finite chain of subgroups $G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n$ such that

  (i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, ..., n,

  (ii) N_{i-1} / N_i is abelian for i = 1, 2, ..., n, and

  (iii) $N_n = \{e\}$.

- A finite group G is solvable if and only if there exists a finite chain of subgroups $G = N_0 \supseteq N_1 \supseteq ... N_n$ such that

  (i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, . . ., n,

  (ii) N_{i-1} / N_i is cyclic of prime order for i = 1, 2, . . ., n, and

  (iii) $N_n = \{e\}$.

- Let p be a prime number. Any finite p-group is solvable.

- Let G be a group. An element g in G is called a **commutator** if

  $$g = aba^{-1}b^{-1}$$

  for elements a,b in G.

- The smallest subgroup that contains all commutators of G is called the **commutator subgroup** or **derived subgroup** of G, and is denoted by G′.

- Let G be a group. A chain of subgroups $G = N_0 \supseteq N_1 \supseteq ... \supseteq N_n$ such that

  (i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, . . ., n,

  (ii) N_{i-1} / N_i is simple for i = 1, 2, . . ., n, and

  (iii) $N_n = \{e\}$

  is called a **composition series** for G.

- The factor groups N_{i-1} / N_i are called the **composition factors** determined by the series.

Notes

13.3 Keywords

Commutator Subgroup: The smallest subgroup that contains all commutators of G is called the **commutator subgroup** or **derived subgroup** of G, and is denoted by G′.

Let G be a group. A chain of subgroups $G = N_0 \supseteq N_1 \supseteq ... \supseteq N_n$ such that

(i) N_i is a normal subgroup in N_{i-1} for i = 1, 2, . . ., n,

(ii) N_{i-1} / N_i is simple for i = 1, 2, . . ., n, and

(iii) $N_n = \{e\}$

is called a **composition series** for G.

Jordan-Hölder: Any two composition series for a finite group have the same length. Furthermore, there exists a one-to-one correspondence between composition factors of the two composition series under

13.4 Review Questions

1. Prove the normal series

   $Z_{60} \supset \{ 3 \} \supset \{ 15 \} \supset \{ 0 \}$

   $Z_{60} \supset \{ 4 \} \supset \{ 20 \} \supset \{ 0 \}$

   of the group Z_{60} are isomorphic.

2. Let G and H be solvable groups. Show G × H is also solvable.

3. If G has a composition series and if N is a proper normal subgroup of G, Show the n exists a composition series containing N.

4. Let N be a normal subgroup of G. If N and G/N have composition series, then G must also have a composition series.

5. Let N be a normal subgroup of G if N and G/N are solvable groups. Show that G is also solvable group.

6. Prove that G is a solvable group if and only if G has a series of subgroups $G = P_n \supset P_{n-1} \supset ... P_1 \supset P_0 = \{ e \}$

   where p_i is normal in p_{i+1} and the order p_{i+1}/p_i is prime.

Answers: Self Assessment

1. (c) 2. (a) 3. (a) 4. (b)

13.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 14: Rings

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define and give examples of rings
- Discuss some elementary properties of rings from the defining axioms of a ring
- Define and give examples of commutative rings, rings with identity and commutative rings with identity

Introduction

With this unit, we start the study of algebraic system with two binary operations satisfying certain properties. Z, Q and R are examples of such a system, which we shall call a ring.

Now, you know that both addition and multiplication are binary operations on Z. Further, Z is an abelian group under addition. Though it is not a group under multiplication, multiplication is associative. Also, addition and multiplication are related by the distributive laws

$$a(b + c) = ab + nc, \text{ and } (a + b)c = ac + bc$$

for all integers a, b and c. We generalise these very properties of the binary operations to define a ring in general. This definition is given by the famous algebraist Emmy Noether.

After defining rings we will provide several examples of rings. You will also learn about some propertics of rings that follow from the definition itself. Finally, we shall discuss certain types of rings that are obtained when we impose more restrictions on the “multiplication” in the ring.

As the contents suggest, this unit lays the foundation for the rest of this course. So make sure that you have attained the following objectives before going to the next unit.

14.1 What is a Ring?

You are familiar with Z, the set of integers. You also know that it is a group with respect to addition. Is it a group with respect to multiplication too? No. But multiplication is associative and distributes over addition. These properties of addition and multiplication of integers allow us to say that the system (Z, +, .) is a ring. But, what do we mean by a ring?

Definition: A non-empty set R together with two binary operations, we mean usually called addition (denoted by f) and multiplication (denoted by .), is called a **ring** if the following axioms are satisfied:

R 1) $a + b = b + a$ for all a, b in R, i.e., addition is commutative.

R 2) $(a + b) + c = a + (b + c)$ for all a, b, c in R, is., addition is associative.

R 3) There exists an element (denoted by 0) of R such that

$a + 0 = a = 0 + a$ for all a in R, i.e., R has an additive identity.

R 4) For each a in R, there exists x in R such that $a + x =: 0 = x + a$, i.e., every elements of R has an additive inverse.

R 5) $(a \,.\, b).c = a.(b \,.\, c)$ for all a, b, c in R, i.e., multiplication is associative.

R 6) $a.(b + c) = a \,.\, b + a \,.\, c$, and

$(a\, t\, b) \,.\, i = a \,.\, d + b \,.\, c$

for all a, b, c in R,

i.e., multiplication distributes over addition from the left as well as the right.

The axioms RI-R4 say that (R, +) is an abelian group. The axiom R5 says that multiplication is associative. Hence, we can say that the system (R, +, .) is a ring if

(i) (R, +) is an abelian group,

(ii) (R, .) is a semigroup, and

(iii) for all a, b, c in R, $a.(b + c) = a \,.\, b\, t\, a \,.\, c$, and $(a + b) = a \,.\, c + b \,.\, c$.

As you know that the addition identity 0 is unique, and each element a of R has a unique additive inverse (denoted by - a). We call the element 0 the zero element of the ring.

By convention, we write a – b for a + (–b).

Let us look at some examples of rings now. You have already seen that Z is a ring. What about the sets Q and R? Do (Q, +, .) and (R, +, .) satisfy the axioms R1 – R6? They do.

Therefore, these systems are rings.

The following example provides us with another set of examples of rings

Example: Show that (nZ, +, .) is a ring, where $n \in Z$.

Solution: You know that $nZ = \{ nm\ I\ m \in Z \}$ is an abelian group with respect to addition. You also know that multiplication in nZ is associative and distributes over addition from the right as well as the left. Thus, nZ is a ring under the usual addition and multiplication.

So far the examples that we have considered have been **infinite rings,** that is, their underlying sets have been infinite sets. Now let us look at a **finite ring,** that is, a ring (R, +. .) where R is a finite set. Our example is the set Z,,. Let us briefly recall the construction of Z,, the set of residue classes modulo n.

If a and b are integers, we say that a is congruent to b modulo n if a – b is divisible by n; in symbols, a ≡ b (mod n) if n I (a – b). The relation 'congruence modulo n' is an equivalence relation in Z. The equivalence class containing the integer a is

$$\bar{a} = \{ b \in Z \text{ (} a - b \text{ is divisible by } n \}$$

$$= \{ a + m p \mid m \in Z \}.$$

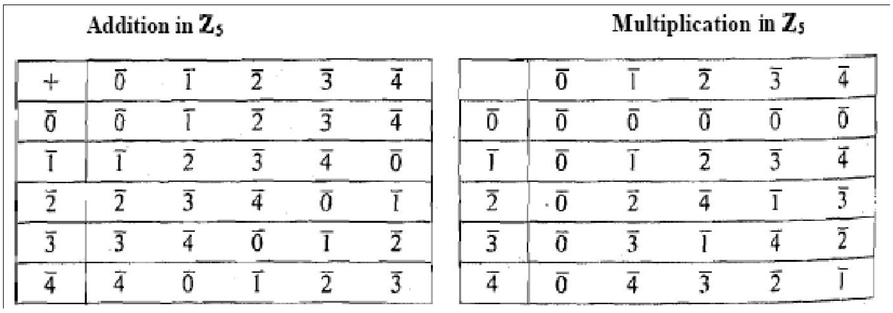
It is called the **congruence class of a modulo n** or the **residue class of a modulo n.** The set of all equivalence classes is denoted by Z,,. So

$$Z\,,\,, = \{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\}.$$

We define addition and multiplication of classes in terms of their representatives by

$$\bar{a} + \bar{b} = \overline{a+b} \text{ and}$$
$$\bar{a}\,.\,\bar{b} = \overline{ab}\ \forall\ \bar{a}, \bar{b} \in Zn.$$

To help you regain some practice in adding and multiplying in Z,,, consider the following Cayley tables for Z_n.



Addition in Z_5

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Multiplication in Z_5

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Now let us go back to looking for a finite ring.

Example: Show that (Z_n, +, .) is a ring.

Solution: You already know that (Z_n, +) is an abelian group, and that multiplication is associative in Z,. Now we need to see if the axiom R6 is satisfied.

For any $\bar{a}, \bar{b}\,\bar{c} \in Z_n$,

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

Similarly, ($\bar{a}$ + 6) . = L.; + $\bar{b}.\bar{c}\ \forall\ \bar{a}, \bar{b}\,\bar{c} \in Z,$.

So, (Z_n, +,) satisfies the axioms R1-R6. Therefore, it is a ring.

Now let us look at a ring whose underlying set is a subset of C.

Example: Consider the set

Z + iZ = { m + in | m and n are integers }, where i^2 = – I.

We define '+' and '.' in Z + iZ to be the usual addition and multiplication of complex numbers. Thus, foram + in and s + it in Z + iZ,

$(m + in) + (s + it) = (m + s) + i(n + t)$, and

$(m + in) . (s + it) = (p – nt) + i(mt + ns)$.

Verify that Z + iZ is a ring under this addition and multiplication. (This ring is called the ring of Gaussian integers, after the mathematician Carl Friedrich Gauss.)

Solution: Check that (Z + iZ, +) is a subgroup of (C, I–). Thus, the axioms RI-R4 are satisfied. You can also check that

$((a + ib) . (c + id)) . (m + in) = (a + ib) . ((c + id) . (m + in))$

$\forall$ a + ib, c + id, m + in $\in$ Z + iZ.

This shows that R5 is also satisfied.

Finally, you can check that the right distributive law holds, i.e.,

$((a + ib) + (c + id)) . (m + in) = (a + ib) . (m + in) + (c + id) . (m + in)$ for any a + ib, c + id, m + in $\in$ Z + iZ.

Similarly, you can check that the left distributive law holds. Thus, (Z + iZ, + , .) is a ring. The operations that we consider in it are not the usual addition and multiplication.

Example: Let X be a non-empty set, $\wp$ (XI) be the collection of all subsets of X and A denote the symmetric difference operation. Show that ($\wp$ (X), A, n) is a ring.

Solution: For any two subsets A and B of X,

$A \Delta B = (A\backslash B) \cup (B\backslash A)$

It is clear that ($\wp$ (X), A) is an abelian group. You also know that $\cap$ is associative. Now let us see if $\cap$ distributes over A.

Let A, B, C E $\wp$ (X). Then

$A \cap (B \cap C) = A \cap [(B\backslash C) \cup (C\backslash B)]$

$= [A \cap (B\backslash C)] \cup [A \cap (C\backslash B)]$, since n distributes over U.

$= [(A \cap B)\backslash(A \cap C)] \cup [(A \cap C)\backslash(A \cap B)]$, since $\cap$ distributes over complementation.

$= (A \cap B)\ A\ (A \cap C)$.

So, the left distributive law holds.

Also, $(B \cap C) \cap A = A \cap (B \cap C)$, since $\cap$ is commutative.

$= (A \cap B)\ P\ (A \cap C)$

$= (B \cap A)\ A\ (C \cap A)$.

Therefore, the right distributive law holds also.

Therefore, ($\wp$ (X), A, $\cap$) is a ring.

So' far you have seen examples of rings in which both the operations defined on the ring have been commutative. This is not so in the next example.

Example: Consider the set

$$M_2(R) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| \text{ a, } a_{12}, a_{21}, \text{ and a; are real numbers} \right\}$$

Show that $M_2(R)$ is a ring with respect to addition and multiplication of matrices.

Solution: You can check that $(M_2(R), +)$ is an abelian group. You can also verify the associative property for multiplication. We now show that A · (B + C) = A · B A- A · C for A, B, C in $M_2(R)$.

$$A\,.\,(B + C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}+\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}\right)$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}(b_{11}+c_{11})+a_{12}(b_{21}+c_{21}) & a_{11}(b_{12}+c_{12})+a_{12}(b_{22}+c_{22}) \\ a_{21}(b_{11}+c_{11})+a_{22}(b_{21}+c_{21}) & a_{21}(b_{12}+c_{12})+a_{22}(b_{22}+c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}b_{11}+a_{12}c_{21})+(a_{11}c_{11}+a_{12}c_{21}) & (a_{11}b_{12}+a_{12}b_{22})+(a_{11}c_{12}+a_{12}c_{22}) \\ (a_{21}b_{11}+a_{22}c_{21})+(a_{21}c_{11}+a_{22}c_{21}) & (a_{21}b_{12}+a_{22}b_{22})+(a_{21}c_{12}+a_{22}c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}+\begin{bmatrix} a_{11}c_{11}+a_{12}c_{21} & a_{11}c_{12}+a_{12}c_{22} \\ a_{21}c_{11}+a_{22}c_{21} & a_{21}c_{12}+a_{12}c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}+\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

= A.B + A.C

In the same way we can obtain the other distributive law, i.e., (A + B) . C = A. C + B . C ∀ A, B, C ∈ $M_2(R)$.

Thus, $M_2(R)$ is a ring under matrix addition and multiplication.

Note Multiplication over $M_2(R)$ is not commutative. So, we can't say that the left distributive law implies the right distributive law in this case.

Example: Consider the class of all continuous real valued functions defined on the closed interval [0, 1]. We denote this by C [0, 1]. If f and g are two continuous functions on [0, 1], we define f + g and fg as

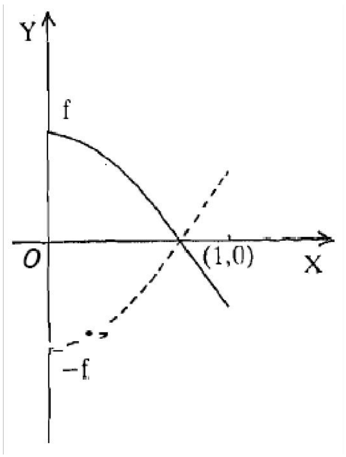
(f + g) (x) = f(x) + g(x) (i.e., pointwise addition)

and (f. g) (x) = f(x). g(x) (i.e., pointwise multiplication)

for every x ∈ [0, 1]. From the Calculus course you know that the function f + g and fg are defined and continuous on [0, 1], i.e., if f and g ∈ C[0, 1], then both f + g and f .g are in C [0, 1]. Show that C [0, 1] is a ring with respect to + and

Solution: Since addition in R is associative and commutative, so is addition in C [0, 1]. The additive identity of C [0, 1] is the zero function. The additive inverse off ∈ C [0, 1] is (–f), where (–f)(x) = – f(A) ∀ x ∈ [0, 1]. See figure 14.1 for a visual interpretation of (- f). Thus, (C [0, 1], +) is an abelian group. Again, since multiplication in R is associative, so is multiplication in C [0, 1].

Figure 14.1: The Graphs of f and (–f) over [0, 1]



Now let us see if the axiom R6 holds.

To prove f . (g + h) = f . g + f . h, we consider (f . (g + h) (x) for any x in [0, 1].

Now (f . (g + h)(x) = f(x) (g + h) (x)

= f(x) g(x) +h(x))

= f(x) g(x) + f(x)h(x), since, distributes over + in R.

= (f.g)(x) + (f.h)(x)

Since multiplication is commutative in C [0, 1], the other distributive law also holds. Thus, R6 is true for C [0, 1]. Therefore, (C [0, 1], +, .) is a ring.

This ring is called the ring of continuous functions on [0, 1].

The next example also deals with functions.

Example: Let (A, +) be an abelian group. The set of all endomorphisms of A is

End A = (f : A – A | f(a + b) = f(a) + f(b) $\forall$ a, b $\in$ A)

For f, g $\in$ End A, we define f + g and f . g as

(f + g) (a) = f(a) + g(a), and ...(1)

(f. g) (a) = fog(a) = f(g(a)) $\forall$ a $\in$ A

Show that (End A, +,.) is a ring. (This ring is called the endomorphism ring of A.)

Solution: Let us first check that + and . defined by (1) are binary operations on End A.

For all a, b $\in$ A,

(f + g) (a + b) = f(a + b) f g(a + b)

= (f(a) + f(b)) + (g(a) + g(b))

= (f(a) + g(a)) + (f(b) + g(b))

= (f + g) (a) + (f + g) (b), and

(f. g) (a + b) = f(g(a + b))

= f(g(a) + g(b))

= f(g(a)) + f(g(b))

= (f . g)(a) + (f . g) (b)

Thus, f + g and f . g ∈ End A.

Now let us see if (End A, +, .) satisfies Rl-R6.

Since + in the abelian group A is associative and commutative, so is + in End A. The zero homomorphism on A is the zero element in End A. (– f) is the additive inverse of f E End A. Thus, (End A, +) is an abelian group.

You also know that the composition of functions is an associative operation in End A.

Finally, to check R6 we look at f . (g + h) for any f, g, h ∈ End A. Now for any a ∈ **A,**

[f . (g + h)l (a) = f((g + h) (8))

= f(g(a) + h(a))

= f(g(a)) + f(h(a))

= (f . g) (a) + (f . h) (a)

= (f . g + f . h) (a)

∴ f.(g + h) = f . g + f . h.

We can similarly prove that (f + g) . h = f . h + g . h.

Thus, R1-R6 are true for End **A.**

Hence, (End A, +, .) is a ring.

Note It is not commutative since fog need not be equal to gof for f, g ∈ End A.

Now, let us look at the Cartesian product of rings.

Example: Let (A, +,.) and (B, ⊞, ⊡) be two rings. Show that their Cartesian product A X B is a ring with respect to ⊕ and * defined by

(a, b) ⊕ (a′, b′) = (a + a′, b ⊞ b′), and

(a, b) * (a′, b′) = (a . a′, b ⊡ b′)

for a11 (a, b), (a′, b′) in A X B.

Solution: We have defined the addition and multiplication in A X B componentwise. The zero element of A X B is (0, 0). The additive inverse of (a, b) is (–a, ⊟ b), where ⊟ b denotes the inverse of b with respect to ⊟.

Since the multiplications in A and B are associative, * is associative in A × B. Again, using the fact that R6 holds for A and B, we can show that R6 holds for A × B. Thus, (A × B, 0, *) is a ring.

14.2 Elementary Properties

In this section we will prove some simple but important properties of rings which are immediate consequences of the definition of a ring. As we go along you must not forget that for any ring R, (R, +) is an abelian group. Hence, the results obtained for groups in the earlier units are applicable to the abelian group (R, +). In particular,

(i) the zero element, 0, and the additive inverse of any element is unique.

(ii) the cancellation law holds for addition; i.e., $\forall$ a, b, c $\in$ R , a + c = b + c $\Rightarrow$ a = b.

As we have mentioned earlier, we will write a – b for a + (–b) and ab for a. b, where a, b $\in$ R.

So let us state some properties which follow from the axiom R6, mainly.

Theorem 1: Let R be a ring. Then, for any a, b, c $\in$ R,

(i) a0 = 0 = 0a,

(ii) a(–b) = (–a)b = –(ab),

(iii) (– a) (– b) = ab,

(iv) a(b – c) = ab – ac, and

Proof:

(i) Now, 0 + 0 = 0

$\Rightarrow$ a(0 + 0) = a0

$\Rightarrow$ a0 + a0 = a0, applying the distributive law.

= a0 + 0, since 0 is the additive identity.

$\Rightarrow$ a0 = 0, by the cancellation law for (R, +).

Using the other distributive law, we can similarly show that 0a = 0.

Thus, a0 = 0 = 0a for all a $\in$ R.

(ii) From the definition of additive inverse, we know that b + (– b) = 0.

Now, 0 = a0, from (i) above.

= a(b + (– b)), as 0 = b + (– b).

= ab + a(– b), by distributivity.

Now, ab + [– (ab)] = 0 and ab + a(– b) = 0. But you know that the additive inverse of an element is unique.

Hence, we get – (ab) = a(– b).

In the same manner, using the fact that a + (–a) = 0, we get – (ab) = (– a)b.

Thus, a(– b) = (– a)b = – (ab) for all a, b $\in$ R.

(iii) For a, b $\in$ R,

(– a) (– b) = – (a(– b)), from (ii) above.

= a(– (– b)), from (ii) above.

= ab, since b is the additive inverse of (– b).

(iv) For a, b, c $\in$ R,

$$a(b - c) = a(b + (-c))$$
$$= ab + a(-c), \text{ by distributivity.}$$
$$= ab + (-(ac)), \text{ from (ii) above.}$$
$$= ab - ac.$$

If k is an integer ($k \geq 2$) such that the sum of k elements in a ring R is defined, we define the sum of (k + 1) elements $a_1, a_2 ..., a_{k+1}$ in R, taken in that order, as $a_1 + .., + a_{k+1} = (a_k + ... + a_k) + a_{k+1}$.

In the same way if k is a positive integer such that the product of k elements in R is defined, we define the product of (k + 1) elements $a_1, a_2, ..., a_{k+1}$ (taken in that order) as

$a_1.a_{12} ... a_{k+1} = (a_1.a_2 .... .a_k) . a_{k+1}$.

As we did for groups, we can obtain laws of indices in the case of rings also with respect to both + and ., in fact, we have the following results for any ring R.

(i) If m and n are positive integers and a $\in$ R, then

$a^m . a^n = a^{m+n}$, and

$(a^m)'' = a^{mn}$.

(ii) If m and n are arbitrary integers and a, b $\in$ R, then

(n + m)a = na + ma,

(nm)a = n(ma) = m(na),

n(a + b) = na + nb,

m(ab) = (ma)b = a(mb), and

(ma) (nb) = mn (ab) = (mna)b.

(iii) If $a_1 + a_2, ..., a_r, b_1, ..., b_n, \in$ R then

$(a_1, + ... + a_m) (b_1 + ... + b_n)$

$= a_1 b_1 + ... + a_1b_n + a_2a_1 + ... + a_2b_n + ... + a_mb_1 + ... + a_mb_n$.

There are several other properties of rings that we will be discussing throughout this block. For now let us look closely at two types of rings, which are classified according to the behaviour of the multiplication defined on them.

14.3 Two Types of Rings

The definition of a ring guarantees that the binary operation multiplication is associative and, along with +, satisfies the distributive laws. Nothing more is said about the properties of multiplication. If we place restrictions on this operation we get several types of rings. Let us introduce you to two of them now.

Definition: We say that a ring (R, +, .) is commutative if . is commutative, i.e., if ab = ba for all a, b $\in$ R.

For example, Z, Q and R are commutative rings.

Definition: We say that a ring (R, +, .) is a ring with identity (or with unity) if R has an identity element with respect to multiplication, i.e., if there exists an element e in R such that

ae = ea = a for all a $\in$ R.

Can you think of such a ring? Aren't Z, Q and R examples of a ring with identity?

Definition: We say that a ring (R, +, .) is a commutative ring with unity, if it is a commutative ring and has the multiplicative identity element 1.

Thus, the rings Z, Q, Rand C are all commutative rings with unity. The integer 1 is the multiplicative identity in all these rings.

We can also find commutative rings which are not rings with identity. For example, 2Z, the ring of all even integers is commutative. But it has no multiplicative identity.

Similarly, we can find rings with identity which are not commutative. For example, $M_2(R)$ has the unit element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

But it is not commutative. For instance,

if $A = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \text{and}$$

$$BA = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 4 & 0 \end{bmatrix} \text{and}$$

Thus, $AB \neq BA$.

Now, can the trivial ring be a ring with identity? Since 0 . 0 = 0, 0 is also the multiplicative identity for this ring. So ((0), +, .) is a ring with identity in which the additive and identities coincide. But, if R is not the trivial ring we have the following result.

Theorem 2: Let R be a ring with identity 1. If $R \neq \{ 0 \}$ then the elements 0 and 1 are distinct.

Proof: Since $R \neq \{ 0 \}$, $\exists\, a \in R, a \neq 0$. Now suppose 0 = 1. Then a = a . 1 = a . 0 = 0 (by Theorem 1). That is, a = 0, a contradiction. Thus, our supposition is wrong. That is, $0 \neq 1$.

Now let us go back when will A × B be commutative? A × B is commutative if and only if both the rings A and B are commutative. Let us see why. For convenience we will denote the operations in all three rings A, B and A × B by + and . . Let (a, h) and $(a', b') \in A \times B$.

Then (a, b) . (a', b') = (a', b') . (a, b)

$\Rightarrow$ (a.a ', b . b') = (a'. a, b' . b)

$\Rightarrow$ a.a' = a'.a and b . b'= b'. b .

Thus, A × B is commutative iff both A and B are commutative rings.

We can similarly show that A × B is with unity iff A and B are with unity. If A and B have identities e_1 and e_2 respectively, then the identity of A × B is (e_1, e_2).

Now we will give an important example of a non-commutative ring with identity. This is the ring of real quaternions. It was first described by the Irish mathematician William Rowan Hamilton (1805-1865). It plays an important role in geometry, number theory and the study of mechanics.

Notes

Example: Let H = (a + bi + cj + dk | a, b, c, d ∈ R), where i, j, k are symbols that satisfy $i^2 = -1 = j^2 = k^2$, ij = k = – ji, jk = i = – kj ki = j = – ik.

We define addition and multiplication in H by

$(a + bi + cj + dk) + (a_i + b_1 i + c_i j + d_1 k)$

$= (a + a_1)\ (b + b_1)_i + (c - c_1)_j\ t\ (d + d_1)k$, and

$(a + bi + cj + dk)\ (a_1 + b_1 i + cj + d_1 k) = (aa_1 - bb_1 - cc_1 - dd_1) + (ab_1 + ha_1 + cd_1 - dc_1)_i + (ac_1 - bd_1 + ca_1 + db_1)j - (ad_1 + bc_1 - cb_1 + da_1)k$

(This multiplication may seem complicated. But it is not so. It is simply performed as for polynomials, keeping the relationships between i, j and k in mind.)

Show that H is a ring.

Solution: Note that (± 1, ± i, ± j, ± k] is the group QH.

Now, you can verify that (H, +) is an abelian group in which the additive identity is 0 = 0 + 0i + 0j + 0k, multiplication in H is associative, the distributive laws hold and

I = 1 + 0i + 0j + 0k is the unity in H.

Do you agree that H is not a commutative ring? You will if You remember that ij ≠ ji, for example.

So far, in this unit we have discussed various types of rings. We have seen examples of commutative and non-commutative rings. Though non-commutative rings are very important for the sake of simplicity we shall only deal with commutative rings henceforth. Thus, from now on, for us **a ring will always mean a commutative ring.** We would like you to remember that both + and . are commutative in a commutative ring.

Now, let us summarise what we have done in this unit.

Self Assessment

1. For each a in R. There exists X in R such that a + X = :0 = ... i.e. every elements of R has an additive inverse.

   (a) a . x (b) x + a

   (c) $x^{-1} + a$ (d) $a^{-1} + x$

2. If a and b are integers, we say that a is congruent to b modulo n : f .... is divisible by n.

   (a) a + b (b) a – b

   (c) a . b (d) a/b

3. A × B is with unity if A and B are with unity. If A and B have identies e_1 and e_2 respectively, then the identity of A × B is ....

   (a) $e_1 + e_2$ (b) $e_2 + e_1^{-1}$

   (c) (e, e_2) (d) (e_1^{-1}, e_2^{-1})

4. The .... for addition and multiplication and the generalised distributive law.

   (a) law of indices (b) Ring

   (c) Subring (d) ideal

5. If m and n are arbitrary integers and a, b ∈ R then (n + m) a = na + ma and n(a + b) =

   (a) na + nb　　(b) $a^n + b^n$

   (c) nab + nba　　(d) $an + bn^{-1}$

14.4 Summary

In this unit we discussed the following points.

- Definition and examples of a ring.
- Some properties of a ring like

  a . 0 = 0 = 0 . a,

  a(– b) = – (ab) = (– a) b,

  (– a) (– b) = ab,

  a(b – c) = ab – ac,

  (b – c)a = ba – ca

  ∀ a, b, c in a ring R.
- The laws of indices for addition and multiplication, and the generalised distributive law.
- Commutative rings, rings with unity and commutative rings with unity.

Henceforth, we will always assume that a ring means a commutative ring, unless otherwise mentioned.

14.5 Keywords

Ring: A non-empty set R together with two binary operations, usually called addition (denoted by f) and multiplication (denoted by .), is called a **ring** if the following axioms are satisfied.

Commutative Rings: We say that a ring (R, +, .) is commutative if . is commutative, i.e., if ab = ba for all a, b ∈ R. For example, Z, Q and R are commutative rings.

14.6 Review Questions

1. Write out the Cayley tables for addition and multiplication in Z_6^*, the set of non-zero elements of Z_6. Is $(Z_6^*,+,'.)$ a ring? Why?

2. Show that the set $Q+\sqrt{2}Q=\{p+\sqrt{2}q \mid p,q\in Q\}$ is a ring with respect to addition and multiplication of real numbers.

3. Let R = $\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \text{a,b are real numbers}\right\}$. Show that R is a ring under matrix addition and multiplication.

4. Let R = $\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| \text{a,b are real numbers}\right\}$. Prove that R is a ring under matrix addition and multiplication.

Notes

5. Why is $(\wp(X), \cup, \cap)$ not a ring?

6. Show that { 0 } is a ring with respect to the usual addition and multiplication. (This is called the trivial ring.)

7. Prove that the only ring R in which the two operations are equal (i.e., $a + b = ab \ \forall \ a, b \in R$) is the trivial ring.

8. Show that the set of matrices $\left\{\begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle| \, x \in R \right\}$ is a commutative ring with unity.

9. Let R be a Boolean ring (i.e., $a^2 = a \ \forall \ a \in R$). Show that $a = -a \ \forall \ a \in R$. Hence show that R must be commutative.

Answers: Self Assessment

1. (b) 2. (a) 3. (c) 4. (a) 5. (a)

14.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 15: Subrings

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss examples of subrings and ideals of some familiar rings
- Explain whether a subset of a ring is a subring or not
- Describe whether a subset of a ring is an ideal or not
- Define and give examples of quotient rings

Introduction

In this unit, we will study various concepts in ring theory corresponding to some of those that we have discussed in group theory. We will start with the notion of a subring, which corresponds to that of a subgroup, as you may have guessed already.

Then we will take a close look at a special kind of subring, called an ideal. You will see that the ideals in a ring play the role of normal subgroups in a group. That is, they help us to define a notion in ring theory corresponding to that of a quotient group, namely, a quotient ring.

After defining quotient rings, we will look at several examples of such rings. But you will only be able to realise the importance of quotient rings in the future units.

We hope that you will be able to meet the following objectives of this unit, because only then you will be comfortable in the future units of this course.

15.1 Subrings

In last unit we introduced you to the concept of subgroups of a group. In this unit we will introduce you to an analogous notion for rings. Remember that for us a ring means a commutative ring.

In the previous unit you saw that, not only is Z $\subseteq$ Q, but Z and Q are rings with respect to the same operations. This shows that Z is n subring of Q, as you will now realise.

Definition: Let (R, +, .) be a ring and S be a subset of R. We say that S is a **subring** of R, if (S, +, .) is itself a ring, i.e., S is a ring with respect to the operations on R.

For example, we can say that 2Z, the set of even integers, is a subring of Z.

Before giving more examples, let us analyse the definition of a subring. The definition says that a subring of a ring R is a ring with respect to the operations on R. Now, the distributive, commutative and associative laws hold good in R. Therefore, they hold good in any subset of R also. So, to prove that a subset S of R is a ring we don't need to check all the 6 axioms R1-R6 for S. It is enough to check that

(i) S is closed under both + and . ,

(ii) $0 \in S$, and

(iii) for each a S, $-a \in S$.

If S satisfies these three conditions, then S is a subring of R. So we have an alternative definition for a subring.

Definition: Let S be a subset of a ring (R, +, .). S is called a subring of R if

(i) S is closed under + and . , i.e., a + b, a. b $\in$ S whenever a, b $\in$ S,

(ii) $0 \in S$, and

(iii) for each $a \in S$, $-a \in S$.

Even this definition can be improved upon. For this, recall from Unit 3 that $(S, +) \le (R, +)$ if $a - b \in S$ whenever $a, b \in S$. This observation allows us to give a set of conditions for a subset to be a subring, which are easy to verify.

Theorem 1: Let S be a non-empty subset of (R, +, .). Then S is a subring of R if and only if

(a) $x - y \in S\ \forall\ x, y \in S$; and

(b) $xy \in S\ \forall\ x, y \in S$.

Proof: We need to show that S is a subring of R according to our definition iff S satisfies (a) and (b). Now, S is a subring of R iff $(S, f) \le (R, f)$ and S is closed under multiplication, i.e., iff (a) and (b) hold.

So, we have proved the theorem.

This theorem allows us a neat way of showing that a subset is a subring.

Let us look at some examples.

We have already noted that Z is a subring of Q. In fact, you can use Theorem 1 to check that Z is subring of R, C and Z + iZ too. You can also verify that Q is a subring of R, C and $Q + \sqrt{2}Q = \{a + \sqrt{2}\beta \mid \alpha, \beta \in Q\}$.

Example: Consider Z_6, the ring of integers modulo 6. Show, that $3Z_6 = (3.\bar{0}, 3.\bar{1}, \ldots\ldots, 3.5)$ is a subring of Z_6.

Solution: Firstly, do you agree that $3Z_6 = (\bar{0}, \bar{3})$? Remember that 6 = 0, 9 = 3, and so on. Also,

$\bar{0} - 5 = -3 = 5$. Thus, $x - y \in 3Z_6\ \forall\ x, y \in 3Z_6$. You can also verify that $xy \in 3Z_6\ \forall\ x, y \in 3Z_6$. Thus, by Theorem 1, $3Z_6$ is a subring of Z_6.

Example: Consider the ring $\wp$ (X). Show that S = { ϕ, X) is a subring of $\wp$ (X).

Solution: Note that $A\ A\ A = \phi\ \forall\ A \in \wp(X)$. $\therefore A = -A$ in $\wp$ (X).

Now, to apply Theorem 1 we first note that S is non-empty.

Next, $\phi \Delta \phi = \phi \in S$, $X \Delta X = \phi \in S$,

$\phi \Delta X = X \in S$, $\phi \cap \phi = \phi \in S$, $X \cap X = X \in S$, $\phi \cap X = \phi \in S$.

Thus, by Theorem 1, S is a subring of $\wp$ (X).

For each proper subset of X we get a subring of $\wp$(X). Thus, a ring can have, several subrings. Let us consider two subrings of the ring Z^2.

Example: Show that S = ((n, 0) } | n $\in$ Z } is a subring of Z × Z. Also show that

D = ((n,n) | n $\in$ Z } is a subring of Z × Z.

Solution: You can recall the ring structure of Z^2. Both S and D are non-empty. Both of them satisfy (a) and (b) of Theorem 1. Thus, S and D are both subrings of Z^2.

We would like to make a remark here which is based on the examples of subrings that you have seen so far.

Remark: (i) If R is a ring with identity, a subring of R may or may not be with identity. For example, the ring Z has identity 1, but its subring nZ ($n \geq 2$) is without identity.

(ii) The identity of a subring, if it exists, may not coincide with the identity of the ring. For example, the identity of the ring Z × Z is (1, 1). But the identity of its subring Z × {0} is (1, 0).

Example: Let R be a ring and $a \in R$. Show that the set aR = (ax | $x \in R$ } is a subring of R.

Solution: Since $R \neq \phi$, $aR \neq \phi$. Now, for any two elements ax and ay of aR,

$ax - ay = a(x - y) \in aR$ and $(ax)(ay) = a(xay) \in aR$.

Thus, by Theorem 1, aR is a subring of R.

Using Example we can immediately say that $\overline{m}Z_n$ is a subring of Z_n $\forall$ $\overline{m}$ E Z. This also shows us a fact that we have already seen : nZ is a subring of Z $\forall$ $n \in Z$.

Now let us look at some properties of subrings. From Unit 3 you know that the intersection of two or more subgroups is a subgroup. The following result says that the same is true for subrings.

Theorem 2: Let S_1 and S_2 be subrings of a ring R. Then $S_1 \cap S_2$ is also a subring of R.

Proof: Since 0 E S_1 and 0 E S_2, 0 E $S_1 \cap S_2$. $\therefore S_1 \cap S_2 \neq \phi$.

Now, let $x, y \in S_1 \cap S_2$. Then x, y E S_1 and $x, y \in S_2$. Thus, by Theorem 1, x – y and xy are in S_1 as well as in S_2, i.e,, they lie in $S_1 \cap S_2$.

Thus, $S_1 \cap S_2$ is a subring of R.

On the same lines as the proof above we can prove that the intersection of any family of subrings of a ring R is a subring of R.

Now let us look at the Cartesian product of subrings.

Theorem 3: Let S_1 and S_2 be subrings of the rings R_1 and R_2, respectively. Then $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

Proof: Since S_1 and S_2 are subrings of R_1 and R_2, $S_1 \neq \phi$ and $S_2 \neq \phi$. $S_1 \times S_2 \neq \phi$.

Now, let (a, b) and (a′, b′) $\in S_1 \times S_2$. Then a, a′ E S_1 and b, b′ E S_2. As S_1 and S_2 are subrings, a – a′, a. a′ $\in S_1$ and b – b′, b b′ $\in S_2$.

(We are using + and . for both R_1 and R_2 here, for convenience.) Hence,

(a, b) – (a′, b′) = (a – a′, b – b′) $\in S_1 \times$ Sz, and

(a, b) . (a′, b′) = (aa′, bb′) $\in S_1 \times S_2$.

Thus, by Theorem 1, $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

Self Assessment

1. Let S be a subset of a ring (R, +,.). S is called .... of R of O $\in$ S

   (a) ring (b) subring

   (c) polynomial ring (d) ideals

2. S be a .... subset of (R, +,.). Then S is a subring of R. If and only if x – y $\in$ SY X, y $\in$ S,

   (a) empty (b) non-empty

   (c) null set (d) real set

3. Let R be a ring and a $\in$ R then the set aR = (ax | x $\in$ R) is a .... of R.

   (a) subring (b) ring

   (c) ideal (d) polynomial

15.2 Summary

- Let (R, +, .) be a ring and S be a subset of R. We say that S is a **subring** of R, if (S, +, .) is itself a ring, i.e., S is a ring with respect to the operations on R.

  For example, we can say that 2Z, the set of even integers, is a subring of Z.

  Before giving more examples, let us analyse the definition of a subring. The definition says that a subring of a ring R is a ring with respect to the operations on R. Now, the distributive, commutative and associative laws hold good in R. Therefore, they hold good in any subset of R also. So, to prove that a subset S of R is a ring we don't need to check all the 6 axioms R1-R6 for S. It is enough to check that

  (i) S is closed under both + and . ,

  (ii) 0 $\in$ S, and

  (iii) for each a S, – a $\in$ S.

  If S satisfies these three conditions, then S is a subring of R. So we have an alternative definition for a subring.

- Let S be a subset of a ring (R, +, .). S is called a subring of R if

  (i) S is closed under + and . , i.e., a + b, a. b E S whenever a, b E S,

Notes

(ii) 0 E S, and

(iii) for each a E S, - a E S.

- Even this definition can be improved upon. For this, recall from Unit 3 that (S, f) ≤ (R, +) ifa – b E S whenever a, b E S. This observation allows us to give a set of conditions for a subset to be a subring, which are easy to verify.

15.3 Keyword

Subring: Let (R, +, .) be a ring and S be a subset of R. We say that S is a **subring** of R, if (S, +, .) is itself a ring, i.e., S is a ring with respect to the operations on R.

15.4 Review Questions

1. Show that S = $\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in Z\right\}$. is a subring of R = $\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in R\right\}$. Does S have a unit element?

   If yes, then is the unit element the same as that of R?

2. For any ring R, show that {0} and R are its subrings.

3. Show that if A is subring of B and B is a subring of C, then A is a subring of C.

4. Give an example of a subset of Z which is not a subring.

5. Show that $\{a, \bar{3}\}$ and $\{\bar{0}, \bar{2}, \bar{4}\}$ are proper ideal of Z_6.

Answers: Self Assessment

1. (b) 2. (b) 3. (a)

15.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Notes

Unit 16: Ideals

Objectives

After studying this unit, you will be able to:

- Discuss ideals of some familiar rings
- Explain whether a subset of a ring is an ideal or not
- Define and give examples of quotient rings

Introduction

In earlier unit, you have studied normal subgroups and the role that they play in group theory. You saw that the most important reason for the existence of normal subgroups is that they allow us to define quotient groups. In ring theory, we would like to define a similar concept, a quotient ring. In this unit, we will discuss a class of subrings. These subrings are called ideals. While exploring algebraic number theory, the 19th century mathematicians Dedekind, Kronecker and others developed this concept. Let us see how we can use it to define a quotient ring.

Consider a ring (R, + , .) and a subring I of R. As (R, +) is an abelian group, the subgroup, I is normal in (R, +), and hence the set $R/I = (a + 1 \mid a \in R \}$, of all cosets of I in R, is group under the binary operation + given by

$$(a + I) + (b + I) = (a + b) + I \qquad \text{..... (1)}$$

for all $a + I, b + I \in R/I$. We wish to define. on R/I so as to make R/I a ring. You may think that the most natural way to do so is to define

$$(a + I) . (b + I) = a\,b + I \ \forall\ a + 1, b + I \in R \qquad \text{..... (2)}$$

But, is this well defined? Not always. For instance, consider the subring Z of R and the set of cosets of Z in R. Now, since $1 = 1 - 0 \in Z$, $1 + Z = 0 + Z$.

Therefore, we must have

$(\sqrt{2} + Z) . (1 + Z) = (\sqrt{2} + Z) . (0 + Z)$, i.e,, $\sqrt{2} + Z = O + Z$, i.e., $\sqrt{2} \in Z$.

But this is a contradiction. Thus, our definition of multiplication is not valid for the set R/Z.

But, it is valid for R/I if we add some conditions on I: What should these conditions be? To answer this, assume that the multiplication in (2) is well defined.

Then, $(r + I). (0 + I) = r . 0 + I = 0 + I = I$ for all $r \in R$.

Now, you know that if $x \in I$, then $x + I = 0 + I = I$.

As we have assumed that is well defined, we get

$(r + I) (x + I) = (r + I) . (0 + I) = 0 + I$ whenever $r \in R, x \in I$.

i.e., $rx + I = I$ whenever $r \in R, x \in I$

Thus, $rx \in I$, whenever $r \in R, x \in I$.

So, if ' . ' is well defined we see that the subring I must satisfy the additional condition that $rx \in I$ whenever $r \in R$ and $x \in I$.

We will prove that this extra condition on I is enough to make the operation a well defined one and (R/I, +, .) a ring. In this unit we will consider the subrings I of R on which we impose the condition $rx \in I$ whenever $r \in R$ and $x \in I$.

Definition: We call a non-empty subset I of a ring (R, +, .) an ideal of R if

(i) $a - b \in I$ for all $a, b \in I$, and

(ii) $ra \in I$ for all $r \in R$ and $a \in I$.

Over here we would like to remark that we are always assuming that our rings are commutative. In the case of non-commutative rings the definition of an ideal is partially modified as follows.

A non-empty subset I of a non-commutative ring R is an ideal if

(i) $a - b \in I \ \forall a, b \in I$, and

(ii) $ra \in I$ and $ar \in I \ \forall \ a \in I, r \in R$.

Now let us go back to commutative rings. From the definition we see that a subring I of a ring R is an ideal of R iff $ra \in I \ \forall r \in R$ a and $a \in I$.

Let us consider some examples. You saw that for any ring R, the set (0) is a subring. In fact, it is an ideal of R called the **trivial ideal** of **R.** Other ideals, if they exist, are known as **non-trivial ideals** of R.

You can also verify that every ring is an ideal of itself. If an ideal I of a ring R is such that $I \neq R$, then I is called a **proper ideal** of **R.**

For example, if $n \neq 0,1$, then the subring $nZ = \{ nm \mid m \in Z)$ is a proper non-trivial ideal of Z. This is because for any $z \in Z$ and $nm \in nZ$, $z(nm) = n(zm) \in nZ$.

Example: Let X be an infinite set. Consider I, the class of all finite subsets of X. Show that I is an ideal of $\wp$ (X).

Solution: $I = \{ A \mid A$ is a finite subset of $X \}$. Note that

(i) $\phi \in I$, i.e., the zero element of $\wp$ (X) is in I,

(ii) $A - B = A + (-B) = A + B$, as $B = -B$ in $\wp (X) = A \Delta B$.

Thus, if $A, B \in I$, then A - B is again a finite subset of X, and hence $A - B \wp I$.

(iii) $AB = A \cap B$. Now, whenever A is a finite subset of X and B is any element of $\wp$ (X), $A \cap B$ is a finite subset of X. Thus, $A \in I$ and $B \in P (X) \Rightarrow AB \in I$.

Hence, I is an ideal of $\wp$ (X).

Example: Let X be a set and Y be a non-empty subset of X. Show that

$I = \{ A \in \wp (x) \mid A \cap Y = \phi \}$ is an ideal of $\wp$ (X).

In particular, if we take $Y = \{x_0\}$; where X_0 is a fixed element of X, then

$I = \{ A \in \wp (X) \mid x_0 \notin A \}$ is an ideal of $\wp$ (X).

Solution: Firstly, $\phi \in 1$,

Secondly, $\forall$ A, B E I,

$(A - B) \cap Y = (A \Delta B) \cap Y = (A \cap Y) \Delta (B \cap Y) = \phi \Delta \phi = \phi$, so that $A - B \in I$.

Finally, for $A \in I$ and B E $\wp$(X),

$(AB) \cap Y = (A \cap B) \cap Y = (A \cap Y) \cap B = \phi \cap B = \phi$, So that $AB \in I$

Thus, I is an ideal of $\wp$ (X).

Example: Consider the ring C[0, 1]

Let $M = (f \in C[0, 1] \mid f(1/2) = 0)$. Show that M is an ideal of C[0, 1].

Solution: The zero element 0 is defined by $0(x) = 0$ for all $x \in [0, 1]$. Since $0(1/2) = 0$, O E M.

Also, if $f, g \in M$, , then $(f - g) (l /2) = f (1/2) - g (1/2) = 0 - 0 = 0$.

So, $f - g \in M$.

Next, iff $\in$ M and $g \in C [0, 1]$ then $(fg) (1/2) = f(1/2) g (1/2) = 0 g(1/2) = 0$, so $f_g \in M$.

Thus, M is an ideal of C[0, 1].

When you study Unit 17, you will see that M is the kernel of the homomorphism

$\phi : C[0, 1] \rightarrow R : \phi (f) = f(1/2)$.

Example: For any ring R and $a_1, a_2 \in R$, show that $Ra_1 + Ra_2 = \{ x_1a_1 + x_2a_2 \mid x_1, x_2 \in R)$ is an ideal of R.

Solution: Firstly, $0 = 0a_1 \text{ t } 0a_2$. $\quad \therefore 0 \in Ra_1 + Ra_2$.

Next, $(x_1a_1 + x_2a_2) - (y_1a_1 + y_2a_2)$

$= (x_1 - y_1)a_1 + (x_2 - y_2)a_2 \in Ra_1 + Ra_2 \forall\ x_1, x_2, y_1, y_2 \in R$.

Finally, for $r \in R$ and $x_1a_1 + x_2a_2 \in Ra_1 + Ra_2$,

$r(x_1a_1 \in x_2a_2) = rx_1a_1 + rx_2a_2 \in Ra_1 + Ra_2$.

Thus, $Ra_1 + Ra_2$ is an ideal of R.

This method of obtaining ideals can be extended to give ideals of the form $\{ x_1a_1 + x_2a_2 + ... + x_na_n \mid x_i \in R \}$ for fixed elements $a_1..,...$, a, of R. Such ideals crop up again and again in ring theory. We give them a special name.

Definition: Let a_1, ..., a, be given elements of a ring R. Then the ideal generated by a_1, ..., a,, is

$Ra_1 + Ra_2 + ... + Ra_n = (x_1a_1 + x_2a_2 + ... + x_na_n \mid$ x, E R). a_1, ..., a,, are called the generators of this ideal.

We also denote this ideal by < a_1, a_2, ..., an >

When n = 1, the ideal we get is called a principal ideal. Thus, if a ∈ R, then Ra = < a > is a principal ideal of R. In the next unit you will be using principal ideals quite a lot.

Tasks

1. Let R be a ring with identity. Show that < 1 > = R.
2. Find the principal ideals of Z_{10} generated by $\overline{3}$ and $\overline{5}$.

Definition: An element a of a ring R is called nilpotent if there exists a positive integer n such that a″ = 0.

For example, $\overline{3}$ and $\overline{6}$ are nilpotent elements of Z_9, since $\overline{3}^2 = \overline{9} = \overline{0}$ and $\overline{6}^2 = \overline{36} = \overline{0}$. Also, in any ring R, 0 is a nilpotent element.

Now consider the following example.

Example: Let R be a ring. Show that the set of nilpotent elements of R is an ideal of R.

This ideal is called the nil radical of R.

Solution: Let N = { a ∈ R | a^n = 0 for some positive integer n }. Then 0 EN.

Also, if a, b ∈ N, then a^n = 0 and b^m = 0 for some positive integers m and n.

Now, $(a-b)^{m+n} = \sum_{r=0}^{m+n} {}^{m+n}C_r a^r (-b)^{m+n-r}$

For each r = 0, 1, ..., m + n, either r ≥ n or m + n – r ≥ m, and hence, either a^r = 0 or b^{m+n-r} = 0. Thus, the term a^r b^{m+n-r} = 0. S0 (a – b)$^{m+n}$ = 0.

Thus, a – b ∈ N whenever a, b ∈ N.

Finally, if a ∈ N, a″ = 0 for some positive integer n, and hence, for any

r ∈ R, $(ar)^n = a^n r^n = 0$, i.e., ar ∈ N.

So, N is an ideal of R.

Let us see what the nil radicals of some familiar rings are. For the rings Z, Q, R or C, N = {0}, since the power of any non-zero element of these rings is non-zero.

For Z_4, N = $\{\overline{0}, \overline{2}\}$.

Theorem 1: Let R be a ring with identity 1. If I is an ideal of R and I E I, then I = R.

Proof: We know that I ⊆ R. We want to prove that R ⊆ I. Let r E R. Since 1 E I and I is an ideal of R, r = r . 1 ∈ I. So, R ⊆ I. Hence I = R.

Using this result we can immediately say that Z is not an ideal of Q. Does this also tell us whether Q is an ideal of R or not’? Certainly Since 1 ∈ Q and Q ≠ R, Q can’t be an ideal of R.

Now let us shift our attention to the algebra of ideals. In the previous section we proved that the intersection of subrings is a subring. We will now show that the intersection of ideals is an ideal. We will also show that the sum of ideals is an ideal and a suitably defined product of ideals is an ideal.

Notes

Theorem 2: If I and J are ideals of a ring R, then

(a) $I \cap J$,

(b) $I + J = \{ a + b \mid a \in I \text{ and } b \in J \}$, and

(c) $IJ = \{ x \in R \mid x$ is a finite sum $a_1b_1 + ... + a_mb_m$, where ai 1 and bi $\in J \}$ are ideals of R.

Proof: (a) From Theorem 2 you know that $I \cap J$ is a subring of R. Now, if $a \in 1 \cap J$, then $a \in I$ and $a \in J$. Therefore, $ax \in I$ and $a \in J$ for all x in R. So $ax \in I \cap J$ for all $a \in I \cap J$ and $x \in R$. Thus, $I \cap J$ is an ideal of R.

(b) Firstly, $0 = 0 + 0 \in 1 + J$ $\therefore I + J = f$.

Secondly, if $x, y \in 1 + J$, then $x = a_1 + b_1$ and $y = a_2 + b_2$ for some $a_1, a_2, \in I$ and $b_1, b_2 \in J$.

So $x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2)\ (b_1 - b_2) \in I + J$.

Finally, let $x \in I + J$ and $r \in R$. Then $x = a + b$ for some $a \in I$ and $b \in J$. Now

$xr = (a + b)r = ar + br \in I + J$, as $a \in I$ implies $ar \in I$ and $b \in J$ implies $br \in J$ for all $r \in R$.

Thus, I + J is an ideal of R.

(c) Firstly, $IJ \neq \phi$, since $I \neq \phi$ and $J \neq \phi$.

Next, let $x, y \in IJ$. Then $x = a_1b_1 + ... + a_mb_m$ and

$y = a'_1b'_1 + ... + a'_nb'_n$ for some $a_1, ..., a, a'_1, .. ., a', \in I$ and $b_1, .., b_m, b'_1, ..., , b'_n \in J$.

$\therefore x - y = (a_1b_1 + ... + a_mb_m) - (a'_1b'_1 + ... + a'_nb'_n)$

$= a_1b_1 + ... + a_mb_m + (-a'_1)b'_1 + ... + (-a'_n)b'_n$

which is a finite sum of elements of the form ab with $a \in I$ and $b \in J$.

So, $x - y \in IJ$.

Finally, let $x \in IJ$ say $\mathbf{x} = a_1b_1 + ... + a_nb_n$ with $a, \in 1$ and b, E J. Then, for any r E R

$xr = (a_1b_1 + ... + a_nb_n)r = a_1(b_1r)\ ... + a_n(b_nr)$,

which is a finite sum of elements of the form ab with $a \in 1$ and $b \in J$.

(Note that $b_i \in J \Rightarrow b_ir \in J$ for all r in R.)

Thus, IJ is an ideal of R.

Over here, we would like to remark that if we define IJ = { ab | a E I, b ∈ J }, then IJ need not even be a subring, leave alone being an ideal. This is because if x, y E IJ, then with this definition of IJ it is not necessary that $x - y \in IJ$.

Let us now look at the relationship between the ideals obtained. Let us first look at the following particular situation:

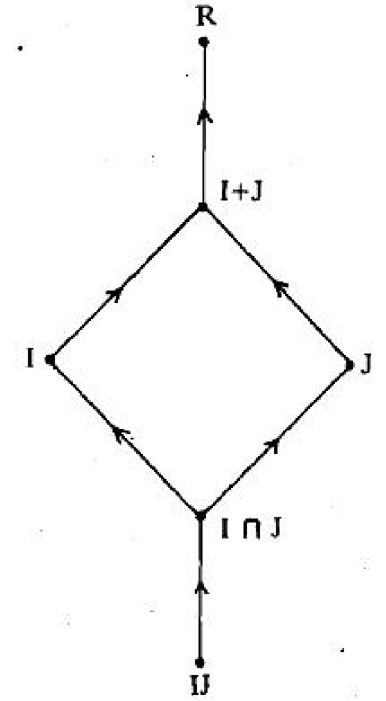
R = Z, I = 22 and J = 10Z. Then $I \cap J = J$, since $J \subseteq I$. Also, any element of I + J is ot the form x = 2n + 10m, where $n, m \in 2$. Thus, $x = 2(n + 5m) \in 2Z$. On the other hand, $2Z = f \subseteq I + J$. Thus , I + J = < 2 , 1 0 > = < 2 >.

Similarly, you can see that IJ = < 20 >.

Note that $IJ \subseteq I \cap J \subseteq I \subseteq I + J$.

In fact, these inclusions are true for any I and J. We show the relationship in figure 16.1.

Figure 16.1: The Ideal Hierarchy



16.1 Quotient Rings

You have studied quotient groups. You know that given a normal subgroup N of a group *G*, the set of all cosets of N is a group and is called the quotient group associated with the normal subgroup N. Using ideals, we will now define a similar concept for rings. At the beginning we said that if (R, +, .) is a ring and I is a subring of R such that

(R/I, +, .) is a ring, where + and . are defined by

$(X + I) + (y + I) = (\mathbf{x} + y) + I$ and

$(x + I) \cdot (y + I) = xy + I \ \forall \ x + I, y + I \in R/I,$

then the subring I should satisfy the extra condition that $rx \in I$ whenever $r \in R$ and $x \in I$, i.e., I should be an ideal. We now show that if I satisfies this extra condition then the operations that we have defined on R/I are well defined.

From group theory we know that (R/I, +) is an abelian group. So we only need to check that is well defined, i.e., if

$a + I = a' + I, b + I = b' + I$, then $ab + I = a'b' + I$.

Now, since $a + I = a' + I$, $a - a' \in I$.

Let $a - a' = x$. Similarly, $b - b' \in 1$, say $b - b' = y$.

Then $ab = (a' + x)(b' + y) = a'b' + (xb' + a'y + xy)$.

$\therefore$ $ab - a'b' \in I$, since $x \in I$. $y \in I$ and I is an ideal of R.

$\therefore$ $ab + I = a'b' + I$.

Notes

Thus, is well defined on R/I.

Now our aim is to prove the following result.

Theorem 3: Let R be a ring and I be an ideal in R. Then R/I is a ring with respect to addition and multiplication defined by

$(X + I) + (y + I) = (x + y) + I$, and

$(x + I) . (y + I) = x y + I \ \forall \ x,y \in R.$

Proof: As we have noted earlier, (R/I, +) is an abelian group. So, to prove that R/I is a ring we only need to check that . is commutative, associative and distributive over +.

Now,

(i) . is commutative : (a + I). (b + I) = ab + I = ba + I = (b + I), (a 4- I) for all a + I,b + I ∈ R/I.

(ii) . is associative : ' ∀ ' a, b, c ∈ R

$$\begin{aligned}((a + I). (b + I)). (c + I) &= (ab + I). (C + I)\\ &= (ab)c + I\\ &= a(bc) + I\\ &= (a + I) . ((b + I) . (c + I))\end{aligned}$$

(iii) Distributive law : Let a + I, b + I, c + I ∈ RA. Then

$$\begin{aligned}(a + I). ((b + I) + (c + 1)) &= (a + I) [(b + \boldsymbol{6)} + I]\\ &= a(b + c) + I\\ &= (ab + ac) + I\\ &= (ab + I) + (ac + I).\\ &= (a + I). (b + I) + (a + I).(c \mathbf{-1} I)\end{aligned}$$

Thus, R/I is a ring.

This ring is called the **quotient ring of R by the ideal** I.

Let us look at some examples. We start with the example that 'gave rise to the terminology 'R mod I'.

Example: Let R = Z and I = nZ. What is R/I?

Solution: You have seen that nZ is, an ideal of Z. From Unit 2 you know that

Z/nZ = { nZ., I + nZ, ..., (n – 1) + nZ }.

$= \{\bar{0},\bar{1},....,\overline{n-1}\}$, the same as the set of equivalence classes modulo n.

So, R/I is the ring Z_n.

Now let us look at an ideal of Z_n, where n = 8.

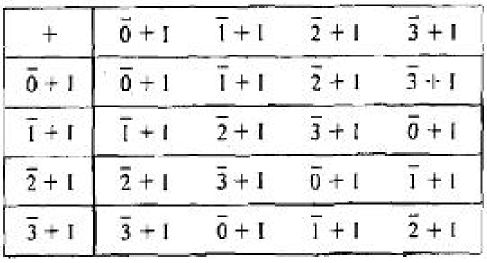
Example: Let R = Z_8. Show that I = $\{\bar{0},\bar{4}\}$ is an ideal of R. Construct the Cayley tables for + and, in R/I.

Solution: I = $\bar{4}$ R, and hence is an ideal of R. From group theory you know that the number 8 of elements in R/I = o(R/I) = $\frac{o(R)}{o(I)} = \frac{8}{2} = 4.$

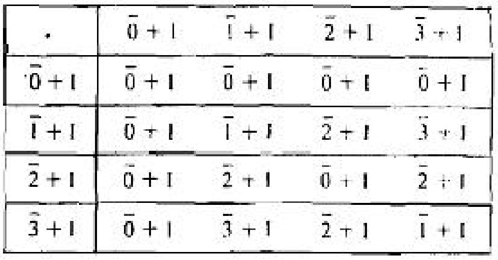
You can see that these elements are

$0 + 1 = \{\bar{0}, \bar{4}\}, 1 + 1 = \{\bar{1}, \bar{5}\}$, $2 + 1 = \{\bar{2}, \bar{6}\}, 3 + I = (\bar{3}, \bar{7}\}$.

The Cayley tables for + and . in R/I are



+	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{0}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{1}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$
$\bar{2}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$
$\bar{3}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$



.	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$
$\bar{1}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$
$\bar{3}+I$	$\bar{0}+I$	$\bar{3}+I$	$\bar{2}+I$	$\bar{1}+I$

Self Assessment

1. A non-empty subset I of a ring (R+,.) an .... of R of a – b ∈ I for all a, b ∈ I.

   (a) ring (b) subring

   (c) polynomial (d) ideal

2. If n ≠ 0, 1. Then the subring nZ = {nm | m ∈ Z} is a proper .... ideal of Z.

   (a) non-trivial (b) trivial

   (c) direct (d) indirect

3. X be a set and Y be a non-empty subset of X. Then I = {A ∈ δ(x) | A .... y = ϕ} is an ideal of δ(x).

   (a) ∩ (b) ⊃

   (c) ∪ (d) ⊂

4. If I and J are ideals of a ring R, then I .... J are ideals ring R.

   (a) ⊃ (b) ⊂

   (c) ∩ (d) ∪

5. A normal subgroup N of a group G, the set of all cosets of N is a group and is called .... associated with the normal subgroup N.

   (a) quotient group (b) ring

   (c) subring (d) ideal

16.2 Summary

- We call a non-empty subset I of a ring (R, +, .) an ideal of R if

  (i) a – b ∈ I for all a, b ∈ I, and

  (ii) ra ∈ I for all r ∈ R and a ∈ I.

Over here we would like to remark that we are always assuming that our rings are commutative. In the case of non-commutative rings the definition of an ideal is partially modified as follows.

A non-empty subset I of a non-commutative ring R is an ideal if

(i) $a - b \in I \; \forall \; a, b \in I$, and

(ii) $ra \in I$ and $ar \in I \; \forall \; a \in I, r \in R$.

- Now let us go back to commutative rings. From the definition we see that a subring I of a ring R is an ideal of R iff $ra \in I \; \forall \; r \in R$ a and $a \in I$.
- You can also verify that every ring is an ideal of itself. If an ideal I of a ring R is such that $I \neq R$, then I is called a **proper ideal** of **R.**
- For example, if $n \neq 0,1$, then the subring $nZ = \{ nm \mid m \in Z)$ is a proper non-trivial ideal of Z. This is because for any $z \in Z$ and $nrn \in nZ$, $z(nm) = n(zm) \in nZ$.
- An element a of a ring R is called nilpotent if there exists a positive integer n such that $a'' = 0$.
- For example, $\bar{3}$ and $\bar{6}$ are nilpotent elements of Z_9, since $\bar{3}^2 = \bar{9} = \bar{0}$ and $\bar{6}^2 = \overline{36} = \bar{0}$. Also, in any ring R, 0 is a nilpotent element.

16.3 Keywords

Proper Ideal: We call a non-empty subset I of a ring (R, +, .) an ideal of R if

(i) $a - b \in I$ for all $a, b \in I$, and

every ring is an ideal of itself. If an ideal I of a ring R is such that $I \neq R$, then I is called a **proper ideal** of **R.**

Nilpotent: An element a of a ring R is called **nilpotent** if there exists a positive integer n such that $a'' = 0$.

Quotient Group: A normal subgroup N of a group G, the set of all cosets of N is a group and is called the **quotient group** associated with the normal subgroup N.

This ring is called the **quotient ring of R by the ideal** I.

16.4 Review Questions

1. Let S be a subring of a ring R. Can we always define a ring homomorphism whose domain is R and kernel is S? Why?
2. Prove Theorem 8.
3. In the situation of Theorem 8 prove that

   (a) if g o f is 1 – 1, then so is f.

   (b) if g o f is onto, then so is g.
4. Use Theorem 8 to show that the function $h : Z \times Z \rightarrow Z_2$ defined by $h((n, m)) = \bar{m}$ is a homomorphism.
5. Which of the following functions are ring isomorphisms?

   (a) $f : Z \rightarrow : f(n) = n$

(b) $f : Z \to 5Z : f(n) = 5n$

(c) $f : C \to C : f(z) = \bar{z}$, the complex conjugate of z.

6. Show that the composition of isomorphisms is an isomorphism.

Answers: Self Assessment

1. (d) 2. (a) 3. (a) 4. (c) 5. (a)

16.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 17: Ring Homomorphisms

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss whether a function is a ring homomorphism or not
- Explain the kernel arid image of any homomorphism
- Explain examples of ring homomorphisms and isomorphisms
- Prove and use some properties of a ring homomorphism; state, prove and apply the Fundamental Theorem of Homomorphisms for rings

Introduction

You have studied about the functions between groups that preserve the binary operation. You also saw how useful they were for studying the structure of a group. In this unit, we will discuss functions between rings which preserve the two binary operations. Such functions are called ring homomorphisms. You will see how homomorphisms allow us to investigate the algebraic nature of a ring.

If a homomorphism is a bijection, it is called an isomorphism. The role of isomorphisms in ring theory, as in group theory, is to identify algebraically identical systems. That is why they are important. We will discuss them also.

Finally, we will show you the interrelationship between ring homomorphism, ideals and quotient rings.

17.1 Homomorphisms

Analogous to the notion of a group homomorphism, we have the concept of a ring homomorphism. Recall that a group homomorphism preserves the group operation of its domain. So it is natural to expect a ring homomorphism to preserve the ring structure of its domain. Consider the following definition.

Notes

Definition: Let (R_1, +, .) and (R_1,+ . .) be two rings and f : R_1 – R_2 be a map. We say that f is a ring homomorphisms if

f(a + b) = f(a) 4 – f(b), and

f(a . b) = f(a) . f(b) for all a, b in R_1.

Note that the + and . occurring on the left hand sides of the equations in the definition above are defined on R_1, while the + and . occurring on the right hand sides are defined on R_2.

So, we can say that f : R_1 – R_2 is a homomorphism if

(i) the image of a sum is the sum of the images, and

(ii) the image of a product is the product of the images.

Thus, the ring homomorphism f is also a group homomorphisms from (R_1,+) into (R_2, +).

Just as we did in Unit 6, before giving some examples of homomorphisms let us define the kernel and image of a homomorphism. As is to be expected, these definitions are analogous to the corresponding ones in Unit 6.

Definition: Let R_1 and R_2 be two rings and f : R_1 – R_2 be a ring homomorphism. Then we define

(i) the image of f to be the set lm f = {f(x) | x $\in$ R_1},

(ii) the kernel off to be the set Ker f = {x $\in$ R_1 | f(x) = 0).

Note that lm f $\subseteq$ R_2 and Ker f $\subseteq$ R_1,

If Im f = R_2, f is called an epimorphism or an onto homomorphism, and then R_2 is called the homomorphic image of R_1.

Now let us look at some examples.

Example: Let R be a ring. Show that the identity map I_K is a ring homomorphism. What are Ker I_R and Im I_R?

Solution: Let x, y $\in$ R. Then

$I_R(x + y) = x + y = I_R(x) + I_R(y)$, and

$I_R(xy) = xy = I_R\{(X) I_R(y)$.

Thus, $I_R(xy) = xy = I_R(x) \cdot I_R(y)$.

Thus, IR is a ring homomorphism.

Ker I_R = { x $\in$ R | $I_R(x)$ = 0 }

=.{x $\in$ R | x = 0)

= {0}

I_m I_R = {($I_R(x)$ [x $\in$ R]}

={x | x $\in$ R]

= R.

Thus, I_R, is a surjection, and hence an epimorphism.

Example: Let s $\in$ N. Show that the map f : Z – Z, given by f(m) = $\overline{m}$ for all m $\in$ Z is a homomorphism. Obtain Ker f and Im f also.

Solution: For any m, n $\in$ Z,

$f(m + n) = \overline{m\,t\,n} = \overline{m} + \overline{n} = f(m) + f(n)$, and

$f(mn) = \overline{mn} = \overline{m} + \overline{n} = f(m)\,f(n)$.

Therefore, f is a ring homomorphism.

Now, Kerf = $(m \in Z \mid f(m) = \overline{0} \mid$

$= \{m \in Z \mid m = 01$

$= (m \in Z \mid m \in 0 \text{ (mod s)})$

= sz.

Im f = $(f(m) \mid m \in Z)$

$= (\overline{m} \mid m \in Z)$

$= Z_s$,

showing that f is an epimorphism.

Example: Consider the map $f : Z_6 - Z_3 : f(n \text{ (mod 6)}) = n\text{(mod 3)}$. Show that f is a ring homomorphism. What is Ker f?

Solution: Firstly, for any n, m $\in$ Z,

$f(n(\text{mod } 6) + m(\text{mod } 6)) = f((n + m) \text{ (mod 6)}) = (n + m) \text{ (mod 3)}$

$= n \text{ (mod 3)} + m(\text{mod } 3)$

$= f(n \text{ (mod 6)}) + f(m(\text{mod } 6))$

You can similarly show that

$f(n(\text{mod } 6) \,.\, m(\text{mod } 6)) = f(n(\text{mod } 6)) \,.\, f(m(\text{mod } 6))$.

Thus, f is a ring homomorphism.

Ker f = $\{n(\text{mod}.6) \mid n \equiv 0(\text{mod } 3)) = \{n(\text{mod } 6) \mid n \in 3Z)$

$= \{\overline{0}, \overline{3}\}$, bar denoting 'mod 6'.

Before discussing any more examples, we would like to make a remark about terminology. In future we will use the term 'homomorphism' for 'ring homomorphism'. You may remember that we also did this in the case of group homomorphisms.

Now let us look at some more examples.

Example: Consider the ring C[0, 1] of all real valued continuous functions defined on the closed interval [0, 1].

Define $\phi : C[0, 1] + R : \phi\,(f) = f(1/2)$. Show that ϕ is a homomorphism.

Solution: Let f and g $\in$ C [0, 1]

Then $(f + g)\,(x) = f(x)\,f\,g(x)$ and

$(fg)\,(x) = f(x)\,g(x)$ for all $x \in C[0, 1]$.

Notes

Now, $\phi(f + g) = (f + g)(1/2) = f(1/2) + g(1/2) = \phi(f) + \phi(g)$, and

$f(fg) = (fg)(1/2) = f\left(\frac{1}{2}\right)g\left(\frac{1}{2}\right) = \phi(f)\phi(g)$.

Thus, ϕ is a homomorphism.

Example: Consider the ring $R = \left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in R\right\}$ under matrix addition and multiplication.

Show that the map $I : Z \to 13 : f(n) = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$ is a homomorphism.

Solution: Note that $f(n) = nI$, where I is the identity matrix of order 2. Now you can check that $f(n + m) = f(n) + f(m)$ and $f(nm) = f(n) f(m)$ $\forall$ n, m $\in$ Z. Thus, f is a homomorphism.

Example: Consider the ring $\wp$ (X) of Unit 14.

Let Y be a non-empty subset of X .

Define $f : \wp(X) \to \wp(Y)$ by $f(A)\ I= A \cap Y$ for all A in $\wp(X)$. Show that f is a homomorphism. Does $Y' \in$ Ker f ? What is Im f ?

Solution: For any A and B in $\wp$ (X),

$$\begin{aligned} f(A \Delta B) &= f((A\backslash B) \cup (B\backslash A)) \\ &= ((A\backslash B) \cup (B\backslash A \cap Y)) \\ &= ((A\backslash B) \cap Y) \cup ((B\backslash A) \cap Y) \\ &= ((A \cap Y)\backslash(B \cap Y)) \cup ((B \cap Y)\backslash(A \cap Y)) \\ &= (f(A)\backslash f(B) \cup (f(B)\backslash f(A)) \\ &= f(A)\ A\ f(B), \text{ and} \end{aligned}$$

$$\begin{aligned} f(A \cap B) &= (A \cap B) \cap Y \\ &= (A \cap B) \cap (Y \cap Y) \\ &= (A \cap Y) \cap (B \cap Y), \text{ since } \cap \text{ is associative and commutative.} \\ I &= f(A) \cap f(B). \end{aligned}$$

So, f is a ring homomorphism from $\wp$ (X) into $\wp$ (Y).

Now, the zero element of $\wp$ (Y) is ϕ. Therefore,

Ker f = $\{ A \in \wp(X) \mid A \cap Y = \phi)$. $\therefore Y^c \in$ Ker f.

We will show that f is surjective.

Now, Im f = $\{A \cap Y \mid A \in \wp(x)]$

Thus, Im f $\subseteq \wp$ (Y). To show that $\wp(Y) \subseteq$ Im f, take any $B \in \wp$ (Y).

Then $B \in \wp$ (X) and $f(B) - B \cap Y = B$. Thus, $B \in$ Im f.

Therefore, Im f = $\wp$ (Y).

Thus, f is an onto homomorphism.

Notes

Tasks

1. Let A and B be two rings. Show that the projection map P : A × B → A : p(x, y) = x is a homomorphism. What are Ker p and Im p?

2. Is $f : Z + \sqrt{2}Z \rightarrow Z + \sqrt{2}Z : f(a + \sqrt{2}b) = a - \sqrt{2}b$ a homomorphism?

3. Show that the map $\phi : C[0, 1] \rightarrow R \times R : \phi (f = (f(0), f(1))$ is a homomorphism.

Having discussed many examples, let us obtain some basic results about ring homomorphisms.

17.2 Properties of Homomorphisms

Let us start by listing some properties that show how a homomorphism preserves the structure of its domain. The following result is only a restatement of Theorem **1** of Unit **6.**

Theorem 1: Let $f : R_1 + R_2$ be a homomorphism from a ring R_1 into a ring R_2. Then

(a) $f(0) = 0$,

(b) $f(-x) = -f(x) \;\forall\; x \in R_1$, and

(c) $f(x - y) = f(x) - f(y) \;\forall\; x, y \in R_1$.

Proof: Since f is a group homomorphism from $(R_1, +)$ to $(R_2, +)$, we can apply Theorem 1 of Unit 6 to get the result.

Theorem 2: Let $f : R_1 - R_2$ be a ring homomorphism. Then

(a) if S is a subring of R_1, f(S) is a subring of R_2;

(b) if T is a subring of R_2, $f^{-1}(T)$ is a subring of R_1.

Proof: We will prove (b) and leave the proof of (a) to you. Let us use Theorem 1 of Unit 16.

Firstly, since $T \neq \phi$, $f^{-1}(T) \neq \phi$. Next, let $a, b \in f^{-1}(T)$. Then $f(a), f(b) \in T$

$\Rightarrow f(a) - f(b) \in T$ and $f(a) f(b) \in T$

$\Rightarrow f(a - b) \in T$ and $f(ab) \in T$

$\Rightarrow a - b \in f^{-1}(T)$ and $ab \in f^{-1}(T)$

$\Rightarrow f^{-1}(T)$ is a subring.

Now, it is natural to expect an analogue of Theorem 2 for ideals. But consider the inclusion i : Z – R : i(x) = x. You know that 22 is an ideal of Z. But is i(2Z) (i.e., 22) an ideal of R? No. For example, $2 \in 22$, $\frac{1}{4} \in R$, but $2.\frac{1}{4} = \frac{1}{2} \notin 2Z$. Thus, the homomorphic image of an ideal need not be an ideal. But, all is not lost. We have the following result.

Theorem 3: Let $f : R_1 - R_2$ be a ring homomorphism.

(a) Iff is surjective and I is an ideal of R_1, then f (I) is an ideal of R,.

(b) If I is an ideal of R_2, then $f^{-1}(1)$ is an ideal of R_1 and Ker $f \subseteq f^{-1}(J)$.

Proof: Here we will prove (a)

Firstly, since I is a subring of R_1, f(1) is a subring of R_2.

Secondly, take any $f(x) \in f(1)$ and $r \in R_2$. Since f is surjective, $\exists$ $s \in R_1$ such that $f(s) = r$.

Then

$rf(x) = f(s)\,f(x) = f(sx) \in f(I)$, since $sx \in I$.

Thus, f(1) is an ideal of R_2.

Now, consider an epimorphism $f : R \to S$ and an ideal I in R. By Theorem 3 you know that f(1) is an ideal of S and $f^{-1}(f(I))$ is an ideal of R. How are I and $f^{-1}(f(I))$ related? Clearly, $I \subseteq f^{-1}(f(1))$. Can $f^{-1}(f(T))$ contain elements of R\I? Remember that Ker $f \subseteq f^{-1}(f(1))$ also. Thus,

I + Ker $f \subseteq f^{-1}(f(1))$. In fact, I + Ker f = $f^{-1}(f(1))$. Let us see why.

Let $x \in f^{-1}(f(l))$. Then $f(x) \in f(1)$. Therefore, f(x) = f(y) for sdme $y \in I$. Then

$f(x - y) = 0$.

$\therefore$ $x - y \in$ Ker f, i.e., $x \in y$ + Ker $f \subseteq I$ + Ker f.

$\therefore$ $f^{-1}(f(I)) \subseteq I$ + Ker f.

Thus, $f^{-1}(f(I)) = I$ + Ker f.

This tells us that if Ker $f \subseteq I$, then

$f^{-1}(f(I)) = I$ (since Kerf $\subseteq I \Rightarrow I$ + Ker f = I).

Theorem 4: Let $f : R \to S$ be an onto ring homomorphism. Then

(a) if I is an ideal in R containing Ker f, $I = f^{-1}(f(I))$

(b) the mapping 1 – f(I) defines a one-to-one correspondence between the set of ideals of R containing Ker f and the set of ideals of S.

Proof: We have proved (a) in the discussion above. Let us prove (b) now.

Let A be the set of ideals of R containing Ker f, and B be the set of ideals of S.

Define $\phi : A \to B : 4(I) = f(I)$.

We want to show that ϕ is one-one and onto.

ϕ is onto : If $J \in B$ then $f^{-1}(J) \in A$ and Ker $f \subseteq f^{-1}(J)$ by Theorem 3.

Now $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$,

ϕ is one-one : If I_1 and I_2 are ideals in R containing Ker f, then

$$\begin{aligned}\phi(I_1) = \phi(I_2) &\Rightarrow f(I_1) = f(I_2)\\ &\Rightarrow f^{-1}(f(I_1)) = f^{-1}(f(I_2))\\ &\Rightarrow I_1 = I_2, \text{ by (a).}\end{aligned}$$

Thus, ϕ is bijective.

And now let us look closely at the sets Ker f and Im f, where f is a ring homomorphism. In Unit 6 we proved that iff : $G_1 - G_2$ is a group homomorphism then Ker f is a normal subgroup of G_1 and Im f is a subgroup of G_2. We have an analogous result for ring homomorphisms, which you may have already realised from the examples you have studied so far.

Theorem 5: Let f : $R_1 - R_2$ be a ring homomorphism. Then

(a) Ker f is an ideal of R_1.

(b) Im f is a subring of R_2.

Proof: (a) Since (0) is an ideal of R_2, by Theorem 3(b) we know that f-1({o}) is an ideal of R_1. But f^{-1}({o}) = Ker f.

Thus, we have shown that Ker f is an ideal of R_1.

(b) Since R_1 is a subring of R_1, $f(R_1)$ is a subring of R_2, by Theorem 2(a). Thus, Im f is a subring of R_2.

This result is very useful for showing that certain sets are ideals. For example, from Theorem 5 you can immediately say that $\{\bar{0},\bar{3}\}$ is an ideal of Z_6. As we go along you will see more examples of this use of Theorem 5.

Let us look a little more closely at the kernel of a homomorphism. In fact, let us prove a result analogous to Theorem 4 of Unit 6.

Theorem 6: Let f : R_1 – R_2 be a homomorphism. Then f is injective iff Ker f = {0}

Proof: f is injective iff f is an injective group homomorphism from (R_1, +) into (R_2, +). This is true iff Ker f = {0}, by Theorem 4 of Unit 6. So, our result is proved.

So far we have seen that given a ring homomorphism f : R — S, we can obtain an ideal of R, namely, Ker f. Now, given an ideal I of a ring R can we define a homomorphism f so that

Ker f = I?

The following theorem answers this question. Before going to the theorem recall the definition of quotient rings.

Theorem 7: If I is an ideal of a ring R, then there exists a ring homomorphism f : R → R/I whose kernel is I.

Proof: Let us define f : R → R/I by f(a) = a + I for all a ∈ R. Let us see iff is a homomorphism. For this take any a, b ∈ R. Then

f(a + b) = (a + b) + I = (a + I) + (b + I) = f(a) + f(b), and

f(ab) = ab + I = (a + I) (b + I) = f(a) f(b).

Thus, f is a homomorphism.

Further, Kerf = {a ∈ R | f(a) = 0 + I} = { a ∈ R | a + I = I }

= {a ∈ R | a ∈ I} = I .

Thus, the theorem is proved.

Also note that the homomorphism f is onto.

We call the homomorphism defined in the proof above the canonical (or natural) homomorphism from R onto R/I.

Now let us look at the behaviour of the composition of homomorphisms. We are sure you find the following result quite unsurprising.

Theorem 8: Let R_1, R_2 and R_3 be rings and f : R_1 — R_2, and g : $R_2 \to R_3$ be ring homomorphisms. Then their composition gof : $R_1 \to R_3$ given by (gof (x) = g(f(x)) for all x ∈ R_1 is a ring homomorphism.

The proof of this result is on the same lines as the proof of the corresponding result in Unit 6.

17.3 The Isomorphism Theorems

We discussed group isomorphisms and various results involving them. In this section we will do the same thing for rings. So, let us start by defining a ring isomorphism.

Definition: Let R_1 and R_2 be two rings. A function $f : R_1 \rightarrow R_2$ is called a ring isomorphism (or simply an isomorphism) if

(i) f is a ring homomorphism,

(ii) f is 1 – 1, and

(iii) f is onto.

Thus, a homomorphism that is bijective is an isomorphism.

An isomorphism of a ring R onto itself is called an automorphism of R.

Iff : $R_1 \rightarrow R_2$ is an isomorphism, we say that R_1 is isomorphic to R_2, and denote it by $R_1 \simeq R_2$.

Remark: Two rings are isomorphic if and only if they are algebraically identical. That is, isomorphic rings must have exactly the same algebraic properties. Thus, if R_1 is a ring with identity then it cannot be isomorphic to a ring without identity. Similarly, if the only ideals of R_1 are {0} and itself, then any ring isomorphic to R_1 must have this property too.

And now, let us go back to Unit 6 for a moment. Over there we proved the Fundamental Theorem of Homomorphism for groups, according to which the homomorphic image of a group G is isomorphic to a quotient group of G, Now we will prove a similar result for rings, namely, the first isomorphism theorem or the Fundamental Theorem of Homomorphism for rings.

Theorem 9 (The Fundamental Theorem of Homomorphism): Let $f : R \rightarrow S$ be a ring homomorphism. Then R/Ker f $\simeq$ Im f. In particular, iff is surjective, then R/Ker f $\simeq$ S.

Proof: Firstly, note that K/Ker f is a well defined quotient ring since Ker f is an ideal of R. For convenience, let us put Ker f = I. Let us define

ψ : R/I – S by ψ(x t I) = f(x).

As in the case of Theorem 8 of Unit 6, we need to check that ψ, is well defined, i.e., if

x + I = y + I then ψ(x + I) = ψ(y + I).

Now, x t I = y + I $\Rightarrow$ x – y $\in$ I = Ker f $\Rightarrow$ f(x – y) = 0 $\Rightarrow$ f(x) = f(y)

$\Rightarrow \psi(x + I) = \psi(y + I)$.

Thus, ψ is well defined.

Now let us see whether ψ, is an isomorphism or not.

(i) ψ, is a homomorphism : Let x, y $\in$ R. Then

$$\psi((x + I) + (y + I)) = \psi(x + y + I) = f(x + y) = f(x) + f(y)$$

$$= \psi(x + I) + \psi(y + I), \text{ and}$$

$$\psi((x + 1)\ (y + 1)) = \psi(xy + 1) = f(xy) = f(x)\ f(y)$$

$$= \psi(x + 1)\ \psi(y + 1)$$

Thus, ψ is a ring homomorphism.

(ii) Im ψ = Im f : Since ψ(x + I) = f(x) $\in$ Im f $\forall$ x $\in$ R, Im y $\subseteq$ Im f. Also, any element of Im f is of the form f(x) = ψ(x + I) for some x $\in$ R. Thus, Im f $\subseteq$ Im ψ. So, Im ψ = Im f.

Notes

(iii) ψ is 1 – 1. To show this let x, y $\in$ R such that

$\psi(x + I) = \psi(y + I)$. Then f(x) = f(y),

so that f(x – y) = 0, i.e., x – y $\in$ Ker f = I.

i.e., x + I = y + I.

Thus, ψ is I - I

So, we have shown that R/Ker f $\simeq$ 1m f.

Thus, iff is onto, then Im f = S and R/Ker f $\simeq$ S.

Note that this result says that f is the composition ψ o η, where η is the canonical homomorphism: R – R/I : $\eta(a)$ = a + I. This can be diagrammatically shown as

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\eta"'] & & S \\
& R/I \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

Let us look at some examples of the use of the Fundamental Theorem.

Consider p : Z – Z_m : p(n) = $\bar{n}$.p is an epimorphism and Ker p = {n | $\bar{n} = \bar{0}$ in Z,,,} = mZ.

Therefore, Z/mZ $\simeq$ Z,

(Note that we have often used the fact that Z/mZ and Z_m are the same.)

As another example, consider the projection map

p : $R_1 \times R_2 \to R_1$: p(a, b) = a, where R_1 and R_2 are rings. Then p is onto and its kernel is ((0, b) | b $\in$ R_2}, which is isomorphic to R_2.

Therefore, $(R_1 \times R_2)/R_2 \simeq R_1$.

Let us now apply Theorem 9 to prove that any ring homomorphism from a ring R onto Z is uniquely determined by its kernel. That is, we can't have two different ring homomorphisms from R onto Z with the same kernel. (Note that this is not true for group homomorphisms. In fact, you know that I_z and – I_z are distinct homomorphisms from Z onto itself with the same kernel, {0}. To prove this statement we need the following result.

Theorem 10: The only non-trivial ring homomorphism from Z into itself is I_z.

Proof: Let f : Z - Z be a non-trivial homomorphism. Let n be a positive integer.

Then n = 1 + 1 + ... + 1 (n times). Therefore, . ,

f(n) = f(1) + f(1) + ... -1 f(1) (n times) = n f(1).

On the other hand, if n is a negative integer, then –n is a positive integer. Therefore, f(–n) = (–n) f(l), i.e., –f(n) = – nf(1), since f is a homomorphism. Thus, f(n) = n f(1) in this case too.

Also f(0) = 0 = of(1).

Thus, $f(n) = nf(1) \ \forall \ n \in Z$ ..... (1)

Now, since f is a non-trivial homomorphism, f(m) # 0 for some $m \in Z$.

Then, f(m) = f(m . 1) = f(m) f(1).

Cancelling f(m) on both sides we get f(1) = 1.

Therefore, from (1) we see that

$f(n) = n \ \forall \ n \in Z$, i.e., $f = I_z$.

This theorem has an important corollary.

Corollary: Let R be a ring isomorphic. to Z. If f and g are two isomorphisms from R onto Z, then f = g.

Proof: The composition f.g-′ is an isomorphism from Z. onto itself. Therefore, by Theorem 10, fog^{-1} = Iz, i.e., f = g.

We are now in a position to prove the following result.

Theorem 11: Let R be a ring and f and g be homomorphisms from R onto Z such that Ker f = Ker g. Then f = g.

Proof: By Theorem 9 we have isomorphisms

ψ_r : R/Ker f $\rightarrow$ Z and ψ_g : R/Ker g $\rightarrow$ Z.

Since Ker f = Ker g, ψ_r and ψ_g are isomorphisms of the same ring onto Z. Thus, by the corollary above, $\psi_r = \psi_g$.

Also, the canonical maps ηr : R $\rightarrow$ R/Ker f and η_g : R $\rightarrow$ R/Ker g are the same since Ker f = Ker g.

$\therefore$ $f = \psi r \text{ o } \eta_f = \psi_g \text{ o } \eta_g = g$.

Let us halt our discussion of homomorphisms here and briefly recall what we have done in this unit. Of course, we have not finished with these functions. We will be going back to them again and again in the future units.

Self Assessment

1. If $R_1 + R_2$ be two rings and $f : R_1 \rightarrow R_2$ be a ring .... then we define imf = $\{f(x) \mid x \in R_1\}$.

   (a) isomorphisms (b) automorphism

   (c) homomorphism (d) polynomial

2. If im f = R_2, f is called an .... or onto homomorphism, then R_2 is called the homomorphic image of RZ.

   (a) epimorphism (b) hemomorphism

   (c) isomorphism (d) analogous

3. Two rings are isomorphic if and only if they are algebraically ....

   (a) designed (b) identical

   (c) onto (d) isomorphic

4. A homomorphism that is .... is an isomorphism

   (a) subjective (b) bijective

   (c) onto (d) injective

5. The only .... ring homomorphism from Z into itself is Z_2.

   (a) trivial (b) non-trivial

   (c) direct (d) indirect

17.4 Summary

1. The definition of a ring homomorphism, its kernel and its image, along with several examples.
2. The direct or inverse image of a subring under a homomorphism is a subring.
3. Iff : R - S is a ring homomorphism, then

   (i) Im f is a subring of S,

   (ii) Ker f is an ideal of R,

   (iii) $f^{-1}(1)$ is an ideal of R for every ideal I of S.

   (iv) iff is surjective, then f(I) is an ideal of S.
4. A homomorphism is injective iff its kernel is {0}.
5. The composition of homomorphisms is a homomorphism.
6. The definition and examples of a ring isomorphism.
7. The proof and applications of the Fundamental Theorem of Homomorphism which says that iff : $R \to S$ is a ring homomorphism, then $R/\text{Ker } f \simeq \text{Im } f$.

17.5 Keyword

Isomorphism: If a homomorphism is a bijection, it is called an isomorphism.

17.6 Review Questions

1. Which of the following rings are not fields?

   $2Z, Z_5, Z_6, Q \times Q$
2. Will a subring of a field be a field? Why?
3. Show that char $\wp(X) = 2$, where X is a non-empty set.
4. Let R be a ring and char R = m. What is char (R × R)?

Answers: Self Assessment

1. (c) 2. (a) 3. (b) 4. (b) 5. (b)

17.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 18: Integral Domains

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss whether an algebraic system is an integral domain or not
- Explain the characteristic of any ring
- Describe whether an algebraic system is a field or not

Introduction

In the earlier units, we have introduced you to rings, and then to special rings whose speciality lay in the properties of their multiplication. In this unit, we will introduce you to yet another type of ring, namely, an integral domain. You will see that an integral domain is a ring with identity in which the product of two non-zero elements is again a non-zero element. We will discuss various properties of such rings.

Next, we will look at rings like Q, R, C, and Z,, (where p is a prime number). In these rings, the non-zero elements form an abelian group under multiplication. Such rings are called fields. These structures are very useful, one reason being that we can "divide" in them.

Related to integral domains and fields are certain special ideals called prime ideals and maximal ideals. In this unit, we will also discuss them and their corresponding quotient rings.

18.1 Integral Domains

You know that the product of two non-zero integers is a non-zero integer, i.e., if m, n $\in$ Z such. that m $\neq$ 0, n $\neq$ 0, then mn $\neq$ 0. Now consider the ring Z_6. We find that $\overline{2} \neq \overline{0}$ and $\overline{3} \neq \overline{0}$, yet $\overline{2}\,.\,\overline{3} = \overline{0}$. So, we find that the product of the non-zero elements $\overline{2}$ and $\overline{3}$ in Z_6 is zero.

As you will soon realise, this shows that $\overline{2}$ (and 3) is a zero divisor, i.e., $\overline{0}$ is divisible by $\overline{2}$ (and $\overline{3}$).

So, let us see what a zero divisor is.

Definition: A non-zero element a in a ring R is called a zero divisor in R if there exists: a non-zero element b in R such that ab = 0.

Now do you agree that $\bar{2}$ is a zero divisor in Z,? What about $\bar{3}$ in Z_4? Since $\bar{3}\ x \neq \bar{0}$ for every non-zero x in Z_4, $\bar{3}$ is not a zero divisor in Z_4.

Now let us look at an example of a zero divisor in C[0, l]. Consider the function

f ∈ C[0, 1] given by

$$f(x) = \begin{cases} x - \dfrac{1}{2}, 0 \leq x \leq 1/2 \\ 0, 1/2 \leq x \leq 1 \end{cases}$$

Let us define g : [0, 1] + R by

$$g(x) = \begin{cases} 0, 0 \leq x \leq 1/2 \\ x - 1/2, 1/2 \leq x \leq 1 \end{cases}$$

Then g ∈ C[0, 1], g ≠ 0 and (fg) (x) = 0 ∀ x ∈ [0,1]. Thus, fg is the zero function. Hence, f is a zero divisor in C[0, 1].

For another example, consider the Cartesian product of two non-trivial rings A and B. For every a ≠ 0 in A, (a, 0) is a zero divisor in A × B. This is because, for any b ≠ 0 in B. (a . 0) (0.b) = (0.0).

Now let us look at the ring ℘(X), where X is a set with at least two elements, Each non-empty proper subset A of X is a zero divisor because $A.X^C = A \cap A^C = \phi$, the zero element of ℘(X).

Let us now talk of a type of ring that is without zero divisors.

Definition: We call a non-zero ring R an integral domain if

(i) R is with identity, and

(ii) R has no zero divisors.

Thus, an integral domain is a non-zero ring wilh identity in which the product of two non-zero elements is a non-zero element.

This kind of ring gets its name from the set of integers, one of its best known examples. Other examples of domains that immediately come to mind are Q, R and C. What about C[0,1]? You have already seen that it has zero divisors. Thus C[0,l] is not a domain.

> *Note* Several authors often shorten the term 'integral domain' to 'domain'. We will do so too.

The next result gives us an important class of examples of integral domains.

Theorem 1: Z_p is an integral domain iff p is a prime number.

Proof: Firstly, let let us assume that p is a prime number. Then you know that Zp is a non-zero ring with identity. Let us see if it has zero divisors. For this, suppose $\bar{a}, \bar{b} \in Z_p$ satisfy $\bar{a}, \bar{b} = 0$. Then $\overline{ab} = \bar{0}$, i.e., p | ab. Since p is a prime number, we see that p | a or p | b. Thus, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$.

Notes

What we have shown is that if $a \neq \overline{0}$ and $\overline{b} \neq 6$, then $\overline{a}\overline{b} = 6.$ Thus, Z_p is without zero divisors, and hence, is domain.

Conversely, we will show that if p is not a prime, then Z_p is not a domain, So, suppose p is not a prime. If p = 1, then Z , is the trivial ring, which is not a domain.

If p is composite number and m | p, you know that $\overline{m} \in Z_p$ is a zero divisor. Thus, Z_p has zero divisors. Hence, it is not a domain.

> *Task* Which of the following rings are not domains? Why?
>
> Z_4, Z_5, 2Z, Z + iZ, R × R, {0}.

Now consider a ring R. We know that the cancellation law for addition holds in R, i.e., whenever acb = acc in R, then b = c. But, does ab = ac imply b = c? It need not. For example, 0.1 = 0.2 in **Z** but 1 # 2. So, if a = 0, ab = ac need not imply b = c. But, if a # 0 and ab = ac, is it true that b = c′? We will prove that this is true for integral domains.

Theorem 2: A ring R has no zero divisors if and only if the cancellation law for multiplication holds in R (i.e., if a, b, c ∈ R such that a ≠ 0 and ab = ac, then b = c.)

Proof: Let us first assume that R contains no zero divisors. Assume that a, b, c ∈ R such that a ≠ 0 and ab = ac. Then a(b – c) = ab – ac = 0. As a ≠ 0, and R has no zero divisors, we get b – c = 0, i.e., b = c.

Thus if ab = ad and a ≠ 0, then b = c.

Conversely, assume that the cancellation law for multiplication holds in R. Let a ∈ R such that a ≠ 0. Suppose ab = 0 for some b ∈ R. Then ab = 0 = a0. Using the cancellation law for multiplication, we get b = 0. So, a is not a zero divisor, i.e., R has no zero divisors.

Using this theorem we can immediately say that the cancellation law holds for multiplication in an integral domain.

Now let us introduce a number associated with an integral domain in fact, with any ring. For this let us look at Z_4 first. We know that $4x = \overline{0} \ \forall\ x \in Z_4.$ In fact, $8x = \overline{0}$ and $12\,x = \overline{0}$ also for any $x \in Z_4$.

But 4 is the least element of the set $\{\, n \in N \mid nx = \overline{0} \ \ \forall\ \ x \in Z_4$). This shows that 4 is the characteristic of Z_4, as you will see now.

Definition: Let R be a ring. The least positive integer n such that nx = 0 ∀ x ∈ R is called the characteristic of R. If there is no positive integer n such that nx = 0 ∀ x ∈ R, then we say that the characteristic of R is zero.

We denote the characteristic of the ring R by char R.

You can see that char Z_n = n and char Z = 0.

Now let us look at a nice result for integral domains. It helps in considerably reducing our labour when we want to obtain the characteristic of a domain.

Theorem 3: Let m be a positive integer and R be an integral domain. Then the following conditions are equivalent.

(a) $m_1 = 0$.

(b) ma = 0 for all $a \in R$.

(c) ma = 0 for some $a \neq 0$ in R.

Proof: We will prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b) : We know that m 1 = 0.

Thus, for any $a \in R$, ma = m (la) = (ml) (a) = 0a = 0, i.e., (b) holds.

(b) $\Rightarrow$ (c) : If ma = 0 $\forall$ $a \in R$, then if is certainly true for some $a \neq 0$ in R.

(c) $\Rightarrow$ (a) : Let ma = 0 for some $a \neq 0$ in R. Then 0 = ma = m (la) = (ml) a. As $a \neq 0$ and R is without zero divisors, we get $m_1 = 0$.

What Theorem 3 tells us is that to find the characteristic of a domain we only need to look at the set in $\{n.1 \mid n \in N\}$.

Let us look at some examples.

(i) char Q = 0, since $n.1 \neq 0$ for any $n \in N$.

(ii) Similarly, char R = 0 and char C = 0.

(iii) You have already seen that chat Z, = n. Thus, for any positive integer n, there exists a ring with characteristic n.

Now let us look at a peculiarity of the characteristic of a domain.

Theorem 4: The characteristic of an integral domain is either zero or a prime number.?

Proof: Let R be a domain. We will prove that if the characteristic of K is not zero, then it is a prime number. So suppose char R = m, where $m \neq 0$. So m is the least positive integer such that m.1 = 0. We will show that m is a prime number by supposing that it is not, and then proving that our supposition is wrong.

So suppose m = st, where $s, t \in N$, $1 < s < m$ and $1 < t < m$. Then m.1 = 0 $\Rightarrow$ (st).l = 0 * (s.1) (t.1) = 0. As R is without zero divisors, we get s.1 = 0 or t.1 = 0. But, s and t are less than m. So, we reach a contradiction to the fact that m = char R. Therefore, our assumption that m = st, where $1 < s < m$, $1 < t < m$ is wrong. Thus, the only factors of m are 1 and itself. That is, m is a prime number.

We will now see what algebraic structure we get after we impose certain restrictions on the multiplication of a domain.

18.2 Field

Let (R, +, .) be a ring. We know that (R, +) is an abelian group. We also know that the operation is commutative and associative. But (R,.) is not an abelian group. Actually, even if R has identity, (R,.) will never be a group since there is no element $a \in R$ such that a.0 = 1. But can (R\{0}) be a group? It can, in some cases. For example, from Unit 2 you know that Q* and R* are groups with respect to multiplication. This allows us to say that Q and R are fields, a term we will now define.

Definition: A ring (R, +,.) is called a field if (R\{0},.) is an abelian group.

Thus, for a, system (R,+,.) to be a field it must satisfy the ring axioms R_1 to R_6 as well as the following axioms.

(i) is commutative,

(ii) R has identity (which we denote by 1) and $1 \neq 0$, and

(iii) every non-zero element x in R has a multiplicative inverse, which we denote by x^{-1}.

Just as a matter of information we would like to tell you that a ring that satisfies only (ii) and (iii) above, is called a division ring or a skew field or a non-commutative field. Such rings are very important in the study of algebra, but we will not be discussing them in this course.

Let us go back to fields now. The notion of a field evolved daring the 19th century through the research of the German mathematicians Richard Dedekind and Leopold Kronecker in algebraic number theory. Dedekind used the German word Körper, which means field, for this concept. This is why you will often find that a field is denoted by K.

As you may have realised, two of the best known examples of fields are R and C. These were the fields that Dedekind considered. Yet another example of a field is the following ring.

Example: Show that $Q + \sqrt{2}Q = \{a + \sqrt{2}b \mid a, b \in Q\}$ is field.

Solution: From Unit 14 you know that $F = Q + \sqrt{2}Q$ is a commutative ring with identity 1 + $\sqrt{2}$.

Now, let $a + \sqrt{2}b$ be a non-zero element of F. Then either a ≠ 0 or b ≠ 0. Now, using the rationalisation process, we see that

$$\left(a + \sqrt{2}b\right)^{-1} = \frac{1}{a + \sqrt{2}b} = \frac{1 - \sqrt{2}b}{(a + \sqrt{2}b)(a - \sqrt{2}b)} = \frac{a - fib}{a^2 - 2b^2}$$

$$= \frac{1}{a^2 - 2b^2} + \sqrt{2}\frac{(-b)}{a^2 - 2b^2} \in F$$

(Note that $a^2 - 2b^2 \neq 0$, since $\sqrt{2}$ is not rational and either a ≠ 0 or b ≠ 0.)

Thus, every non-zero element has a multiplicative inverse. Therefore, $Q + \sqrt{2}Q$ is a field.

Can you think of an example of a ring that is not a field? Does every non-zero integer have a multiplicative inverse in Z? No. Thus, Z is not a field.

By now you have seen several examples of fields. Have you observed that all of them happen to be integral domains also? This is not a coincidence. In fact, we have the following result.

Theorem 5: Every field is an integral domain.

Proof: Let F be a field. Then F ≠ {0} and 1 ∈ B. We need to see if F has zero divisors. So let a and b be elements of F such that ab = 0 and a ≠ 0. As a ≠ 0 and P is a field, a^{-1} exists.

Hence, b = I . b = (a – la) b = ad^{-1} (ab) = a^{-1} 0. Hence, if a ≠ 0 and ab = 0, we get b = 0, i.e., F has no zero divisors. Thus, F is a domain.

Theorem 5 may immediately prompt you to ask if every domain is a field. You have already seen that Z is a domain but not a field. But if we restrict ourselves to finite domains, we find that they are fields.

Theorem 6: Every finite integral domain is a field.

Proof: Let R = {a, = 0, a_1 = 1, a_2,....., a,] be a finite domain. Then R is commutative also. To show that R is a field we must show that every non-zero element of R has a multiplicative inverse.

So, let a = a_j be a non-zero element of R (i.e., i ≠ 0). Consider the elements aa_1, ..., aa_n. For every j ≠ 0, $a_j \neq 0$; and since a ≠ 0, we get $aa_j \neq 0$.

Hence, the set { aa_1, ..., aa_n } G (a,, ..., a,}.

Also, aa, , aa ,..., aa, are all distinct elements of the set {a,, ..., a,}, since $aa_j = na_k \Rightarrow a_j = a_j$, using the cancellation law for multiplication.

Thus, {aa_1, ..., aa_n} = [a; ,...., a_n}.

In particular, a, = aa_j, i.e., 1 = aa_j for some j. Thus, a is invertible in R. Hence every non-zero element of R has a multiplicative inverse. Thus, M is a field.

Using this result we can now prove a theorem which generates several examples of finite fields.

Theorem 7: Z_n is a field if and only if n is a prime number.

Proof: From theorem 1 you know that Z_n is a domain if and only if n is a prime number. You also know that Z_n has only n elements. Now we can apply Theorem 6 to obtain the result.

Theorem 7 unleashes a load of examples of fields : Z_2, Z_3, Z_5, Z_7,, and so on. Looking at these examples, and other examples of fields, can you say anything about the characteristic of a field? In fact, using Theorems 4 and 5 we can say that.

Theorem 8: The characteristic of a field is either zero or n prime number.

So far the examples of finite fields that you have seen have consisted of p elements, for some prime p. In the following exercise we give you an example of a finite field for which this is not so.

Theorem 9: Let R be a ring with identity. Then R is a field if and only if R and {0} are the only ideals of R.

Proof: Let us first assume that R is a field. Let I be an ideal of R. If I ≠ {0), there exists, a non-zero element x ∈ I. As x ≠ 0 and R is a field, xy = 1 for some y ∈ R. Since x ∈ I and I is an ideal, xy ∈ I, i.e., 1 ∈ I.

Conversely, assume that R and { 0 } are the only ideals of R. Now, let a ≠ 0 be an element of R. Then you know that the set Ra = [ra | r ∈ R] is a non-zero ideal of R. Therefore, Ra = R.

Now, 1 ∈ R = Ra. Therefore, 1 = ba for some b ∈ R, i.e., a^{-1} exists. Thus, every non-zero element of R has a multiplicative inverse. Therefore, R is a field.

Using Theorem 9, we can obtain some interesting facts about field homomorphisms (i.e., ring homomorphisms from one field to another). We give them to you in the form of an exercise.

Now that we have discussed domains and fields, let us look at certain ideals of a ring, with respect to which the quotient rings are domains or fields.

Self Assessment

1. Several authors often shorten the term .... to domain.

   (a) integral domain (b) abstract domain

   (c) different domain (d) prime domain

Notes

2. Zp is an integral domain if p is a .... number.

   (a) even (b) odd

   (c) prime (d) integer

3. A ring R has .... zero divisor if and only if the cancellation law for multiplication holds in R.

   (a) 1 (b) 2

   (c) 0 (d) 3

4. A ring (R, +,.) is called a .... if (R | { 0 }.) is an abelian group.

   (a) field (b) domain

   (c) range (d) ideal

5. Every .... integral domain is a field.

   (a) infinite (b) finite

   (c) direct (d) indirect

18.3 Summary

- The definition and examples of an integral domain.
- The definition and examples of a field.
- Every field is a domain.
- A finite domain is a field.
- The characteristic of any domain or field is either zero or a prime number.

18.4 Keywords

Zero Divisor: A non-zero element a in a ring R is called a zero divisor in R if there exists: a non-zero element b in R such that ab = 0.

Prime Number: Z_p is an integral domain iff p is a prime number.

Abelian Group: A ring (R, +,.) is called a field if (R\{0},.) is an abelian group.

18.5 Review Questions

1. Let n ∈ N and m | n | < m < n. Then show that $\overline{m}$ is a zero divisor in Z_n.
2. List all the zero divisors in Z.
3. For which rings with unity will 1 be a zero divisor?
4. Let R be a ring and a ∈ R be a zero divisor. Then show that every element of the principal ideal Ra is a zero divisor.
5. In a domain, show that the only solutions of the equation $x^2 = x$ are x = 0 and x = 1.
6. Prove that 0 is the only nilpotent element in a domain.

Answers: Self Assessment

Notes

1. (a) 2. (c) 3. (b) 4. (c) 5. (a)

18.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu