NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE AND TECHNOLOGY

COURSE CODE: MTH 312

COURSE TITLE: GROUPS AND RINGS

COURSE GUIDE

MTH 312
GROUPS AND RINGS

Course Adapted From	IGNOU
Course Adapter	Bankole Abiola National Open University of Nigeria Lagos.
Programme Leader	Prof. A. Adebanjo National Open University of Nigeria Lagos.
Course Coordinator	Bankole Abiola National Open University of Nigeria Lagos.

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

First Printed 2007

ISBN: 978-058-292-4

Printed By ……..
For
National Open University of Nigeria

TABLE OF CONTENT PAGES

Introduction

This course is a group and rings which we have introduced in MTH 211.

The course elaborated on a class of subgroups which have some characteristics to make us call them normal subgroups.

We also consider the concept of some algebraically indistinguishable systems. We say such systems are isomorphic. The word isomorphism was first used in 1870 by the mathematician Camille Jordan, to describe two groups that are not equal but have the same algebraic behaviour.

Isomorphisms are special cases of homomorphism, which are functions between groups that preserve the algebraic structure of their domains.

All concepts will also be learnt in module 2 of this course which is on Rings Theory.

Our exposition of ring theory will follow the path we used for group theory.

We shall define ring and sub-rings and give different types of rings and sub-rings.

We shall also deal with ring homomorphism and isomorphisms.

What you will learn in this course

This course consists of two modules. Module 1 is divided into fours units and Module 2 is divided into three units.

During this course you will learn about sub-groups and normal sub-groups, quotient groups, Isomorphism, rings subrings and Ideals, and Ring Homomorphism.

This course is a core course in pure mathematics and as such it is recommended as part of the course a career in mathematics.

Course Aims

This course aims as giving understanding of core concepts in algebra. This could be achieved through the following measures:

- Inducing you to normal subgroups
- Explaining concepts of isomorphism and homomorphism in groups

- Introducing you to rings, sub-ring and ideals, and developing another groups and rings using normal subgroups and ideals

Course Objective

At the end of this course you should be able to define the following concepts successfully

- Normal subgroups,
- Group isomorphism and homomorphism,
- Quotient groups
- Ring and Sub-rings
- Ideals
- Solve problems on the above concepts currently.

Working Through This Course

For you to successfully complete this course you are required t master all the contents in MTH 211, and then proceed on this one.

You will also do a lot of exercises. However the materials are well written and self contained as possible.

Course Materials

Study units

There are seven study units divided into two modules

Module 1

Unit 1 Normal – Subgroup
Unit 2 Group Homomorphism
Unit 3 Permutation groups
Unit 4 Finite groups

Module 2

Unit 1 Rings
Unit 2 Subrings and Ideals
Unit 3 Ring Homomorphisms

Self Assessment Exercise

Self Assessment Exercises are given as you proceed on the units, you should solve the exercises as they serve to introduce you to a new concept or emphasis the ones you have learnt, already.

Tutor Marked Assignment

These assignments are to be submitted at the end of each unit as they will form part of your final grade in the course.

Final Assessment

At the end of the course you will be assessed to determine how well you have master the course. The tutor marked assignment will form 30% of the total grade whole examination will be 70%.

Course Code	MTH 312
Course Title	Groups and Rings
Course Adapted From	IGNOU
Course Adapter	Bankole Abiola National Open University of Nigeria Lagos.
Programme Leader	Prof. A. Adebanjo National Open University of Nigeria Lagos.
Course Coordinator	Bankole Abiola National Open University of Nigeria Lagos.

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

First Printed 2007

ISBN: 978-058-292-4

Printed by .....

For
National Open University of Nigeria

TABLE OF CONTENTS PAGE

MODULE 1

UNIT 1 NORMAL SUBGROUPS

CONTENTS

1.0 INTRODUCTION

In MTH 211, you studied subgroups and cosets. We start this unit by discussing a special class of subgroups, called normal subgroups. You will see that the sets of such a subgroup form a group with respect to a suitably defined operation. These groups are called quotient groups we will discuss them in some detail in sec. 3.2.

Once you are comfortable with normal subgroups and quotient groups, you will find it easier to understand the concepts and results that are presented in the next unit. So make sure that you have met the following objectives before going to the next unit.

2.0 OBJECTIVES

After reading this unit, you should be able to

- Verity whether a subgroup is normal or not,
- Obtain a quotient group corresponding to a given normal subgroup.

3.0 MAIN CONTENT

3.1 Normal Subgroups

When we treated Lagrange's theorem in MTH 211 you saw that a left coset of a subgroup H, aH, need not be same as the right coset Ha. But, there are certain subgroups for which the right and left cosets represented by the same element coincide. This type of subgroup is very important in group theory, and we give it a special name.

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 $N \underline{\Delta} G$.

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 another example.

Example 1: Show that every subgroup of Z is normal in Z.

Solution: from Example 4 of unit 3, of MTH 211, you know that if H is a subgroup of Z, then $H = mZ$, for some $m \in Z$. Now, for any $z \in Z$,

$H + z = \{\ldots, -3m + z, -2m + z, -m + z, z, m + z, 2m + z, \ldots\}$
$= \{\ldots, -3m, z - 2m, z - m, z, z, +m, z + 2m \ldots\}$ (since + is commutative)
$= z + H.$
$\therefore H \underline{\Delta} Z.$

Example 1 is a special case of the fact that every subgroup of a commutative group is a normal subgroup. We will prove this fact later (in Theorem 2).

Try the following exercise now.

SELF ASSISMENT EXERCISE 1

Show that $A_3 \underline{\Delta} S_3$ (see Example 3 of unit 4in MTH 211).

Let us now prove a result that gives equivalent conditions for subgroups to be normal

Theorem 1: Let H be a subgroup of a group G: The following statement 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) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a). This will show that the three statements are equivalent.

(a) $\Rightarrow$ (b) : Since (a) is true, $Hg = gH \ \forall g \in G$. We want to prove (b). for this, consider $g^{-1}Hg$ for $g \in G$. Let $g^{-1}Hg$.

Since $hg \in Hg = gH, \exists h_1 \in H$ such that $hg = gh_1$.
$\therefore g^{-1}hg = g^{-1}gh_1 = h_1 \in H$.
$\therefore$ (b) holds.

(b) $\Rightarrow$(c): Now, we know that (b) holds, i.e., for $g \in G$, g-1Hg $\subseteq$H. We want to show that $H \subseteq g^{-1}Hg$. Let h$\in$H. Then.
H = chc = $(g^{-1}g)$ h $(g^{-1}g)$
$= g^{-1}(ghg^{-1})g$
$= g^{-1}\{(g^{-1})^{-1}hg^{-1}\}$ g$\in g^{-1}$Hg, since $(g^{-1})g^{-1}hg^{-1} \in (g^{-1})^{-1}$ H(g-1) $\subseteq$ H
$\therefore$H $\subseteq g^{-1}$ Hg.
$\therefore$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-1Hg) = gH, that is, Hg = gH
$\therefore$H $\underline{\Delta}$G, that is,)a) holds.

We should like to make the following remark about Theorem 1

Remark: Theorem 1 says that H$\underline{\Delta}$G $\Leftrightarrow$ $g^{-1}Hg = H \ \forall g \in G$. This does not mean that $g^{-1}hg = h \forall h \in H$ and $g \in G$.

For example, in E1 you have shown that $A_3 \ \underline{\Delta} S_3$. Therefore, by theorem 1,
$(1\ 2)^{-1}A_3(1\ 2)^{-1}(1\ 3\ 2)\ (1\ 2) \neq (1\ 3\ 2)$. In fact, it is (1 2 3).
Try the following exercise now.

SELF ASSISMENT EXERCISE 2

Consider the subgroup $SL_2(R) = \{A \in GL_2(R) \mid \det(A) = 1\}$ of $GL_2(R)$ (see Example 5 of unit 2ofMTH211). Using the facts that

$\det(AB) = \det(A)^{-1}) = \dfrac{1}{\det(A)}$,

prove that $AL_2(R) \ \underline{\Delta} \ GL_2(R)$.

We now prove a simple result that we stated after Example 1. it is actually a corollary to Theorem 1.

Theorem 2: Every subgroup of a commutative group is normal.

Prove: Let G be an abelian group, and $H \leq G$. For any $g \in G$ and $h \in H$, $g^{-1}hg = (g^{-1}g)h = h \in H. \therefore g^{-1}Hg \subseteq H$. Thus, $H \trianglelefteq G$.

Theorem 2 says G be an abelian, then all its subgroup are normal. Unfortunately, the converse of this is not true. That is, there are non commutative group where 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 2: consider the Klein 4-group, K_4, given in Example 7 of unit 3.of MTH 211, Show that both its subgroups $< a >$ and $< b >$ are normal.

Solution: Consider the table of the operation given in Example 7 of Unit 3.of MTH 211, 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-1hg $\in H \ \forall g \in K_4$ and $h \in H$.

Now, $g^{-1}eg = e \in H \forall g \in K_4$.

Further, $e^{-1}ae = a \in H$, $a^{-1}aa = a \in H$, $b^{-1}ab = bab = a \in H$ and $(ab)^{-1}a(ab) = b^{-1})a^{-1}aa)b = bab = a \in H$.
$\therefore H \trianglelefteq K_4$.

By a similar proof we can show that $< b > \trianglelefteq K_4$.

In Example 2, 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 $x \in G. \therefore x \in N$ or $x \in yN$.

Since $N \cap Nx = \emptyset$, $x \notin N. \therefore xN = yN$.

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 $x \notin N. \therefore nx \in xN$.

Thus, $Nx \subseteq xN$.

By a similar argument we can show that $xN \subseteq Nx$.

$\therefore Nx = xN$, and $N \trianglelefteq G$.

We will use this theorem in Unit 7 to show that, for any $n \geq 2$, the alternating group A_n is a normal subgroup of S_n.

In fact, if you go back to the end of sec. 4.3in MTH 211, you can see that $A_4 \trianglelefteq S_4$, since Lagrange's theorem implies that

$$|S_4:A_4| = \frac{o(S_4)}{o(A_4)} = \frac{4!}{12} = 2.$$

Now let us look at an example to show that the converse of Theorem 2is not true.

Consider the quaternion group Q_8, which we discussed in Example 4 of unit 4of MTH211,. It has the following 6 subgroups: $H_0 = \{1\}$, $H_1 = \{1, -1\}$, $H_2 = \{1, -1, A, -A\}H_3$, $= \{1, -1, B, -B\}$,
$H_4 = \{1, -1, C, -C\}$, $H_5 = Q_8$.

You know that H_0 and H_5 are normal in Q_8. Using theorem 3, you can see that H_2, H_3 and H_4 are normal in Q_8.

By actual multiplication you can see that

$g^{-1}H_1g \subseteq H_1 \ \forall \ g \in Q_8 \ \therefore H_1 \trianglelefteq Q_8$.

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 3: 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)
= (3 2 1) (2 3) = (1 3) $\notin$ < (1 2) >
Therefore, < (1 2)> is not normal in s_3.

Try the following exercise now.

SELF ASSISMENT EXERCISE 3

Consider the group of all 2 x 2 diagonal matrices over R*, with respect to multiplication. How many of its subgroups are normal?

SELF ASSISMENT EXERCISE 4

Show that Z(G), the center of G, is normal in G. (Remember that $Z(G) = \{x \in G | xg = gx \forall g \in G\}$.)

SELF ASSISMENT EXERCISE 5

Show that $< (2\ 3)>$ is not normal in S_3.

In Unit 3of MTH211, we prove that if $H \leq G$ and $K \leq H$, then $K \leq G$. That is, '$\leq$ ' is a transitive relation. But '$\underline{\Delta}$' is not a transitive relation. That is, if $H \underline{\Delta} N$ and $N \underline{\Delta} G$, it is not necessary that $H \underline{\Delta} G$. We'll give you an example in Unit3 of this course.. But, corresponding to the property of subgroups given in Theorem 4 of unit 3, we have the following result,

Theorem 4: let H and K be normal subgroups of a group G. Then $H \cap K \underline{\Delta} G$.

Proof: From Theorem 4 of unit 3, you know that $H \cap K \leq G$. We have to show that $g^{-1} zg \in H \cap K \ \forall \ x \in H \cap K$ and $g \in G$.

Now, let $x \in H \cap K$ and $g \in G$. then $x \in H$ and $H \underline{\Delta} G$. $\therefore g^{-1} xg \in H$.
Similarly, $g^{-1}xg \in K$. $\therefore g^{-1}xg \in H \cap K$.
Thus, $H \cap K \ \underline{\Delta} G$.

In the following exercise we ask you to prove an important property of normal subgroups.

SELF ASSISMENT EXERCISE 6

i. Prove that if $H \underline{\Delta} G$ and $K \leq G$, then $HK \leq G$.
(**Hint**: Use Theorem 5 unit 3.)

ii. prove that if $H \ \underline{\Delta} G$, $K \ \underline{\Delta} G$ then $HK \underline{\Delta} G$.

Now consider an important group, which is the product of two subgroups, of which only one normal.

SELF ASSESSMENT EXERCISE 7

Let G be the group generated by
$\{x, y | x^2 = e, y^4 = e, xy = y^{-1}x\}$.
Let $H = < x >$ and $K = < y >$.

Then show that $K \trianglelefteq G$, $H \trianglelefteq G$ and $G = HK$.

Solution: Not that the elements of G are of the form $x^i y^j$, where i = 0, I 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 $xy = y^{-1}$ 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, $H \trianglelefteq G$.

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 the following (see Fig. 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.

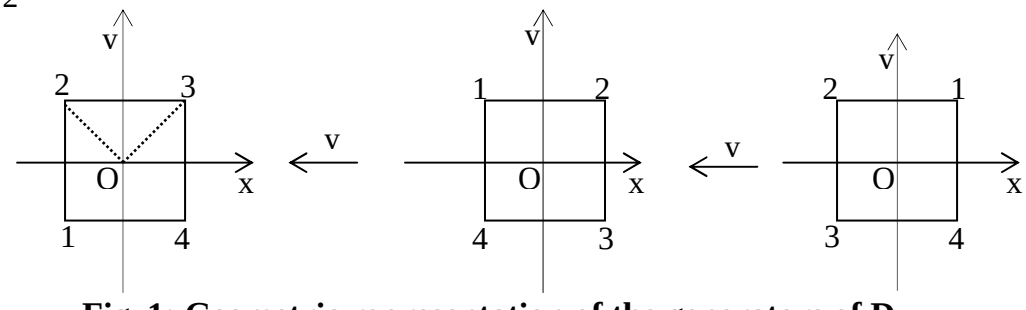


Fig. 1: Geometric representation of the generators of D_8.

We can generalize D_8 to the dihedral group
$D_{2n} = < \{x, y | x^2 = e, y^n = e, xy = y\text{-}1x\} >$, for $n > 2$.

Try the following exercise now.

E7) Describe D_6 and give its geometric interpretation.

Let us now utilize normal subgroups to form new algebraic structures.

3.2 Quotient Groups

In this section 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

$(Hx)(Hy) = H(xH)y$, using associativity,
$= Hhxy$, using normality of H,
$= Hxy$, since $HH = H$ because H is a subgroup.

Now, we define the product of two cosets Hx and Hy and G/H by
$(Hx)(Hy) = Hxy$ for all x, y in G.

Our definition seems to depend on the way in which we represent a coset. Let us explain this. 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 think: Does C_1C_2 depends 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 $C_1C_2 = Hx\,y$? Actually, we will show you that $Hxy = Hx_1y_1$, that is, the product of cosets is well defined.

Since $Hx = Hx_1$ and $Hy = hy_1$, $xx_1^{-1} \in H$, $yy_1^{-1} \in H$
$\therefore (xy)(x_1 y_1)^{-1} = (xy)(y_1^{-1}x_1^{-1}) = x(yy_1^{-1})x_1^{-1}$
$= x(yy_1^{-1}x_1^{-1})x_1^{-1}(xx_1^{-1}) \in H$, since $xx_1 \in H$ and $H \underline{\Delta} G$.
i.e., $(xy)(x_1y_1)^{-1} \in H$.
$\therefore Hxy = Hx_1y_1$.

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∈ G.

The coset H = He is the identity of G/H and the inverse of Hx is the coset Hx^{-1}.

Proof: We have already observed that the product of two cosets is a coset.

This multiplication is also associative, since
((Hx) (Hy)) (Hz) = (Hxy) (Hz)
= Hxyz, as the product in G is associative,
= Hx (yz)
= (hx) (hyz)
= (Hx) ((Hy) (Hz)) for x, y, z ∈ G.

Now, if e is the identity of g, then Hx, He = Hxe = Hx and He Hx = Hex Hx for every x ∈ G. Thus, He = H is the identity element of G/H.

Also, for any x ∈ G, Hx hx^{-1}.
So, we have prove 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 ≤ G, then H $\underline{\Delta}$ 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 5: Obtain the group G/H, where G = S_3 and H = A_3 = {1, (1 2 3), (1 3 2)}

Solution: Firstly, note that $A_3 \underline{\Delta} S_3$, since $|S_3:A_3| = 2$.
From example 3 of unit 4 you that g/H is a group of order 2 whose elements are H and (1 2) H.

Example 6: 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 nodulo n, that is, the elements of Zn (see Sec. E.5.1).

Thus, Z/nZ = $\{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$.
∴ o(Z/nZ) = n.
Note that addition in Z/nZ is given by $\bar{a} + \bar{b} = \overline{a+b}$.

Try these simple exercises now.

SELF ASSISMENT EXERCISE 8

For any group G, determine the quotient groups corresponding to {e} and G.

SELF ASSISMENT EXERCISE 9

Show that the quotient group of a cyclic group is cyclic.
(**Hint**: if G = < x>, then show that G/H = < Hx.>

Now, do G and G/H always have the same algebraic properties?

On solving the following exercise you will see that if G is abelian, then so is G/H; but the converse need not be true. That is, G may not so. Thus, G and G/H need not have the same algebraic properties.

SELF ASSISMENT EXERCISE 10

Show that if a group G is commutative, then so is G/H, for any $H \underline{\Delta} G$.

SELF ASSISMENT EXERCISE 11

Take the group D_8 of Example 4. Show that D_8/K is abelian, even though D_8 is non-abelian.

You may be surprised to know that given a group G, we can always defined a normal subgroup H, such that G/H is abelian. This subgroup is the commutator subgroup.

Definition: Let G be a group and x,y ∈ 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 commutator is called the commutator of G. It is denoted by [**G,G**]

For example, if G is a commutative group, then
$x^{-1}y^{-1}xy = x^{-1}xy^{-1} = e \forall\ x,y \in G. \therefore [G,G] = \{e\}$.

Try this exercise now.

SELF ASSISMENT EXERCISE 12

Obtain [G,G], where g is cyclic.

Now, let us prove the commutativity of the factor group corresponding to the commutator subgroup.

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-1y-1xy and for any g $\in$ G,
$g^{-1}(x^{-1}y^{-1}xy)g = \in [G, G]$.

Now $g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}xg)^{-1}\ (g^{-1}yg)^{-1}\ (g^{-1}xg)\ (g^{-1}yg) \in [G,G]$.
$\therefore [G, G] \underline{\Delta} G$.

Now, for x, y $\in$ G,

$HxHy = HyHx \Leftrightarrow Hxy = Hyx \Leftrightarrow (yx)\ (yx)\text{-}1 \in H$
$\Leftrightarrow xy\ x\text{-}1y\text{-}1 \in H$.

Thus, since $xy\ x\text{-}1y\text{-}1 \in H\ \forall\ x, y \in G$, $HxHy = HyHx\ \forall\ x, y \in G/H$ is abelian.

Note that we have defined the quotient group G/H only if H $\underline{\Delta}$ G. But if H Δ 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. The following exercise will give you an example.

SELF ASSISMENT EXERCISE 13

For G = S3 and H = < (12) >, show that the product of right cosets in G/H is not well defined.

(Hint: Show that H(1 2 3) = H(2 3) = H(2 3) and H1 3 2) = H(1 3), but H(1 2 3) (1 3 2) $\neq$ H(2 3) (1 3))

Self Assessment Exercise 13 leads us to the following remark.

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, for any $h \in H$, $x^{-1}hx = ex^{-1}hx \in Hx^{-1}Hx = H$.
That is, $x^{-1}Hx \subseteq H$ for any $x \in G$.
$\therefore H \trianglelefteq G.$

Let us now summarise what we have done in this unit.

4.0 CONCLUSION

We have been able to establish a fundamental mathematical structure of group theory which make the study very interesting. You are to master every detail in order to be able to follow subsequent development of the course.

5.0 SUMMARY

In this unit we have brought out the following points.

- 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 a 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 $H \trianglelefteq G$.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$
You can check that
$A_3 1 = A_3 = 1A_3$, $A_3(1\ 2) = (1\ 2)\ A_3$, and so on.
$\therefore A_3 \trianglelefteq S_3$.

SELF ASSISMENT EXERCISE 2

For any $A \in GL_2(R)$ and $B \in SL_2(R)$,
$\det(A^{-1}BA) = \det(A^{-1}) \det(B) \det(A)$

$$= \frac{1}{\det(A)} \det(A), \text{ since } \det(B) = 1$$

$= 1$
$\therefore A^{-1}BA \in SL_2(R)$.
$\therefore SL_2(R) \trianglelefteq GL_2(R)$.

SELF ASSISMENT EXERCISE 3

All, since this group is abelian.

SELF ASSISMENT EXERCISE 4

Let $\in G$ and $x \in Z(G)$. Then
$g^{-1}xg = g^{-1}gx$, since $x \in Z(G)$
$= x \in Z(G)$
$\therefore g^{-1}Z(G)g \subseteq Z(G)\ \forall\ g \in G$.

$\therefore Z(G) \trianglelefteq G$.

SELF ASSISMENT EXERCISE 5

Since $(1\ 2\ 3)^{-1}\ (2\ 3)\ (1\ 2\ 3) = (1\ 2) \notin \langle(2\ 3)\rangle$, $\langle(2\ 3)\rangle \not\trianglelefteq S_3$

SELF ASSISMENT EXERCISE 6

a) Take any element $hk \in HK$. Since $H \trianglelefteq G$, $k^{-1}hk \in H$. Let $k^{-1}hk = h_1$. Then $hk = kh_1 \in KH$.
$\therefore hk \in KH\ \forall\ hk \in HK\ \therefore HK \subseteq KH$.
Again, for any $kh \in KH$, $khk^{-1} \in H$. Let $khk^{-1} = h_2$. Then $kh = h_2k \in HK$.
$\therefore kh \in HK\ \forall\ kh \in KH$.
$\therefore KH \subseteq HK$.

Thus, we have shown that $HK = KH$.
$\therefore HK \leq G$.

b) From (a) we know that $HK \leq G$. To show that $Hk \underline{\Delta} G$, consider $g \in G$ and $hk \in HK$. Then. $G\text{-}1hkg = g^{-1}h(gg^{-1})kg = (g^{-1}hg)(g^{-1}kg) \in HK$, since $H \underline{\Delta} G$, $K \underline{\Delta} G$.
$\therefore g^{-1}HKg \subseteq HK \ \forall \ g \in G$.
$\therefore HK \underline{\Delta} G$.

SELF ASSISMENT EXERCISE 7

D_6 is generated by x and y, where $x^2 = e, y^2 = e, y^3 = e$ and $y = y^{-1}x$.

This is the group of symmetries of an equilateral triangle. Its generators are x and y, where x corresponds to the reflection about the altitude through a fixed vertex and y corresponds to a rotation about the centroid through 120^o (see fig. 2).

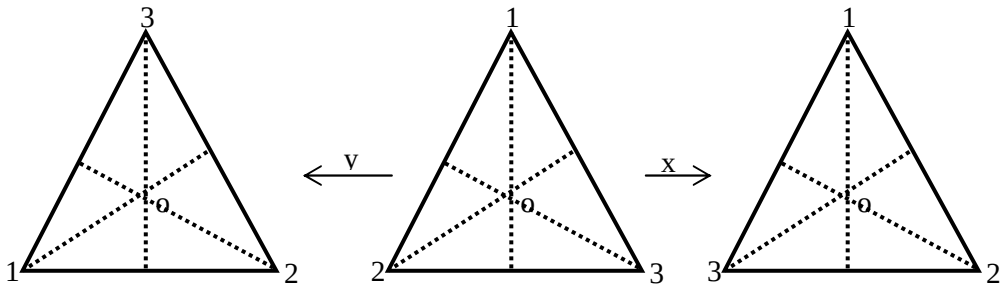


Fig.2: Generators of D_6

SELF ASSISMENT EXERCISE 8

$G/\{e\} = \{ \{e\} g \mid g \in G\} = \{ \{g\} \mid g \in G\}$
$G/G = \{Gg \mid g \in G\} = \{G\}$, since $Gg = G \forall \ g \in G$.
So G/G consists of only one element, namely, the identity.

SELF ASSISMENT EXERCISE 9

Let $G = < x >$ and G/H be a quotient group of G. any element of G/H is of the form $Hxn = (Hx)n$, since any element of G is of the form xn, $\therefore G/H = <Hx>$.

SELF ASSISMENT EXERCISE 10

for any two elements Hx and Hy in G/H,
$(Hx)(Hy) = Hxy = Hyx$, since G is abelian
$= (Hy)(Hx)$.
$\therefore$ G/H is abelian.

SELF ASSISMENT EXERCISE 11

D8/K = {K,Kx}, you can check that this is abelian. You have already seen that $xy \neq yx$, $\therefore D_8$ is not abelian.

SELF ASSISMENT EXERCISE 12

Since G is cyclic, it is abelian. $\therefore [G, G] = \{e\}$

SELF ASSISMENT EXERCISE 13

Now, (1 2 3) (1 3 2) = 1, (2 3) (1 3) = (1 2 3).
$\therefore$H(1 2 3) (1 3 2) = H1 = H = {1,(1 2)}, and
H(2 3) (1 3) = H(1 2 3) = {(1 2 3), (2 3)}.

So H(1 2 3) = H(2 3) and H (1 3 2) = H(1 3), but H(1 2 3) (1 3 2) $\neq$ H(2 3) (1 3).

6.0 TUTOR MARKED ASSIGNMENT

Show that every subgroup of a commutative is normal. Is the converse true? Justify your answer.

7.0 REFERENCES/FURHTER READINGS

Blacksell: Topics in Algebra.

Birkhaffand Melhnew (1972): Survey of Modern Algebra.

UNIT 2 GROUP HOMOMORPHISMS

CONTENTS

1.0 INTRODUCTION

So far in this course we have not discussed functions from one group to another. You may have wondered why we reviewed various aspects of functions. In this unit you will see why.

In sec. 3.1 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, a term introduced by the mathematician Klein in 1893. This concept is analogous to the concept of a vector space homomorphism that you studied in the Linear Algebra course.

In Sec. 3.2 we will introduce you to a very important mathematical idea, an isomorphism. You will see that an isomorphism is a bijective homorphism. The importance of isomorphisms lies in the fact that two groups are isomophic if and only if they have exactly the same algebraic properties.

In Sec. 3.3 we will prove a very basic theorem of group theory, namely, the Fundamental Theorem of Homomorphism. We will also give some of its important consequences.

Finally, in sec. 3.4 we will discuss automorphisms, which are isomophisms of a group onto itself. We shall look at the group of inner automorphisms in particular. This allows us to have an insight into the structure of the quotient group of G by its center, for any group G.

Before starting this unit, we suggest that you go through sec. 1.5 and unit 5.

2.0 OBJECTIVES

After reading this unit you should be able to

- Verify whether a function between groups is a homomorphis or not;
- Obtain the kernel and image of any homomorphisms;
- Check whether a function between groups is an isomorphism or not;
- State, prove and apply the Fundamental Theorem of Homomorphism;
- Prove that Inn G $\underline{\Delta}$ Aut G and G/Z(G) $\simeq$ Inn G, for any group G.

3.0 MAIN CONTENT

3.1 Homomorphisms

Let us start our study of functions from one group to another with an example.

Consider the groups (Z, +) and ({1, - 1},.). If we define

$$F:Z \rightarrow \{1, -1\} \text{ by } f(n) = \begin{cases} 1, \text{if } n \text{ is even} \\ -1, \text{if } n \text{ is odd,} \end{cases}$$

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 $f:G_1 \rightarrow G_2$ is said to be a group homoorphism (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 produce $x *_1 y$ in G_1 to the product $f(x) *_2 f(y)$ in G_2.

Before discussing examples, let us define two sets related to a given homomorphism.

Definition: Let (G1, $*_2$) and (G2 $*_2$) be two groups and f: G1 $\rightarrow$ G2 be a homomorphism.

Then we define

i) The image of f to be set
Im f = $\{f(x) \mid x \in G_1\}$.

ii) The kernel of f is defined to be the set
Ker f = $\{x \in G_1 \mid f(x) = e_2\}$, where e_2 is the identity of G_2.

Note that Im f $\subseteq G_2$, and Ker f = $f^1(\{e_2\}) \subseteq G_1$.

Now let us consider some examples.

Example 1: Consider the two groups (R, +) and (R∗,.). Show that the map exp: (R, +) $\rightarrow$ (R∗,.) : exp(r)= e^r is a group homomorphis. Also find Im exp and Ker exp.

Solution: For any n, $r_2 \in$ R, we know that $e^{r1+r2} = e^{r1}.e^{r2}$.
$\therefore \exp(r_1 + r_2) = \exp(r_1).\ \exp(r_2)$.

Hence, exp is a homomorphism from the additive group of real numbers to the multiplicative group of non-zero real numbers.

Now, Im exp = $\{\exp(r) \mid r \in R\} = \{e^r \mid r \in R\}$.
Also, Ker exp = $\{r \in R \mid e^r = 1\} = \{0\}$.

Note that exp takes the identity 0 of R to the identity 1 of R∗. exp also carries the additive inverse – r of r to the multiplicative inverse of exp (r).

Example 2: Consider the groups (R, +) and C, +) and define
F: C, +) $\rightarrow$ (R, +) by f(x + iy) = x, the real part of x + iy. Show that f is a homomorphism. What aree 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.
Im f = $\{f(x + iy) \mid x, y \in R\} = \{x \mid x \in R\} = R$.
So, f is a surjective functon (see sec. 1.5).
Ker f = $\{x + iy \in C \mid f(x + iy) = 0\} = \{x + iy\ C \mid x = 0\}$
= $\{iy \mid y \in R\}$, the set of purely imaginary numbers.

Note that f carries the additive identity of C to the additive identity of R and (and (- z) to – f(z), for any z ∈ C.

The following exercise will help you to see if you have understood what we have covered to far.

SELF ASSISMENT EXERCISE 1

Show that r: $(I^*,.) \rightarrow (R, +)$: f(x) = Inx, the natural logarithm of x, is a group homomorphism. Find Ker f and Im f also.

SELF ASSISMENT EXERCISE 2

Is f: $(GL_3(R),.) \rightarrow (R^*,.)$: f(A) a homomorphism? If so, obtain Ker f and Im f.

In Example 1 and 2 we observed that the homomorphisms carried 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 $e_{1 *1} x = x$. 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 G2
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 $x \in G_1$, $f(x) f(x^{-1}) = f(x_{*1} x^{-1}) = f(e_1) = e_2$.

Similarly, $f(x^{-1})_{*3} f(x) – e_3$.

Hence, $f(x^{-1}) = [f(x)]^{-1} \forall x \in G_1$.

Note that the converse of Theorem 1 is false. That is, if f: G1 → G2 is a function such that f(e1) = e2 and [f(x)-1 = f(x-1) $\forall$ x ∈ G1, then f need not be a homomorphism. For example, consider f: Z → Z: f(0) = 0 and

$$f(n) = \begin{matrix} n+1 \forall n > 0 \\ n-1 \forall n < 0 \end{matrix}$$

Since f(1 + 1) ≠ f(1) + f(1), 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 3: let $H \underline{\Delta} G$. Consider the map $p: G \rightarrow G/H : p(x) = Hx$. Show that p is a homomorphism. (pis called the natural or canoical group homomorphis.) 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 $p = \{ p(x)| x \in G\} = \{Hx| x \in G\} = G/H$. therefore, p is onto.
Ker $p = \{x \in G| p(x) = H\}$. (Remember, H is the identity of G/H.)
$= \{x \in G| Hx = H\}$
$= \{x \in G| x \in H \}$, by theorem 1 unit 4.
$= H$.

In this example you can see that Ker $p \underline{\Delta} G$. You can also check that theorem 1 is true here.

Before looking at more examples try the following exercises.

SELF ASSISMENT EXERCISE 3

Define the natural homomorphism p from S_3 to s_3/A_3. Does $(1\ 2) \in$ Ker p? Does $(1\ 2) \in$ Im p?

SELF ASSISMENT EXERCISE 4

Let $S = \{z \in C| |z| = 1\}$ (see Example 1 of Unit 3).

Define f: $(R, +) \rightarrow (S,.) : f(x) = e^{inx}$, where n is a fixed positive integer. Is f a homomorphism? If so, find Ker f.

SELF ASSISMENT EXERCISE 5

Let G be a group and $H \underline{\Delta} G$. show that there exists a group G and a homomorphism $f: G \rightarrow G1$ such that Ker f = H.
(Hint: Does Example 3 help?)

Another class of examples of homomorphisms concerns the inclusion map.

Example 4: 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 $i(h_1h_2) = h_1h_2 = i(h_1)i(h_2)\ \forall\ h_1, h_2 \in H$, 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 $m \leq n$.

Then, we can consider $Sm \leq Sn$, where any $\sigma \in$ Sm, written as

$\begin{bmatrix} 1 & 2 & \ldots. & m \\ \sigma(1) & \sigma(2) & \ldots. & \sigma(m) \end{bmatrix}$, is considered to be the same as

$\begin{bmatrix} 1 & 2 & \ldots.. & m & m+1 & \ldots..n \\ \sigma(1) & \sigma(2) & \ldots..\sigma(m) & m+1 & \ldots.. & n \end{bmatrix}, \in S_n$, i.e., $\sigma(k) = k$ for $m + 1 \leq k \leq n$.

Then we can define an inclusion map i $S_m \rightarrow S_n$.

For example, under i: $S_3 \rightarrow S_4$ $(1\ \ 2)$ goes to $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}$

Try this exercise now.

SELF ASSISMENT EXERCISE 6

what are the kernel and image of the inclusion map i :$3Z \rightarrow Z$?

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 homomrphism? Let us see.

Theorem 2: If f G1 $\rightarrow$ G_2 and g:$G_2 \rightarrow G_3$ are two group homomorphisms, then the composite map $g \circ f$: $G_1 \rightarrow g_3$ is also a group homomorphism.

Proof: Let $x, y \in G_1$. Then

$g \circ f(xy) = g(f(xy))$
$= g(f(x)f(y)$, since f is a homoorphism.
$= g(f(x))\ g(f(y)$, since g is a homomorphism.
$= g \circ f(x).\ g \circ f(y)$.

Thus, $g \circ f$ is a homomorphism.

Now, using Theorem 2, try and solve the following exercise.

SELF ASSISMENT EXERCISE 7

Let $n \in N$. Show that the composition $f \circ f: Z \to Z: f(x) = nx$ and $G: Z \to Z/nZ: g(x) = x$ is a homomorphism. What are $Ker(g \circ f)$ and $Im(g \circ f)$?

So far you have seen that the Kernel and image of a hommorphism are sets. In the examples we have discussed so far you may have noticed that they are subgroups. We will now prove that the kernel of a homomorphism is a normal subgroup, and the image is a subgroup.

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 $f(e_1) = e_2$, $e_1 \in$ Ker f. $\therefore$ Ker f $\neq$ ø.

Now, if $x, y \in$ Ker f, then $f(x) = e_2$ and $f(y) = e_2$
$\therefore f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\, [f(y)]^{-1} = e_2$
$\therefore xy^{-1} \in$ Ker f.
Therefore, by Theorem 1 of unit 3, Ker f $\leq G_1$. Now, for any $y \in G_1$ and $x \in$ Ker f
$F(y^{-1}xy) = f(y^{-1})\, f(x) f(y)$
$= [f(y)]^{-1} e_1 f(y)$, since $f(x) = e_2$ and by Theorem 1
$= e_2$.
$\therefore$ Ker f $\underline{\Delta}\, G_1$

b) Im f $\neq$ ø, since $f(e_1) \in$ 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 $f(y_1) = y_2$.

$\therefore x_2 y_2^{-1} = f(x_1)\, f(y_1^{-1}) = f(x_1 y_1^{-1}) \in$ Im f.
$\therefore$ Im f $\leq G_2$.

Using this result, from Example 2 we can immediately see that the set of purely imaginary numbers is a normal subgroup of C.

Let us also consider another example, which is a particular case of E 4(when n = 1

Consider ø: (R +) $\to$ (C*,.) :$\phi(x) = \cos x + i \sin x$. We have seen that (x)ø(y), that is, ø is a group homomorphism. Now ø (x) = I iff $x = 2\pi n$)

for some $n \in Z$. Thus, by Theorem 3 Ker $\varnothing = [2\pi \mid n \in Z\}$ is a normal subgroup of R +)

Note that this is cyclic, and 2π is a generator.

Similarly, Im $\varnothing$ 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 center (0.0)

You may have noticed that sometimes the kernel of a homomorphism is {e} (as in Example 1), and sometimes it is a large subgroup (as in Example 2), Does the six of the kernel indicate anything? We will prove that a homomorphism is 1-1 iff its kernel is {e}.

Theorem 4: Let f: $G_1 \rightarrow G_2$ be a group homomorphism. Then f is injective iff Ker f ={e1}. 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, Ker f = $\{e_1\}$.

Conversely, suppose Ker f =$\{e_1\}$. Let $x, y \in G_1$ such that
$F(x) = f(y)$. then $f(xy^{-1}) = f(x)\, f(y^{-1})$
$= f(x)\, [f(y)]^{-1} = e_2$.
$\therefore xy^{-1} \in$ Ker f = $\{e_1\}$. $\therefore xy^{-1} = e_1$ and x = y.
this shows that f is injective.

So, by using Theorem 4 and Example 4, we can immediately say that any inclusion i:H $\rightarrow$ G is 1-1, since Ker i= {e}.

Let us consider another example.

Example 5: Consider the group T of translations of R^2 (Example 6, unit 2). We define a map ϕ: $(R^2, +) \rightarrow (T,o)$ by $\phi\ (a, b) = f_{a.b}$. Show that ϕ is an onto homomorphism, which is also 1-1.

Solution: for (a,b), (c, d) in R^2, we have seen that
$F_{a+c,b+d} = f_{a,b}\ \ f_{e,d}$
$\therefore \phi(a, b) + (c, d)) = \phi(a, b)\ \ \phi(c, d)$.

Thus, $\varnothing$ is a homomorphism of groups.

Now, any element of t is fa,b = ø(a, b). Therefore, ø is injective. We now show that ϕ is also injective.

Let (a,b) ∈ Ker ø. Then ø(a,b) = $f_{0.0}$,

i.e., $f_{a,b} = f_{0,0}$

∴ $f_{a,b}(0,0) = f_{0,0}(0,0)$,

i.e., (a,b) = (0,0).

∴Ker ø = { (0,0)}

∴ø is 1-1,

so we have proved that ø is a homomorphism, which is bijective

Try the following exercise now.

SELF ASSISMENT EXERCISE 8

For any n > 1, consider Z_n and U_n (the group of nth roots of unity discussed in Example 5 of unit 3). Let ω demote an nth root of unity that generates U_n. Then $U_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. Now, consider the map $f:Z_n \rightarrow U_n : {}_1(r) = \omega^r$. Show that f is a group homomorphism. Is f 1-1? Is f surjecive?

And now let us look at a very useful property of a homomorphism that is surjective.

Theorem 5: If $f:G_1 \rightarrow G_2$ is an onto group homomorphism and S is a subset that generates G1, then f(S) generates G_2.

Proof: We know that

$G_1 = <S> = \{x_1^{r1}x_2^{r2}\ldots x_m^{rm} \mid m \in N, x, \in S_i\ r_i \in Z$ 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 $y \in G_1$, $y = x_1^{r1} \ldots x_m^{rm}$, for some $m \in N$, where $x_i \in S$ and $r_i \in Z$, $1 \leq i \leq m$.

Thus. X = f(y) = f(xir1… xmrm)

$= (f(x_1))^{r1} \ldots (f(x_m))^{rm}$, since f is a homomorphism.

$\Rightarrow x \in < f(S) >$, since $f(x_i) \in f(S)$ for every i = 1, 2, …, r.

Thus. $G_2 = < f(S) >$.

In the following exercise we present an important property of cyclic groups which you can prove by using Theorem 5.

SELF ASSISMENT EXERCISE 9

show that the homomorphic image of a cyclic group is cyclic, i.e., if G is a cyclic group and f:G → G is a homomorphism, then f(G) is cyclic.

Once you have solved E 9, you can immediately say that **any quotient group of a cyclic group is cyclic.**
So far you have see examples of various kinds of homomorphisms – injective, surjective and bijective. Let us now look at bijective homomorphisms in particular.

3.2 Isomorphism

In this section we will discuss homomorphisms that are 1-1 and onto. We start with some definitions.

Definitions: Let G_1 and G_2 be two groups. A homomorphism $f:G_1 \rightarrow G_2$ 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 $G_1 \simeq G_2$.

An isomorphism of a group G onto itself is called an automorphism of G. For example, the identity function I_G : G → G : 1G (x) = is an automorphism.
Let us look at another example of an isomorphism.

Example 6: Consider the set G = $\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \text{a, b} \in \text{R} \right\}$

Ten g is a group with respect to matrix addition.

Show that f:G → C:f $\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \right)$ = a + ib is an isomorphism.

Solution: Let us first verify tha f is a homomorphism. Now, for anytwo elements.

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ in G,

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = f\left(\begin{bmatrix} a+c & b+d \\ -(b+d & a+c \end{bmatrix}\right) = (a + c) + i(b + d)$$

$$= (a + ib) + (c + id)$$
$$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$$

There, f is a homomorphism.

Now, Ker $f = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a + ib = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a = 0, b = 0 \right\} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$

Therefore, by Theorem 4 f is 1-1

Finally, since Im f = C, 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 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: $G \to H$ is a group isomorphism and $x \in G$, then $\langle x \rangle \simeq \langle f(x) \rangle$
Therefore,

i) if x is of finite order, then o(x) = o(f(x)).
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 $f|_k: K \to f(K)$. Since f is bijective, so is its restriction f | k. $\therefore K \simeq f(K)$ for any subgroup K of G. In particular, for any $x \in G$, $\langle x \rangle \simeq f(\langle x \rangle) = \langle f(x) \rangle$, by E9.

Now if x has finite order, then $o(x) = o(\langle x \rangle) = o(\langle f(x) \rangle) = o(fx))$, proving (i).

To prove (ii) assume that x is of infinite order. Then <x> is an infinite group.
Therefore, <f(x)> is an infinite group, and hence, f(x) is infinite order, so, we have proved (ii).

Try the following exercise now.

SELF ASSISMENT EXERCISE 10

Show that $Z \simeq nZ$, for a fixed integar n.
Hint: Consider f: (Z, +) $\rightarrow$ (nZ, +) : f(k) = nk.)

SELF ASSISMENT EXERCISE 11

Is f: Z$\rightarrow$ X: f(x) = 0 a homomorphism? An isomorphism?

The next two exercises involve general properties of an isomorphism. E 12 is the isomorphism analogue of theorem 2 E 13 gives us another example to support that isomorphic groups have the same algebraic properties.

SELF ASSISMENT EXERCISE 12

If $\phi : G \rightarrow H$ and $\theta : H \rightarrow K$ are two isomorphisms of groups, then show that $\theta \circ \phi$ is an isomorphism of G onto K.

SELF ASSISMENT EXERCISE 13

If f: G $\rightarrow$ H is an isomorphis of groups and G is abelian, then show that H is also abelian.

So far we have seen examples of isomorphic groups. Now consider the following example.

Example 7: Show that (R*,.) is not isomorphic to (C*,.).
Solution: Suppose they are isomorphic, and f: C*$\rightarrow$ R* is an isomorphism. Then
o(i) = o(f(i), by Theorem 6. Now o(i) = 4. $\therefore$ o(f(i)) = 4.

However, the order of any real number different from $\pm$ 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.

Try these exercises now.

SELF ASSISMENT EXERCISE 14

Show that (C*,.) is not isomorphic to (R, +).

SELF ASSISMENT EXERCISE 15

Is $Z \simeq Z/nZ$, for any $n \neq 1$?

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: $G_1 \rightarrow G_2$ is an isomorphism of groups, then $f^{-1}: G_2 \rightarrow G_1$ is also an isomorphism.

Proof: From Unit 1 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 apply 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 Example 5 and Theorem 7 we can immediately say that
$\phi^{-1} : T \rightarrow R^2 : \phi^{-1}(f_{a,b}) = (a, b)$ is an isomorphism.

Theorem 7 says that if $G1 \simeq G_2$, then $G_2 \simeq G_1$. We will be using this result quite often (e.g., while proving Theorem 9)

Let us now look at a very important theorem in group theory. In Block 3 you will study its analogue in ring theory and in the Linear Algebra course you have already studied its analogue for linear transformations.

3.3 The Isomomorphism Theorems

In this section we shall prove some results about the relation 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.

Theorem 8 (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 G1/Ker f $\simeq G_2$.

Proof: Let Ker f = H. Note that H $\underline{\Delta} G_1$. Let us define the function $\psi : G_1/H \to \text{Im } f$: ψ (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 ψ(Hx) = ψ(Hy). This will prove that ψ is a well-defined function.

Now, Hx = Hy $\Rightarrow xy^{-1} \in H = \text{Ker } f \Rightarrow f(y^{-1}) = e_2$, the identity of G_2.
$\Rightarrow f(x)[f(y)]^{-1} = e_2 \Rightarrow f(x) = f(y)$.
$\Rightarrow$ ψ (Hx) = ψ (Hy).

Therefore, ψ is a well-define function.

Now, let us check that ψ is a homomorphism. For Hx, Hy $\in G_1/H$,
ψ ((Hx)(Hy)) = ψ(Hxy)
= f((xy)
= f(x) f(y), since f is a homomorphism.
= ψ (Hx) ψ (Hy).

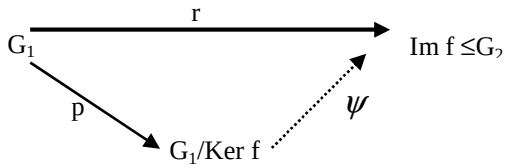
Therefore, ψ is a group homomorphism.

Next, Let us see whether ψ is bijective or not
Now, ψ(Hx) = ψ(Hy) for Hx, Hy in G_1/H
$\Rightarrow$ f(x) = f(y)
$\Rightarrow$f(x) $[f(y)]^{-1} = e_2$
$\Rightarrow f(xy^{-1}) = e_2$
$\Rightarrow xy^{-1} \in$ Ker f = H.
$\Rightarrow$ Hx = Hy
Thus, ψ is 1-1
Also, any element of Im f is f(x) = (Hx), where x $\in G_1$
$\therefore$ Im ψ = Im f.

so, we have proved that is bijective, and hence, an isomorphism. Thus, $G_1/\text{Ker } f = \text{Im } f$.

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 8 can be show in the following diagram.



Here, p is the natural homomorphism (see example 3).

The diagram says that if you first apply p, and then ψ, to the elements of G1, it is the same as applying f to them. That is,

ψ P = f.

Also, note that Theorem 8 says that two elements of G1 have the sane 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 $I_G : G \to G$. On applying theorem 8 here, we see that $G/\{e\} \simeq G$. we will be using this identification of G/{e} and G quite often.

Now for some non-trivial examples.

Example 8: Prove that $C/R \simeq R$.

Solution: Define f: C→R: f(a + ib) = b. Then f is a homomorphism, Ker f = R and Im f = R. Therefore, on applying Theorem 8 we see that C/R $\simeq$ R.

Example 9: Consider f: Z → ({1, - 1},.) : $f(n) = \begin{cases} 1, & \text{if n is even} \\ 1, & \text{if n is odd} \end{cases}$

At the beginning of Sec. 6.2, you saw that f is a homomorphism. Obtain ker f and Im f. What does Theorem 8 say in this case?

Solution: Let Z_c and Z_o denote the set of even and odd integers, respectively. Then
Ker f = {n ∈ Z | f(n) = 1} = Z_c.
Im f = {f(n) | n ∈ Z } = {1, - 1}
Thus, by Theorem 8, $Z/Z_c \simeq \{1, - 1\}$

This also tells us that $o(Z/Z_c) = 2$. The two cosets of Z_c in Z are Z_c and Z_o,

$\therefore \{Z_c, Z_o\} \simeq \{1, -1\}$.

Example 10: show that $GL_2(R)/SL_2(R) \simeq R^*$, where
$SL2(R) = \{A \in GL2(R) \mid \det(A) = 1\}$.

Solution: We know that the function
$F:GL2(R) \rightarrow R^* : f(A) = \det(A)$ is a homomorphism. Now, Ker f= SL2(R).

Also, Im f = R*, since any $r \in R^*$ can be written as $\det\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}\right)$.

Thus, using Theorem 8, $GL2(R)/SL2(R) \simeq R^*$.

Try the following exercises now.

SELF ASSISMENT EXERCISE 16

Consider the situation in Example 1 show that $(R, +) \simeq (R^*, .)$, the group of positive real numbers.

SELF ASSISMENT EXERCISE 17

Let U_4 be the multiplicative group of 4^{th} roots of unity.

Define $f: Z \rightarrow U_4$: $f(n) = in$. Use Theorem 8 to show that $Z_4 \simeq U_4$. ($I = \sqrt{-1}$.)

Now we will use the fundamental Theorem of Homomorphism to prove a very important result, which classifies all cyclic groups.

Theorem 9: Any cyclic group is isomorphic to $(Z, +)$ or $Z_n, +)$.

Proof: Let $G = \langle x \rangle$ be a cyclic group. Define
$f:Z \rightarrow G : f(n) = x^n$.
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 f – Ker f = {0} or Ker f ≠ {0}.
Case 1 (Ker f = {0}): In this case f is 1-1. Therefore, f is an isomorphism. Therefore, by Theorem 7, f1 is an isomorphism. That is, $G \simeq (Z, +)$.

Case 2 (Ker f $\neq$ {0}): Since Ker f $\leq$ Z, from example 4 of Unit 3 we know that Ker f = nZ, for some n $\in$ N. Therefore, by the fundamental Theorem of Homomorphism, Z/nZ $\simeq$G.

$\therefore$G$\simeq$Z/nZ = (Z_n, +).

Over here note that since <x> $\simeq Z_n$, o(x) = n. so, a finite cyclic group is isomorphic to Z_n, where n is the order of the group.

Using Theorem 9 we know that all cyclic groups f order 4 are isomorphic, since they are all isomorphic to Z_4. Similarly, all infinite cyclic groups are isomorphic.

And now you can prove the following nice result.

SELF ASSISMENT EXERCISE 18

Let S be the circle group {z$\in$C | z | = 1}. Show that R/Z $\simeq$S.
(**Hint**: Define f: R $\rightarrow$ S: f(x) = e$2^{\pi ix}$. Show that f is an onto homomorphism and Ker f = Z).

We will now prove the second isomorphism theorem with the help of the Fundamental Theorem of Homomorphism. It is concerned with intersections and products of subgroups. To prove the theoremyou will need the results given in the following exercise. So why not do this exercise first!

SELF ASSISMENT EXERCISE 19

Let G be a group, H $\leq$G and K $\underline{\Delta}$ G. Then

i. H $\cap$ K $\underline{\Delta}$H; and

ii. if A $\leq$ G such that K $\subseteq$A, then K$\underline{\Delta}$A.

Now let us discuss the theorem.

Theorem 10: 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-define. From E 19 you know that H $\cap$ K $\underline{\Delta}$ H. from E 6 of unit 5 you know that HK $\leq$ G. Again, from E 19 you know that K$\underline{\Delta}$ HK. Thus the given quotient groups are meaningful.

Now, what we want to do is to find an onto homorphism f : H $\rightarrow$ (HK)/K with kernel H $\cap$ K. then we can apply the Fundamental Theorem of Homorphism and get the result. We define f:H $\rightarrow$(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.

Im f = { f(h) | h $\in$ H} ={hK | h $\in$ H}

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 othr hand, any element of (HK)>K is hkK = hK, since k $\in$ K.
$\therefore$ hkK $\in$ Im f. $\therefore$ (HK)/K $\subseteq$ Im f.
$\therefore$ Im f = (HK)/K

Finally, Ker f = {h$\in$ H | f(h) = K} = {h $\in$ H| hK = K}
= {h$\in$ H| 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 10 says that

(H + K)/K $\simeq$ H/H $\cap$ K.

Now you can use Theorem 10 to solve the following exercises.

SELF ASSISMENT EXERCISE 20

Let H and K be subgroups of a finite group G, and H $\underline{\Delta}$ G. show that

O(HK) = $\frac{o(H)o(K)}{o(H \cap K)}$

SELF ASSISMENT EXERCISE 21

Show that 3Z/12Z $\simeq$ Z_4
(**Hint:** Take H = 3Z, K = 4Z).

And now for the third isomorphism theorem. This is also a corollary to Theorem 8.

Theorem 11: 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-define because $Kx = Ky$ for $x, y \in G$

$\Rightarrow xy^{-1} \in K \subseteq H \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy \Rightarrow f(Kx) = f(Ky)$

Now we leave the rest of the proof to you (see the following exercise).

SELF ASSISMENT EXERCISE 22

Show that f is an onto homomorphism and Ker f = H/K.

Let us now look at isomorphisms of a group onto itself.

3.4 Automorphisms

In this section we will first show that the set of all automorphisms of a group forms a group.
Then we shall define a special subgroup of this group.

Let G be a group. Consider
Aut G = {f: $G \to G$| f is an isomorphism }.

You have already seen that the identity map $I_G \in$ Aut G. From E 12 you know that Aut G is closed under the binary operation of composition. Also. Theorem 7 says that if $f \in$ Aut G, then $f^{-1} \in$ Aut G. We summarize this discussion n the following theorem.

Theorem 12: let G be a group. Then Aut G, the set of automorphisms of G, is a group.

Example 11: show that Aut $Z \simeq Z_2$.

Solution: Let f:$Z \to Z$ be an automorphism. Let f(1) = n. We will show that n = 1 or n= -1

. Since f is onto and $1 \in Z$, $\exists$ m $\in$ Z such that f(m) = 1 , i.e., mf(1) = 1,i.e. mn = 1.
$\therefore$ n = 1 or n = -1.

Thus, there are only two elements in Aut Z, 1 and – 1.

So Aut Z = < - 1> $\simeq Z_2$.

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 fg is an automorphism of G.

i) fg is a homorphism : If $x, y \in G$, then
$f_g(xy) = g(xy)\, g^{-1}$
$= gx(e)\, yg^{-1}$, where e is the identity of G.
$= gx(g^{-1}g)\, yg^{-1}$
$= (gxg^{-1})\, gyg^{-1})$
$= f_g(x)\, f_g(y)$.

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) fg is onto: If $y \in G$, then
$y = (gg^{-1})y\,(gg^{-1})$
$= g(g^{-1}yg)\, g^{-1}$
$= f_g(g^{-1}yg) \in \text{Im } f_g$.

Thus, f_g is an automorphism of G. We give this automorphism a special name.

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 Im G.

For example, consider S_3. Let us compute $f_g(1)$. $f_g(1\ 3)$ and $f_g(1\ 2\ 3)$.Where
g = (1 2). Note that $g^{-1} = (1\ 2) = g$.
Now. $f_g(1) = g \circ 1 \circ g^{-1} = 1$.
$f_g(1\ 3) = (1\ 2)\ (1\ 3)\ (1\ 2) = (2\ 3)$,
$f_g(1\ 2\ 3) = (1\ 2)\ (1\ 2\ 3)\ (1\ 2) = (1\ 3\ 2)$.

The following exercise will give you some practice in obtaining inner automorphisms.

SELF ASSISMENT EXERCISE 23

Obtain the image of $fg \in$ Inn G, where

a) $G = GL2(R)$ and $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

b) $G = Z$ and $g = 3$.

c) $G = Z/5Z$ and $g = 4$.

You will now see that Im G is a normal subgroup of Aut G.

Theorem 13: Let G be a group. Then Inn G is a normal subgroup of Aut G.

Proof: Inn G is non-empty, because $I_G = f_g \in$ Inn G, where e is the identity in G.

Now, Let us see if $f_g \circ f_h \in$ Inn G for g, h$\in$.

For any $x \in G$ $f_g \circ f_h(x) = f_g(hxh^{-1})$

$= g(hxh^{-1})\, g^{-1}$

$= (gh)\, x\, (gh)^{-1}$

$= f_{gh}(x)$.

Thus, $f_{gh} = f_g \circ f_h$, i.e., Inn G is closed under composition. Also $f_g = 1_G$ belongs to Inn G.

Now, for $f_g \in$ Inn G, $\exists\ f_g^{-1} \in$ Inn G such that

$f_g \circ f_g^{-1} = fgg^{-1} = f_c = I_G$. Similarly, $f_g^{-1} \circ f_g = I_G$.

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 G $\underline{\Delta}$ Aut G, let ø$\in$ Aut and G and $f_g \in$ Inn G. then, for any $x \in G$

ø-1 $\circ f_g \circ$ ø $(x) =$ ø $^{-1} \circ f_g$ (ϕ $(x))$

$= ø^{-1}\ (g\ ø(x)g^{-1})$

$= ø^{-1}\ (g)\ ø^{-1}\ (ø\ (x))\ ø^{-1}(g^{-1})$

$= ø^{-1}\ (g)\ x\{\ ø^{-1}(g)\}^{-1}$

$=$ f $ø^{-1}(g)\ (x)$. Note that $ø^{-1}(g) \in G$.)

$\therefore$ ø -1 f_g ø $= f_{\phi}^{-1}(g) \in$ Inn G $\forall$ ø $\in$ Aut G and $f_g \in$ Inn G.

$\therefore$ Inn G $\underline{\Delta}$ Aut G.

Now for some exercises! From E 23 you may have already got a hint of the

useful result that we give in E 24.

SELF ASSISMENT EXERCISE 24

Show that a group G is commutative iff Inn G = $\{I_G\}$.

SELF ASSISMENT EXERCISE 25

Show that if $x \in G$ such that $f_g(x) = x \forall\ g \in G$, then $\langle x \rangle \underline{\Delta}\ G$.

Now we will prove an interesting result, which relates the costs of the center of a group G to Inn G. Recall that the center of G, $Z(G) = \{x \in G | xg = gx = \forall\ g \in G\}$.

Theorem 14: Let G be a group. Then $G/Z(G) \simeq$ Inn G.
Proof: As usual, we will use the powerful Fundamental Theorem of Homomorphism to prove this result.

We define $f: G \rightarrow$ Aut G: $f(g) = f_g$.

Firstly, f is a homomorphism because for $g, h \in G$,
$F(gh) = f_{gh}$
$= f_g \circ fh$ (see proof of Theorem 13)
$= f(g) \circ f(h)$.

Next, Inn $f = \{fg | g \in G\}$ = Inn G.

Finally, Ker $f = \{g \in G | f_g = I_G\}$
$= \{g \in G | f_g(x) = x \forall x\ vG\}$
$= \{f \in G | gxg^{-1} = x \forall x \in G\}$
$= \{g \in G | gx = xg \forall\ x \in G\}$
$= Z(G)$.

Therefore, by the Fundamental Theorem
$G/Z(G) \simeq$ Inn G.

Now you can use Theorem 14 to solve the next exercise.

SELF ASSISMENT EXERCISE 26

Show that $S3 \simeq$ Inn S3.

Now let us see what have done in this unit.

4.0 CONCLUSION

In this unit we have established some basic fact about group isomorphism namely that if group G_1 and group G_2 are isomorphic groups they must have the same algebraic structure and satisfy the same algebraic properties.

5.0 SUMMARY

In this unit we have covered the following points.

- The definition and example of a group homomorpism .
- Let f: $G \rightarrow G_2$ be a group homomorphism. Then $f(e_1) = e_2$,
  - $[f(x)\}^{-1} = f(x-1)$, Im $f \leq G_2$, Ker of $\underline{\Delta}$ 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 the same algebraic structure.
- The composition of group homomorphisms (isomorphisms) is a group homomorphism (isomorphism).
- The proof of the Fundamental Theorem of Homomorphism, which says that if $f:G_2 \rightarrow G_2$ is a group homomorphism, then G_1 /Ker f $\simeq$ Im f.
- Any infinite cyclic group is isomomorphic to (Z, +). Any finite cyclic group of order n is isomorphic to $(Z_m, +)$.
- Let G be a group, $H \leq G$, $K \underline{\Delta} G$. Then $H/(H \cap K) \simeq (HK)/K$
- Let G be a group, $H \underline{\Delta} G$, $K \underline{\Delta} G$, $K \subseteq H$. Then (G/K) /(H/K) $\simeq$G/H.
- The set of automorphisms of a group G, Aut G, is a group with respect to the composition of functions.
- Inn G $\underline{\Delta}$ Aut G, for any group G.
- G/Z(G) $\simeq$Inn G, for any group G.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

For any x, y $\in$ R*, f(xy) = In(xy) = Inx + Iny.
$\therefore$ f is a homomorphism.
Ker f = {x $\in$ R*| f(x) =)} = {1}.
Im f = { f(x) | x$\in$R*} = {In x| x $\in$R*}.

SELF ASSISMENT EXERCISE 2

For any $A,B \in GL_2(R)$,
$F(AB) = \det(AB) = \det(A)\det(B) = f(A)\,f(B)$
$\therefore f$ is a homomorphism.
$\text{Ker } f = \{A \in GL_3(R) \mid f(A) = 1\} = \{A \in GL_3(R) \mid \det(A) = 1\}$
$= SL_3(R)$, the special linear group of order 3.
$\text{Im } f = \{ \det(A) \mid A \in GL_3(R) \}$

$= R^*$ (because for any $r \in R^*, \exists\ A = \begin{bmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(R)$ such that $\det(A) = r$.)

SELF ASSISMENT EXERCISE 3

$p: S_3 \to S_3/A_3 : p(x) = A_3x$
Note that $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.
Now $\text{Ker } p = A_3 \therefore (1\ 2) \notin \text{Ker } p$.
$\text{Im } p = \{ A_3x \mid x \in S_3\}$. $\therefore (1\ 2) \notin \text{Im } p$.

SELF ASSISMENT EXERCISE 4

For any $x, y \in r$, $f(x) + y) = e^{in(x+y)}$
$= e^{inx}\, e^{iny} = f(x).\, f(y)$.
$\therefore f$ is a homomorphism
$\text{Ker } f = \{ x \in R \mid f(x) = 1\} = \{x \in R \mid e^{inx} = 1\}$
$= \{ x \in R \mid nx \in 2\pi Z \} = \frac{2\pi}{n} Z$.

SELF ASSISMENT EXERCISE 5

From Example 3, we know that if we take G1 = G/H and take f to be the natural homomorphism from G onto G/H, then Ker f = H.

SELF ASSISMENT EXERCISE 6

$i: 3Z \to Z: I(3n) = 3n$.
$\text{Ker } i = \{3n \mid 3n = 0\} = \{0\}$
$\text{Im } i = 3Z$.

SELF ASSISMENT EXERCISE 7

$g \circ f: Z \to Z/nZ : g \circ f(x) =$
Then, for any $x, y \in Z$
$g \circ f(x + y) = \quad g \circ f(x) + g \circ f(y)$.

$\therefore$ g f is a homomorphism.
Ker (g $\circ$f) = Z, Im (g f) = { $\bar{0}$ }.

SELF ASSISMENT EXERCISE 8

For any $\bar{r}, \bar{s} \in Z_n$.
$F(\bar{r} + \bar{s}) = f(\overline{r+s}) = \omega^{r+s} = \omega\text{-}r\omega^{s} = f(\bar{r}).f(\bar{s})$.
$\therefore$ f is a homomorphism.
F is 1-1 because
$f(R) = 1 \Rightarrow \omega^{r} = 1$
$\Rightarrow r|\ o(\omega) = n$ (see Unit 4)
$\Rightarrow \bar{r} = \bar{0}$
$\therefore$ Ker f = {0}
f is surjective because any element of Un is ω^{r} for $0 \leq r \leq n - 1$, and ω^{r} = f(f).

SELF ASSISMENT EXERCISE 9

let G = < x > and f: G $\rightarrow$ G be a homomorphism. Then f:G $\rightarrow$ f(G) is an onto homomorphism.
Therefore, by Theorem 5, f(G) = < f(x)>, i.e., f(G) is cyclic.

SELF ASSISMENT EXERCISE 10

a) The function f:Z $\rightarrow$ nZ: f(k) = nk is a well-defined function.
Now, f(m + k) = nm + nk = f(m) + f(k) $\forall$ m, k $\in$ Z.
$\therefore$ f is a homomorphism
Ker f = {0}, $\therefore$ f is 1-1
Im f = nZ. $\therefore$ f is surjective.
$\therefore$ f is an isomorphism and Z $\simeq$nZ.

SELF ASSISMENT EXERCISE 11

f is a homorphism, but not 1-1, $\therefore$ f is not an isomorphism.

SELF ASSISMENT EXERCISE 2

By Theorem 2, $\theta \circ \phi$ is a homomorphism. Now let x $\in$ Ker ($\theta \circ \phi$).
Then, $(\theta \circ \phi)(x) = 0 \Rightarrow \theta(\phi(x)) = 0$
$\Rightarrow \phi(x) = 0$, since θ is 1-1.
$\Rightarrow x = 0$, since ϕ is 1-1.
$\therefore$ Ker ($\theta \circ \phi$) = {0}. $\therefore$ $\theta \circ \phi$ is 1-1

Finally, take any k $\in$ K. Then k = θ(h), for some h $\in$ H, since θ is onto.

Now, h = ø(g), for some g ∈ G, since ø is onto.

∴ k = θ ∘ø (g). ∴ θ ∘ø is onto.

∴ θ ∘ø is an isomorphism.

SELF ASSISMENT EXERCISE 13

Let a, b ∈ H. then ∃ x, y ∈ G such that a = f(x), b = f(y).
Now ab = f(x) f(y) = f(xy).
= f(yx), since G is abelian.
= f(y) f(x)
= ba.
∴ H is abelian.

SELF ASSISMENT EXERCISE 14

Suppose C* ≃ R and f: C* → R is an isomorphism. Then o*f(i) = 4. But, apart from 0, every element of (R, +) is of infinite order, and o(0) = 1. so, we reach a contradiction.

∴ C* and R are not isomorphic.

SELF ASSISMENT EXERCISE 15

Since Z is infinite and Z/nZ is finite, the two groups can't be isomorphic.

SELF ASSISMENT EXERCISE 16

Im exp = $\{e^r | r \in R\} = R^+$.
Ker exp = {0}.

Thus, by the Fundamental Theorem of Homomorphism, R ≃ R^+.

SELF ASSISMENT EXERCISE 17

U_4 = {1, I, i2, i3} = {± 1, ± I}.
F is a homomorphism, Ker f = $\{n | i^n = 1\}$ = 4Z
Im f = U_4.

∴ Z/4Z ≃ U_4

In Unit 5 we have seen that Z/4Z is the same as Z_4.
∴ Z_4 U_4.

SELF ASSISMENT EXERCISE 18

$f(x + y) = e^{2\pi i(x+y)} = e2^{\pi ix}\, e2^{\pi iy} = f(x)f(y)$.

$\therefore$ f is a homomorphism.

Now any element of S is of the form $\cos\theta + i \sin\theta$

$= \cos 2\pi \frac{\theta}{2\pi} + i \sin 2\pi \frac{\theta}{2\pi} = f\left(\frac{\theta}{2\pi}\right)$.

$\therefore$ f is onto

Also Ker $f = \{x \in R | e2^{\pi ix} = 1\}$

$= \{x \in R | \cos 2\pi x + i \sin 2\pi x = 1\}$

$= Z$, since $\cos\theta + i \sin\theta = 1$ iff $\theta \in 2\pi Z$.

Therefore, by the Fundamental Theorem of Homomorphism, $R/Z \simeq S$.

SELF ASSISMENT EXERCISE 19

a) you know that $H \cap K \leq H$. Now, let $\in H$ and $x \in H \cap K$.
Then $h^{-1}xh \in H$, since $h, x \in H$.
Also, $h^{-1}xh \in K$, since $x \in K$ and $K \underline{\Delta} G$.
$h^{-1}xh \in H \cap K$. $\therefore H \cap K \quad H$.

b) Since $K \leq G$, $K \leq A$. also, for any $a \in A$, $a \in G$.
Therefore, since $K \underline{\Delta} G$, $a^{-1}Ka = K$. $\therefore K \underline{\Delta} A$.

SELF ASSISMENT EXERCISE 20

by theorem 10. $(HK)/H \simeq K/(H \cap K)$.

$\therefore \frac{o(HK)}{o(H)} = \frac{o(K)}{o(H \cap K)}$, i.e. $o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}$

SELF ASSISMENT EXERCISE 21

Let $H = 3Z$, $K = 4Z$. By Theorem 10 we know that $(H + K)/K \simeq H/(H \cap K)$.

Now $H + K = 3Z + 3Z + 4Z = Z$. (Use E 9 of Unit 3 and the fact that $1 = 4 - 3$.)

Also $H \cap K = 3Z \cap 4Z = 12Z$(since $x \in 3Z \cap 4Z$ iff $3|x$ and $4|x$).

Thus, by Theorem 10, $Z/4Z \simeq 3Z/12Z$.

You also know that $Z/4Z \simeq Z_4$.

$\therefore 3Z/12Z \simeq Z4$.

SELF ASSISMENT EXERCISE 22

For any Kx, Ky in G/K,
$F((K x)(Ky)) = f(Kxy) = Hxy = (Hx)(Hx)(Hy) = f(Kx)f(Ky)$.
$\therefore$ f is a homomorphism.

Now, any element of G/H is of the form Hx. And
$Hx = f(Kx) \in \text{Im } f$: $\therefore \text{Im } f = G/H$.
Finally, $\text{Ker } f = \{Kx \in G/K \mid f(Kx) = H\}$
$= \{Kx \in G/K \mid Hx = H\}$
$= \{Kx \in G/K \mid x \in H\}$
$= H/K$

Therefore, by Theorem 8, $(G/K)/(H/K) \simeq G/H$.

SELF ASSISMENT EXERCISE 23

a) $f_g : GL_2(R)$: $f_g\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = g \begin{bmatrix} a & b \\ c & d \end{bmatrix} g^{-1}$

Now, $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \therefore g^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$\therefore g \begin{bmatrix} a & b \\ c & d \end{bmatrix} g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$

$\therefore f_g(GL_2(r) = \left\{ \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(R) \right\}$

b) $f_g : Z \to Z : f_g(x) = g + x + (-g) = x$.
$\therefore f_g = 1, \therefore f_g(Z) = Z$.

c) Here too, since G is abelian, $f_g = 1$.

SELF ASSISMENT EXERCISE 24

Firstly assume tht G is abelian. Then, for any $fg \in \text{Inn } G$.
$F_g^{-1}(x) = gxg^{-1} = gg^{-1}x = x \; \forall \; x \in G$.
$\therefore f_g = 1_G$.
$\therefore \text{Inn } G = \{1_G\}$.

Conversely, assume that $\text{Inn } G = \{1_G\}$.
Then, for any $x, y \in G$, $fg(y) = y$.

$\Rightarrow xyx^{-1} = y \Rightarrow xy = yx$

therefore, any two elements of G commute with each other. That is, G is abelian.

SELF ASSISMENT EXERCISE 25

To show that $g^{-1} <x> g = <x> \forall g \in G$, it is enough to show that $g^{-1}xg \in <x> \ \forall g \in G$. Now, for any $g \in G$, we are given that
$f_g^{-1}(x) = x$.
$\Rightarrow g^{-1}x(g^{-1})^{-1} = x$
$\Rightarrow g^{-1}xg = x$.
$\therefore g^{-1} <x> g = <x>$. $\therefore <x> \ \underline{\Delta} G$.

SELF ASSISMENT EXERCISE 26

We know that $S_3/Z)S_3) \simeq$ Inn S_3.

But, $Z(S_3) = \{1\}$. $\therefore S_3 \simeq$ Inn S_3.

6.0 TUTOR MARKED ASSIGNMENT

Let G be a group. Then AutG, the set of automorphism of G is a group. Prove!

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra.

Birkhaff and Melhnew(1972): A Survey of Modern Algebra.

UNIT 3 PERMUTATION GROUPS

CONTENTS

1.0 INTRODUCTION

In this unit we discuss, in detail, a group that you studied in Sec. 2.5.2. This is the symmetric group. As you have often seen in previous units, the symmetric group S_n, as well as its subgroups, have provided us with 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 present all the information about permutation groups that you have studied so far, as well as some more. We will discuss the structure of permutations, and look at even permutations in particular. We will show that the set of even permutations is a group called the alternating group. We will finally prove a result by the mathematician Cayley, which says that every group is isomorphic to a permutation group. This result is what makes permutation groups so important.

We advise you to read this unit carefully, because it gives you a concrete basis for studying and understanding the theory of groups. We also suggest that you go through Sec. 2.5.2 again, before tackling this unit.

2.0 OBJECTIVES

After reading this unit, you should be able to

- Express any permutation in S_n as a product of disjoint cycles;
- Find out whether an element S_n is odd or even;
- Prove that the alternating group of degree n is normal in S_n and is of order
- Prove and use Cayley's theorem.

3.0 MAIN CONTENT

3.1 Symmetric Group

From Sec. 2.5.2, you know that a permutation on a non-empty set X is a bijective function from X onto X. We denote the set of all permutations on X by S(X).

Let us recall some facts from Sec. 2.5.2.

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 a 2-line form as

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

Now, there are n possibilities for (1), 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_n has n! elements.

Now, let us look 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 again 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 $f \circ g$ we first apply g and then apply f.

$\therefore f \circ g\,(1) = f(g(1)) = f(4) = 3.$

$f \circ g\,(2) = f(g(2)) = f(1) = 2.$

$f \circ g\,(3) = f(g(3)) = f(3) = 1.$

$f \circ g\,(4) = f(g(4)) = f(2) = 4.$

$$\therefore f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

We show this process diagrammatically in fig. 1.

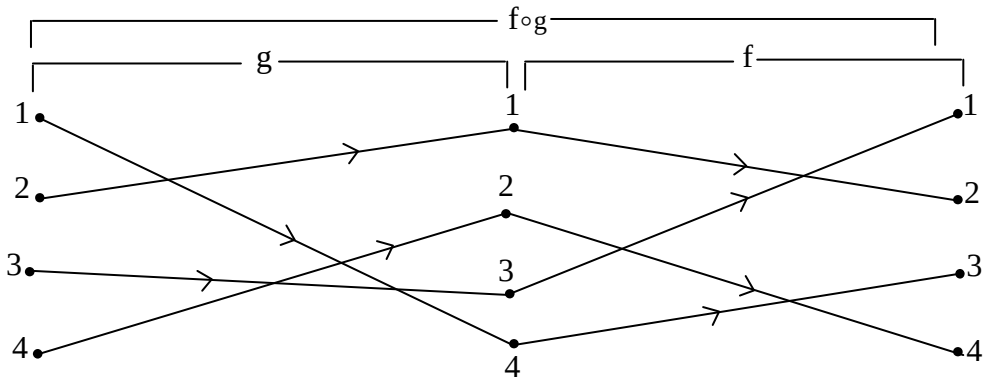


Fig. 1: (1 2 4 3) ∘(1 4 2) in S_4.

Now, let us go back to S(X), for any set X. We have proved the following result in Sec. 2.5.2.

Theorem 1: Let X be a non-empty set. Then the system (S(X), ∘) 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 $r \in S_n$, then

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

Now, with the experience that you have gained in previous units, try the following exercise.

SELF ASSISMENT EXERCISE 1

show that $(S_n,\circ)$ is a non-commutative group for $n \geq 3$.

Hint: Check that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ don't commute.)

At this point we would like to make a remark about our terminology and notation.
Remark: From now on we will refer to the composition of permutations as multiplication of permutations. We will also drop the composition sign. Thus, we will write f∘g as fg.

Te 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.

3.2 Cyclic Decomposition

In this section we will first see how to write permutations conveniently, as a product of cycles. Let us first see what a cyclic is.

Consider the permutation f= $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.Choose any one of the symbols, say 1.

Now, we write down a left hand bracket followed by 1:(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),
after the symbol we close the brackets (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 Fig 2.
Such a permutation is called a 4-cyclic, or a cyclic of length 4.Fig 2 can give you an indication as to why we give this name.

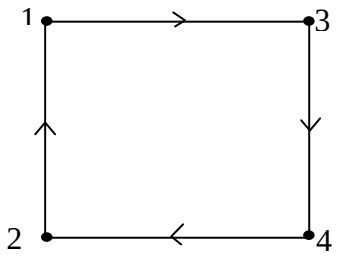


Fig. 2: (1 3 4 2)

Let us give a definition now.

Definition: A permutation f $\in$ S_n is called an r-cyclic (or cyclic of length r) if there are r distinct integers i_1, i_2, i_3, …, i, lying between 1 and n such that
$f(i_1) = i_2$, $f(i_2) = i_3$, …., $f(i_{r-1}) = i_r$, f(ir) = i1.
And $f(k) = k \; \forall \; k \notin \{i_1, i_2, ….,i_r\}$

Then, we write f = (i_1 i_2 ….. i_r)

In particular, 2-cycles are called transpositions. |For example, the permutation
$f = (2\ 3) \in S_3$ is a transposition. Here f(1) = 1, 3 and f(3) = 2.

Later in this section you will see that transpositions play a very important role in the theory of permutations.

Now consider any 1-cycles (i) in S_n. It is simply the identity permutation
$1 = \begin{pmatrix} 1 & 2 & ..... & n \\ 1 & 2 & ..... & n \end{pmatrix}$, 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-cycles 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).

The following exercise will help you to see if you've understood what a cycles is.

SELF ASSISMENT EXERCISE 2

Write down 2 transpositions, 2 3-cycles and a 5-cycle in S_5.

Now, can we express any permutation as a cycles? No. Consider the following example from S5. Let 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 process 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 Fig.3 we represent g by a diagram, which shows the 3-cycle, and the 2-cycle clearly.

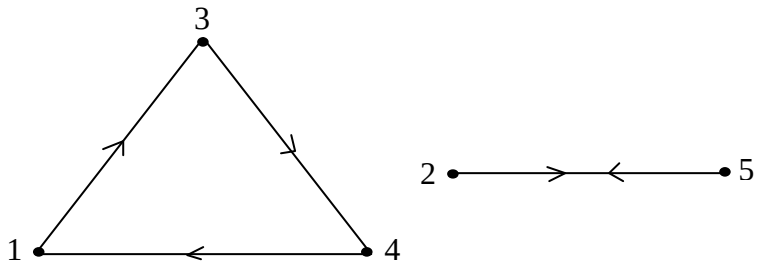


Fig. 3:1 3 4) (2 5)

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 cycles disjoint if they have no symbol in common. Thus, disjoint cycles move disjoint sets of elements. (Note that $f \in S_n$ moves a symbol i if $f(i) \neq i$. We say that fixes i if $f(i) = i$)

So, for example, the cycles (1 2) and (3 4) on S_4 are disjoint. But (1 2) and (1 4) are not disjoint, since they both move 1.

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).

If you have understood our discussion so far, you will be able to solve the following exercises.

SELF ASSISMENT EXERCISE 3

Express each of the following permutations as products of disjoint cycles in the manner demonstrated above.

i. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$

ii. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 7 & 2 & 1 & 3 & 6 & 5 \end{pmatrix}$

iii. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$

SELF ASSISMENT EXERCISE 4

Do the cycles (1 3) and (1 5 4) commute? Why?

What you have seen in E 3 is true in general. We state the following result.

Theorem 2: Every permutation $f \in S_n$, $f \neq 1$, can be expressed as a product of disjoint cycles.

The proof of this statement is tedious. It is the same process that you have applied in E 3. So we shall not do it here.

Now we will give you some exercise in which we give some interesting properties of permutations.

SELF ASSISMENT EXERCISE 5

Show that every permutation in S_n is a cycle iff $n < 4$.

SELF ASSISMENT EXERCISE 6

If $f = (i1\ i_2 \ldots i_r) \in S_n$, then show that
$f^{-1} = (i_r\ i_{r-1} \ldots i_2\ i_1)$.

SELF ASSISMENT EXERCISE 7

If f is an r-cycle, then show that $o(f) = r$, i.e., $f^r = 1$ and $f^5 \neq 1$, if $s<r$.
(**Hint**: if $f = (i_1\ i_2 \ldots i_r)$, then $f(i_1) = i_2\ f^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_r$)

and now let us see how we can write a cycle as a product of transpositions. Consider the cycle (1 5 3 4 2) in S_5. You can check that this is the same as the product

(1 2) (1 4) (1 3) (1 5). Not that these transpositions are not disjoint. In fact, all of them move the element 1.

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 $(i_1\ i_r)$ $(i_1\ i_{r-1})$ ….. $(i_1\ i_2)$, a product of transpositions.

Note that, since the transpositions aren't disjoint, they need not commute.

Try the following exercise now.

SELF ASSISMENT EXERCISE 8

Express the following cycles as products of transpositions:
a) (1 3 5), b) (5 3 1), c) (2 4 5 3).

Now we will use Theorem 2 to state a result which shows why transpositions are so important in the theory pf permutation.

Theorem 3: Every permutation in Sn ($n \geq 2$) can be written as a product of transpositions.

Proof: The proof is really very simply. By Theorem 2 every permutation, apart from 1, is a product pf disjoint cycles. Also, you have just seen that every cycle is aproduct of transpositions. Hence, every permutation, apart from 1 is a product of transposition.

Also, 1 = (1 2) (1 2) Thus, 1 is also a product of transpositions. So, the theorem is proved.

Let us see how Theorem 3 works in practice. The permutation in E 3(a) is (1 5 3 2 4). 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).
Now you can try your hand at this process.

SELF ASSISMENT EXERCISE 9

Write the permutation in E 3(b) as a product of transpositions.

SELF ASSISMENT EXERCISE 10

Show that (1 2….10) = (1 2) (2 3) ….(9 10).

The decomposition given in Theorem 3 leads us to a subgroup of S_n that we will now discuss.

3.3 Alternating Group

You have seen that a permutation in S_n can be written as a product of transpositions. From E 10 you can see that the factors in the product are not uniquely determined. But all such representations have one thing in common – if a permutation in S_n is the product of an odd number of transposition in one such representation, then it will be a product of a odd number of transpositions in any such representation, similarly, if $\in$ 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 define to be

$$\text{Sign } f = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{f(j)-f(i)}{j-i}$$

for example, for $f = (1\ 2\ 3) \in S_3$,

$$\text{sign } f = \frac{f(2)-f(1)}{2-1}\ \frac{f(3)-f(1)}{3-1}\ \frac{f(3)-f(2)}{3-2}$$

$$= \left(\frac{3-2}{1}\right)\left(\frac{1-2}{2}\right)\left(\frac{1-3}{1}\right) = 1.$$

Similarly, if $f = (1\ 2), \in S_3$, then

$$\text{Sign } f = \frac{f(2)-f(1)}{2-1}\ \frac{f(3)-f(1)}{3-1}\ \frac{f(3)-f(2)}{3-2}$$

$$= \left(\frac{1-2}{1}\right)\left(\frac{3-2}{2}\right)\ \left(\frac{3-1}{1}\right) = -1.$$

Henceforth, whenever we talk of sign f, we shall assume that $f \in S_n$ for some $n \geq 2$.

Try this simple exercise now.

SELF ASSISMENT EXERCISE11

What is the signature of $1 \in S_n$?

Have you noticed that the signature define a function
Sign: $S_n \rightarrow Z$? We will now show that this function is a homomorphism.

Theorem 4: Let $f,g \in S_n$. Then sign $(f \circ g)$ = (sign g).

Proof: By definition,

$$\text{Sign } f \circ g = \prod_{i,j=1}^{n} \frac{f(g(j)) - f(g(i))}{j - i}$$

$$i<j$$

$$\prod_{i,j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \prod_{i,j} \frac{g(j) - g(i)}{j - i}$$

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

$$\therefore \prod_{i,<j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} = \text{sign f.}$$

$\therefore$ sign $(f \circ g)$ = (sign f) (sign g).

Now we will show that Im (sign) = {1, - 1}.

Theorem 5: a) If $t \in S_n$ is a transposition, then sign t = - 1.
b) sign f = 1 or –1 $\forall$ f $\in$ Sn.
c) Im (sing) = {1, - 1}.

Proof: a) Let t = (p q), where p < q.

Now, only one factor of sign t involves both p and q, namely,

$$\frac{t(q) - t(p)}{q - p} = \frac{p - q}{q - p} = -1.$$

Every factor of signt 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.

$$\frac{t(i) - t(p)}{i - p} \frac{t(i) - t(q)}{i - q} = \frac{i - q}{i - p} \frac{i - p}{i - q} = 1, \text{ if } i > q,$$

$$\frac{t(i) - t(p)}{i - p} \frac{t(q) - t(i)}{q - i} = \frac{i - q}{i - p} \frac{p - i}{q - i} = 1, \text{ if } q > i > p,$$

$$\frac{t(p)-t(i)}{p-i}\ \frac{t(q)-t(i)}{q-i} = \frac{q-i}{p-i}\ \frac{p-i}{q-i} = 1, \text{ if } i< p.$$

Taking the values of all the factors of sign t, we see that sign t = -1.

b) Let $f \in S_n$. By Theorem 3 we know that $f = t_1t_2 \ldots..t_r$ for some transpositions

$t_1, \ldots.. t_r$ in S_n

$\therefore$ sign f = sign $(t_1\ t_2 \ldots.\ t_r)$

= (sign t1) (sign t2) ….. sign (t_r), by Theorem 4.

= (- 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 1 = 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 6: Let $f \in S_n$ and let

$f = t_1t_2 \ldots..t_r = t_1t_2 \ldots t_s$

X two factorization 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: $S_n \rightarrow \{1, - 1\}$ to $f = t_1t_2 \ldots..t_r$.

By Theorem 5 we see that

Sign f = (sign t_1) (sign t_2) ….. (sign t_1) = $(-1)^r$.

$\therefore$ sign $(t_1t_2 \ldots..t_{s)} = (- 1)^r$, substituting $(t_1t_2 \ldots..t_s$ 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 $f \in S_n$, the number of factors occurring in any factorization of f into transpositions 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 number of transposition. f is called off 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 $(i\ jk)\ (i\ k)\ (i\ j)$.

Now, see if you've understood what odd and even permutations are

SELF ASSISMENT EXERCISE 12

Which of the permutation in E 8 and 9 are odd?

SELF ASSISMENT EXERCISE 13

If $f, g \in S_n$ are odd, then is $f \circ g$ odd too?

SELF ASSISMENT EXERCISE 14

Is the identity permutation odd or even?

Now, we define an important subset of S_n namely,
$An = \{f \in S_n | f \text{ is even}\}$.

We'll sow that $A_n \trianglelefteq S_n$, and that $o(A_n) = \frac{n!}{2}$, for $n \geq 2$.

Theorem 7: The set An, of even permutations in S_n, forms a normal subgroup of S_n of order $\frac{n!}{2}$

Proof: Consider the signature function,
Sign: $S_n \rightarrow \{1, -1\}$.

Note that $\{1, -1\}$ is a group with respect to multiplication. Now Theorem 4 says that sign is a group homomorphism and Theorem 5 says that Im (sign) = $\{1, -1\}$. Let us obtain Ker (sign).

$$\begin{aligned}\text{Ker (sign)} &= \{f \in S_n \mid \text{sign } f = 1\} \\ &= \{f \in S_n \mid f \text{ is even}\} \\ &= A_n.\end{aligned}$$

$\therefore A_n \trianglelefteq S_n$.

Further, by the Fundamental Theorem of Homomorphism

$S_n/A_n \simeq \{1, -1\}$.

$\therefore o(S_n/A_n) = 2$, that is, $\frac{o(S_n)}{o(A_n)} = 2$.

$\therefore o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}$.

Note that this theorem says that the number of even permutations in S_n equals the number of odd permutations in S_n.

Theorem 7 leads us to the following definition.

Definition: A_n, the group of even permutations in S_n, is called the alternating group of degree n.

Let us look at an example that you already seen in previous units, A_3. Now, Theorem 7 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, 1 $\in A_3$.
$\therefore$ A3 = {1, (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 $(i_1 i_2 \ldots . i_r) = (i_1 i_r)(i_1 i_{r-1})$ …… $(i_1 i_2)$, a product of (r – 1) transpositions. Use this fact to do the following exercise.

SELF ASSISMENT EXERCISE 15

Write down all the elements of A_4.

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 $\underline{\Delta}$ A_4 (see Theorem 3 unit 5). Now A_4/H is a group of order 2. Therefore, by E 8 of unit 4,
$(Hg)^2 = H \; \forall \; g \in A_4$. (Remember H is the identity of A_4/H.)
$\therefore g^2 \in H \; \forall \; g \in A_4$.
Now, (1 2 3) $\in A_4$ $\therefore$ (1 2 3)2 = (1 3 2) $\in$ H.
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, 1 $\in$ 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 Unit 5 we'd said that if $H \underline{\Delta} N$ and $N \underline{\Delta} G$, then H need not be normal in G. well, here's the example.
Consider the subset $Y_4 = \{1(1\ 2)\ (3\ 4), (1\ 4)\ (2\ 3), (1\ 3)\ (2\ 4))$ of A_4.

SELF ASSISMENT EXERCISE 16

Check that $(V_4, \circ)$ is a normal subgroup of A_4.

Now, let $H = \{1,(1\ 2)\ (3\ 4)\}$. Then H is a subgroup of index 2 in V_4. $\therefore$ $H \underline{\Delta} V_4$.

So, $H \underline{\Delta} V_4$, $V_4 \underline{\Delta} A_4$. But $H \underline{\Delta} A_4$. why? Well, $(1\ 2\ 3) \in A_4$ is such that $(1\ 2\ 3)\text{-}1\ (1\ 2)\ (3\ 4)\ (1\ 2\ 3) = (1\ 3\ (2\ 4) \notin H$.

And now let us see why permutation groups are so important in group theory.

3.4 Cayley's Theorem

Most finite groups that first appeared in mathematics were groups of permutations. It was the English mathematician Cayley who first realized 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 8 (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
$f_a: G \rightarrow G: f_a(x) = ax$.
fa is 1-1, since
$f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y\ \forall x, y \in G$.
f_a is onto, since any $x \in G$ is $f_a(a^{-1}x)$.
$\therefore f_a \in Z(G)\ \forall\ a \in G$.
(Note that S(G) is the symmetric group on the set G.)
now we define a function $f: G \rightarrow S(G) : f(a) = f_a$.
we will show that f is an injective homomorphism. For this we note that
$(f_a \circ f_b)(x) = f_a(bx) = abx = f_{ab}(x)\ \forall\ a, b \in G$.
$\therefore\ f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b)\ \forall a, b \in G$.
that is, f is a homomorphism.
Now, Ker $f = \{a \in G |\ fa = IG\}$

$= \{a \in G | fa(x) = x \ \forall \ x \in G\}$
$= \{a \in G \mid ax = x \ \forall \ x \in G\}$
$= \{e\}$.

Thus, by the Fundamental Theorem of Homomorphism,

$G/\text{Ker } f \simeq \text{Im } f \leq S(G)$,
That is, G is isomorphic to a subgoup of S(G).

As an example of Cayley's theorem, we will show you that the Klein 4 – group K4 (ref. Example 7, unit 3) is isomorphic to the subgroup V4 of S4. the multiplication table for K4 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 ASSISMENT EXERCISE 17

Check that $f_e = 1$, $f_a = (e\ a)\ (b\ c)$, $f_b = (e\ b)\ (a\ c)$, $f_c = (e\ c)\ (a\ b)$.

On solving E 17 you can see that

$K_4 \simeq \{1,(e\ a)\ (b\ c), (e\ b)\ (a\ c), (e\ c)\ (a\ b)\}$. Now, just replace the symbols e, a, b, c by 1, 2, 3, 4 and you'll get V_4.

$\therefore K_4 \simeq V_4$.

Try the following exercise now.

SELF ASSISMENT EXERCISE 18

Obtain the subgroup of S_4, to which Z_4 is isomorphic. Is $Z_4 \simeq A_4$?

So let us see what we have done in this unit.

4.0 CONCLUSION

In this unit we have studied permutation groups and the structure of permutations. We have studied the set of even permutation which is called the alternating group. We also proved Cayley's Theorem which says every group is isomorphic to a permutation group. This singular result makes permutation groups so important**.**

5.0 SUMMARY

In this unit we have discussed the following points.

1. The symmetric group S(X), for any set X and the group S_n, in particular.
2. The definitions and some properties of cycles and transpositions.
3. Any non-identity permutation in S_n can be expressed as a disjoint product of cycles.
4. Any permutation in S_n ($n \geq 2$) can be written as a product of transpositions.
5. The homomorphism sign: $S_n \rightarrow \{1, -1\}$, $n \geq 2$.
6. odd and even permutations.
7. An, the set of even permutations in S_n, is a normal subgroup of S_n of order $\frac{n!}{2}$, for $n \geq 2$
8. Any group is isomorphic to a permutation group.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

Since $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

These two permulations don't commute.
$\therefore$ S_3 is non-abelian.
In Unit 6 (after Example 4) we showed how $S_3 \leq S_n \ \forall n \geq 3$.
$\therefore S_n$ will be non-abelian $\forall n \geq 3$.

SELF ASSISMENT EXERCISE 2

There can be several andswers.
Our answer is (1 2), (2 4), (1 3 5), (1 2 3), (2 5 1 4 3).

SELF ASSISMENT EXERCISE 3

a) (1 5 3 2 4)
b) (1 8 5) (2 4) (3 7 6)
c) (1 4) (2 5)

SELF ASSISMENT EXERCISE 4

No Because

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

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

SELF ASSISMENT EXERCISE 5

You know that all the elements of S_1, S_2 and S_3 are cycles. So, if nc, every permuation is a cycle in $S_{n.}$
Conversely we will show that if $n \geq 4$, then there is a permutation in S_n which is not a cycle. Take the element (1 2) (3 4). This is an element of $S_n \ \forall n \geq 4$, but it is not a cycle.

SELF ASSISMENT EXERCISE 6

Since $(i_1\ i_2.....i_r)\ (i_r\ i_{r-1}.....i_2\ i_1) = I = (i_r\ i_{r-1}.....i_2\ i_1)\ (i_1\ i_2.....i_r)$
$(i_1\ i_2.....i_r)^{-1} = (i_r\ i_{r-1}.....i_2\ i_1)$.

SELF ASSISMENT EXERCISE 7

Let f = $(i_1\ i_2.....i_r)$.
Then $f(i_1) = i_2$, $f(i_2) = i_3$, ……., $f(i_{r-1}) = i_r$, $f(i_r) = i_1$.
$\therefore\ f^2(i_1) = f(i_2)$, $f^3(i_1) = f(i_3) = i_4$, ……., $f^r(i_1) = f(i_r) = i_1$.
Similarly, $f^r(i_k = i_k\ \forall k = 2$, ……., r.
$\therefore f^r = 1$.
Also \, for s <r, $f^s(i_{1)\ =\ i}s+1 \neq i_1\ \therefore\ f^s \neq 1$.
$\therefore o(f) = r$.

SELF ASSISMENT EXERCISE 8

a) (1 5) (1 3)
b) (5 1) (5 3)
c) (2 3) (2 5) (2 4)

SELF ASSISMENT EXERCISE 9

(1) (1 8) (2 4) (3 6) (3 7)

SELF ASSISMENT EXERCISE 10

For y three symbols i, j and k,
(i j) (j k) = (i j k).
Then, if m is yet another symbol.
(i j k) (k m) = (i j k m), and so on.
$\therefore$(1 2) (2 3) … (9 10)
= (1 2 3) (3 4) …..(9 10)
= (1 2 3 4) ….(9 10)
= (1 2 3 …..10)

SELF ASSISMENT EXERCISE 11

Sing 1 = $\prod_{\substack{i,j=i \\ i<j}}^{n} \frac{I(j)-I(i)}{j-I} = \prod_{\substack{i,j=i \\ i<j}}^{n} \frac{j-i}{j-i} = 1.$

SELF ASSISMENT EXERCISE 12

The permutation in E 8 (c) and E 9 are odd.

SELF ASSISMENT EXERCISE 13

Sign (f) = sign (g) = - 1
$\therefore$sign (f $\circ$ g) = (- 1) (- 1) = 1
$\therefore$f $\circ$ g is even.

SELF ASSISMENT EXERCISE 14

Sign 1 = 1. $\therefore$1 is even.

SELF ASSISMENT EXERCISE 15

We know that o(A_4) = $\frac{4!}{2}$ = 12. Now I $\in$ A_4. Then, all the 3-cycles are in A_4
The are (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), 1 4 3), (2 3 4), (2 4 3).
Then we have all the possible disjoint products of two transpositions.
They are (1 2) (3 4) (1 3) (4 2), (1 4) (2 3)
So we have obtained all the 12 elements of A_4d

SELF ASSISMENT EXERCISE 16

By actual multiplication you can see that V_4 ios closed with respect to $\circ$, and each element of V_4 is its own inverse.
$\therefore V_4 \leq A_4$
again, by actual multiplication, you can see that
$f^{-1}fg \in V_4$ and $g \in V_4$.
$\therefore V_4 \trianglelefteq A_4$.

SELF ASSISMENT EXERCISE 17

$F_e(x) = ex = x \forall x \in K_4$. $\therefore f_e = I$
Now, $f_a(e) = a$, $f_a(a) = e$, $f_a(b) = c$, $f_a(c) = b$.

$\therefore f_a = (e\ a\ (b\ c)$.

Similarly, $f_b = (e\ b)\ (a\ c)$ and $f_c = (e\ c)\ (a\ b)$.

SELF ASSISMENT EXERCISE 18

We know that $Z_4 = <\bar{1}>$ and $o(\bar{1}) = 4$. Therefore, the subgroup of S_4 isomorphic to Z_4 must be cyclic of order 4

It is general by the permutation $f_{\bar{1}}$.

Now $f_{\bar{1}} = (x) = \bar{1} + x \forall x \in Z_4$.

$\therefore f_{\bar{1}} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \end{pmatrix}$, which is the same as (1 2 3 4).

$\therefore Z_4 \simeq <(1\ 2\ 3\ 4)>$, which is certainly not isomorphic to A_4

6.0 TUTOR MARKED ASSIGNMENT

Let (GL2) be a set of nxn matrices , show that S(GL2) form a group called the symmetric group of GL2

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra.

Birkhaff and Melhnew(1972): A Survey of Modern Algebra.

UNIT 4 FINITE GROUPS

CONTENTS

1.0 INTRODUCTION

By now you are familiar with various finite and infinite groups and their subgroups. In this unit we will pay special attention to certain finite groups and discuss their structures. For example, you will see that any group of order 6 is cyclic or is isomorphic to S_3.

To be able to describe the structure of a finite group we need some knowledge of a direct product of groups. In Sec.3.2 and 3.3 we will discuss external and internal direct product.

In Sec. 3.4 we discuss the uses of certain results obtained by the famous mathematician Sylow (1832-1918). These theorems, as well as a theorem by Cayley, allow us to determine various subgroups of some finite groups.

Finally, in 3.5, we use the knowledge gained in Sec. 3.3 and Sec.3.4 to describe the structures of several finite groups. In particular, we discuss groups of order less than or equal to 10.

With this unit we wind up our discussion of group theory. In the next module you will start studying ring theory. Of course, you will keep using what you have learnt in the first two blocks, because every ring is a group also, as you will see.

2.0 OBJECTIVES

After reading this unit you should be able to

- Construct the direct product of a finite number of groups;
- Check if a group is a direct product of its subgroup;
- Use Sylow's theorem to obtain the possible subgroups and structures of finite groups.
- Classify groups of order p, p2 or pq where p and q are primes such that p > q and q χ p – 1.

3.0 MAIN CONTENT

3.1 Direct Product of Groups

In this section we will discuss a very important method of constructing new groups by using given groups as building blocks. 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.

3.2 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 $G = G_1 \text{ X } G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$

Can we define a binary operation on G by using the operations on G1 and G2? Let us try the obvious method, namely, componentwise multiplication. That is, we define the operation $*$ on G by $(a, b) * (c, d) = (a *_1 c, b *_2 d) \forall a, c \in G_1, b, d \in G_2$.

The way we have defined $*$ ensures that it is a binary operating.

To check that $(G, *)$ is a group, you need to solve the following exercise.

SELF ASSISMENT EXERCISE 1

Show that the binary operation $*$ on G is associative. Element and the inverse of any element (x, y) in G.

If you have proved that G - G_1 x 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, +)X(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 line.

Definition: Let $(G_1, *_1)$ $(G_2, *_2)$, ….., $(G_n, *_n)$ be n groups. Their external direct product is the, be n group $(G, *)$, where
$G = G_1 \text{ X } G_2 \ldots\ldots \text{ X } G_n$ and
$(x_1, x_2\ldots., x_n) * (y_1, y_2\ldots\ldots,y_n) = (x_1 *_1 y1, x2 *2 y2,\ldots\ldots,xn *n yn) \forall x_1, y_1 \in G_1.$

Thus, R^n is the external direct product of n copies of R.

We would like to make a remark about notation now.
Remark 1: Henceforth, we will assume that all the operations $*$, $*$ 1……, $*$ n are multiplication, unless mentioned otherwise. Thus, the operation on
$G = G_1 \text{ X } G_2 \text{ X}\ldots\text{X } G_n$ will be given by
$(a_1\ldots.a_n), (b_1,\ldots.., b_n)$
$= (a_1b_1, a_2 b_2,\ldots..,a_nb_n) \forall a_1, b_1 \in G_1.$

Now try the following exercise.

SELF ASSISMENT EXERCISE 2

Show that $G_1 \text{ X } G_2 \quad G_2 \text{ X } G_1$, for any two groups G_1 and G_2.

Because of E 2 we can speak of the direct product of 2 (or n) groups without bothering about their order.

Now, let G be the external direct product G_1 X G_2. Consider the projection map
$\pi 1: G_1 \text{ X } G_2 \rightarrow G_1: \pi_1 (x, y) = x.$
then π_1 is a group homomorphism, since
$\pi_1 ((a, b) (c, d))) = \pi_1 (ac, bd)$
$= ac$
$= \pi_1 (a, b)\ \pi_1(c, d)$
$\pi 1$ is also onto, because any $x \in G_1$ is $\pi_1 (x, e_2)$
Now, let us look at Ker π_1.
$\text{Ker } \pi_1 = \{(x, y) \in G_1 \text{ X } G_2 \mid \pi_1 (x, y) = e_1\}$
$= \{(e_1, y) \mid y \in G_2\} = \{e_1\} \text{ X } G_2.$
$\therefore \{e_1\} \text{ X } G_2 \trianglelefteq G_1 \text{ x } G_2.$

Also, by the Fundamental theorem of Homomorphism $(G_1 \text{ x } G_2)/ (\{e_1\} \text{ x } G_2) \simeq G_1$.

We can similarly prove that $G_1x\{e_2\} \triangleq D_1 xG_2$ and $(G_1xG_2)/(G_1 x\{e_2\}) \simeq G_2$.

In the following exercise we give you general facts about external direct products of groups.

SELF ASSISMENT EXERCISE 3

Show that $G_1 x G_2$ is the product of its normal subgroups $H = G_1x\{e_2)$ and $K = \{e_1\}x G_2$.

Also show that $G_1 x \{e_2\}) \cap (\{e_1\} x G_2) = \{(e_1, e_2)\}$.

SELF ASSISMENT EXERCISE 4

Prove that $Z(G_1 X G_2) = Z(G_1) Z(G_2)$, where (G) denote Im Theorem 2 of unit 3).

SELF ASSISMENT EXERCISE 5

Let A and B be cyclic groups of order m and n, respectively, Then apply

Prove that AXB is cyclic of order mn.

Hint: Define $f: Z \rightarrow Z_m X Z_m : f(r) = (r + mZ, r + nZ)$. Then apply Fundamental Theorem of Homomorphism to show that $Z_m X Z_n \simeq Z_{mn}$.

So far we have seen the construction of $G_1 X G_2$ 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.

3.3 Internal Direct Product

Let us begin by recalling from Unit 5 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 $G = H X K$.

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, $K_4 = HK$

$\therefore K_4 = H \times K$.

Note that $H \simeq Z_2$ and $K \simeq Z_2$ $\therefore K_4 \simeq Z_2 \times Z_2$.

For another example, consider Z_{10}. it is the internal direct product of its subgroups
H = {0, 5} and K = {0, 2, 4, 6, 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) $H \cap K = \{0\}$.

Now, can an external direct product also be an internal direct product? Well, go back to E 3. What does if 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 2: 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) $G = H_1H_2 \ldots\ldots H_n$, and

ii) $H_1 \cap H_1 \ldots\ldots H_{i-1}H_{i+1}\ldots..H_n = \{e\} \forall\ i =, \ldots.., n$

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 X K, where H, K are subgroups of Z From Example 4 of Unit 3 you know that H = <m> and K = <n> for some m, n $\in$ Z. Then mn $\in$ H $\cap$ K. But if H X 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 X H_2 X …..X H_n, where Hi≤ Z ∀ i = 1, 2, ….., 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 ∀ $h \in H$, $k \in K$.

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, $k_1k^{-1} = e$, so that $k_1 = k$.
Thus, the representation of x as product of an element of H and an element of K is unique.

c) The best way to show that two elements x and y commute is to show that their commutator z-1y-1 xy is identity. So, let $h \in H$ and $k \in K$ and consider $h^{-1}k^{-1}hk$. Since
$K \underline{\Delta} G$, $h^{-1}k^{-1}h \in K$.
$\therefore h^{-1}k^{-1}hk \in K$.
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.

Try the following exercise now.

SELF ASSISMENT EXERCISE 6

Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that G = HXK.

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 X K. Then G/H $\simeq$K and G/H $\simeq$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.

We now give a result which immediately follows Theorem 2 and which will be used in Sec. 8.4.

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).

We leave the proof to you (see the following exercise).

SELF ASSISMENT EXERCISE 7

Use Theorem 2 to prove Theorem 3.

And now let us discuss some basic results about the structure of any finite group.

3.4 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 or the group. We also said that if G is a **finite cyclic group** and m| o(G), then G has a subgroup of order m. 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. An immediate consequence of this result is the following

Theorem 5: If a prime p divides the order of a finite group G, then g contains a subgroup or 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 2 let us see what this powerful theorem is.

Theorem 6 (First Sylow Theorem): Let G be a finite group such that $o(G) = p^n m$, where
A prime, $n \geq 1$ and $(p, m) = 1$. Then G contains a subgroup of order $p \forall$ $k = 1, \ldots, n$

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.

Can you do the following exercise now?

SELF ASSISMENT EXERCISE 8

Show that $H \underline{\Delta} G$ iff the only conjugate of H in G is H itself.

Now we define Sylow p-subgroups.

Definition: Let G be a finite group and p be a prime such that $p^n \mid o(G)$ but p^{n+1} $o(G)$, some $n \geq 1$. Then a subgroup of G of order pn is called a Sylow p-subgroup of G.

So, if $o(G)$ $p^n m$, $(p, m) = 1$, then a subgroup of G of order p^n 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 to G, is given by $n_p = 1 + kp$ for some $k \geq 0$. And further, $n_p \mid o(G)$.

We would like to make a remark about the actual use of Theorem 8.

Remark 3: Theorem 8 says that $n_p \equiv 1 \pmod{p}$ (see Sec. 2.5.1). $\therefore (n_p, p^n) = 1$. also, since $n_p \mid o(G)$, using theorem 9 of Unit 1 we find that $n_p \mid m$. This fact helps us to cut down the possibilities for n_p, as you will see in the following examples.

Example 1: show that any group of order 15 is cyclic.

Solution: let g be group pf order 15 = 3 X 5. Theorem 6 says that G has a Sylow 3-subgroup. Theorem 8 says that the number of such subgroups must divide 5 and must be congruent to 1 (Mod 3). Thus, the only possibility is 1. Therefore, G has a unique Sylow 3-subgroup, say H. Hence, by Theorem 7 and E 8 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 $x \in K$.
$\therefore o(x) \mid o(H)$ and $o(x) \mid o(K)$ (by E 8 of Unit 4), i.e., $o(x) \mid 3$ and $o(x) \mid 5$.
$\therefore o(x) = 1$. $\therefore x = e$. That is, $H \cap K = \{e\}$. Also,

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = 15 = o(G).$$

$\therefore G = HK$.

So, $G = H \text{ X } K \simeq Z_3 \text{ X } Z_5 \simeq Z_{15}$, by E 5.

Example 2: 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 are {e} and G itself.

Solution: Since 30 = 2 x 3 x 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 (by Remark 3). 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-subgroup is 6. Each of these subgroups are distinct cyclic groups of order 5, the only 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-subgroups, then it has only 1 Sylow 3-subgroup.
This will be normal in G.

Try the following exercise now.

SELF ASSESSMENT EXERCISE 9

Show that every group of order 20 has a proper normal non-trivial subgroup.

SELF ASSESSMENT EXERCISE 10

Determine all the Sylow p-subgroups of Z24, where p varies over all the primes dividing 24.

SELF ASSESSMENT EXERCISE 11

Show that a group G of order 255 (= 3 X 5 X 17) has either 1 or 51 Sylow 5-subgroups. How many Sylow 3-subgroups can it have?

Now let us use the powerful Sylow theorem to classify groups of order 1 to 10. In the process we will show you the algebraic structure of several types of finite groups.

3.5 Groups of Order 1 To 10

In this section we will apply the result of the previous section to study some finite groups. In particular, we will list all the groups of order 1 to 10, onto 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 χ p – 1. Then G is cyclic.

Proof: Let P be a Sylow p-subgroup ad 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 $\in$ 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 $P \underline{\Delta} G$.

Again, the number of distinct Sylow q-subgroups of G is $n_p = 1 + k_q$ for some k, and $n_q \mid p$. Since p is a prime, its only factors are 1 and p. $\therefore n_q = 1$ or $n_q = p$. Now if $1 + k_q = p$, then $q \mid p - 1$. But we started by assuming that $q \chi p - 1$. So we reach a contradiction. Thus, $n_q = 1$ is the only possibility. Thus, the Sylow q-subgroup Q is normal in G.

7. Let o(G) = p2, p a prime. Then
   i) G is abelian.
   ii) G is cyclic or $G \simeq Zp \text{ X } Zp$.

8. 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 X Z_2
5	Z_5
6	Z_6 or Z_3
7	Z_7
8	Z_8 or Z_4 X Z_2 or Z_2 XZ_2 X Z_2 (if G is abelian)
	Q_8 or D_8 (if G is non-abelian)
9	Z_9 or Z_3 X Z_3
10	Z_{10} or D_{10}

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

$*$ is associative: Let $(a_1, b_1),)a_2, b_2), (a_3, b_3) \in G$.
Use the fact that $*_1$ and $*_2$ are associative to prove that
$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3))$.
The identity element of G is (e_1, e_2), where e_1 and e_2 are the identities of G_1 and G_2 respectively.
The inverse of $(x, y) \in G$ is $x^{-1}, y^{-1})$.

SELF ASSISMENT EXERCISE 2

Define f: $G_1 \text{ X } G_2 \rightarrow G_2$: f(a, b) = (b, a).
Then f is 1-1, surjective and a homomorphism. That is, f is an isomorphism

$\therefore G_1 \text{ X } G_2 \simeq G_2 \text{ X } G_1$

SELF ASSISMENT EXERCISE 3

We need to show that any element of G_1 X G_2 is of the form hk, where h $\in$ H and k $\in$ K
Now, any element of G_1 X G_2 is (x, y) = (x, e_2) (e_1, y) and (x, e_2) $\in$ H, (e_1, y) $\in$ K.
$\therefore G_1 G_2$ = HK
Now, let us look a H $\cap$ K. Let (x, y) $\in$ H $\cap$ K.
Since (x, y) $\in$ H, y = e_2. Since (x, y) $\in$ K, x = e_1.
$\therefore$(x, y) = (e_1, e_2). $\therefore$H K = {e_1, e_2)}.

SELF ASSISMENT EXERCISE 4

Now, (x, y) $\in$ Z (G_1 X G_2).
$\Rightarrow$ (x, y) (a, b) = (a, b) (x,y) $\forall$ (a, b) $\in$ G_1 X G_2)
$\Rightarrow$ (xa, yb) = (ax, by) $\forall$ a $\in$ G_1, b $\in$ G_2
$\Rightarrow$ xa = ax $\forall$ a $\in$ G_1 and yb = by $\forall$ b $\in$ G_2
$\Rightarrow$ x $\in$ Z(G_1) and y $\in$ Z(G_2)
$\Rightarrow$ (x,y) $\in$ Z(G_1) X Z(G_2)
$\therefore$Z(G_1X G_2) = Z(G_1) X Z(G_2).

SELF ASSISMENT EXERCISE 5

Let A = <x> and B = <y>, where o(x) = m, o(y) = n.

Then A $\simeq$$Z_m$ and B $\simeq$$Z_n$.

If we prove that Z_m X Z_n $\simeq$$Z_{mn}$. Then we will have proved that A X B Z…. that is , A X B is cyclic of order mn.
So, let us prove that if (m, n) = 1, then Z_{mn} Z_m X Z_n
Define f: Z $\rightarrow$ Z_m X Z_n: f(r) = (r +mZ, r + nZ).
(Remember that Z, = Z/sZ, for any s $\in$ N.)
Now, f is a homomorphism because
F(r + s) = ((r + s) + mZ, (r + s) + nZ)
= (r + mZ, r + nZ) + (s + mZ, s + nZ).
= f(r) + f(s).
Ker f = {f$\in$ Z | r $\in$ mZ $\cap$ nZ}
= {r $\in$ | r $\in$ mnZ}
mnZ.

Finally, we will show that f is surjective. Now, kate any element (u + mZ, v + nZ) $\in$ Z_m X Z_n. Since (m, n) = 1, $\exists$ s, t $\in$ Z such that ms + nt = 1 (see Sec. 1.6). using this equation we see that
f(u(1 – ms) + v(1 – nt)) = (u + mZ, v + nZ).
Thus, f is surjective.

Now, we apply the Fundamental Theorem of Homomorphism and find that

Z/Ker f $\simeq$Im f, that is, Z/mnZ $\simeq Z_m$ X Z_n, that is, $Z_{mn} \simeq Z_m$ X Z_n.
$\therefore$A X B is cyclic of order mn.

SELF ASSISMENT EXERCISE 6

We know that each x $\in$ G can expressed as hk, where h $\in$ H and k $\in$ K.
$\therefore$ G = HK.
We need to show that H $\cap$ K = {e}. let x $\in$ H $\cap$ K.
Then x $\in$ H and x $\in$ K. $\therefore$ xe $\in$ HK and ex $\in$ HK.
So, x has two representations, xe, as a product of an element of H and an element of K. but we have assume that each elemnt must have only on such representation. So the two representations xe and ex must coincide, that is,
X =e. $\therefore$H $\cap$K = {e}.
$\therefore$ G = H X K.

SELF ASSISMENT EXERCISE 7

G = H X K $\Rightarrow$ G/H $\simeq$K $\Rightarrow$o(G/H) = o(K) $\Rightarrow$ o(G)/o(H) = o(K).
$\Rightarrow$ o(G) = o(H) o(K).

SELF ASSISMENT EXERCISE 8

H$\underline{\Delta}$G $\Leftrightarrow$ g^{-1}Hg = H $\forall$g $\in$ G $\Leftrightarrow$ the only conjugate of H in G is H.

SELF ASSISMENT EXERCISE 9

Let G e a group of order 20. Since 20 = 2_2 X 5, G has a Sylow 5 subgroup. The number of such subgroups is congruent to 1 (mod 5) and divides 4. Thus, the number is 1. Therefore, the Sylow 5-subgroup of G is normal in G, and is the required subgroup.

SELF ASSISMENT EXERCISE 10

o(Z_{24}) = 24 = 2^3 X 3.
$\therefore Z_{24}$ has a Sylow 2-subgroup and a Sylow 3-subgoup. The number of Sylow 2-subgroups is 1 or 3 and the number of Sylow 3-subgroups is 1 or 4. Now, if Z_{24} has only 1 Sylow 2-subgroup, this account for 8 elements of the group. So, we are left with 16 elements of order 3. But this is not possible because we can only have at most 4 distinct Sylow 3-subgroups (i.e., 8 elements of order 3). So, we reach a contradiction.
$\therefore Z_{24}$ must have 3 Sylow 2-subgroups. And then it will have only 1 Sylow 3-subgroup. These are all the Sylow p-subgroups of Z_{24}.

SELF ASSISMENT EXERCISE 11

255 = 5 X 5 X 17 = 5 X 51.
The number of Sylow 5-subgroups is congruent to 1(mod 5) and must divide 51.
Thus, it is 1 or 51.
Since 255 = 3 X 85, the number of Sylow 3-subgroups that g can have is congruent to 1 (mod 3) and must divide 85. Thus, it is 1 or 85.

SELF ASSISMENT EXERCISE 12

We can apply Theorem 10 here.

SELF ASSISMENT EXERCISE 13

apply Theorem 12, we see that

i) $o(G) = 4 \Rightarrow G \simeq Z_4$ or $G \simeq Z_2 \text{ X } Z_2$.

ii) $o(G) = 9 \Rightarrow G \simeq Z_9$ or $G \simeq Z_3 \text{ X } Z_3$.

4.0 CONCLUSION

So far we have shown the algebraic structure of all groups of order to 10, except groups of order 8. Note that if G is an abelian group of order 8, then

1) $G=Z_{8,}$ the cyclic group of order 8,
2) $G=Z_4XZ_2$,or
3) $G=Z_2XZ_2XZ_2$

If G is a non-abelian group of order 8 then
$G=Q_8$ the quaternion group discussed in Example 4 of Unit 4 of MTH 211
$G=D_8$ the dihedral group discussed in Unit 1

5.0 SUMMARY

In this unit we have discussed the following points.

1) The definition and examples of external direct product of groups
2) The definition and examples of internal direct products of normal subgroups
3) If (m,n)=1 then $Z_m \text{ X } Z_n = Z_{mn}$
4) $o(H \text{ X } K) = o(H)o(K)$
5) The statement and application of Sylow's theorems
6) Let $o(G) = p^2$, p is a prime. Then
   i) G is abelian or (ii) G is cyclic or $G= Z_p \text{ X } Z_p$

6.0 TUTOR MARKED ASSIGNMENT

1) Show that H is a normal subgroup of G iff the only conjugate of H in G is H itself.
2) Show that any group of order 15 is cylic**.**

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra.

Birkhaff and Melhnew(1972): A Survey of Modern Algebra.

MODULE 2 ELEMENTARY RING THEORY

UNIT 1 RINGS

CONTENTS

1.0 INTRODUCTION

With this unit we start the study of algebraic systems 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.

$a(b+c) = ab + ac$, and $)a +b) c = ac + bc$
For all integers a, b and c. We generalize these very properties of the binary operations to define a ring in general. This definition is due to the famous algebraist Emmy Noether.

After defining rings we shall give several examples of rings. We shall also give some properties 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.

2.0 OBJECTIVES

After reading this unit, you should be able to

- Define and give examples of rings
- Derive some elementary properties of rings from the defining axioms of a ring;
- Define and give examples of commutative rings, rings with identity and commutative ring with identity.

3.0 MAIN CONTENT

3.1 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 distributive 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, usually called addition (denoted by +) and multiplication (denoted by .), is called a ring if the following axioms are satisfy:

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, e in R, i.e., addition is associative
R 3) There exists and 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 element of R has an additive inverse.
R5) $(a .b).c = a.(b.c)$ for all a, b, c in R, i.e., multiplication is associative.
R 6) $a.(+ c) = a. b + a . c$, and
$(a + b).c = a.c + .bc$
for all a, b, c in R,
i.e., multiplication distributive over addition from the left as well as the right.

The axioms R1 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 + a .c and (a + b).c = a. c + b c.

From MTH 211, 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 ring 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 examples provide us with another set of examples of rings.

Example 1: Show that (nZ, +, .) is a ring, were $n \in Z$.

Solution: You know that $nZ = \{nm \mid m \in Z\}$ 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_n that you studied in earlier .Let us briefly recall the construction of Z_n, the set of residue classes of 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, $a \equiv b \pmod n$ if $n \mid (a - b)$. The relation 'congruence modulo n' is an equivalence relation in Z. The equivalence class containing the integer a is

$\bar{a} = \{b \in Z \mid a - b \text{ is divisible by n}\}$
$= \{a + mn \mid m \in \}.$

It is called the **congruence class of a modulo n** or the **residue class of a modulo n.** The set of all equialence classes is denote by Z_n. So
$Z_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}.$

We define addition and multiplication of classes in terms of their representative by
$\bar{a} + \bar{b} = \overline{a+b}$ and
$\bar{a}.\bar{b} = \overline{ab} \quad \forall\ \bar{a}, \bar{b} \in Z_n.$

Earlier in our algebra course, you have seen that these operations are well defined in Z_n, to the help you regain some practice in adding and multiplying in Z_n, consider the following Cayley table for Z_n.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Now let us go back to looking for a finite ring.

Example 2: 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_n. Now we need to see if the axiom R6 is satisfied.

For any $\bar{a}, \bar{b}, \bar{c} \in Z_n$, $\bar{a}.(\bar{b}+\bar{c}) = \overline{\quad\quad} = \overline{\quad\quad} = a.b + \overline{\quad} = \bar{a}.\bar{b} + \bar{a}.\bar{c}$
Thus, $\bar{a}.(\bar{b}+\bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.

Similarly, $(\bar{a}+\bar{b}).\bar{c} = \bar{a}.\bar{c} + \bar{b}.\bar{c} \quad \forall\ \bar{a}, \bar{b}, \bar{c} \in Z_n$.
So, $(Z_n + ,.)$ satisfies the axioms R1 – R6. therefore, it is a ring.

Try this exercise now.

SELF ASSISMENT EXERCISE 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?

Now let us look at a ring whose underlying set is a subset of C.

Example 3: Consider the set

$Z + iZ = \{m + in \mid m \text{ and } n \text{ are integers }\}$, where $i^2 = -1$.

We define '+' and '.' in Z + iZ to be the usual addition and multiplication of complex numbers. Thus, for m+ in and s + it in Z+iZ,
(m+in) + (s + it) = (m + s) + I(n + t), and
(m + in . (s + it) = (ms – 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, +). Thus, the axioms R1 – 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 tha 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 next example is related to example 8 of unit 2. The operations that we consider in it are not the usual addition and multiplication.

Example 4: Let X be a non-empty set, $\wp$ (X) be the collection of all subsets of X and Δ denote the symmetric difference operation. Show that ($\wp$(X), Δ, $\cap$) is a ring.

Solution: for any two subsets A and B of X,
A Δ B = (A\B) $\cup$ (B\A)

In example 8 of unit 2 we showed that ($\wp$(X), Δ) is an abelian group. You also know that $\cap$ is associative. Now let us see if $\cap$ distributes over Δ..

Let A, B, C $\in$ $\wp$(X). Then
A $\cap$ (B Δ C) = A $\cap$ [(B\C) $\cup$ (C\B)]
= [A $\cap$ (B\C)] $\cup$ [A $\cap$ (C\B)], since $\cap$ distributes over $\cup$.
= [(A $\cap$ B)\(A $\cap$ C)\(A $\cap$ B)], since $\cap$ distributes over complementation.
= (A$\cap$ B) Δ (A $\cap$ C).

So the left distributive law holds.

So, (B Δ C) $\cap$ A = A$\cap$ (B Δ C), since $\cap$ is commutative.
=(A $\cap$B) Δ (A $\cap$ C)
= (B $\cap$ A) Δ (C $\cap$ A)

Therefore, the right distributive law holds also.

Therefore, $(\wp(X)\ \Delta, \cap)$ is a ring.
So far you have examples of rings in which both the operations define on the ring have been commutative. This is not so in the next example.

Example 5: Consider the set

$$M_2(R) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| \ a_{11}, a_{12}, a_{21} \text{ and } a_{22} \text{ are real numbers} \right\}$$

Show that $M_2(R)$ is a ring with respect to addition and multiplication of matrices.

Solution: Just as we have solved Example 2 of Unit 3,of MTH 211. you can check that $(M_2(R))$ is an abelian group. You can also verify the associative property for multiplication. (Also see example 5 of Unit 2.ofMTH 211) we now show that A.(B+C) = A.B + A.C for A,B,C in $M_2(R)$.

$$A.(B+C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} + & c_{11} & b_{12} + & c_{12} \\ b_{21} + & c_{21} & b_{22} + & c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}(b_{11}+c_{11}) + a_{12}(b_{21}+c_{21}) & a_{11}(b_{12}+c_{12}) + a_{12}(b_{22}+c_{22}) \\ a_{21}(b_{11}+c_{11}) + a_{22}(b_{21}+c_{21}) & a_{11}(b_{12}+c_{12}) + a_{12}(b_{22}+c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}b_{11}+a_{12}b_{21}) + (a_{11}c_{11}+a_{12}c_{21}) & (a_{11}b_{12}+a_{12}b_{22}) + (a_{11}c_{12}+a_{12}c_{22}) \\ (a_{21}b_{11}+a_{22}b_{21}) + (a_{21}c_{11}+a_{22}c_{21}) & (a_{21}b_{12}+a_{22}b_{22}) + (a_{21}c_{12}+a_{22}c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{21} \end{bmatrix} + \begin{bmatrix} a_{11}c_{11}+a_{12}c_{21} & a_{11}c_{12}+a_{12}c_{22} \\ a_{21}c_{11}+a_{22}c_{21} & a_{21}c_{12}+a_{12}c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$= A..B + A.C.$$

In the same way we can obtain the other distributive law, i.e. (A + B). C = A.C + B.C $\forall$A.
B,B $\in$ **$M_2(R)$.**

Thus, **$M_2(R)$** is a ring under matrix addition and multiplication.

Note that multiplication over $\mathbf{M_2(R)}$ is not commutative so, we can't say that the left distributive law implies the right distributive law in this case.
Try the following exercises now.

SELF ASSISMENT EXERCISE 2

Show that the set $Q + \sqrt{2Q} = \{p+\sqrt{2q} \mid p,q \in Q\}$ is a ring with respect to addition and multiplication of real numbers.

SELF ASSISMENT EXERCISE 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.

SELF ASSISMENT EXERCISE 4

Let R = $\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle\| \text{ a, b are real number } \right\}$. Prove that R is a ring under matrix addition and multiplication.

SELF ASSISMENT EXERCISE 5

Why is $(\wp(X), \cup, \cap)$ not a ring?

Let us now look at ring whose elements are functions.

Example 6: 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 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 $x \in [0, 1]$. 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 $g \in C[0, 1]$, then f + g and f.g are in C[0, 1]. Show that C[0, 1] is a ring with respect + 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 of $f \in C[0, 1]$ is (- f), where (- f)(x) = -f(x) $\forall x \in [0, 1]$. See fig. 2 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].

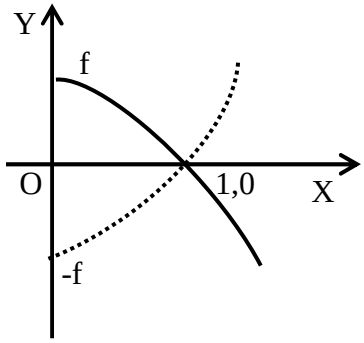


Fig. 2 The graphs of f and (-1) over [0,1].

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 one + in R
= (f.g) (x) + (f.h) (x)
= (f.g) (x) + (f.h) (x)
= (f.g + f.h)(x)

Hence, f.(g + h) = f.g + f.h.

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 7: 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
(f.g) (a) = fog(a) = f(g(a)) $\forall$ a $\in$ A] …. (1)

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) + 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 $f.g \in$ End A.

Now let us see if (End A, +,.) satisfies R1 = R6.

Since + in the abelian group A is associative and commutative, so is + in End A. The zero homomorphism on A is the aero element in End A. (-f) is the additive inverse of $f \in$ 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 $f,g,h \in$ End A. Now for any $a \in A$,
$[f.(g + h(] (a) = f((g + h)(a))$
$=f(g(a) + h(a))$
$=f(g(a) + f(h(a))$
$= (f.g)(a) + (f.h)(a)$
$= (f.g + f.h)(a)$
$\therefore f.(g + h) = f.g + f.h.$

We can similarly prove that $(f + g).h = f.h + g.h$.
Thus, R1 = R6 are true for End A.
Hence, (End A, +,.) is ring.
Note that is not commutative since $f \circ g$ need not be equal to $g \circ f$ for f, g $\in$ End A.

You may like to try these exercises now.

SELF ASSISMENT EXERCISE 6

Let X be a non-empty set and (R, +,.) be any ring. Define the set Map(X,R) to be the set of all functions from X to R. That is
Map (X, R) = $\{f| f:X \rightarrow R\}$.
Define + and . in Map (X, R) by pointwise addition and multiplication. Show that (Map (X, R), +,.) is a ring.

SELF ASSISMENT EXERCISE 7

Show that the set R of real numbers is a ring under addition and multiplication given by $a \oplus b = +b + 1$, and $a \odot b = a.b + a + b$
For all $a,b \in R$, where + and .denote the usual addition and multiplication of real numbers.

On solving Exercise 7 you must have realized that a given set can be an underlying set of many different rings.

Now, let us look at the Cartesian product of rings.

Example 8: Let (A, +,.) and $(B, \boxplus, \boxdot)$ be two rings. Show that their Cartesian product
AX B is a ring with respect to $\oplus$ and $*$ defined by
$(a, b) \oplus (a', b') = (a + a', b \boxplus b')$ and
$(a, b) * (a', b') = (a.a', b \boxdot b')$

for all (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, $\boxdot$ b), where $\boxdot$ b denotes the inverse of b with respect to $\boxplus$

Since the multiplication in A and B are associative, $*$ is associative in A X B. Again, using in fact that R6 holds for A and B, we can show that R6 holds for A X B. Thus,
$(A \text{ X } B, \oplus, *)$ is a ring.

If you have understood this example, you will be able to do the next exercise.

SELF ASSISMENT EXERCISE 8

Write down the addition and multiplication tables for $Z_2 \text{ X } Z_3$.

Before going further we would like to make a remark about notational conventions in the case of groups, we decided to use the notation G for $(G, *)$ for convenience. Here too, in future, we shall use the notation R for (R, +,.) for convenience. Thus, we shall assume that + and . are known. We shall also denote the product of two ring element a and b by ab instead of a.b.

So now let us begin studying various properties of rings.

3.2 Elementary Properties

In this section we will prove some simple but important proterties of ring 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 mention 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 (b – c) = ba – ca.

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 distributivity.
$= ab$, since b is the additive inverse of $(-b)$.

iv) for $a, b, c \in R$,
$a(b - c) = a(b + (-c))$
$= ab + a(-c)$, by distributivity
$= ab + (-(ac))$, from (ii) above.
$= ab - ac$.

We can similarly prove (v).

Try this exercise now.

SELF ASSISMENT EXERCISE 9

Show that $\{0\}$ is a ring with respect to the usual addition and multiplication. (This is called the trivial ring.)

Also show that if any singleton is a ring, the singleton must be $\{0\}$.

SELF ASSISMENT EXERCISE 10

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.

Now let us look at the sum and the product of three or more elements of a ring. We define them recursively, as we did in the case of groups (see Unit 2 MTH 211).

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 $a_1, a_2, \ldots, a_{k+1}$ in R, taken in that order, as

$+ \ldots + a_{k+1} = (a_1 a_2 \ldots a_k).a_{k+1}$.

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 of $a_1, a_2, \ldots, a_{k+1}$ (taken in that order) as

$a_2. \ldots a_{k+1} = (a_1 a_2 \ldots a_k).a_{a+1}$.

As we did for groups, we can obtain laws of indices in the case of ring also with respect to both + and ,. In fact, we have the following results for any ring R.

If m and n are positive integers and $a \in R$, then

i) $a^m . a^n = a^{m+n}$, and
$(a^m)^n = a^{mn}$.

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 $a_1, a_2, \ldots, a_m\ b_1, \ldots, b_n \in R$ then
$a(_1 + \ldots + a_{m)}(b_1 + \ldots + b_n)$
$= a_1b_1 + \ldots + a_1b_n + a_2b_1 + \ldots + a_2b_n + \ldots + a_mb_1 + \ldots + a_mb_n$.

Try this simple exercise now

SELF ASSISMENT EXERCISE 11

If R is a ring and $a, b \in r$ such that ab =ba, then use induction on $n \in N$ to derive the **binomial expansion.**
$(a + b)^n = a^n + {}^nC_1a^{n-1}b + \ldots + {}^nC_ka^{n-k}b^k + \ldots + {}^nC_{n-1}ab^{n-1} + b^{n,}$
where ${}^nC_k =$

There are several other properties of rings tat 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.

3.3 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. , i.e.it 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 (orwith 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?

Try this quickly before we go to our next definition.

SELF ASSISMENT EXERCISE 12

Prove that if a ring R has an identity element with respect to multiplication, then it is unique. (We denote this unique identity element in a ring with identity by the symbol 1.)

Now let us combine the previous two definitions.

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, R and C** are all commutative rings with unity. The integer 1 is the multiplication 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

$$AB = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 10 \\ 2 & \end{bmatrix} \text{ and}$$

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

Thus, $AB \neq BA$

Try this exercise now.

SELF ASSISMENT EXERCISE 13

Which of the rings in Example 1, 2, 3, 4, 6, 7 are commutative and which have unity?
Give the identity, whenever it exists.

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 multiplicative 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 to example 8. When will A X B be commutative? A X 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 X B by + and .. Let (a, b) and $(a'b') \in$ A X B.

Then (a, b) . $(a'b')$ = $(a'b')$. (a, b)
$\Leftrightarrow (a.a', b.b') = (a', b').(a, b)$
$\Leftrightarrow a.a' = a'.a$ and $b.b' = b'.b$.
Thus, A X B is commutative iff both A and B are commutative rings.

We can similarly show that A X 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 AXB is (e_1 e_2).

Now for some exercises about commutative rings with identity.

SELF ASSISMENT EXERCISE 14

Show that the ring in E7 is a commutative ring with identity .

SELF ASSISMENT EXERCISE 15

Show that the set of matrices $\left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle\| x \in R \right\}$ is a commutative with unity.

SELF ASSISMENT EXERCISE 16

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.

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 Hamillion (1805 – 1865). It plays an important role in geometry, number theory and the study of mechanics.

Example 9: Let $H = \{a + bi + cj + dk \mid a,b, c, d \in \mathbf{R}\}$, where i,j, k are symbols the satisfy $1^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = I = -kj$, $ki = j = -ik$.

We define addition and multiplication in **H** by

$+ bi + cj + dk) + (a_1 + b_1i + cj + d_1k)$
$(a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k$, and
$(+ bi + cj + dk) (a_1 + b_1j + c_1j + d_1k) = (aa_1 – bb_1 – cc_1\ dd_1)$
$(ab_1 + 1 + cd_1 – dc_1) + (ac_1 + bd_1 + ac_1 + bd1)j + (ad_1 + bc_1 – cb_1 + da_1)k$.

This multiplication may . But it is no so, it is simply performed as for keeping the relationship between i, j and k in mind)

Solution: Note that $\{\pm 1, \pm i, \pm j, \pm k .\}$ is the group Q_8 (Example 4, Unit 4).

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 $1 = 1 + 0i + 0j + 0k$ is the unity in **H.**
Do you agree that **H** is not a commutative ring? You will if you remember that $ij \neq ji$, for example.

4.0 CONCLUSION

So far, in this unit we have discussed various types of rings. We have seen examples of commutative and non-commutatve 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.

5.0 SUMMARY

In this unit we discussed the following points.

- definition and examples f a ring.
- Some properties of a ring like
  $a.0 = 0 = 0.a$,
  $a(-b) = -(ab) = (-a)b$,
  $(-a)(-b) = ab$,
  $a(b-c) = ab - ac$,
  $(b-c)a = ba - ca$
  $\forall a, b, c$ in a ring R.

- The laws of indices for addition and multiplication, and the generalized distributive law.

- Commutative rings, rings unit and commutative rings with unit.

Henceforth, we will always assume that a ring means a commutative ring, unless otherwise mentioned.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

Addition in Z_6^* **Multiplication in Z_6^***

+	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the tables you can see that neither addition nor multiplication are binary operations in Z_6^*, since $0 \notin Z_6^*$. Thus, $(Z_6^*, +, .)$ can't be a ring.

SELF ASSISMENT EXERCISE 2

We define addition and multiplication in $Q + \sqrt{2}Q$ by
$(a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c) + \sqrt{2}(b + d)$, amd
$(a + \sqrt{2}b).(c + \sqrt{2}d) = (ac + 2bd) + \sqrt{2}(ad + bc) \quad \forall a, b, c, d \in Q.$
Since + is associative and commutative I n R, the same holds for + in

$Q + \sqrt{2}Q.0 = 0 + \sqrt{2}.0$ is the additive identity and $(- a) + \sqrt{2}(-b)$ is the additive inverse of $a + \sqrt{2}b$.

Since multiplication in r is associative, R5 holds also. Since multiplication distributes over addition in R, it does so in $Q + \sqrt{2}\,Q$ as well Thus, $(Q + \sqrt{2}\,Q,+,.)$ is a ring.

SELF ASSISMENT EXERCISE 3

+ and are well defined binary operations on R.R1, R2, R5 and R6 hold since the same properties are true for $\mathbf{M_2(R)}$ (Example 5).

The zero element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.The additive inverse of $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is $\begin{bmatrix} a & 0 \\ 0 & -b \end{bmatrix}$
Thus, R is ring.

SELF ASSISMENT EXERCISE 4

+ and. Are binary operations on r. you can check that (R, +,.) satisfies R1 – R6.

SELF ASSISMENT EXERCISE 5

$\cup$ and $\cap$are well defined binary operations on $\wp(x)$. let us check which of the axioms **R1-R6 is not satisfied by (**$\wp$ (X), $\cup$, $\cap$). Since $\cup$ us abelian, R1 is satisfied.
Since $\cup$ is associative, R2 is satisfied.

Also, for any $A \subseteq X$, $A \cup \emptyset = A$. thus, ø is the identity with respect to $\cup$.
Thus, R3 is satisfied.
Now, for any $A \subseteq X$, $A \neq \emptyset$, there is no $B \subseteq X$ such that $A \cup B = \emptyset$.
Thus R4 is not satisfied. Hence ($\wp$(X), $\cup$, $\cap$) is not a ring.

SELF ASSISMENT EXERCISE 6

Since satisfies R1, R2, R5 and R6, so does Map (X,R). the zero element is 0: $X \rightarrow R$:)(x) = 0. The additive inverse of f: $X \rightarrow R$ is (-f) : $X \rightarrow R$.
Thus, (Map (X, R,), +,.) is a ring.

SELF ASSISMENT EXERCISE 7

Firstly, $\oplus$ and $\odot$ are well defined binary operations on

R. Next, let us check if (**R,** $\oplus$,$\odot$)satisfies R1-R6 $\forall$ a, b, c $\in$ R.

R1: $(a \oplus b = a + B + 1 = b + a + 1 = b \oplus a$.
R2: $(a \oplus b) \oplus c = (a + b + 1) \oplus c = a + b + 1 + c + 1$
$= a + (b + c + 1) + 1 = a \oplus (b \oplus c)$
R3: $a \oplus (-1) = a - 1 + 1 = a \ \forall \ a \in R$. Thus, (-1) is the identity with respect to $\oplus$

R4: $a \oplus (-1 - 2) = a + (-a - 2) + 1 = -1$. Thus, $-a - 2$ is the inverse pf a with respect to $\oplus$.

R5: $(a \odot b) \odot c = (ab + a + b) \odot c = (ab + a + b)c + (ab + a + b) + c$
$= a(bc + b + c) + a + (bc + b + c)$
$= a \odot (b \odot v)$.

R6: $a \ (b \oplus c) = a \odot (b + c + 1) = a(b + c + 1) + a + (b + c + 1)$
$= (ab + a + b) + (ac + a + c) + 1$
$= (a \odot b) \oplus (a \odot c)$.

Thus, $(R, \oplus, \odot)$ is a ring.

SELF ASSISMENT EXERCISE 8

$Z_2 = \{\bar{0}, \bar{1}\}$, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\therefore Z_2 \times Z_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}) (\bar{0}, \bar{2}), (\bar{1}, \bar{0}) (\bar{1}, \bar{2})\}$.

Thus, the tables are

+	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$
$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{0})$
$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$
$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$
$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{0},\bar{0})$
$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$

·	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{1}.\bar{2})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$
$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$
$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{1})$
$(\bar{1}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{0})$	$(\bar{1}.\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{1}.\bar{0})$

$(\bar{1}.\bar{1})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{1})$	$(\bar{0}.\bar{2})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{1})$	$(\bar{0}.\bar{2})$
$(\bar{1}.\bar{2})$	$(\bar{0}.\bar{0})$	$(\bar{0}.\bar{2})$	$(\bar{0}.\bar{1})$	$(\bar{1}.\bar{0})$	$(\bar{1}.\bar{2})$	$(\bar{1}.\bar{1})$

SELF ASSISMENT EXERCISE 9

Note that + and . are binary operations on {0}. The properties R1 – R6 are invially satisfied.

Now, suppose a singleton {a} is a ring. Then this must contain the additive identity).
Thus, {a} = {0}.

SELF ASSISMENT EXERCISE 10

We know that $a + 0 = a \forall a \in R$. But, by Theoren 1 we know that $a. 0 = 0$. Thus, $a = 0 \forall a \in R$.
That is, R = {0}

SELF ASSISMENT EXERCISE 11

Since $(a+b)^1 = a^1 + b^1$, the statement is true for n = 1. Assume that the equality is true for n = m, i.e.,

$$(a+b)^m = a^m + {}^mC_1 a^{m-1}b + \ldots + {}^mC_{m-1}\, ab^{m-1} + b^m.$$

Now, $(a+b)^{m+1} = (a+b)\,(a+b^m = (a+b)\,(\sum_{k=0}^{m} {}^mC_k\, a^{m-k}\, b^k)$

$= \sum_{k=0}^{m} {}^mC_k\, a^{m-k+1}\, b_k + \sum_{k=0}^{m} {}^mC_k\, a^{m-k}\, b^{k+1}$, by distributivity.
$= (a^{m+1} + {}^mC_1\, a^{m+1-1}\, b + {}^mC_2\, a^{m+1-2}\, b^2 + \ldots + {}^mC_m\, ab^m)$
$\quad + ({}^mC_0\, a^m b + {}^mC_1\, a^{m-1}\, b^2 + \ldots {}^mC_{m-1}\, ab^m + b^{m+1})$
$= a^{m+1} + ({}^mC_1 + {}^mC_0)\, a^{m+1-1}\, b + \ldots + ({}^mC_k + {}^mC_{k-1})\, a^{m+1-k}b^k + \ldots + b^{m+1}$
$= a^{m+1} + {}^{m+1}C_1\, a^{m+1-1}\, b + \ldots + {}^{m+1}C_k a^{m+1-k}b^k + \ldots + {}^{m+1}C_m\, an^m + b^{m+1}$
(Since ${}^mC_k + {}^mC_{k-1} = {}^{m+1}C_k$)

Thus, the equality is true for n = m + 1 also.

Hence, by the p[principle of induction, it is true for all n.

SELF ASSISMENT EXERCISE 12

Let e and e' be two multiplicative identity elements of R. then
$e = e.\ e'$, since e is multiplicative identity.
$= e'$, since e is multiplicative identity.
Thus, $e = e'$, i.e., the mtliplicative identity of R is unique.

SELF ASSISMENT EXERCISE 13

for n = 1, nZ = Z is a commutative ring with identity 1.
$\forall$ n > 1, nZ is commutative, but without identity.

Zn is commutative with identity $\bar{1}$.
Z + iZ is commutative with identity 1 + i0.
$\wp$(X) is commutative with identity X, since A $\cap$ X = A $\forall$ A $\subseteq$ X.
C{0, 1} is commutative with identity : {0, 1} $\rightarrow$ R: 1 (x) = 1
End A is not commutative. It has identity 1_A: A $\rightarrow$ A: 1_A(x) = x.

SELF ASSISMENT EXERCISE 14

Since a $\odot$b = b$\odot$ a $\forall$ a, b $\in$ R, $\odot$is commutative. Also, a $\odot$0 = a $\forall$ a$\in$ R.
Thus, 0 is the multiplicative identity.

SELF ASSISMENT EXERCISE 15

you must first check that the set satisfies R1-R6.
Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity.
Then you should check that AB = BA for any two elements A and B.
thus, the ring is commutative. It has identity $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$.

SELF ASSISMENT EXERCISE 16

for any a $\in$ R, a^2 = a.
In particular, $(2a)^2$ =2a $\Rightarrow$ $4a^2$ = 2a $\Rightarrow$ 4a = 2a $\Rightarrow$ 2a = 0 $\Rightarrow$ a = -a.

Now, for any a, b $\in$ R, a + b $\in$ R.
$\therefore$ $(a + b)^2$ = a + b $\Rightarrow$ a^2 + ab + ba + b^2 = a + b
$\Rightarrow$ a _ ab + ba + b = a + b, since a^2 = a and b^2 = b
$\Rightarrow$ ab = - ba
$\Rightarrow$ ab = ba, since – ba = ba.
Thus, R is commutative.

6.0 TUTOR MARKED ASSIGNMENT

1) Show that the set of matrices is a commutative ring with unity.
2) Let R be a Boolean ring,(i.e a^2 = a $\forall$ a$\in$ R). Show that a= -a for every a$\in$ R. Hence show that R must be commutative.

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra

Birkhaff and Melhnew(1972): A Survey of Modern Algebra.

UNIT 2 SUBRINGS AND IDEALS

CONTENTS

1.0 INTRODUCTION

In this unit we will study various concepts in ring theory corresponding to some of those that we discussed in group theory. We start with the notion of a subring, which corresponds to that of a subgroup as you may have guessed already.

Then we take a close look at a special kind of subgring, 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 realize 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 will you be comfortable in the future unit of this course.

2.0 OBJECTIVES

After reading this unit you should be able to

- give examples of subgrings and ideals of some familiar rings;
- check whether a subset of a ring is a subgring or not;
- check whether a subset of a ring is an ideal or not;
- define and give examples of quotient ring.

3.0 MAIN CONTENT

3.1 Subrings

In Unit 3 of MTH 211, we introduced you to the concept of subgroups of a group. In this section we will introduce you to an analogous notion for rings. Remember that **for us a ring means a commutatiove 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 a subring of Q, as you will now realize.

Definition: Let (R +,.) be a ring and S be 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, using Example 1 unit 1 of this module 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 will 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 $a \in S$, $-a \in S$.

If S satisfies these three conditions, then S is a subring of R. so we have an alternative definition for 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 of MTH 211, that $(S; +) \leq (R, +)$ if $a - b \in S$ whenever $a, b \in S$. This observation allow 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 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 satisfies (a) and (b). now S is a subring of R iff$(S, +) \leq (R,+)$ and S is closed under multiplication, i.e. if (a) and (b) hold.

So, we have proved the theorem.

This theorem allows us a neat way of showing that a subnset is a subring..

Let us look at some exmples.
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 $Q + \sqrt{2Q} = \{\alpha + \sqrt{2\beta \mid \alpha, \beta \in Q}\}$.

The following exercise will give you some more examples of subrings.

SELF ASSISMENT EXERCISE 1

Show that R is a subring of C, Z + iZ is a subring of C and Q + $\sqrt{2Q}$ is a subring of R.

Now, let us look at some examples of subring other than the sets of numbers.

Example 1: Consider Z_6, the ring of integers modulo 6. show, that $3Z_6$ = {3.0, 3.1……, 3.5} is a subring of Z_6

Solution: firstly, do you agree that $3Z_6 = \{\bar{0}, \bar{3}\}$? Remember that $\bar{6} = \bar{0}, \bar{9} = 3$, and so on.

Also, $\bar{0} - \bar{3} = -\bar{3} = \bar{3}$. Thus, $x - y \in 3Z_6$ is a subring of Z_6.

Example 2: Consider the ring $\wp(X)$ given in Example 4 if unit 1 of this module . show that S = {ø, X} is a subring of $\wp(X)$.

Solution: Note that $A \Delta A = ø \ \forall A \in \wp(X)$. $\therefore A = -A$ in $\wp(X)$.
Now to apply theorem 1 we first note that S is non-empty.
Next, $ø \Delta ø = ø \in S$, $X \Delta X = ø \in S$,
$ø \Delta X = X \in S$, $ø \cap ø = ø \in S$, $X \cap X = X \in S$, $ø X = ø \in S$.
Thus, by Theorem 1 , S is a subring of $\wp(X)$.

Try a related exercise now.

SELF ASSISMENT EXERCISE 2

Let $A \subsetneq X$, $A \neq \emptyset$. Show that $S = \{\emptyset, A, A^c, X\}$ is a subring of $\wp(X)$.

E 2 shows that 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 3: show that $S = \{n, 0) | n \in Z\}$ is a subring of Z X Z. Also show that $D = \{(n, n) \mid n \in Z\}$ is a subring of Z X Z.

Solution: You can recall the ring structure of Z^2 from example 8 of unit 1. 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 X Z is (1, 1).

But the identity of its subring Z X {0} is (1.0).

Try the following exercise now.

SELF ASSISMENT EXERCISE 3

show that $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \, a, b \in Z \right\}$ is a subring of

$R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\}$. Does S have a unit element?

If yes, then is the unit element the same as that of R?

Now let us look at an example which throws up several subrings of any ring.

Example 4: Let R be a ring and $a \in R$. Show that the set $aR = \{ ax \mid x \in R\}$ is a subring of R.

Solution: Since $R \neq \emptyset$, $aR \neq \emptyset$. 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 4 we can immediately say that $\bar{m}Z_n$ is a subring of Z_n $\forall \bar{m} \in Z_n$. This also shows us a fact that we have already seen: nZ is a subring of Z $\forall n \in Z_n$.

Try these exercises now.

SELF ASSISMENT EXERCISE 4

For any ring R, show that {0} and R are its subrings.

SELF ASSISMENT EXERCISE 5

Show that if A is a subring of B and B is a subring of C, then A is a subring of C.

SELF ASSISMENT EXERCISE 6

Give an example of a subset of Z which is not a subring.

SELF ASSISMENT EXERCISE 7

Is very useful. For instance, E1 and E5 tell us that $Q + \sqrt{2Q}$ is a subring of C.

Now let us look at some properties of subrings. From unit 3 you know that the intersection of two or more subgroup is a subgroup. The following result says that the same is true for subrings.

Theorem 2: Let S_1 and S_2 be subring of a ring R. Then $S_1 \cap S_2$ is also a subring of R.

Proof: Since $0 \in S_1$ and $0 \in S_2$, $0 \in S_1 \cap S_2$. $\therefore S_1 \cap S_2 \neq \emptyset$.

Now, let X, $y \in S_1 \cap S_2$. Then x, $y \in S_1$ and z, $y \in S_2$. thus, by Theorem 1, x – y and xy are in S_1 as well as in S_2, 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 subring of a ring R is a subring of R.**

Now consider the union of subrings of a ring. So you think it will be a subring? Consider the following exercise.

SELF ASSISMENT EXERCISE 8

You know that Z + iZ and Q are subrings of C. Is their union a subring of C? why?

Now let us look at the Cartesian product of subrings.

Theorem 3: Let S_1 and S_2 be subring of the rings R_1 and S_2, respectively. Then S_1 X S_2 is a subring of R_1 X R_2.
Proof: since S_1 and S_2 are subrings of R_1 and R_2, $S_1 \neq \emptyset$ and $S_2 \neq \emptyset$. $\therefore S_1$ X $S_2 \neq \emptyset$.

Now, let (a, b) and $(a', b') \in S_1$ X S_2. Then a, $a' \in S_1$ and b, $b' \in S_2$. 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 R2 here, for convenience.) Hence, $(a, b) - (a', b') = (a - a', b - b') \in S_1$X S_2, and

$(a,b) . (a', b') - a a', b b') \in S_1$ X S_2.

You can use this result to solve the following exercise.

SELF ASSISMENT EXERCISE 9

Obtain two proper non-trivial subrings of Z X R (i.e., subrings which are neither zero nor the whole ring).

Let us now discuss an important class of subrings.

3.2 Ideals

In Module 1, you 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 section we will discuss a class of subrings that will help us to do so. These subrings are called Ideals. While exploring algebraic number theory, the 19^{th} 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 1 of R. As (R +) is an abelian group, the subgroup, 1 is normal in (R,+), and hence the set R/1 = {a +1|

$a \in R\}$, of all cosets of 1 in R, is a group under the binary operation + given by
$(a + 1) + (b + 1) = (a + b) + 1$
for all $a + 1, b + 1 \in R/1$. we wish to define. on R/1 so as to make R/1 a ring. You may think that the most natural way to do so is to define
$(a + 1) . (b + 1) = ab + 1 \forall a + 1, b + 1 \in R$

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., $\sqrt{2} + Z = 0 + Z$, 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/1 if we add some conditions on 1. What should these conditions be? To answer this, assume that the multiplication in (2) is well defined.

Then, $(r + 1) . (0 + 1) = r.0 + 1 = 0 + 1 = 1$ for $r \in R$.

Now, you know that if $x \in 1$, then $x + 1 = 0 + 1 = 1$
As we have assumed that is well defined, we get
$(r + 1) . (x + 1) = (r + 1) . (0 + 1) = 0 + 1$ whenever $r \in R, x \in 1$.
i.e., $rx + 1 = 1$ whenever $r \in R, x \in 1$.

Thus, $rx \in 1$, whenever $r \in R, x \in 1$.
So, if. is well defined we see that the subring 1 must satisfy the additional condition that $rx \in 1$ whenever $r \in R$ and $x \in 1$.

In sec3.3 we will prove that this extra condition on 1 is enough to make the operation, a well defined one and (R/1, +,.) a ring. In this section we will consider the subrings 1 of R on which we impose the condition
$rx \in 1$ whenever $r \in R$ and $x \in 1$.

Definition: We call a non-empty subset 1 of a ring (R, +,.) an ideal of R if
i) $a – b \in 1 \forall a, b \in 1$, and
ii) $ra \in 1$ for all $r \in R$ and $a \in 1$.

Over here we would like to remark that we are always assuming that our rings are commutative. In the cse of non-commutative rings the definition of an ideal is partially modified as follows.
A nomn-empty subset 1 of a non-commutative ring R is an ideal if

i) $a - b \in 1 \forall a, b \in 1$, and
ii) $ra \in 1$and $ar \in 1 \forall a \in 1\ r \in R$.

Now let us consider some examples. In E 4 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 1 of a ring R is such that $1 \neq R$, then 1 is called **a proper ideal of R**.

For example, if $n \neq 0, 1$, then the subring $nZ = \{nm|\ m \in Z\}$ is a proper non-trivial ideal of Z. This is because for any $z \in Z$, $z(nm) = n(zm) \in nZ$.

Try this exercise now

SELF ASSISMENT EXERCISE 10

Show that $\{\bar{0} \quad \bar{3}\}$ and $\{\bar{0}, \bar{2}, \bar{4}\}$ are proper ideads of Z_6.

Now let us consider some more examples of ideals.

Example 5: Let X be an infinite set. Consider 1, the class of all finite subsets of X. Show that 1 is an ideal of $\wp(X)$.

Solution: $1 = \{A|\ A$ is a finite subset of $X\}$. Note that
i) $ø \in 1$, i.e., the zero element of $\wp(X)$. is in 1.
ii) $A - B = a + (\_\ B) = A + B$, as $B = -B$ in $\wp(X)$.
$= A \Delta B$.

Thus, if $A, B \in 1$, then $A - B$ is again a finite subset of X, and hence $A - B \in 1$./

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, $A \in 1$ and $B \in \wp(X)$. $\Rightarrow AB \in 1$.

Hence, 1 is an ideal of $\wp(X)$.

Example 6: Let X be a set and Y be a non-empty of X. Show that $1 = \{A \in \wp(X)|\ A \cap Y = ø\}$ is an ideal of $\wp(X)$.

In particular, if we take $Y = \{x_0\}$, where x_0 is a fixed element of X, then $1 = \{A \in \wp(X) \mid x_0 \notin A\}$ is an ideal of $\wp(X)$.
Solution: Firstly, $ø \in 1$.

Secondly, $\forall A,. B \in 1$,
$(A - B) \cap Y = (A \Delta B) \cap Y = (a \cap Y) \quad (B \cap Y) = ø \Delta ø = ø$, so that $A - B \in 1$

Finally, for $A \in 1$ and $B \in \wp(X)$,
$(AB) \cap Y = (A \cap B) \cap Y = (A \cap Y) \cap B = ø \cap B = ø$, so that $AB \in 1$.
Thus, 1 is an ideal of $\wp(X)$.

Example 7: Consider the ring C[0, 1] given in Example 6 of Unit 9.
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 **o** is defined by **0**(x) = 0 for all $x \in [0,1]$.
Sinc $0(1/2) = 0$, $\mathbf{0} \in M$.

Also, if $f, \in M$ and $g \in C[0,1]$ then $(fg)(1/2) = f(1/2)\, g(1/2) = 0\, g(1/2) = 0$, so $fg \in M$.

Thus, M is an ideal of C[0,1].

When you study Unit 11, you will see that M is the kernel of the homomorphism
Ø: C[0, 1] → R: ø(f) = f(1/2).

Now you can try an exercise that is a generalization of example 7.

SELF ASSISMENT EXERCISE 11

Let $a \in [0, 1]$. Show that the set
$1_a = \{ f \in C[0, 1] \mid f(a) = 0 \}$ is an ideal of C[0, 1].

In the next exercise we ask you to look at the subring in Example 4.

SELF ASSISMENT EXERCISE 12

Let R b a ring and $a \in R$. show that Ra is an ideal of R.

Now that you've solved E 11, solving E 9 is a matter of seconds! Let us see if E 11 can be generalized.

Example 8: For any ring R and $a_1, a_2 \in R$, show that
$Ra_1 + Ra2 = \{x_1a_1 + x_2, x_2 | \in R \}$ is an ideal of R.

Solution: Firstly, $0 = 0a_1 + 0a_2$. $\therefore 0 \in Ra_1 + ra_2$.
Next, $(x_1a_1 + x_2a_2) - (y_1a_1 + y_2a_2)$
$= (x_1 - y_1)a_{1 + (x}2 - y_2)a_2 \in Ra_1 + Ra_2 \quad \forall x_1, x_1, y_1, y_2 \in R$.

Finally, for $r \in R$ and $x_1a_1 + x_2a_2 \in Ra_1 + + Ra_2$,
$R(x_1a_1 + x_2a_2) = rx_1a_1 \in Ra_1 + Ra_2$.
Thus, $Ra_1 + Ra_2$ is an ideal of R.

This method of obtaining ideals can extended to give ideals of the form $\{x_1a_1 + {}_2a_2 + \ldots + x_na_n \mid x_1 \in R\}$ for fixed elements $a_1, \ldots, a_n$ of R. such ideals crop up again and again in ring theory. We give them a special name.

Definition: Let $a_1, \ldots, a_n$ be given elements of a ring R. Then the ideal generated by $a_1, \ldots, a_n$ is
$Ra_1 + Ra_2 + \ldots + Ra_n = \{ x_1a_1 + x_2a_2 + m + x_na_n \mid x_1 \in R\}$. $a_1, \ldots, a_n$ are called the generators of this ideal.

We also denote this ideal by $<a_{1,}\, a2_{,\ldots..,}\, an>$
When n = 1, the ideal we get is called a **principal ideal**. Thus, if $a \in R$, then Ra = is a principal ideal of R. In the next block you will be using principal ideals quite a lot.

Now an exercise on principal ideals.

SELF ASSISMENT EXERCISE 13

Let R be a ring with identity\. Show that <1> = R.

SELF ASSISMENT EXERCISE 14

Find the principal ideals of Z_{10} generated by $\bar{3}$ and $\bar{5}$.

Now we look at a special ideal of a ring. But, to do so we need to give a definition.

Definition: An element a of a ring R is called **nilpotent** if there exists a positive integer n such that $a^n = 0$.

For Example, $\bar{3}$ and $\bar{6}$ are nilpotent elements of Z_9, since $\bar{3}^2 = \bar{9} = \bar{0}$ and $\bar{6}^2 = \bar{36} = \bar{0}$. Also, in any ring R, 0 is a nilpotent element.

Now consider the following example.

Exmple 9: Let R be a ring. Show that the set of nilpotent element of R is an ideal of R. This ideal is called the **nil radical of R**.

Solution: Let $N = \{a \in R \mid a^n = 0$ for some positive integers $n\}$. Then $0 \in N$.

Also, if $a, b \in N$, then $a^n = 0$ and $b^m = 0$ for some positive integers m and n.

Now, $(a - b)^{m+n} = \sum_{r=0}^{m+n} {}^{m+n}C_r \, a_r(- b)^{m+n-r}$ (see E 11 of Unit 9.

For each $r = 0, 1, \ldots, m + n$, neither $r \geq n$ or $m + n - r \geq m$, and hence, either $a^r = 0$ or $b^{m+n-r} = 0$. Thus, the term $a^r b^{m+n-r} = 0$. So $(a- b)^{m+n} = 0$. Thus, $a (ar)^n = a^n r^n = 0$, i.e., $ar \in N$.

Finally, if $a \in N$, $a^n = 0$ for some positive integer n, and hence, for any $r \in$, $(ar)^n = a^n r^n = 0$, i.e., $ar \in N$.

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, $N = \{\bar{0}, \bar{2}\}$.

Try the following exercises now.

SELF ASSISMENT EXERCISE 15

Find the nil radicals of Z_8 and $\wp(X)$.

SELF ASSISMENT EXERCISE 16

Let R be a ring and $a \in R$. show that $1 = \{r \in R \mid ra = 0 \}$ is an ideal of R. (This ideal is called the annihilator of a.)

By now you must be familiar with the concept of ideals. Let us now obtain some results about ideals.

Theorem 4: let R be a ring with identity 1. If 1 is an ideal of R and $1 \in 1$, then $1 = R$.

Proof: We know that $1 \subseteq R$. We want to prove that $R \subseteq 1$. Let $r \in R$. Since $1 \in 1$ and 1 is an ideal of R, $r = r.1 \in 1$. So, $R \subseteq 1$. Hence $1 = R$.
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 $1 \in Q$ and $Q \neq R$, 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.

Theorem 5: If I and J are ideals of a ring R, then

a) $I \cap J$,
b) $I + J = \{a + b | a \in I \text{ and } b \in J\}$, and
c) $IJ = \{x \in R \mid x \text{ is a finite sum } a_1b_1 + \ldots a_mb_m$, where $a_i \in I$ and $b_i \in J\}$ and ideals of R.

Proof: a) From Theorem 2 you know that $I \cap J$ is a subring of R. Now, if $a \in I \cap J$, then $a \in I$ and $a \in J$. Therefore, $ax \in I$ and $ax \in J$ 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, $0 = 0 + 0 \in I + J \therefore I+J \neq \phi$.
Secondly, if $x\ y \in I + J$, 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, $IJ \neq \text{ø}$ and $J \neq \text{ø}$.
Next, let $x, y \in IJ$. Then $x = a_1b_1 + \ldots + a_mb_m$ and
$y = a'_1b'_1 + \ldots + a'_nb'_n$ for some $a_1, \ldots, a$ ---------- $\in I$ and $b_1, \ldots, b_m, b_1$

$\therefore x - y = (a_1b_1 + \ldots + a_mb_m) - (a'_1b'_1 + \ldots + a'_nb'_n)$
$= a_1b_1 \ldots + a_mb_m + (-a'_1)b'_1 + \ldots + (-a'_n)b'_n$
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 $x = a^1b^1 + \ldots + a_n b_n$ with $a_1 \in I$ and $b_1 \in J$. Then, for any $r \in R$
$xr = (a_1b_1 + \ldots a_nb_n)r = a_1(b_1r) + \ldots + a_n(b_nr)$,
which is a finite sum of elements of the form ab with $a \in I$ and $b \in J$.
(Note that $b_1 \in J \Rightarrow b_1r \in J$ 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 ∈ I, b∈ J}, then IJ need not even be a subring, leave alone being an ideal. This is because if x, y ∈ IJ, then with this definition of IJ it is not necessary that x - y∈ IJ.

Let us now look at the relationship between the ideals obtained in Theorem 5. let us first look at the following particular situation:
R = Z, I = 2Z and J = 10Z. Then I ∩ J = J, since J ⊆I. Also, any element of 1 + J is of the form x = 2n + 10m, where n, m ∈ Z. thus, x = 2(n + 5m) ∈ 2Z. on the other hand 2Z = I ⊆ I + J. thus, I + J = < 2, 10> = <2>. Similarly, you can see that IJ = <20>.
Note that IJ ⊆ I ∩ J ⊆ I ⊆ I + J.
In fact, these inclusions are true for any I and J (see E 16). We show the relationship in Fig. 1

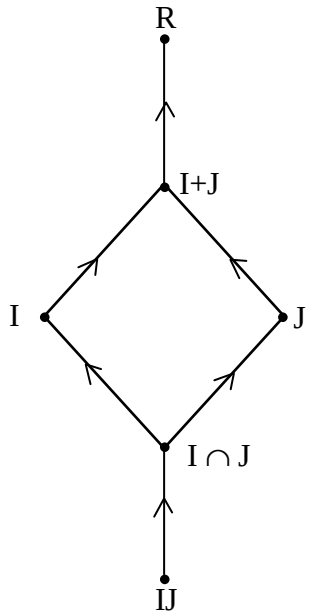


Fig. 1: The ideal hierarchy!

SELF ASSISMENT EXERCISE 17

If I and J are ideals of a ring R, then show that

a) IJ ⊆ I ∩ J ⊆ I ⊆ I + J
and IJ ⊆ ∩ J ⊆ J ⊆ I + J;

b) I + is the smallest ideal containing both the ideals I and J, i.e., if A is an ideal of R containing both I and J, then A must contain I + J;
c) I ∩ J is the largest ideal that is contained in both I and J;
d) If I ∈ R and I + J = R, then IJ = I ∩ J, i.e., if top two of fig. 1 are equal, then so are the lowest two.

Let us now go back to what we said at the beginning of this section – the importance of ideal.

3.3 Quotient Rings

In Unit 5 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 define a similar consept for rings. At he beginning of sec---- 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
$(x + I) + (y + I) = (x + y) + I$ and
$(x + I) . (y + I) = xy + I \ \forall\ x + I, y + I \in R/I$,
then the subring I should satisfy the extra condition that $rx \in I$ whenever $\in R$ 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 $a = a' = c$ similarly, $b - b' \in I$, 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.
$\therefore ab + I = a'b' + I$.
Thus, . is well defined on R/I.

Now our aim is to prove the following result.

Theorem 6: 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
$(x + I) . (y + I) = xy + I \ \forall x, y \in R$.

Proof: As we have noted earlier, (R/I, +) is an abelian group. So to prove that R/I is a ring we only ned to check that . is commutative, associative and distributive over +.

Now,
i) . is commutative: $(a + I). (b + I) = ab + I = ba + I = (b + I). (a + I)$ for all $a + I, b + I \in R/I$.

ii) . is associative: $\forall\ a, b, c \in R$
$((a + I). (b + I)). (c + I) = (ab + I). (c + I)$
$= (ab)c + I$

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

iii) Distributive law: let a + I, b + I, c + I ∈ R/I. then
(a + I). ((b +I) + (c+ I)) = (a + I) [(b + c) + I}
= a(b + c) + I
= (ab + ac) + I
= (ab + I) + (ac +I).
= (a + I). (b + I) + (a + I). (c + I)

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 and I'.

Example 10: Let R = Z and I = nZ. What is R/I?

Solution: In Sec------- you have seen that nZ is an ideal of Z. From Unit 2 you know that
Z/nZ = {nZ, I + nZ, + nZ, …, (n – 1) + nZ}

= $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$, 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 11: 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 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 + I = $\{\bar{0}, \bar{4}\}$, 1 + 1 = $\{\bar{1}, \bar{5}\}$, 2 + 1 = $\{\bar{2}, \bar{6}\}$, 3 + 1 = $\{\bar{3}, \bar{7}\}$.

The Cayley tables for + and . in R/I are

+	$\bar{0}+1$	$\bar{1}+1$	$\bar{2}+1$	$\bar{3}+1$
$\bar{0}+1$	$\bar{0}+1$	$\bar{1}+1$	$\bar{2}+1$	$\bar{3}+1$
$\bar{1}+1$	$\bar{1}+1$	$\bar{2}+1$	$\bar{3}+1$	$\bar{0}+1$
$\bar{2}+1$	$\bar{2}+1$	$\bar{3}+1$	$\bar{0}+1$	$\bar{1}+1$
$\bar{3}+1$	$\bar{3}+1$	$\bar{0}+1$	$\bar{1}+1$	$\bar{2}+1$

•	$\bar{0}+1$	$\bar{1}+1$	$\bar{2}+1$	$\bar{3}+1$
$\bar{0}+1$	$\bar{0}+1$	$\bar{0}+1$	$\bar{0}+1$	$\bar{0}+1$
$\bar{1}+1$	$\bar{0}+1$	$\bar{1}+1$	$\bar{2}+1$	$\bar{3}+1$
$\bar{2}+1$	$\bar{0}+1$	$\bar{2}+1$	$\bar{0}+1$	$\bar{2}+1$
$\bar{3}+1$	$\bar{0}+1$	$\bar{3}+1$	$\bar{2}+1$	$\bar{1}+1$

Try this exercise now.

SELF ASSISMENT EXERCISE 18

Show that if R is a ring with identity, then R/I is a ring with identity fir any ideal 1 of R.

SELF ASSISMENT EXERCISE 19

If R is a ring with identity 1 and I is an ideal of containing 1, then what does R/I look like?

SELF ASSISMENT EXERCISE 20

Let N be the nil radical of R. Show that R/N has non-zero nilpotent elements.

4.0 CONCLUSION

You will realize the utility and importance of quotient rings after we discuss homomorphisms in the next unit and when we discuss polynomial rings (Block 4).

Now let us briefly summarize what we have done in this unit.

5.0 SUMMARY

In this unit we have discussed the following points, with the assumption that all rings are commutative.

1) The definition and examples of a subring.
2) The proof and use of the fact that a non-empty subset S of a ring R is subring of R iff $x - y \in S$ and $xy \in S \ \forall x, y \in S$.
3) The intersection of subring of a ring is a subring of the ring.

4) The Cartesian product of subrings is a subring of the Cartesian product of the corresponding rings.
5) The definition and examples of an ideal.
6) The definition of an ideal generated by n elements.
7) The set of nilpotent elements in a ring is an ideal of the ring.
8) If I is an ideal of a ring R with identity and $I \in I$, = R.
9) If I and J are ideal of a ring R, then $I \cap J$, I + J and IJ are also ideals of R.
10) The definition and examples of a quotient ring.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

$\forall$ x, y $\in$ R, x – y $\in$ R and xy $\in$ R. Thus, R is a subring of C. Similarly, you can check the other cases.

SELF ASSISMENT EXERCISE 2

Clearly, S is non-empty.
Also, for any x, y $\in$ S, x – y = x Δ y
(As pointed out in Example 2).
You can check that x Δ y $\in$ S $\forall$ x, y $\in$ S.
Also, for any x, y $\in$ S, xy = x $\cap$ y $\in$ S, as you can check.
Thus, S is a subring of $\wp$(X).

SELF ASSISMENT EXERCISE 3

Firstly, S $\neq$ ø. Secondly, for any A = $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and C = $\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ in S,

A – C = $\begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$ and AC = $\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$.

Thus, S is a subring of R.

The unit element of S = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = the unit element of R.

SELF ASSISMENT EXERCISE 4

Both {0} and R are non-empty and satisfy (a) and (b) of Theorem 1.

SELF ASSISMENT EXERCISE 5

Since A is a subring of B, $A \neq \emptyset$ and $\forall x, y \in A$, $x - y \in A$ and $xy \in A$. here the addition and multiplication are those defined on B. but these are the same as those defined on C since B is a subring of C. Thus, A satisfies Theorem 1, and hence is a subring of C.

SELF ASSISMENT EXERCISE 6

There are several examples. We take {I}. in fact, any finite subset of Z, apart from {0}, will do.

SELF ASSISMENT EXERCISE 7

$1 + i$ and $\frac{1}{2}$ are elements of the union.

But $1 + i - \frac{1}{2} = \frac{1}{2} + i \notin Z + iZ \cup Q$ is not a subring of C.

SELF ASSISMENT EXERCISE 8

2Z X R, 3Z X {0} are two among infinitely many examples.

SELF ASSISMENT EXERCISE 9

note that the two sets are $\bar{3}Z_6$ and $\bar{2}Z_6$. From Example 4 you know that they are subrings of Z_6. Now, by element wise multiplication you can check that $rx \in \bar{3}Z_6 \forall r \in Z_6$ and $x \in \bar{3}Z_6$. (for instance, $\bar{5}.\bar{3} = \overline{15} = \bar{3} \in \bar{3}Z_6$.)

You can similarly see that $rx \in \bar{2}Z_6 \forall r \in Z_6$ $x \in \bar{2}Z_6$.

Thus, $\bar{3}Z_6$ and $\bar{2}Z_6$ are ideals of Z_6.

SELF ASSISMENT EXERCISE 10

$1_a \neq \emptyset$, since $0 \in 1_a$

$f, g \in 1_a \Rightarrow (f - g)(a) = f(a) - g(a) = 0 \Rightarrow f - g \in 1a.$

$f \in 1_a, g \in C[0, 1] \Rightarrow (fg)(a) = f(a)\, g(a) \backslash= 0.g(a) = 0 \Rightarrow fg \in 1_a.$

$\therefore 1_a$ is an ideal of C[0, 1].

SELF ASSISMENT EXERCISE 11

Ra is a subring of R (see Example 4).

Also for $r \in R$ and $xa \in Ra$,

$R(xa) = (rx)a \in Ra.$

$\therefore$ Ra is an ideal of R.

SELF ASSISMENT EXERCISE 12

We know that <1> $\subseteq$ R. we need to show that R $\subseteq$ <1>.
Now, for any r$\in$ R, r = r.1 $\in$ <1>. Thus, R $\subseteq$ <1>.
$\therefore$ R = <1>.

SELF ASSISMENT EXERCISE 13

$\bar{3}Z_{10} = \{\bar{3}x \mid x \in Z_{10}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$
$= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{2}, \bar{5}, \bar{8}, \bar{1}, \bar{4}, \bar{7}\}$
$= Z_{10.}$
$\bar{5}Z_{10} = \{\bar{0}, \bar{5}\}$.

SELF ASSISMENT EXERCISE 14

Let the nil radical of Z_8 be N. then $\bar{0} \in$ N.
$\bar{1} \notin$ N since $\bar{1}^n = \bar{1} \neq \bar{0}$ for all n.
$\bar{2}^3 = \bar{0} \Rightarrow \bar{2} \in$ N.
$\bar{3}^n \neq \bar{0} \forall$ n. $\therefore \bar{3} \notin$ N.
Similarly, you can check that $\bar{4}, \bar{6} \in$ N and $\bar{5}, \bar{7} \notin$ N.
$\therefore$ N = $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.
For any A $\in \wp$(X), A^n = A $\cap$ A $\cap$ …. $\cap$ A = A $\forall$ n.
Thus, A^n = ø iff A = ø. Thus, the nil radical of $\wp$(X) is { ø}.

SELF ASSISMENT EXERCISE 15

Firstly, 1 $\neq$ ø since 0 $\in$ 1.
Secondly, r, s $\in$ 1 $\Rightarrow$ ra = 0 = sa $\Rightarrow$ (r – s)a = 0 $\Rightarrow$ r – s $\in$ 1.
Finally, r $\in$ 1 and x $\in$ R $\Rightarrow$ (rx)a = x(ra) = x0 = 0 $\Rightarrow$ rx $\in$ 1.
Thus, 1 is an ideal of R.

SELF ASSISMENT EXERCISE 16

a) For any a $\in$ I and b $\in$ J, ab $\in$ I and ab $\in$ J.
Thus, ab$\in$ I $\cap$ J. since I $\cap$ J is an ideal, any finite sum of such elements will lso be in I$\cap$ J. Thus, IJ $\subseteq$ I $\cap$ J.
Clearly, I$\cap$ J $\subseteq$ I and I$\cap$ J$\subseteq$ J.
Also, I $\subseteq$ I + J, J $\subseteq$ I + J is obvious.

b) Let A be an ideal of R containing I as well as J. Then certainly I + J $\subseteq$ A. Thus, (b) is proved.

c) Let B be an ideal of R such that $B \subseteq I$ and $B \subseteq J$. Then certainly, $B \subseteq I \cap J$. Thus, (c) is proved.

d) We want to show that $I \cap J \subseteq IJ$.
Let $x \in I$ and $x \in J$.
Since $I \subseteq \in R = I + J$, $I = I + j$, for some $i \in I$ and $j \in J$.
$\therefore x = x, I = xi + xj = ix + xj \in IJ$
Thus, $I \cap J \subseteq IJ$.

SELF ASSISMENT EXERCISE 17

1 + I is the identity of R/I.

SELF ASSISMENT EXERCISE 18

from Theorem 4, you know that I = R.
$\therefore R/I = \{\bar{0}\}$.

SELF ASSISMENT EXERCISE 19

Let $x + N \in R/N$ be a nilpotent element.
Then $(x + N)^n = N$ for some positive integer n.
$\Rightarrow x^n \in N$ for some positive integer n.
$\Rightarrow (n^n)^m = 0$ for some positive integer m.
$\Rightarrow x^{nm} = 0$ for some positive integer nm.
$\Rightarrow x \in N$
$\Rightarrow x + N = 0 + N$, the zero element of R/N.
Thus, R/N has no non-zero nilpotent elements.

6.0 TUTOR MARKED ASSIGNMENT

1. Show that if R is a ring with identity, then R/I is a ring with identity for any ideal I of R
2. Let N be nil radical of R. Show that R/N has no non-zero nilpotent element

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra

UNIT 3 RING HOMOMORPHISMS

CONTENTS

1.0 INTRODUCTION

In Unit 2 you studied about functions between groups that preserved 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 homomorphisms, ideals and quotient rings.

2.0 OBJECTIVES

After reading this unit, you should be able to

- Check whether a function is a ring homomorphism or not;
- Obtain the kernel and image of any homomorphism;
- Give examples of ring homomorphisms and isomorphisms;
- Prove and use some properties of a ring homomorphism;
- State, prove and apply the Fundamental Theorem of Homomorphism for rings.

3.0 MAIN CONTENT

3.1 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 natural to expect a ring homomorphism to preserve the ring structure of its domain. Consider the following definition.

Definition: Let $(R_1, +,.)$ and $(R_2, +,.)$ be two rings and $f: R_1 \rightarrow R_2$ be a map. We say that f is a ring homomorphism if
$f(a + b) = f(a) + f(b)$, 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 $f: R_1 \rightarrow R_2$ 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 homomorphism 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 ring and $f: R_1 \rightarrow R_2$ be a ring homomorphism. Then we define.

i) the image of f to be the set $\text{Im } f = \{f(x) \mid x \in R_1\}$.

ii) the kernel of f to be the set $\text{Ker } f = \{x \in R_1 \mid f(x) = 0\}$.

Note that $\text{Im } f \subseteq R_2$ and $\text{Ker } f \subseteq R_1$.
If $\text{Im } f = R_2$, 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 1: Let R be a ring. Show that the identity map 1_R is a ring homomorphism. What are $\text{Ker } 1_R$ and $\text{Im } 1_R$?

Solution: Let x, y ∈ R. Then
$1_R(x + y) = x + y = 1_R(x) + 1_R(y)$, and
$1_R(xy) = xy = 1_R(x)\ 1_R(y)$.
Thus, $1_R(xy) = xy = 1_R(x)\ 1_R(y)$.
Thus, 1_R is a ring homomorphism.
Ker $1_R = \{x \in R \mid 1_R(x) = 0\}$
$= \{x \in R \mid x = 0\}$
$= \{0\}$
Im $1_R = \{1_R(x) \mid x \in R\}$
$= \{x \mid x \in R\}$
$= R$.

Thus, 1_R is a surjection, and hence an epimorphism.

Example 2: Let s ∈ N, show that the map f: $Z \to Z_s$ given by f(m) = m for all m∈ Z is a homomorphism. Obtain Ker f and Im f also.

Solution: For any m, n ∈ Z,
$f(m + n) = \overline{m + n} = \overline{m+n} = \bar{m} + \bar{n}$ =f(m) + f(n), and
$f(mn) = \overline{mn} = \bar{m}\bar{n} =$ f(n) f(n).
Therefore, f is a ring homomorphism.

Now, Ker $f = \{m \in Z \mid f(m) = \bar{0}\}$
$= \{m \in Z \mid \bar{m} = \bar{0}\}$
$= \{m \in Z \mid m = 0 \pmod s\}$
$= sZ$.
Im $f = \{f(m) \mid m \in Z\}$
$= \{\bar{m} \mid m \in Z\}$
$= Z_s$,
Showing that if an epimorphism.

Example 3: Consider the map f: $Z_6 \to Z_3$: f(n (mod 6)) = n(mod 3).
Show that f is a ring homomorphism. What is Ker f?
Solution: Firstly, for any n, m ∈ Z,
F(n(mod 6) + m(mod 6)) = f((n + m) (mod 6)) = (n + m) (mod 3)
= n(mod 3) + m(mod 3)
= f(n (mod 6)) + f(m(mod 6))

you can similarly show that
f(n(mod 6) . m(mod 6)) = f(mod 6)). f(m(mod 6)).
Thus, f is a ring homomorphism.
Ker f = {n(mod 6) | n ≡ 0(mod 3)} = {n(mod 6) | n ∈ 3Z}
$= \{\bar{0}, \bar{3}\}$, 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 for some exercises.

SELF ASSISMENT EXERCISE 1

If S is a subring of a ring R, then S itself is a ring with the same + and . of R. Show that the inclusion map i: S $\rightarrow$ R: i(x) = x is a homomorphism. What are Ker i and Im i?

SELF ASSISMENT EXERCISE 2

Let R_1 and R_2 be two rings. Define f: $R_1 \rightarrow R_2$: f(x) = 0. Show that f is a homomorphism. Also obtain Ker f and Im f. (This function if called the **trivial homomorphism.)**

SELF ASSISMENT EXERCISE 3

Is f: Z$\rightarrow$ 2Z: f(x) = 2x a homomorphism? Why?

Note that using E1 we know that f: Z $\rightarrow$ Q (or R, or C or Z + iZ) given by f(n) = n is a homomorphism.

Now let us look at some more examples

Example 4: Consider the ring C[0, 1] of all real valued continuous functions defined on the closed interval [0 1].

Define ø: C[0, 1] $\rightarrow$R: ø(f) = f(1/2). Show that ø is a homomorphism.
Solution: Let f and g $\in$ C[0, 1]
Then (f + g) (x) + g(x) and
(fg) (x) = f(x) g(x) for all x $\in$ C[0, 1].
Now, ø(f + g) = (f + g) (1/2) = f(1/2) = f(1/2) = ø(f) + ø(g), and

ø(fg) = (fg) (1/2) = f($\frac{1}{2}$)$g(\frac{1}{2})$ = ø(f) ø(g).
Thus, ø is a homomorphism.

Example 5: Consider the ring R = $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \right.$ a, b $\in$ R $\left. \right\}$ under matrix

addition and multiplication. Show that the map f: Z→R: 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) ∀ n, m ∈ Z. Thus, f is a homomorphism.

Example 6: Consider the ring $\wp(X)$ of Example 4 of unit 9.
Let Y be a non-empty subset of X.

Define f: $\wp(X)$ $\wp(Y)$ by f(A) = A ∩ Y for all A in $\wp(X)$. Show that f is a homomorphism. Does $Y^c \in$ Ker f? What is Im f?

Solution: For any A and B in $\wp(X)$,
f(A Δ B) = f((A\B) ∪ (B\A))
= ((A\B) ∪ (B\A ∩ Y))
= ((A\B) ∩ Y) ∪((B\A) ∩ Y)
= ((A ∩Y)\(B ∩Y)) ∪ ((B ∩ Y)\(A∩ Y))
= (f(A)\f(B)) ∪ (f(B) \f(A))
= f(a) Δ f(B), and
f(A ∩ B) = (A ∩ B) ∩ Y
= (A ∩ B) ∩ (Y ∩Y
= (A ∩ Y) ∩ (B ∩ Y), since ∩ is associative and commutative
= f(A) ∩ f(B).

So, f is a ring homomorphism from $\wp(X)$ into $\wp(Y)$.
Now, the zero element of $\wp(Y)$ is ø . Therefore,
Ker f = {A∈ $\wp(X)$ | A ∩ Y = ø } ∴ $Y^c \in$ Ker f.

We will show that f is surjective.
Now, Im f = {A ∩ Y | A ∈ $\wp(X)$}

Thus, Im f ⊆ $\wp(Y)$. To show that $\wp(Y) \subseteq$ Im f, take any B ∈ $\wp(Y)$.
Then B ∈ $\wp(X)$ and f(B) = B ∩ Y = B. Thus, B∈ Im f.
Therefore, Im f = $\wp(Y)$.
Thus, f is an onto homomorphism.
The following exercises will give you some more examples of homomorphisms.

SELF ASSISMENT EXERCISE 4

Let A and B be two rings. Show that the projection map

P:AXB $\rightarrow$ A: p(x, y) = x is a homomorphism. What are Ker p and Im p?

SELF ASSISMENT EXERCISE 5

Is f: Z + $\sqrt{2}$Z $\rightarrow$ Z+$\sqrt{2}$Z f(a+$\sqrt{2}$ b) = a–$\sqrt{2}$ b a homomorphism?

SELF ASSISMENT EXERCISE 6

Show that the map ø :C[0, 1] R X R: ø If) = (f(0), f(1)) is a homomorphism.

Having discussed many examples. Let us obtain some basic results about ring homomorphisms.

3.2 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: $R_1 \rightarrow R_2$ 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 os unit 6 to get the result.

In the following exercise we ask you to prove another property of homomorphisms.

SELF ASSISMENT EXERCISE 7

Let: $R_1 \rightarrow R_2$ be an onto ring homomorphism. If R_1 is with identity 1, show that R_2 is with identity f(1).

Now, let us look at direct and inverse images of subrings under homomorphisms. (see Sec---------- for the definition of an inverse image.)

Theorem 2: Let f: $R_1 \rightarrow R_2$ be a ring homomorphism. Then
a) if S is a subring of R_1, f(S) is a subring of ;
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 (see E 8). Let us use Theorem 1 of unit 10.

Firstly, since $T \neq \emptyset$. 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.
To complete the proof of Theorem 2, try E 8:

SELF ASSISMENT EXERCISE 8

Prove (a) of Theorem 2

Now, it is natural to expect an analogue of Theorem 2 for ideals. But consider the inclusion i: $Z \rightarrow R$: i(x) = x. you know that 2Z is an ideal of Z. but is i(2Z) an ideal of R? No. For example, $2 \in 2Z$, 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: $R_1 \rightarrow R_2$, be a ring homomorphism.
a) If f is surjective and 1 is an ideal of R_1, then f (I) is an ideal of R_2.
b) If I is an ideal of R_2, then $f^{-1}(I)$ is an ideal of R_1 and Ker $f \subseteq f^{-1}(I)$.

Proof: Here we will prove (a) and leave (b) to you (see E 9)!

Firstly, since I is a subring of R_1, f(I) is a subring of R_2.
Secondly, take any $f(x) \in f(I)$ and $r \in R_2$. since f is surjective, $\exists\ s \in R_1$, such that f(s) = r.
Then
$Rf(x) = f(s) = f(sx) \in f(I)$, since $sx \in I$.
Thus, f(I) is an ideal of R_2.
To finish the proof try E 9.

SELF ASSISMENT EXERCISE 9

Prove (b) of Theorem 3.

Now, consider an epimorphism f: $R \rightarrow S$ and an ideal I in R. By Theorem 3 you know that f(I) 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, $I \subseteq f^{-1}(f(I))$. Can $f^{-1}(f(I))$ contain elements of R\I? Remember that Ker $f \subseteq f^{-1}(f(I))$ also. Thus, I + Ker $f \subseteq f^{-1}(f(I))$. In fact, I + Ker $f = f^{-1}(f(I))$. Let us see why.

Let $x \in f^{-1}(f(I))$. Then $f(x) \in f(I)$. Therefore, $f(x) = f(y)$ for some $y \in I$. Then
$F(x - y) = 0$.
$\therefore x - y \in$ Ker f, i.e., $x \in y + \text{Ker } f \subseteq I + \text{Ker } f$.
$\therefore f^{-1}(f(I)) \subseteq I + \text{Ker } f$.
Thus, $I^{-1}(f(I)) = I + \text{Ker } f$.
This tell us that if Ker $f \subseteq I$, then
$f^{-1}(f(I)) = I$ (since Ker $f \subseteq I \Rightarrow I + \text{Ker } f = I$).

Now you may like to do an easy exercise.

SELF ASSISMENT EXERCISE 10

Let f: R→ S be an onto ring homomorphism. Show that if J is an ideal of S, then $f(f^{-1}(J)) = J$.

Our discussion so far is leading us to the following theorem.

Theorem 4: Let f^{-1} R→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 I → 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 disussion above. Let us prove (b) now. Let A be the set of ideals of R containing Ker f, and B the set of ideals of S.

Define ø: A → B: $ø(I) = f(I_2)$
We want to show that ø is one-on-one and onto.
ø is onto : If $J \in B$ then $f^{-1}(J) \in A$ and Ker $f \subseteq f^{-1}(J)$ by Theorem 3.
Now $ø(f^{-1}(J)) = f(^{-1}(J)) = J$, using E 10.
ø is one-on-one: If I_1 and I_2 are ideals in R containing Ker f, then
$ø(I_1) = ø(I_2) \Rightarrow f(I_1) = f(I_2)$
$\Rightarrow f^{-1}(fI_1)) = f^{-1}(f(I_2))$
$\Rightarrow I_1 = I_2$, by (a).
Thus, ø is bijective.

Use this result for solving the following exercises.

SELF ASSISMENT EXERCISE 11

Find the kernel of the homomorphism
$f:Z \rightarrow Z_{12}$: $f(z) = z$.
Also find the ideals of Z_{12}.

SELF ASSISMENT EXERCISE 12

Show that the homomorphism f :Z→Z X Z : f(n) = (n, n) is not onto. Find an ideal in Z X Z which is not of the form f(I), where I is an ideal of Z.

And now let us look closely at the sets Ker f and Im f, where f is a ring 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 realize from the examples you have studied so fa.

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}({0}) is an ideal of R_1. But f^{-1}({0}) = Ker f.
Thus, we have shown that Ker f is an ideal of R_1.

c) 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 and example 3 you can immediately say that $\{\bar{0}, \bar{3}\}$ is an ideal of Z_6. As we go along you will see ore 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: R1→R2 be a homomorphism. Then f is injective iff Ker f = {0}.

Proof: f is injective iff is an injective group homomorphism from (R_1, +) into (R_2, +). This is true iff Ker f = $\{\bar{0}\}$, by Theorem 4 of unit 6. so, our result is proved.

Using Theorem 6, solve the following exercise.

SELF ASSISMENT EXERCISE 13

Which of the homomorphisms in example 1-6 are 1-1?

So far we have seen the give a ring homomorphism f:R→S, we can obtain an ideal of R, namely, Ker f. Now, give 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 from unit 10.

Theorem 7: If is an ideal of a ring R, then there exists a ring homomorphism f:R→R/I whose kernel is 1

Proof: Let us define f:R→R/1 by f(a) = a + 1 for all a ∈ R. Let let us see if f is a homomorphism. For this take any a, b ∈ R. then
F(a + b) = (a + b) + 1 = (a + 1) + (b + 1) = f(a) + f(b), and
F(ab) = ab + 1 = (a + 1) (b + 1) (b + 1) = f(a) f(b).

Thus, f is a homomorphism.
Further, Ker f = {a ∈ R| f(a) = 0 + 1} = { a ∈ R | a + 1 = 1}
= {∈ R | a ∈ 1} = 1.
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/1.

Try this simple exercise now.

SELF ASSISMENT EXERCISE 14

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?

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 ring and f: $R_1 \to R_2$, and g: $R_2 \to R_3$ be ring homomorphisms. Then their composition $g \circ f$: $R_1 \to R_3$ give by $(g \circ f)(x) = g(f(x))$ for all $x \in R_1$ is a ring homomorphism.

The proof of this result is on the same lines as the proof of the corresponding result in unit 6. We leave it to you (see the following exercise).

SELF ASSISMENT EXERCISE 15

Prove Theorem 8

SELF ASSISMENT EXERCISE 16

In the situation of Theorem 8 prove that
a) if $g \circ f$ is 1 – 1, then so is f.
b) if $g \circ f$ is onto, then so is g.

SELF ASSISMENT EXERCISE 17

Use Theorem 8 to show that the function h: Z X Z $\rightarrow Z_2$ defined by h(n, m)) = $\overline{m}$ is a homomorphism.

Now let us see what the ring analogue of a group isomorphism is.

3.3 The Isomorphism Theorems

In Unit 6 we discuss 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 homomorphosm that is bijective is an isomorphism.

An f: $R_1 \rightarrow R_2$ is an isomorphism, we say that R_1 is **isomorphism** to R_2, and denote it by $R_1 \simeq R_2$.

Over her we would like to make the following remark.

Remark: Two rings are isomorphic if and only if they 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, the any ring isomorphic to R_1 must have this property too.

Try the following exercise now. They will help you in becoming more familiar with isomorphisms.

SELF ASSISMENT EXERCISE 18

Which of the following functions are ring isomorphisms?

a) f:**Z** →**R**: f(n) = n
b) f: **Z** → **5Z:** f(n) = 5n
c) f: **C**→**C**: f(z) = **z**, the complex conjugate of z

SELF ASSISMENT EXERCISE 19

Let ø: $R_1 \rightarrow R2$ be a ring isomorphism. Then $ø^{-1}$: $R_2 \rightarrow R_1$ is a well defined function since ø is bijective. Show that $ø^{-1}$ is also an isomorphism.

SELF ASSISMENT EXERCISE 20

Show that the composition of isomorphism is an isomorphism.

And now, let us go back to Unit 6 for amoment. Overthere we roved the Fundamental Theorem of Homomorphsim for groups, according to which the homomorphic image of a group G is isomorphism theorem or the Fundamental Theorem of Homomorphism for rings.

Theorem 9 (The Fundamental of Homomorphism): let f: R→S be a ring homomorphism. Then R/Ker f $\simeq$ Im f. In particular, if f is surjective, then R/Ker f $\simeq$S

Proof: Firstly, note that R/Ker f is a well-defined quotient ring since Ker f is an ideal of R. For convenience, let us put Ker f = 1. let us define.
ψ : R/1 →S by ψ (x+ 1) = 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 + 1 = y +1 then ψ (x + 1) = ψ (y + 1).
Now, x + 1 = y +1 $\Rightarrow$ x –y $\in$ 1 = Ker f $\Rightarrow$ f(x – y) = 0 $\Rightarrow$ f(x) = f(y)
$\Rightarrow$ ψ (x + 1) = ψ (y + 1).

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
ψ ((x + 1) + (y + 1)) = ψ (x + y + 1) = f(x + y) = f(x) + f(y)
= ψ (x + 1) + ψ (y + 1), and
ψ ((x + 1) (y + 1) = ψ (xy + 1) = f(xy) = f(x) f(y)
= ψ (x + 1) ψ (y + 1)

Thus, ψ is a ring homomorphism.

ii) Im ψ = Im f: since $\psi(x + 1) = f(x) \in$ Im f $\forall$ x $\in$ R. Im $\psi \subseteq$ Im f. Also any element of Im f is of the form f(x) = ψ (x + 1) for some x $\in$ R. Thus, Im f $\subseteq$ Im ψ.

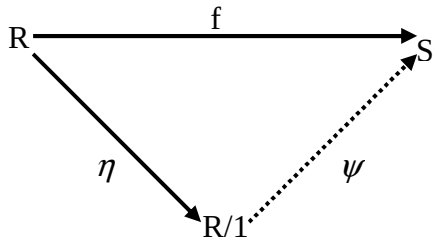
S, Im $\psi \equiv$ Im f.

iii) ψ is 1 –1: To show this let x, y $\in$ R such that ψ (x + 1) = ψ(y + 1). Then f(x) = f(y), so that f(x – y) = 0, i.e., x – y $\in$ Ker f = 1. i.e., x + 1 = y + 1.

Thus, ψ is 1 – 1.

So, we have shown that R/Ker f $\simeq$Im f.
Thus, if f 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 η: R $\rightarrow$R/1: η(a) = a + 1. This can ve diagrammatically shown as



Let us look at some examples of the use of the Fundamental Theorem.

Consider p: Z$\rightarrow$$Z_m$: p(n) = $\bar{n}$.p is an epimorphism and Ker p = {n|$\bar{n} = \bar{0}$ mZ_m} mZ.
Therefore, Z/mZ $\simeq$ Z_m.
(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 X R_2 $\rightarrow$$R_1$: p(a, b) = a, where R_1 and R_2 are rings. Then p is onto and its kernel is
Therefore, (R_1 X R_2)/R_2 $\simeq$ R_1.

Try this exercise now.

SELF ASSISMENT EXERCISE 21

What does the Fundamental Theorem of Homomorphism say in each of the Examples 1 to 6?

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 homomorphism 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 1_Z.

Proof: Let f: Z $\rightarrow$Z be a non-trivial homomorphism. Let n be positive integer. Then
n = 1 + 1 +…. 1 (n times). Therefore,
f(n) = f(1) + f(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(1), 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.

Now, since f is a non trivial homomorphism, f(m) $\neq$ 0 for some $\in$ Z.
Then, 1(m) = 1(m.1) = f(m) f(1).
Canceling 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 = 1_z.
This theorem has an important corollary.

Corollary: Let R be a ring isomorphisc to Z. If f and g are two somorphisms from
R onto Z, the f= g.

Proof: The composition $f \circ g^{-1}$ is an isomorphism from Z onto itself. Therefore, by Theorem 10, $f \circ g^{-1} = 1_Z$, 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_f : R/Ker f$\rightarrow$ Z and ψ_f :R/Ker g $\rightarrow$Z.

Since Ker f = Ker g, ψ_f and ψ_g are isomorphisms of the same ring onto Z. Thus, by the corollary above, $\psi_f = \psi_g$

Also, the canonical maps η_f R $\rightarrow$ R/Ker f and η_g R$\rightarrow$R/Ker g are the same since

Ker f = Ker g.

$\therefore f = \psi_f \circ \eta_f = \psi_g \circ \eta_g = g.$

We will now give you a chance to prove two applications of Theorem 9! They are analogous to Theorem 10 and 11 of unit 6

SELF ASSISMENT EXERCISE 22

(second isomorphism theorem) Let S b a subring and I be an ideal of a ring R. Show that (S + I)/I $\simeq$S/(S $\cap$ I).

SELF ASSISMENT EXERCISE 23

(Third isomorphism theorem) Let I and J be ideal of a ring R such that J $\subseteq$I. Show that I/J is an ideal of the ring R/J and that

(R/J)/(I/J) $\simeq$R/I.

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.

4.0 CONCLUSION

We have laid a solid foundation in this course for you to proceed further in studying further algebra as you progress in your career as a mathematician . Do all the self assessment exercises in order to understand the course better.

5.0 SUMMARY

In this unit we have covered the following points.

- The definition of a ring homomorphism, its kernel and its image, along with several examples
- The direct or inverse image of a subring under ahomomophism is a subring.
- If f: R$\rightarrow$S is a ring homomorphism, then
  - i) Im f is a subrig of S,
  - ii) Ker f is an ideal of R,
  - iii) $f^{-1}(1)$ is an ideal of R for every ideal 1 of S.

iv) If f is surjective, then f(1) is an ideal of S.

- A homomorphism is injective iff its kernel is {0},
- The composition of homomorphisms is a homomorphism.
- The definition and examples of a ring isomorphism.
- The proof and applications of the Fundamental Theorem of Homomorphism which says that if f: R $\rightarrow$S is a ring homomorphism, then R/Ker f $\simeq$ Im f.

SOLUTIONS/ANSWERS

SELF ASSISMENT EXERCISE 1

For x, y $\in$ S,
i(x + y) = x + y = i(x) + i(y), and
i(xy) = xy = i(x) i(y)
$\therefore$i is a homomorphism.
Ker i = {x $\in$ S| i(x) = 0} = {0}
Im i = {i(x) | x $\in$ S} = S.

SELF ASSISMENT EXERCISE 2

For any x, y$\in R_1$, f(x) + y) = 0 = 0 + 0 = f(x) + f(y), and
f(xy) = = 0.0 = f(x) . f(y). $\therefore$f is a homomorphism.
Ker f = { x $\in R_1$ | f(x) = 0 = } = R_1
Im f = {0}.

SELF ASSISMENT EXERCISE 3

f(2.3) $\equiv$ f(6) $\equiv$ 12. But f(2) . (3) $\equiv$ 4.6 $\equiv$ 24
Thus, f(2.3) $\neq$ f(2) f(3)
$\therefore$f is not a homomorphism.

SELF ASSISMENT EXERCISE 4

For any (a, b), (c, d) $\in$ A X B,
P((a, b) + (c, d)) = p(a + c, b + d) = a + c = pa, b) + p(c, d),
P((a, b) (c, d)) = p(ac, bd) = ac = p(a, b) p(c, d).
Ker p = { (a, b) $\in$ A X B | a = 0 } = {0} XB.
Im p = { p(a, b) | (a, b) $\in$ A X B} = { a| (a, b) $\in$ A X B} = A.

SELF ASSISMENT EXERCISE 5

Yes, you can check it.

SELF ASSISMENT EXERCISE 6

For $f, g \in C[0, 1]$,
$\phi(f + g) = ((f + g)(0), (f + g)(1))$
$= (f(0), f(1)) + (g(0), g(1))$
$= \phi(f) + \phi(g)$, and
$\phi(fg) = (fg(0), fg(1) = (f(0), g(0))(f(1), g(1))$
$= \phi(f)\,\phi(g)$.
$\therefore \phi$ is a homomorphism.

SELF ASSISMENT EXERCISE 7

Let $x \in T_2$. Since f is surjective, $\exists\ r \in R_1$ such that $f(r) = x$. since
$r.1 = r$, $f(r)\,f(1) = f(r)$.
Thus, $xf(1) = x$. This is true for any $x \in R_2$.
$\therefore f(1)$ is the identity of R_2.

SELF ASSISMENT EXERCISE 8

Again use Theore 1 of unit 10.

i) $S \neq \phi \Rightarrow f(S) \neq \phi$

ii) Let $a', b' \in f(S)$. Then $\exists\ a, b \in S$ such that $f(a) = a'$, $f(b) = b'$
Now $a' - b' = f(a) - f(b) = f(a - b) \in f(S)$, since $a - b \in S$, and
$a'b' = f(a)\,f(b) = f(ab) \in f(S)$, sine $ab \in S$.
$\therefore f(S)$ is a subring of R_2.

SELF ASSISMENT EXERCISE 9

Since 1 is a subring of R_2, $f^{-1}(1)$ is a subring of R_1. Now, let $a \in f^{-1}(1)$ and $r \in R_1$. We want to show that $ar \in f^{-1}(1)$.
Since $a \in f^{-1}(1)$, $f(a) \in 1$. $\therefore f(a)\,f(r) \in 1$, i.e.,

$f(ar) \in 1$. $\therefore ar \in {}^{-1}(1)$.
Thus, $f^{-1}(1)$ is an ideal of R_1
Also, if $x \in$ Ker f, then $f(x) = 0 \in 1$.
$\therefore x \in f^{-1}(1)$.
$\therefore$ Ker $f \subseteq f^{-1}(1)$.

SELF ASSISMENT EXERCISE 10

Let $x \in f(f^{-1}(J))$. Then $x = f(y)$, where $y \in f^{-1}(J)$,i.e. $f(y) \in J$, i.e., $x \in J$.
Thus, $f(f^{-1}(J)) \subseteq J$.
Now, Let $x \in J$. since f is surjective, $\exists\ y \in R$ such that $f(y) = x$
Then $y \in f^{-1}(x) \subseteq f^{-1}(J)$.

$\therefore x = f(y) \in f(f^{-1}(J))$
Thus, $J \subseteq f(f^{-1}(J))$.
Hence the result is proved.

SELF ASSISMENT EXERCISE 11

Ker f = $\{ n \in Z | n \equiv 0 \pmod{12}\} = 12Z$.
Now, you know that any ideal of Z is a subgroup of Z, and hence must be of the form nZ, $n \in N$. Thus, the ideals of Z containing Ker f are all those nZ such that n|12, i.e., Z, 2Z, 3Z, 4Z, 6Z, 12Z. Thus, by Theorem 4(b) the ideals of Z_{12} are
$Z_{12}, \bar{2}Z_{12}, \bar{3}Z_{12}, \bar{4}Z_{12}, \bar{6}Z_{12}$ and $\{\bar{0}\}$.

SELF ASSISMENT EXERCISE 12

For example, $(0, 1) \notin$ Im f.
For any ideal 1 of Z, f(1) = 1 X 1. Thus, the ideal Z X {0} of Z X Z is not of the form f(1), for any ideal 1 of Z.

SELF ASSISMENT EXERCISE 13

The Homomorphisms in Examples 1 and 5.

SELF ASSISMENT EXERCISE 14

NO. For example, take the subring Z of Q. Since Z is not an ideal of Q, it can't be the kernel of any homomorphism from Q to another ring.

SELF ASSISMENT EXERCISE 15

for any $x, y \in R_1$,
$g \circ f(x + y) = g(f(x + y)) = g(f(x) + f(y))$
$= g \circ f(x) + g \circ f(y)$, and
$g \circ f(xy) = g \circ f(x)\ g \circ f(y)$.
Thus, $g \circ f$ is a homomorphism.

SELF ASSISMENT EXERCISE 16

a) $x \in$ Ker f $\Rightarrow$ f(x) = 0 $\Rightarrow g \circ f(x) = 0 \Rightarrow x = 0$, since $g \circ f$ is 1 – 1.
$\therefore$ Ker f = {0}.
$\therefore$ f is 1 – 1.

b) Let $x \in R_3$. Since $g \circ f$ is onto $\exists\ y \in R_1$ such that $g \circ f(y) = x$, i.e., g(f(y)) = x. Thus, g is onto.

SELF ASSISMENT EXERCISE 17

h is the composition of the projection map p: Z X Z $\rightarrow$ Z: p(n, m) = m and the map f: Z $\rightarrow$ Z_2: f(r) = $\bar{r}$. Both p and f are ring homomorphisms. $\therefore$h is a ring homomorphism.

SELF ASSISMENT EXERCISE 18

a) is not onto and hence, not an isomorphism.
b) is not a homomorphism.
c) ee the appendix of unit 2 for properties of elements of C.

Then you can easily prove that f is an isomorphism.

SELF ASSISMENT EXERCISE 19

Let x, y $\in R_2$ and $ø^{-1}(x) = f$, $ø^{-1}(y) = s$. Then $x = ø(r)$ and $y = ø(s)$.
Therefore,
$x + y = ø(r) + ø(s) = ø(r + s)$ and $xy = ø(rs)$.
$\therefore$ $ø^{-1}(x + y) = r + s = ø^{-1}(x) + ø^{-1}(y)$, and
$ø^{-1}(xy) = rs = ø^{-1}(x)\, ø^{-1}(y)$.
Thus, $ø^{-1}$ is a homomorphism.
You already know that it is bijective. Thus, $ø^{-1}$ is an isomorphism.

SELF ASSISMENT EXERCISE 20

Let $f_1 \rightarrow R_2$ and g: $R_2 \rightarrow R_3$ be ring is isomorphisms. From Theorem 8 you know that g $\circ$ f is a homomorphism. For the rest, proceed as you did in E 12 of unit 6.

SELF ASSISMENT EXERCISE 21

Example 1 : R $\simeq$ R.

Example 2 : What we have just done above, namely, Z/sZ $\simeq$ Z,

Example 3: $Z_6/\{\bar{0}, \bar{3}\} \simeq Z_3$.

Example 4: Ker ø = $\{f \in C[0, 1] | f\left(\frac{1}{2}\right) = 0\}$.

Im ø = R (because given any r $\in$ R we can define the constant function $f_r : [0, 1] \rightarrow R$: $f_r(x) = r$. Then $f_r\left(\frac{1}{2}\right) = r$. Thus, $r = ø(f_r) \in$ Im ø).

Example 5: Z $\simeq \{nI | n \in Z\}$

Example 6: $\wp(X)/\text{Ker } f \simeq \wp(Y)$.

SELF ASSISMENT EXERCISE 22

Since 1 is an ideal of r and $1 \subseteq S + 1$, it is an ideal of $S + 1$
Thus, $(S +1)/1$ is a well-defined ring.
Define f: $S \rightarrow (S + 1)/1 : f(x) = x + 1$.
Then, you can check that $f(x + y) = f(x) + f(y)$, and
$F(xy) = f(x) f(y) \forall x, y \in S$.

As you did in Theorem 10 unit 6, you can check that f is surjective and Ker $f = S \cap 1$.

Thus, $S/(S\cap 1) \simeq (S + 1)/1$.

SELF ASSISMENT EXERCISE 23

Define f: $R/J \rightarrow R/1$: $f(r + J) = r +1$.

As you did in Theorem 11 of unit 2 you can check that f is well defined, f is surjective and Ker $f = 1/J$.

Thus, 1/J is an ideal of R/J and $(R/J)/(1/J) \simeq R/1$.

6.0 TUTOR MARKED ASSIGNMENT

Study eamples 1 to 6 and in each case state the Fundamental Theorem of Homomorphism**.**

7.0 REFERENCES/FURTHER READINGS

Blacksell: Topics in Algebra

Notation and Symbols

$a \equiv b \pmod{n}$	a is congruent to be modulo n.
$\wp(\equiv)$	set of all subsets of X.
A B	$(A \backslash B) \cup (B \backslash A)$
R/I	quotient ring of R by I.
$<a>$	principal ideal generated by a.
$<a_1,\ldots, a_a>$	ideal generated by $a_{1, \ldots,} a_n$
Ker f	kernel of the homomorphism f.
$\simeq$	is isomorphic to.