III-B.Sc

SEMESTER : V
CORE COURSE : VIII

Inst Hour	: 6
Credit	: 5
Code	: 18K5M08

ABSTRACT ALGEBRA

UNIT 1:

Groups: Definitions and Examples of Groups – Elementary Properties of Groups.
Finite Groups, Subgroups: Terminology and Notation – Subgroup Tests – Examples of Subgroups. **Cyclic Groups:** Properties of Cyclic Groups – Classification of Subgroups of Cyclic Groups.
Part 2: Sections 2, 3, 4.

UNIT 2:

Permutation Groups: Definition and Notation – Cycle Notation.
Isomorphisms: Definition and Examples – Cayley's Theorem – Properties of Isomorphisms – Automorphisms.
Cosets and Lagrange's Theorem: Properties of Cosets – Lagrange's Theorem and Consequences (upto Theorem 7.3).
Part 2: Section 5 (Page 99 – 104) , Section 6 (Page 127 – 138) , Section 7 (Page 144 – 151).

UNIT 3:

Normal Subgroups and Factor Groups: Normal Subgroups – Factor Groups – Applications of Factor Groups – Internal Direct Products.
Group Homomorphisms: Definition and Examples – Properties of Homomorphisms – The First Isomorphism Theorem.
Part 2: Sections 9, 10.

UNIT 4:

Introduction to Rings: Definition – Examples of Rings – Properties of Rings – Subrings.
Integral Domains: Definition and Examples – Fields – Characteristic of a Ring.
Ideals and Factor Rings: Ideals – Factor Rings.
Part 3: Sections 12, 13, 14(Page 267 – 271).

UNIT 5:

Ring Homomorphism: Definition and Examples – Properties of Ring – Homomorphism – The Field of Quotients.
Part 3: Section 15.

Text Book

Joseph A.Gallian, Contemporary Abstract Algebra, Cengage Learning, 8th Edition, 2013.

Books for Reference

[1] I.N.Herstein. Topics in Algebra.

Question Pattern (Both in English & Tamil Version)

Section A : 10 x 2 = 20 Marks, 2 Questions from each Unit.
Section B : 5 x 5 = 25 Marks, EITHER OR (a or b) Pattern, One question from each Unit.
Section C : 3 x 10 = 30 Marks, 3 out of 5, One Question from each Unit.

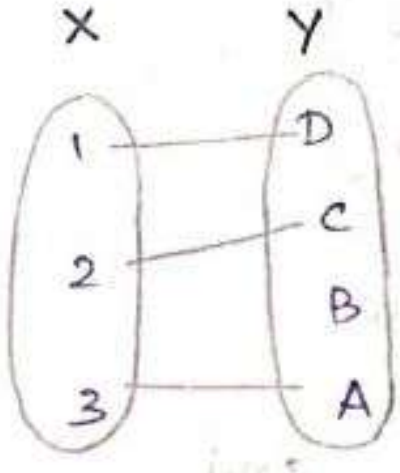
9.3.18

Department of Mathematics
N. GOVERNMENT ARTS COLLEGE
THANJAVUR-613 007

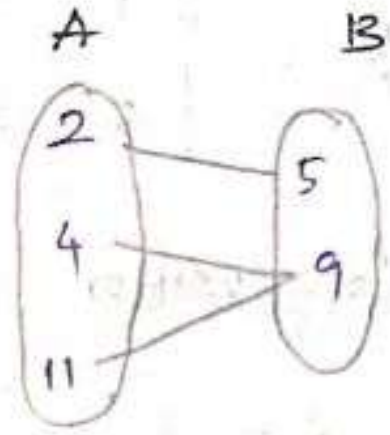
Unit-2

Permutation groups

An injective function or one to one function is a function that maps distinct elements of its domain to distinct elements of its co-domain



one to one



Not one to one.

(i) onto function or surjective

If for every element of B there is atleast one or more than one element matching with A.

Definitions:

permutation of A, permutation group of A.

A permutation of a set A is a function from A to A that is both one to one and onto.

A permutation group of a set A is set of permutations of A that forms a group under function composition.

Example (i)

The permutation β of the set $\{1,2,3,4,5,6\}$ given by

$\beta(1)=5$, $\beta(2)=3$, $\beta(3)=1$, $\beta(4)=6$, $\beta(5)=2$, $\beta(6)=4$ is expressed in array form as

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

(ii) Composition of permutations

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \text{ and}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

$(\beta\alpha)(1) = \beta(2) = 4$

$(\beta\alpha)(2) = \beta(4) = 2$

$(\beta\alpha)(3) = \beta(3) = 1$

$(\beta\alpha)(4) = \beta(5) = 3$

$(\beta\alpha)(5) = \beta(1) = 5$

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

Definition:

Let A be a finite set containing n elements.

The set of all permutations of A is clearly a group under the composition of functions. This group is called the symmetric group of degree n and is denoted by S_n

Example

Symmetric group S_3:

Let S_3 denote the set of all one to one functions from $\{1,2,3\}$ to itself. Then S_3, under function composition, is a group with six elements. The six elements are

$$e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \qquad \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = P_1$$

$$P_2 = \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \qquad \beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = P_3$$

$$P_5 = \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \qquad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_4$$

Note:

$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \neq 2\beta$, so that S_3 is non-Abelian.

In this group, e is the identity elements.

Let now compute the product P_1P_2

P_1 : $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$

P_2 : $\begin{matrix} \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{matrix}$

Hence $P_1 P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

So that $P_1 P_2 = e$

Now $P_1 P_4$: $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{matrix}$

i.e. $P_1 P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_3$

Illy we can compute all the other products and the Cayley table for this group is given by

	e	P_1	P_2	P_3	P_4	P_5
e	e	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	e	P_4	P_5	P_3
P_2	P_2	e	P_1	P_5	P_3	P_4
P_3	P_3	P_5	P_4	e	P_2	P_1
P_4	P_4	P_3	P_5	P_1	e	P_2
P_5	P_5	P_4	P_3	P_2	P_1	e

Thus S_3 is a group containing

$3! = 6$ elements.

Remarks:

(i) $(g \circ f)(x) = g[f(x)]$

Hence to find the image of any element x under $g \circ f$, we first apply f and then g:

To find the image of x under the product P_1P_2. we first apply P_1 and then P_2.

(ii) In S_3, $P_1P_2 = P_2P_1 = e$ so that

the inverse of P_1 is P_2.

In general the inverse of a permutation can be obtained by interchanging.

The rows the permutation

For example if $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$

then the inverse of P is the permutation

given by $P^{-1} = \begin{pmatrix} 3 & 4 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

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

(iii) The symmetric group S_n contains $n!$ elements. For, let $A = \{1, 2 \ldots n\}$. Any permutation on A is given

by specifying the image of each element. The image of '1' can be chosen in 'n' different from ways. Since the images of two is different from the image of 1. it can be chosen in (n-1) different ways and so on.

Hence the number of permutations of A is $n(n-1)\cdots 2.1 = n!$ so that the number of elements in S_n is $n!$

Reflection:

The conceptual operation of inverting a system or event with respect to a plane, each element being transferred perpendicularly through the plane to a point the same distance the other side of it.

Rotation:

Rotation is circular movement. A rotation is the movement of something through one complete circle.

Example 2: Symmetric Group S_n

Let $A = \{1, 2, \cdots n\}$. The set of all permutations of A is called the symmetric group of degree n and is denoted by S_n. Elements of S_n have the form

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}.$$

It is easy to compute the order of S_n. There are n choices of $\alpha(1)$. Once $\alpha(1)$ has been determined, there are $n-1$ possibilities for $\alpha(2)$ [Since α is one-to one, we must have $\alpha(1) \neq \alpha(2)$].

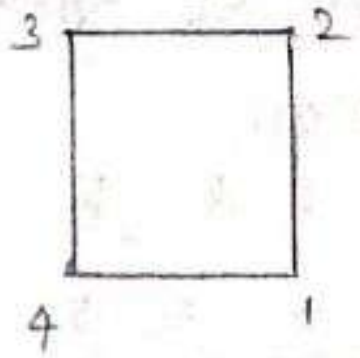
After choosing $\alpha(2)$, there are exactly $n-2$ possibilities for $\alpha(3)$. Continuing along in this fashion, we see that S_n must have $n(n-1)\cdots 3\cdot 2\cdot 1 = n!$ elements. We leave it to the reader to prove that S_n is non-Abelian when $n \geq 3$.

The symmetric groups are rich in subgroups. The group S_4 has 30 subgroups and S_5 has well over 100 subgroups.

Example 3:

Symmetric of a Square

As a third example; we associate each motion in D_4 with the permutation of the locations of each of the four corners of a square. For example, if we label the four corner positions as in the figure below and keep these labels fixed for reference, we may describe a 90° rotation by the permutation.

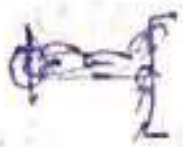


$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

whereas a reflection across a horizontal axis yields

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

These two elements generate the entire group (that is, every element is some combination of the ρ's and ϕ's)



When D_4 is represented in this way, we say that it is a subgroup of S_4.

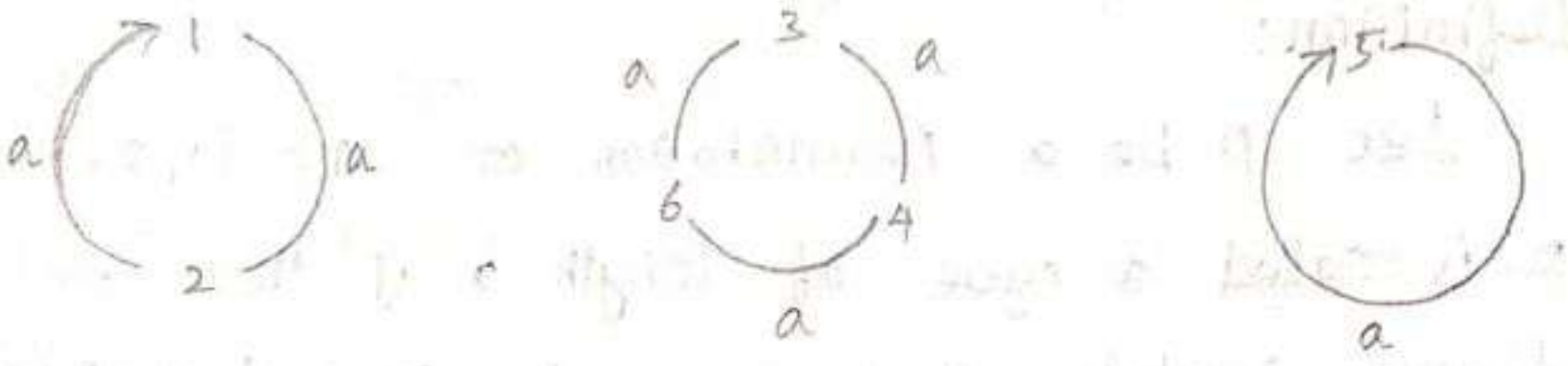
CYCLE NOTATION :

There is another notation commonly used to specify permutations. It is called cycle notation and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical can be readily determined when cyclic notation is used.

As an illustration of cycle notation, let us consides the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$

The assignment of values could be presented schematically as follows:



Although mathematically satisfactory, such diagram are cumbersome. Instead, we leave out the arrows and simply write $\alpha = (1,2)(3,4,6)(5)$.

As second example, consider

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

In cycle notation, β can be written $(2,3,1,5)(6,4)$ or $(4,6)(3,1,5,2)$. Since both of these unambiguously specify the function β, An expression.

Example

Let $A = \{1,2,3,4,5\}$ consider the cycle of length 4 given by

$$p = (2\ 4\ 5\ 1)$$

Then $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

Obviously $(2451) = (4512) = (5124) = (1245)$

Note

The product of cyclic need not be a cycle.

Definition:

Let p be a permutation on $A = \{1, 2, \cdots n\}$ p is called a cycle of length r if there exist distinct symbols $a_1, a_2, a_3 \cdots a_r$ such that $p(a_1) = a_2$, $p(a_2) = a_3 \cdots p(a_{r-1}) = a_r$, and $p(a_r) = a_1$ and $p(b) = b$ for all $b \in A - \{a_1, a_2, \cdots a_r\}$

This cycle is represented by the symbol $(a_1, a_2, \cdots, a_r)$.

Example

Let $P_1 = (2\ 3\ 4)$ and $P_2 (1\ 5)$

Then $P_1 P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$

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

which is not a circle.

Definition:

Two cycles are said to be disjoint if they have no symbols in common.

For example $(2, 5)$ and $(3\ 4)$ are disjoint cycles.

Note:

If P_1 and P_2 are disjoint cycles the symbols which ~~one~~ are moved by P_1 are fixed by P_2 and vice versa.

Hence multiplication of disjoint cycles is Commutative.

Theorem 5.3

Order of a permutation

Statement :

The order of permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof :

Suppose that α and β are disjoint cycles of lengths m and n, and let k be the least common multiple of m and n. It follows from Theorem 4.1 that both α^k and β^k are the identity permutation ε and since α and β Commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus we know by the corollary to Theorem 4. ($a^k = e$ implies that $|a|$ divides k) that the order of $\alpha\beta$. let us call it t - must divide k. But then $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, so that $\alpha^t = \beta^{-t}$. However, it is clear that if α^t and β^{-t} are equal and have no common

Symbol, the same is true for a^t and b^{-t}, since rising a cycle to a power does not introduce new symbols. But if a^t and b^{-t} are equal and have no common symbols, they must both be the identity, because every symbol in a^t is fixed by b^{-t} and vice versa (remember that a symbol not appearing in a permutation is fixed by the permutation).

It follows, then that both m and n must divide t. This means that k, the least common multiple of m and n, divides t also, This shows that $k = t$.

Thus far, we have proved that the theorem is true in the cases where the permutations is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

As we will soon see, a particularly important kind of permutation is a cycle of length 2 - that is a permutation of the form (ab). Many authors call these permutations transpositions, since the effect of (ab) is to interchange of transpose a and b.

Example for every permutation in S_n, $n > 1$ is a product of 2 cycles.

Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

of the set S with six elements. σ sents $1 \to 6$, $6 \to 2$, $2 \to 5$, $5 \to 1$ and so that orbit of 1 is the cycle $(1,6,2,5)$ σ sends $3 \to 4$, $4 \to 1$ and so the σ orbit of 3 is the cycle $(3,4)$

$\therefore \quad \sigma = (1,6,2,5)(3,4)$

$= (1,6)(1,2),(1,5),(3,4)$

Note:

The decomposition of a permutation into 2 cycles is not neccessary disjoint and not unique.

Example:

$(1,2,3) = (1,2)(1,3)$

$= (2,3)(2,1)$

$= (3,1)(3,2)$

$= (1,2)(2,3),(3,2)(1,3)$

Since $(2,3)(3,2) = e$

$(1,2)(2,1)$ so ① is a product of 2 cycles.

Theorem 5.4 (Product of two cycles)

Every permutation in S_n $n>1$, is a product of 2 cycles.

proof:

First note that the identity can be expressed as (1 2)(1 2) and so it is a product of two cycles. By Theorem 5.1, w.k.T every permutation can be written in the form

$$(a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_t) \cdots (c_1 c_2 \cdots c_t).$$

A direct computation shows that this is the same as

$$(a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(b_1 b_t)(b_1 b_{t-1}) \cdots (b_1 b_2)(c_1 c_2)(c_t - 1) \cdots (c_1 c_2).$$

The completes the proof.

The first decomposition in the following example demonstrates this technique. The other products in example 4 show that the decomposition of a permutation into a product of 2 cycles is not unique.

Example 4:

$$(1\,2\,3\,4\,5) = (1\,5)(1\,4)(1\,3)(1\,2)$$
$$= (4\,5)(5\,3)(2\,5)(1\,5)$$
$$= (2\,1)(2\,5)(2\,4)(2\,3)$$
$$= (5\,4)(5\,2)(2\,1)(2\,5)(2\,3)(1\,3)$$

Example 4 even shows that the number of 2 cycles may vary from one decomposition to the next. Theorem 5.5 (due to Cauchy) says, however, that there is one aspect of a decomposition that never varies.

We isolate a special case of Theorem 5.5 as a lemma.

Example:

$$\text{set } S = (1\ 2\ 3\ 4\ 5)$$

$$= (5\ 4)(5\ 2)(2\ 1)(2\ 5)(2\ 3)$$

$$\varepsilon = (5\ 2)(2\ 5)$$

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

$$\alpha = (5\ 4)(2\ 1\ 3)$$

Note:

second principle of mathematical Introduction

Lemma

If $\varepsilon = \beta_1 \beta_2 \cdots \beta_r$ where the β's are 2 cycles then r is even.

proof:

$r \neq 1$ since ε is not a 2 cycle. If $r = 2$ we are done

suppose $r = 2$ we are done

Suppose $r > 2$ and that if $\varepsilon = \beta_1 \beta_2 \cdots \beta_s$ with $s < r$ then s is even

Suppose the right most 2 cycle is ~~(ab)(ab)~~ (ab)

since $(ij) = (ji)$

The product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right (these are 4 possibilities for β_{r-1} if $\beta_r = (ab)$

$$\varepsilon = (ab)(ba)$$

$$(ab)(bc) = (ac)(ab)$$

$$(ac)(cb) = (bc)(ab)$$

$$(ab)(cd) = (cd)(ab)$$

In the first case, we may delete $\beta_{r-1}\beta_r$ from the original product, leaving $\varepsilon = \beta_1 \beta_2 \cdots \beta_{r-2}$ for $r-2$ is even by the second principle of main induction (For every $n \geq b$, if $P_0, P_1 \ldots P_n$ are all true then P_{n+1} is true).

In the other 3 cases, we replace $\beta_{r-1}\beta_r$ by the product on the left, retaining the identity but moving the right most occurance of a into β_{r-1}.

Repeat the above procedure with $\beta_{r-2}\beta_{r-1}$. We either obtain

$\varepsilon = \beta_1 \beta_2 \cdots \beta_{r-2} \beta_{r-1}$ implying

r is even by the second principle of main induction or obtain a new product of r2 cycles for ε with the rightmost a in β_{r-2}

Continuing if the rightmost occurence of a is in β_2, $\beta_1 \beta_2 = \varepsilon$, for if a was moved to β_1 as above, that would its only occurence and so would not be fixed, a contradiction.

Then $\varepsilon = \beta_3 \cdots \beta_r$ also, and again r must be even by the second principle of main induction.

Theorem 5.5

Always Even or Always odd

Statement :

If a permutation α can be expressed as a product of an even number of 2 cycles, then every decomposition of α into a product of 2 cycles must have an even number of 2 cycles. In symbols, if

$$\alpha = \beta_1 \beta_2 \cdots \beta_r \text{ and } \alpha = \gamma_1 \gamma_2 \cdots \gamma_t$$

where the β's and the γ's are 2 cycles, then r and s are both even or both odd.

Definition:

Even and odd permutations

A permutation that can be expressed as a product of an even number of 2 cycles is called an even permutation. A permutation that can be expressed as a product of an odd number of 2 cycles is called an odd permutation.

Theorem 5.6

Statement:

"Even permutations from a group". The set of even permutations in S_n (the symmetric group of degree n) forms a subgroup of S_n.

Proof:

We first show that A_n is a subgroups of S_n. Since S_n is finite (degree n) we must only verify that A_n is closed. [by lemma If it is a non-empty finite subset of a group G1 and H is closed under the product in G1, then H is a subgroup of G J.

Since the product of two even permutations is even s A_n is closed. and Hence A_n is a subgroup of S_n.

Definition :

Alternating Group of Degree n

The group of even permutations of n symbols is denoted and is called the alternating group of degree n.

Cayley's Theorem :

Every group is isomorphic to a group of permutations

Proof :

Let G be any group. Corrosponding to every g in G, we define a map T_g as follows

$$T_g(x) = gx \qquad x \in G$$

$\therefore g \in G, x \in G \Rightarrow gx \in G$

$$T_g : G \to G$$

Further for any $x, y \in G$

$$T_g(x) = T_g(y) \Rightarrow gx = gy$$

$\Rightarrow x = y$ (by cancellation law in G)

$\therefore T$ is one - one.

and for any $x \in G$, there exists $g^{-1}x \in G$

Such that

$T_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = x$

$\therefore T_g$ is onto

As such T_g is a one-one mapping of G onto G itself.

Hence T_g is a permutation of G.

Let $\overline{G} = \{T_g / g \in G\}$.

clearly $\overline{G} \subset S_G$ ($S_G \rightarrow$ of all permutation of G)

Let us now consider the mapping T from G to S_G, defined by

$\phi : G \rightarrow S_G$, $\phi(x) = Tx \quad \forall x \in G$

Now for any $x, y \in G$

$\phi(xy) = T_{xy} = T_x T_y = T(x)\,T(y)$

$\therefore \phi$ is a homomorphism from a group G on to S_G.

Consequently $T(G) = \overline{G}$ is a sub group of the permutation group S_G and ϕ is an onto from G onto $\overline{G}$.

Also for any $g, h \in G$

$\phi(g) = \phi(h) \Rightarrow T_g = T_h$

$\Rightarrow T_g(x) = T_h(x)$

$\Rightarrow gx = hx \Rightarrow g = h.$

$\therefore \phi$ is one-one.

Hence ϕ is an isomorphism from a group G into permutation group $\overline{G}$

Consequently $G \cong \overline{G}$.

Example 8:

For concreteness, let us calculate the left regular representation $U(12)$ for $U(12) = \{1, 5, 7, 11\}$. Writting the permutations of $U(12)$ in array form, we have (remember, T_x is just multiplication by x)

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \quad T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix}$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \quad T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}$$

It is instructive to ~~complet~~ compare the Cayley table for $U(12)$ and its left regular representation $U(12)$

$U12$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\overline{U(12)}$	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

It should be abundantly clear from these tables that $U(12)$ and $\overline{U(12)}$ are only notationally different.

Perhaps the most important aspect of Cayley's Theorem is that it shows that the present day set of axioms we have adopted for a group.

Theorem 6.2

Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then ϕ carries the identity of G to the identity of $\bar{G}$

Proof:

To Prove that $\phi(e) = \bar{e}$ it is enough to Prove that $\bar{a}\,\phi(e) = \phi(e)\bar{a} = \bar{a}$ for all $\bar{a} \in \bar{G}$

Let $\bar{a} \in \bar{G}$. Since $\phi = G \to \bar{G}$ is a Bijection then exist $a \in G$ such that $\phi(a) = \bar{a}$

$$\therefore \bar{a}\,\phi(e) = \phi(a)\,\phi(e) = \phi(ae) = \phi(a) = \bar{a}$$

Illy $\phi(e)\,\bar{a} = \bar{a}$

$$\phi(e) = \bar{e}$$

Property 2:

For every integer n and for every group element a in G,

$$\phi(a^n) = [\phi(a)]^n$$

Proof:

clear by (1) for $n = 0$

by induction for $n \geq 1$

For $n = 2$

$$\phi(a^2) = \phi(a \cdot a)$$

$$= \phi(a)\,\phi(a)$$

$$= [\phi(a)]^2$$

Assume $\phi(a^n) = [\phi(a)]^n$

Then $\phi(a^{n+1}) = \phi(a^n \cdot a)$

$$= \phi(a^n)\,\phi(a)$$

$$= [\phi(a)]^n \phi(a)$$

$$= [\phi(a)]^{n+1}$$

Hence $\phi(a^n) = [\phi(a)]^n$

separately true for $n = -1$

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

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

$$\Rightarrow \phi(aa^{-1}) = \phi(e) = e$$

Hence ϕ from inverse to inverse.

Property 3

For any element a and b in G, a and b commute iff $\phi(a)$ and $\phi(b)$ commute

Proof if $ab = ba$

$\Leftrightarrow \phi(ab) = \phi(ba)$

$\Leftrightarrow \phi(a)\phi(b) = \phi(b)\phi(a)$

Property 4

G is Abelian iff $\bar{G}$ is Abelian

Suppose G is Abelian.

Let $\bar{x}, \bar{y} \in \bar{G}$

Then $\bar{x} = \phi(x)$, $\bar{y} = \phi(y)$

$\bar{x}\bar{y} = \phi(x)\phi(y) \Leftrightarrow \phi(xy) = \phi(yx)$

$\Leftrightarrow \phi(y)\phi(x)$

$\Leftrightarrow \bar{y}\bar{x}$

$\therefore \bar{G}$ is Abelian.

Property 5

$|a| = |\phi(a)|$ for all a in G

(isomorphisms preserve orders).

Let e be the identity of G

$\Rightarrow \phi(e)$ is the identity of $\bar{G}$ (property 4)

Let the order of a be finite and let it be n

$\Rightarrow a^n = e$

$\phi(a^n) = \phi(e)$ (Property 2)

$[\phi(a)]^n = \phi(e)$

order of $|\phi(a)| = n$

If the order of $|a|$ be infinite. Then order of $|\phi(a)|$ can not be finite.

because of order of $|\phi(a)| = m$.

$\Rightarrow [\phi(a)]^m = \phi(a)$

$\Rightarrow \phi(a^m) = \phi(a)$ {$\phi(a^n) = [\phi(a)]^n$ for every integer n}.

$\Rightarrow a^m = e$ a contradiction

$\Rightarrow$ The order of $|\phi(a)|$ is infinite

Hence $|a| = |\phi(a)|$ for all a in G.

Property 6:

G is cyclic iff $\bar{G}$ is cyclic.

Let G be cyclic and a be its generator.

Hence $G = \langle a \rangle$

iff $n \in N \Rightarrow a^n = x$

iff $\phi(a^n) = \phi(x)$

iff $[\phi(a)]^n = \phi(x)$

iff $[\phi(a)]^n$ generators all elements $\bar{G}$

iff $\bar{G}$ is cyclic.

Property 7

For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solns in G as does the equation $x^k = \phi(b)$ in $\bar{G}$.

Soln:

Let a be a soln of $x^k = b$ in G is $a^k = b$.

$\Rightarrow \phi(a^k) = \phi(b)$ (ϕ is one to one)

$\Rightarrow [\phi(a)]^k = \phi(b)$

$\phi(a)$ is soln of $y^k = \phi(b)$ in $\bar{G}$

Hence for every soln $a \in G$ of the first equ, we get a soln $\phi(a) \in \bar{G}$ of the second equation.

Suppose $y \in \bar{G}$ is a soln $x^k = \phi(b)$

Since f is onto, there is an $x \in G$, such that $f(x) = y$.

$\Rightarrow (\phi(x))^k = y^k \Rightarrow \phi(x^k) = \phi(b) = x^k = b$

Since ϕ is one to one, for every soln $y \in \bar{G}$ of the second equation, we get $y \in G$ of the first equation because ϕ is one to one. we have.

Property 8

ϕ^{-1} is an isomorphism from $\bar{G}$ into G.

Since ϕ is one to one and onto, for every $y \in \bar{G}$, there is a unique $x \in G$ such that $\phi(x) = y$.

$$\phi^{-1}(y) = x$$

ϕ^{-1} is one to one,

so $\phi^{-1}(\phi(x)) = x$

$\Rightarrow \phi$ is onto

we need to show that homomorphism property for ϕ^{-1}: $\phi^{-1}(ab) = \phi^{-1}(a)\,\phi^{-1}(b)$

Let $\phi(x) = a$ [so $\phi^{-1}(a) = x$] and

let $\phi(y) = b$ [so $\phi^{-1}(b) = y$]

Then substituting for a and b.

$$\phi^{-1}(ab) = \phi^{-1}\{\phi(x)\,\phi(y)\}.$$

$$= \phi^{-1}\{\phi(xy)\}.$$

$$= xy$$

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

$\therefore \phi^{-1} : G^{-1} \to G$ is an isomorphism

as many x as y and the number of solns of the two equations are equal.

Property 9:

If K is a subgroup of G, then

$\phi(K) = \{\phi(k) / k \in K\}$ is a subgroup of $\bar{G}$.

proof:

Clearly $\bar{e} \in \phi(K)$, so that

$\phi(K)$ is not empty [$e \leftarrow K$, ϕ is an isomorphism]

Let $k_1, k_2 \in K$ so $k_1 k_2^{-1} \in K$ [K is a subgroup of G]

By the definition of $\phi(K), \phi(k_1), \phi(k_2) \in \phi(K)$

$\Rightarrow \phi(k_2^{-1}) \in \phi(K)$ [K is a subgroup of G, $k_2^{-1} \in K$]

So $\phi(k_1) \cdot \phi(k_2^{-1}) = \phi(k_1 k_2^{-1}) \in \phi(K)$

[ϕ is isomorphism and $\bar{K}$ is a subgroup of $\bar{G}$]

$\Rightarrow \phi(K)$ is a subgroup of $\bar{G}$.

Anita Tomar.

Automorphisms:

An isomorphism from a group G onto itself is called an automorphism of G.

Example

Let $G = SL(2,R)$ be a group of 2x2 real matrices with determinant 1. If we define a mapping from G to G itself by $f_M(A) = MAM^{-1}$ for all $A \in G$. Here M is any 2x2 real matrix with det 1. Hence f_M is an automorphism.

The isomorphism of example 7 is an automorphism of $SL(2,R)$.

Example 9:

A function ϕ from C to C given by $\phi(a+bi) = a-bi$ is an automorphism of the group of complex numbers under addition. The restriction of ϕ to C^* is also an automorphism of the group of the non zero complex numbers under multiplication.

Example 10

Let $R^2 = \{|(a,b)| \; a,b \in R\}$. Then $\phi(a,b) = (b,a)$ is an automorphism of the group R^2 under componentwise addition. Geometrically, ϕ reflects each point in the plane across the line $y = x$. More generally, any reflection across a line passing through the origin or any rotation of the plane about the origin is an automorphism of R^2.

The isomorphism in Example 7 is a particular instance of an automorphism that arises often enough to warrant a name and notation of its own.

Definition Inner Automorphism Induced by a.

Let G be a group, and let $a \in G$. The function ϕ_a, defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the inner automorphism of G induced by a.

Example 11:

The action of the inner automorphism of D_4 induced by R_{90} is given below.

x	$\xrightarrow{\phi_{R_{90}}}$	$R_{90} \times R_{90}^{-1}$
R_0	$\longrightarrow$	$R_{90} R_0 R_{90}^{-1} = R_0$
R_{90}	$\longrightarrow$	$R_{90} R_{90} R_{90}^{-1} = R_{90}$
R_{180}	$\longrightarrow$	$R_{90} R_{180} R_{90}^{-1} = R_{180}$
R_{270}	$\longrightarrow$	$R_{90} H R_{90}^{-1} = R_{270}$
H	$\longrightarrow$	$R_{90} H_{270} R_{90}^{-1} = V$
V	$\longrightarrow$	$R_{90} V R_{90}^{-1} = H$
D	$\longrightarrow$	$R_{90} D R_{90}^{-1} = D'$
D'	$\longrightarrow$	$R_{90} D' R_{90}^{-1} = D$

Theorem:

Aut (G) and Inn (G) are groups "The set of automorphism of a group and the set of inner automorphism of a group are both groups under the operation of function composition.

Proof:

Since compositions of isomorphisms are isomorphisms. Thus Aut (G) is closed under composition.

We know function composition is Associative and that the identity map is the identity automorphism.

Suppose $f \in Aut(G)$.

f^{-1} is clearly 1-1 and onto

Now $f^{-1}(xy) = f^{-1}(x) f^{-1}(y)$ (f is 1-1)

iff $xy = f(f^{-1}(x)) f[f^{-1}(y)]$

iff $xy = xy$

Thus f^{-1} is operation preserving and

. $Aut(G)$ is a group.

Now let $f_g, f_h \in Inn(G) \leq Aut(G)$

For all $x \in G$

$$f_g f_h(x) = g(hxh^{-1})g^{-1}$$

$$= ghxh^{-1}g^{-1}$$

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

$$= f_{gh}(x)$$

So $f_{gh} = f_g f_h \in Inn(G)$, and $Inn(G)$ is closed under compositi on.

Also $f_g^{-1} = f_g^{-1}$ since

$f_g^{-1} f_g(x) = f_{g^{-1}}(gxg^{-1})$

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

$= g^{-1} g x g^{-1} g$

$= e x e$

$= f_e(x)$

So, $f_{gg^{-1}} = f_g$ ($f_{g^{-1}} \circ f_g = f_{gg^{-1}}$, Inn (G) is closed under composition)

Thus Inn (G) $\leq$ Aut (G)

Inn (G) are groups

To find Inn (Z_n)

Since $Z_{12} = \{0, 1, 2 \cdots 11\}$

Inn $(Z_{12}) = \{f_0, f_1, f_2 \cdots f_{11}\}$ but the second list may have duplicates

For all $n \in Z_{12}$ and for all $x \in Z_{12}$

$f_n(x) = n + x + (-n)$

$= n + (-n) + x$

$= 0 + x$

$= 0 + x + 0$

$= f_0(x)$, the identity automorphism

Thus Inn $(Z_{12}) = \{f_0\}$.

[Since f_a may be equal to f_b even through $a \neq b$. Thus the only work involved in determining Inn (G) is deciding which distinct elements give the

distinct automorphisms.

Theorem

Aut $(Z_n) \cong U(n)$. For every positive integer n, Aut (Z_n) is isomorphic to $U(n)$

Proof:

Any automorphism a is determined by the value of $a(1)$ and $a(1) \in U(n)$

Now consider the correspondence from Aut (Z_n) to $U(n)$ given by $T : a \to a(1)$

Such that $T(a) = a(1)$

The fact that $a(k) = ka(1)$ implies that T is a one to one mapping

$(a(k)) = a\,(1+1+1 \cdots$ k times)

For if a and b belong to Aut (Z_n) and $T(a) = T(b)$. Then $a(1) = b(1)$.

Then $a(k) = ka(1)$

$= kb(1)$

$= b(k)$ for all k in Z_n

and therefore $a = b$.

To prove that T is onto let $r \in U(n)$ and consider the mapping $a : Z_n \to Z_n$ defined by $a(s) = sr \pmod n$, for all s in Z_n.

First we prove a is in automorphism of Z_n.

Suppose $\Leftarrow a(x) = a(y)$

Then $xr = yr \bmod n$

But r^{-1} exists modulo n

$\Rightarrow xrr^{-1} = yrr^{-1} \bmod n.$

$\Rightarrow x \cdot 1 = y \cdot 1 \bmod n$

$\Rightarrow x = y \bmod n$, so a is 1-1

Suppose $x \in Z_n$, so $s \in Z_n$ and

$a(s) = sr$

$= x$, so x is onto

Now Suppose $x, y \in Z_0$

$a(x+y) = (x+y)r \bmod n$

$= (xr + yr) \bmod n$

$= xr \bmod n + yr \bmod n$

$= a(x) + a(y)$

So $a \in Aut(Z_n)$

Then, since $T(a) = a(1) = r$, T is onto U(n)

Finally we establish the fact that T is operation Preserving,

Let $a, b \in Aut(Z_n)$, we then have

$T(ab) = (ab)(1) = a[b(1)]$

$= a(1+1+\cdots+1)$, $b(1)$ terms

$= a(1) + a(1) + \cdots a(1)$, $b(1)$ terms.

$= a(1)\, b(1)$

$= T(a)\,T(b)$

Thus $Aut(Z_n)$ is isomorphic to $U(n)$.

Cosets and Lagrange's Theorem

Definition

Let G be a group and let H be a non empty subset of G. For any $a \in G$, the set $[ah \mid h \in H]$ is denoted by aH. Analogously $Ha = [ha \mid h \in H]$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a subgroups of G, the set aH is called the left coset of H in G containing a, whereas Ha is called the right coset of H in G containing a. In this case, the element a is called the coset representative of aH or Ha. We use $|aH|$ to denote the number of elements in the set aH, and $|Ha|$ to denote the number of elements in Ha.

Example 1

Let $G = S_3$ and $H = \{(1), (1,3)\}$. Then the left Cosets of H in G are

$(1)H = H$

$(12)H = \{(12)(12)(13)\} = \{(12), (132)\} = (132)H$.

$(1,3)H = \{(13), (1)\} = H$

$(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H$.

Group Isomorphism

An isomorphism ϕ from a group G to a group $\overline{G}$ is a one to one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a, b \text{ in } G.$$

Example 5 :

$U(10) \neq U(12)$. This is a bit trickier to prove. First note that $x^2 = 1$ for all x in $U(12)$. Now, suppose that ϕ is an isomorphism from $U(10)$ onto $U(12)$. Then

$$\phi(9) = \phi(3 \cdot 3) = \phi(3) \cdot \phi(3) = 1$$

and

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = 1$$

Thus $\phi(9) = \phi(1)$. but $9 \neq 1$, which contradicts the assumption that ϕ is one to one.

Properties of Cosets

Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$.
2. $aH = H$ if and only if $a \in H$
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$
4. $aH = bH$ if and only if $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \phi$.
6. $aH = bH$ if and only if $a^{-1}b \in H$.
7. $|aH| = |bH|$
8. $aH = Ha$ if and only if $H = aHa^{-1}$
9. aH is a subgroup of G if and only if $a \in H$.

Proof :

1) $a = ae \in aH$.

2). To verify property 2, we first suppose that $aH = H$. Then $a = ae \in aH = H$. Next we assume that $aH \subseteq H$ and $H \subseteq aH$.

The first inclusion follows directly from the closure of H. To show that $H \subseteq aH$, let $h \in H$. Then since $a \in H$ and $h \in H$, we know that $a^{-1}h \in H$. Thus $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$.

3) This follows directly from $(ab)h = a(bh)$ and $h(ab) = (ha)b$.

4) If $aH = bH$, then $a = ae \in aH = bH$. Conversely if $a \in bH$ we have $a = bh$ where $h \in H$ and therefore $aH = (bh)H = b(hH) = bH$.

5) Property 5 follows directly from property 4, for if there is an element c in $aH \cap bH$, then $cH = aH$ and $cH = bH$.

6) Observe that $aH = bH$ if and only if $H = a^{-1}bH$. The result now follows from property 2.

7) To prove that $|aH| = |bH|$, it suffices to define a one to one mapping from aH onto bH. Obviously, the correspondence $ah \to bh$ maps aH onto bH. That it is one to one follows directly from the cancellation property.

8) Note that $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H$ - that is, if and only if $aHa^{-1} = H$.

9) If aH is a subgroup, then it contains the identity e. Thus $aH \cap eH \neq \phi$ and by property 5, we have $aH = eH = H$. Thus from property 2, we have $a \in H$. Conversely if $a \in H$, then again by property 2, $aH = H$.

Lagrange's Theorem : $|H|$ divides $|G|$.

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover the number of distinct left (right) cosets of H in G is $|G|/|H|$.

Proof :

Let $a_1H, a_2H \cdots a_rH$ denote the distinct left cosets of H in G. Then for each a in G, we have $aH = a_iH$ for some i. Also by property 1 of the lemma, $a \in aH$. Thus each member of G belongs to one of the cosets a_iH. In symbols

$$G = a_1H \cup \cdots \cup a_iH$$

Now property 2 of the lemma shows that this union is disjoint

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Finally since $|a_iH| = |H|$ for each i, we have $|G| = r|H|$

We pause to emphasize that Lagrange's theorem is a candidate criterion : that is, it provides a list of candidates for the orders of the subgroups of a group. Thus a group of order 12 may have subgroup of order $12, 6, 4, 3, 2, 1$ but no others.

A special name and notation have been adopted for the number left (or right) cosets of a subgroup in a group. The index of a subgroup H in G is the number of left cosets of H in G. This number is denoted by $|G:H|$. When G is finite, Lagrange's theorem tells us that $|G:H| = |G|/|H|$.

Corollary 1:

If G is a finite group and H is a subgroup of G, then $|G:H| = |G|/|H|$.

Corollary 2:

In a finite group, the order of each element of the group divides the order of the group.

Corollary 3:

Groups of prime order are cyclic.

A group of prime order is cyclic.

Proof:

Suppose that G has prime order. Let $a \in G$ and $a \neq e$. Then, $|\langle a \rangle|$ divides $|G|$ and $|\langle a \rangle| \neq 1$. Thus $|\langle a \rangle| = |G|$ and the corollary follows.

Fermat's Little Theorem:

For every integer a and every prime p,

$a^p \bmod p = a \bmod p$.

proof:

By the division algorithm $a = pm + r$, where $0 \leq r < p$, Thus $a \bmod p = r$, and it suffices to prove that $r^p \bmod p = r$. If $r = 0$, the result is trivial, so we may assume that $r \in U(p)$. [Recall that $U(p) = 1, 2, \ldots p-1$] under multiplication modulo p.] Then by the preceding corollary $r^{p-1} \bmod p = 1$ and therefore $r^p \bmod p = r$.

Fermat's little theorem has been used in conjuction with computers to test for primality of certain numbers. One case concerned the number $p = 2^{257} - 1$. If p is prime, that we know from Fermat's Little Theorem that 10^p ~~and~~ mod $p = 10 \bmod p$ and therefore $10^{p+1} \bmod p = 100 \bmod p$.

Using multiple precision and a simple loop, a computer was able to calculate $10^{p+1} \bmod p = 10^{2^{257}} \bmod p$ in a few seconds. The result was not 100, and so p is not prime.

Theorem 7.2

For two finite subgroups H and K of a geoup. define the set $HK = \{hk \mid h \in H, k \in K\}$. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof :

Although the set HK has $|H||K|$ products not all of these products need represent distinct group elements. That is, we may have $hk = h'k'$ where $h \neq h'$ and $k \neq k'$. To determine $|HK|$, we must find the extend to which is happen. For every t in $H \cap K$, the product is $hk = (ht)(t^{-1}k)$, se each group element in HK is represented by atleast $|H \cap K|$ products in HK. But $hk = h'k'$ implies ~~$t = h^{-1}h' = kk^{t-1} \in H$~~

$t = h^{-1}h' = kk^{-1} \in H \cap K$, so that $h' = ht$ and $k' = t^{-1}k$.
Thus each element in HK is represented by exactly $|H \cap K|$ products so, $|HK| = \frac{|H||K|}{|H \cap K|}$

Stabilizer of a point:
Let G be a group of permutations of a set S.
For each i in S, let $stab_G(i) = [\phi \in G \mid \phi(i) = i]$.
We call $stab_G(i)$ the stabilizer of i in G.

Orbit of a point:
Let G be a group of permutations of a set S.
For each s in S, let $orb_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $orb_G(s)$ is a subset of S called the orbit of s under G. We use $|orb_G(s)|$ to denote the number of elements in $orb_G(s)$.

Unit-3

Normal Subgroups and factor groups

Def : Normal subgrmp :

A subgrmp H of a grmp G is called a Normal subgrmp of G if $aH = Ha$ for all a in G usually denoted by $H \triangleleft G$.

$\left.\begin{array}{l} \because H < G \text{ - subgrmp} \\ H \triangleleft G. \ N \cdot \text{subgrmp} \end{array}\right\}$

Theorem : Normal Subgroup Test

A subgrmp H of G is normal in G iff

$\boxed{xHx^{-1} \subseteq H}$ $\forall x \in G$ sny $H \triangleleft G$.

Proof:

$\Rightarrow$ suppose $H \triangleleft G$.

we claim $xHx^{-1} \subseteq H$ for any $x \in G$. Let $x \in G$ and then an element in xHx^{-1} look like xhx^{-1} for some $h \in H$. Then observe that $xhx^{-1} = h'xx^{-1}$

$= h' \in H$.

Conversely.

$\Leftarrow$ Suppose $xHx^{-1} \subseteq H$ for all $x \in G$.

We claim $xH = Hx$. Note that :

$xH = xHx^{-1}x \subseteq Hx$ and that

$Hx = xx^{-1}Hx \subseteq xH$.

We have $x^{-1}Hx \subseteq H$ because the supposition is true for x^{-1}.

Example : 1

In an abelian group every subgroup H is normal because for all $h \in H$ and $a \in G$. we have $ah = ha$

Example : 2

The center of a group is a normal subgroup because for all $h \in Z(G)$ and $a \in G$ we have $ah = ha$.

Example : 3

Consider the subgroup $H = \{(), (123), (132)\}$ of S_3. Observe that we have the following left cosets.

$() H = \{(), (123), (132)\}$

$(12) H = \{(12), (23), (13)\}$

$(13) H = \{(13), (12), (23)\}$

$(23) H = \{(23), (13), (12)\}$

$(123) H = \{(123), (132), ()\}$

$(132) H = \{(132), (), (123)\}$

and we have the following right cosets

$H(\,) = \{(\,), (123), (132)\}$

$H(12) = \{(12), (13), (23)\}$

$H(13) = \{(13), (23), (12)\}$

$H(23) = \{(23), (12), (13)\}$

$H(123) = \{(123), (132), (\,)\}$

$H(132) = \{(132), (\,), (123)\}$

We see that we have

$(\,)H = H(\,)$, $(12)H = H(12)$, $(13)H = H(13)$, $(23)H = H(23)$, $(123)H = H(123)$, $(132)H = H(132)$.

Factor Groups : (or) Quotient group

Let G be a group and $H \triangleleft G$. then the set G/H of all cosets of H in G together with the binary Composition defined by

$HaHb = Hab$, where $Ha \in G/H$, $Hb \in G/H$ is a group, and is called the factor group of G by H.

Theorem 9.2 (Hölder, 1889) factor groups

Let G be a group and H a normal subgroup of G. The set $G/H = \{aH / a \in G\}$ is a group under the operation $(aH)(bH) = abH$.

Proof :

Any given left coset will have multiple representatives because we know that aH and $a'H$

can be identical for $a \neq a'$. Consequently we first need to be sure that our operation is well defined, meaning that if we choose $a'H = aH$ and $b'H = bH$ and we do $(a'H)(b'H) = a'b'H$

we $(aH)(bH) = abH$.

In other word we must verify that

$abH = a'b'H$. $\because a'H = aH$ and since $a' \in a'H$ we have $a' = ah_1$ and $b' = bh_2$ $\forall$ $h_1 h_2 \in H$.

$$a'b'H = ah_1 bh_2 H$$
$$= abh_1 h_2 H$$
$$= abH$$

* The identity is eH
* The inverse of aH is $a^{-1}H$
* Associativity follows since $(aH)(bHcH) = (aH)(bcH)$

$$= abcH$$
$$= (abH)(cH)$$
$$= (aHbH)cH.$$

Example : If $G = \mathbb{Z}$ and $h = 4\mathbb{Z}$ then there are four distinct cosets :

$$0+4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8 \ldots\}$$
$$1+4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$2+4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$3+4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

These four cosets form a group with set :

$$\{0+4\mathbb{Z},\ 1+4\mathbb{Z},\ 2+4\mathbb{Z},\ 3+4\mathbb{Z}\}$$

The Operation is :

$$(a+4\mathbb{Z}) + (b+4\mathbb{Z}) = (a+b)+4\mathbb{Z}$$

So for example : $(3+4\mathbb{Z}) + (2+4\mathbb{Z}) = 5+4\mathbb{Z} = 1+4\mathbb{Z}$

We immediately notice that $\mathbb{Z}/4\mathbb{Z} \approx \mathbb{Z}_4$.

Example : cayley table is

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

clearly, then $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$.

$\therefore \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$n > 0$. $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n \cdots\}$. then

$\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

Example :

Let $G = \mathbb{Z}_{18}$ & $H = \langle 6 \rangle = \{0, 6, 12\}$

$G/H = \{0+H,\ 1+H,\ 2+H,\ 3+H,\ 4+H,\ 5+H\}$

Consider, $(5+H) + (4+H) = 9+H$

$= 3+H$

since it absorbs all multiple of 6.

~~Example~~

Theorem : The G/z theorem

State : Let G be a group and let $z(G)$ be the center of G. If $G/z(G)$ is cyclic, then G is Abelian

Proof :

Let $gz(G)$ be a generator of the factor group $G/z(G)$, and let $a, b \in G$. Then there exist integer i and j such that

$$az(G) = (gz(G))^i = g^i z(G)$$

and

$$bz(G) = (gz(G))^j = g^j z(G)$$

Thus, $a = g^i x$ for some x in $z(G)$ and $b = g^j y$ for some y in $z(G)$. It follows then that

$$\begin{aligned} ab = (g^i x)(g^j y) &= g^i (x g^j) y \\ &= g^i (g^j x) y \\ &= (g^i g^j)(xy) \\ &= (g^j g^i)(yx) \\ &= (g^j y)(g^i x) \\ &= ba \end{aligned}$$

Theorem : $G/Z(G) \cong Inn(G)$

Statement :

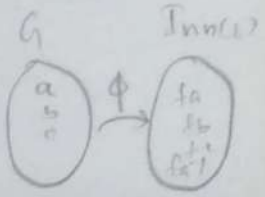
For any group G, $G/Z(G)$ is isomorphic to $Inn(G)$.

Proof :

Let us define a function

$\phi : G \longrightarrow Inn(G)$ defined by

$\phi(a) = f_a^{-1} \quad \forall \ a \in G.$



ϕ is well defined

let $a = b \qquad \forall a, b \in G.$

$$axa^{-1} = bxb^{-1}$$

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

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

$$f_{a^{-1}} = f_{b^{-1}}$$

$$\Rightarrow \quad \phi(a) = \phi(b)$$

$\therefore \phi$ is well defined.

ϕ is homomorphism.

$\phi(ab) = \phi(a) \cdot \phi(b)$

Let $a, b \in G \Rightarrow ab \in G$

$$\phi(ab) = f_{(ab)^{-1}}$$

$$= f_{b^{-1}a^{-1}}$$

$$= fa^{-1} \circ fb^{-1}$$

$$\phi(ab) = \phi(a) \circ \phi(b)$$

$\Rightarrow \therefore \phi$ is a homomorphism

Since $\phi : G \longrightarrow Inn(G)$ is a homomorphism. Therefore by fundamental theorem of group homomorphism, we have

$$\phi(G) \cong \frac{G}{Ker\,\phi}$$

(or) $$\frac{G}{Ker\,\phi} \cong \phi(G) \quad \text{——} (1)$$

ϕ is onto

let $fa^{-1} \in Inn(G)$

$\Rightarrow a^{-1} \in G$

$\Rightarrow a \in G$

s.t $\Rightarrow \phi(a) \in fa^{-1}$

$\therefore \forall\, fa^{-1} \in Inn(G) \quad \exists \quad a \in G$

$\therefore \phi$ is onto

$\Rightarrow \phi(G) = Inn(G) \quad \text{——} (2)$

from (1) and (2),

$$\frac{G}{Ker\,\phi} \cong Inn(G) \quad \text{——} (3)$$

Now we show that,

$$\text{Ker } \phi = z(G) = Z$$

$$\text{Ker } \phi = \{ a \in G : \varphi(a) = I \}$$

$$= \{ a \in G : fa^{-1} = I \}$$

$$= \{ a \in G : fa^{-1}(x) = I(x) \}$$

$$= \{ a \in G : (a^{-1})^{-1} x a^{-1} = x \} \quad \forall x \in G$$

$$= \{ a \in G : axa^{-1} = x \}$$

$$= \{ a \in G : axa^{-1}a = xa \} \quad \forall x \in G$$

$$= \{ a \in G : ax = xa \} \quad \forall x, x \in G$$

$$\therefore \text{Ker } \phi = z(G) \quad \text{---------} \quad (4)$$

from (3) and (4) we have,

$$\frac{G}{z(G)} \cong \text{Inn}(G)$$

Hence the proof.

Cauchy's Theorem

Theorem : Existence of Elements of Prime order.

Statement : Let G be a finite abelian group and let p be a Prime that divides the order of G. Then G has an element of order p.

Proof :

$P(n)$: Let G be a finite abelian group of order n and let 'p' be a Prime that divides n. Then G has an element of order p., $n \geq 2$.

for $n = 2$, which is Prime $\Rightarrow G$ is cyclic

$\Rightarrow G = \langle x^n \rangle$ for $x \in G$

$G = \{e, a\}$

$= |x| = 2$

$P(n)$ is true for $n = 2$.

let assume that,

$P(k)$ is true for $k < n$ —— (1)

We will show that $P(n)$ is true.

Let $o(G) = u$

Claim : G has an element of Prime order.

let $x \in G$ s.t $x \neq e$

Let $|x| = m$, $m > 1$

if m is Prime , we are done.

if m is not prime, then

$m = qr$ for some $q, r \in \mathbb{Z}$ with q is Prime

$$(x^r)^q = x^{qr}$$
$$= x^m$$
$$= e$$

$\Rightarrow |x^r| = q$ which is Prime

$\Rightarrow G$ always has an element of prime order

let that element x with $|x| = q$, is Prime

Let define $H = \langle x \rangle = \{x^m / x \in \mathbb{Z}\}$

$\downarrow$

cyclic subgroup with $|H| = q$

$\Rightarrow H \Delta G$

Let $\frac{G}{H} \Rightarrow O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)} = \frac{n}{q} < n$ $(\because q > 1)$

$\frac{G}{H}$, with abelian and $\left|\frac{G}{H}\right| < n$.

$\left|\frac{G}{H}\right| = \frac{n}{q} \Rightarrow P \left| \frac{n}{q} \right|$ $(\because P/n$ and q is prime$)$

$\Rightarrow P / \left|\frac{G}{H}\right|$

by assumption (1)

we have an element $yH \in \frac{G}{H}$

such that $|yH| = p$

$\Rightarrow (yH)^p = H$ (H is identity of $\frac{G}{H}$)

$\Rightarrow y^p H = H$

$\Rightarrow y^p \in H$

Case-I if $y^p = e$

$\Rightarrow |y| = p \quad y \in G$

Case-II if $y^p \neq e$

$|y^p| = q$

$(y^q)^p = e$

$|y|^q = p$

let $z = y^q \in G$

$\Rightarrow |z| = p$

$|G| \rightarrow |x| = q$

prime $\Rightarrow \frac{G}{H = \langle x \rangle}$

$\therefore |yH| = p$

ii) $y/y^q = p$

Hence the Proof

~ o ~

Def: Internal Direct Product of H and K.

Let H and K be normal subgroups of a group G. we say that G is the internal direct Product of H and K and write $G = H \times K$ if

$$G = HK \quad \text{and} \quad H \cap K = \{e\}$$

Example: In $U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$,

let $H = \{1, 17\}$, $K = \{1, 13\}$ Then

$HK = \{1, 13, 17, 5\}$, since $5 = 17 \cdot 13 \bmod 24$.

Definition: Internal Direct Product of $H_1 \times H_2 \times \dots \times H_n$.

Let $H_1, H_2, \dots, H_n$ be a finite collection of normal subgroups of G. we say that G is the internal direct Product of $H_1, H_2, \dots, H_n$ and write $G = H_1 \times H_2 \times \dots \times H_n$, if

1. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \dots h_n \mid h_i \in H_i\}$
2. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \dots n-1$

Section : Group Homomorphism

Def: Group homomorphism

A homomorphism ϕ from a group G to a group $\bar{G}$ is a mapping from G into $\bar{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a) \cdot \phi(b)$ for all $a, b \in G$.

Def: Kernal of a Homomorphism

The kernal of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernal of ϕ is denoted by $\ker \phi$.

Properties of homomorphisms

Thm: Properties of Elements under homomorphisms.

Let ϕ be a homomorphism from a group G to a group $\bar{G}$ and let g be an element of G. Then

1. ϕ carries the identity of G to the identity of $\bar{G}$.
2. $\phi(g^n) = (\phi(g))^n$
3. If $|g| = n$, then $|\phi(g)|$ divides n.
4. If $\phi(g) = g'$. Then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\ker\phi$.

Proof:

(1). Let e be the identity element of G. and e' be the identity element of G'.

$\therefore e \cdot e = e$

$\Rightarrow \phi(e \cdot e) = \phi(e)$

$\Rightarrow \phi(e) \cdot \phi(e) = \phi(e) \cdot e'$ { $\because$ by properties of homo/- }

Applying left cancellation law

$\phi(e) = e'$

(2). $\phi(g^n) = [\phi(g)]^n$ for all $n \in \mathbb{Z}$

$$\phi(g^n) = \phi(\underbrace{g \cdot g \cdots g}_{n\text{-times}})$$

$$\phi(g^n) = \underbrace{\phi(g) \cdot \phi(g) \cdots \phi(g)}_{n\text{-times}}$$

$\therefore \phi(g^n) = [\phi(g)]^n$.

(3). $|\phi(g)|$ divides $|g|$ if $|g|$ is finite

Let $|g| = n$

$\Rightarrow g^n = e$

Then $\phi(g^n) = \phi(e)$

$\Rightarrow [\phi(g)]^n = e'$ {by Property 2}

$\Rightarrow |\phi(g)|$ divides n

$\Rightarrow |\phi(g)|$ divides $|g|$

Hence the proof.

(A). Let $x \in \phi^{-1}(g')$

$\Rightarrow \phi(x) = g'$

$\Rightarrow \phi(x) = \phi(g)$ (by statement)

$\Rightarrow \phi(\bar{g}^{-1}) \cdot \phi(x) = \phi(\bar{g}^{-1}) \cdot \phi(g)$.

$\Rightarrow \phi(\bar{g}^{-1} \cdot x) = \phi(\bar{g}^{-1} \cdot g)$ (ϕ is homo/-)

$\Rightarrow \phi(\bar{g}^{-1} \cdot x) = \phi(e)$ $\{\because \bar{g}^{-1} \cdot g = e\}$

$\Rightarrow \phi(\bar{g}^{-1} \cdot x) = \bar{e}$ {By prop 1}

$\Rightarrow \bar{g}^{-1} \cdot x \in \ker \phi$

$\Rightarrow x \in g \ker \phi$

$\Rightarrow \phi^{-1}(g') \subseteq g \ker \phi$ —(1)

Conversely,

let $z \in g \ker \phi$

$z = gu$ where $u \in \ker \phi$.

we have to Prove that

$z \in \phi^{-1}(g')$

Now, $\phi(z) = \phi(gu)$

$= \phi(g) \cdot \phi(u)$ $\{\because \phi$ is homo/- $\}$

$= \phi(g) \cdot \bar{e}$ $\{\because u \in \ker \phi\}$

$\therefore \phi(z) = g'$

$\therefore \quad z \in \phi^{-1}(g')$

$\Rightarrow g \ker\phi \subseteq \phi^{-1}(g') \quad \text{—} (2)$

from (1) & (2)

$\phi^{-1}(g') = g \ker\phi$

Hence the Proof.

Theorem: Properties of subgroups under homomorphism.

Let ϕ be a homo/- from a group G to a group $\bar{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{ \phi(h) \mid h \in H \}$ is a subgroup of $\bar{G}$.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. If H is Abelian, then $\phi(H)$ is Abelian.
4. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$
5. If $|\ker\phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.
6. If $|H| = n$, then $|\phi(H)|$ divides n.
7. If $\bar{K}$ is subgroup of $\bar{G}$, then $\bar{\phi}^{-1}(\bar{K}) = \{ k \in G / \phi(k) \in \bar{K} \}$ is a ~~normal~~ subgroup of G.
8. If $\bar{K}$ is a normal subgroup of $\bar{G}$, then $\bar{\phi}^{-1}(\bar{K}) = \{ k \in G / \phi(k) \in \bar{K} \}$ is a normal subgroup of G.

9. If ϕ is onto and $\ker\phi \supset \{e\}$, then ϕ is an isomorphism from G to G'.

Proof: (1) Obviously $\phi(H) \subseteq G'$

Let $a', b' \in \phi(H)$. So

$\phi(a) = a'$ and $\phi(b) = b'$ $\forall\ a, b \in H$.

$\Rightarrow a'b'^{-1} = \phi(a) \cdot [\phi(b)]^{-1}$ $\{\because \phi(g^n) = [\phi(g)]^n\}$.

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

$= \phi(ab^{-1}) \in \phi(H)$

$\Rightarrow \phi(H)$ is a subgroup of G'. $\{\because H$ is subgroup of G, $ab^{-1} \in H\}$.

(2) Let $y \in \phi(H)$ so $\phi(x) = y$ $\forall\ x \in H$.

Let a be a generator of H, so $\forall\ n \in N$ s.t

$a^n = x$.

Now, $[\phi(a)]^n = \phi(a^n)$ $\{\because$ by prop$^{ty}\}$

$= \phi(x)$

$= y \in \phi(H)$.

Since the choice of y is arbitrary, $\phi(a)$ generates all elements of $\phi(H)$, making $\phi(H)$ is cyclic.

Proof (3): Let $a'b' \in \phi(H)$ so

$\phi(a) = a'$ and $\phi(b) = b'$ $\forall\ a^2, b^2 \in H$

so $a' \cdot b' = \phi(a) \cdot \phi(b)$

$= \phi(ab)$

$= \phi(ba)$

$= \phi(b) \cdot \phi(a)$ $\{\because H \text{ is abelian}\}$

$a' \cdot b' = b' a'$

$\Rightarrow \phi(H)$ is abelian

(4). Let $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(G)$

Then $\phi(g) \cdot \phi(h) \phi(\bar{g})^{-1} = \phi(gh\bar{g}^{-1}) \in \phi(H)$.

since H is normal in G, $gh\bar{g}^{-1} \in H$

Hence $\phi(H)$ is normal in $\phi(G)$.

(5). since all cosets of $\ker\phi = \phi^{-1}(e)$

have the same number of elements

$\phi(a) = \phi(b)$ iff

$a \ker\phi = b \ker\phi$

Proof (6) Let $\phi(H)$ denote the restriction of ϕ to the elements of H. Then $\phi(H)$ is a homo- from H onto $\phi(H)$.

$\Rightarrow$ suppose $|\ker \phi(H)| = t$.

Then, by Property (5),

$\phi(H)$ is a t-to-1 mapping.

so $|\phi(H)|\, t = |H|$.

(7). clearly, $e \in \phi^{-1}(K')$, so that $\phi^{-1}(K')$ is not empty.

Let $k_1, k_2 \in \phi^{-1}(K')$.

$\Rightarrow$ By the defn of $\phi^{-1}(K')$, $\phi(k_1), \phi(k_2) \in K'$

$\Rightarrow \phi(k_2)^{-1} \in K'$. $\{\because K'$ is subgroup of $G'\}$

So $\phi(k_1 k_2^{-1}) = \phi(k_1) \cdot \phi(k_2)^{-1} \in K'$

$\Rightarrow k_1 k_2^{-1} \in \phi^{-1}(K')$

(8). Here, $x\phi^{-1}(K')x^{-1} = xKx^{-1}$, where $\phi(k) \in K'$, $x \in G$

Now $\phi(xkx^{-1}) = \phi(x).\phi(k).\phi(x^{-1})$.

$= \phi(x).\phi(k).[\phi(x)]^{-1}$

$\Rightarrow xKx^{-1} \in \phi^{-1}(K')$.

(9). For this we shall show that ϕ is $1-1$

Let $x, y \in G$ s.t $\phi(x) = \phi(y)$.

$\Rightarrow \phi(x).\phi(y^{-1}) = \phi(y)[\phi(y)]^{-1}$

$\Rightarrow \phi(x).\phi(y^{-1}) = e'$

$\Rightarrow \phi(xy)^{-1} = e'$

$\Rightarrow xy^{-1} \in \ker\phi$

$\Rightarrow xy^{-1} = e$

$\Rightarrow (xy^{-1})y = ey$

$\Rightarrow x(y^{-1}y) = ey$

$\Rightarrow x = y$.

~ or ~

Theorem: First Isomorphic Theorem

Statement:

Let ϕ be a group homomorphism from G to $\bar{G}$. Then the mapping from $G/\ker\phi$ to $\phi(G)$ given by $g\ker\phi \to \phi(g)$, is an isomorphism.

In symbols, $G/\ker\phi \approx \phi(G)$.

Proof:

Let $\ker\phi = K$

$$\frac{G}{K} = \{xK : x \in G\}$$

We define $\varphi : \frac{G}{K} \to G'$ such that

$$\phi(gK) = \phi(g)$$

1. ϕ is well defined

Let $g_1K, g_2K \in \frac{G}{K}$ such that

$$g_1K = g_2K$$

$$g_2^{-1}g_1K = g_2^{-1}g_2K$$

$$g_2^{-1}g_1K = K$$

$$\Rightarrow \quad g_2^{-1}g_1 \in K$$

$$\Rightarrow \phi(g_2^{-1}g_1) = e' \qquad \text{(By defn of Ker)}$$

$$\Rightarrow \phi(g_2^{-1})\phi(g_1) = e'$$

$$\phi(g_1) = \phi(g_2)$$

$$\phi(g_1K) = \phi(g_2K)$$

$\Rightarrow$ ϕ is well defined.

2. ϕ is 1-1

Let $g_1K, g_2K \in \frac{G}{K}$ such that

$$\phi(g_1K) = \phi(g_2K)$$

$$\phi(g_1) = \phi(g_2)$$

$$[\phi(g_2)]^{-1}\phi(g_1) = e'$$

$$\Rightarrow \phi(g_2^{-1})\phi(g_1) = e' \quad \text{(by defn of ker)}$$

$$\Rightarrow g_2^{-1}g_1 \in K$$

$$g_2^{-1}g_1K = K$$

$$\Rightarrow g_1K = g_2K$$

$\Rightarrow \phi$ is one-one

3. ϕ is onto:

$$\text{Img}(\phi) = \{\phi(gK) : g \in G$$

$$= \{\phi(g) : g \in G$$

$$= \text{Img}\,\phi$$

$$= G'$$

$\Rightarrow \phi$ is onto

4. ϕ is homomorphism

Let $g_1K, g_2K \in G/K$

$$\phi(g_1Kg_2K) = \phi(g_1Kg_2)$$

$$= \phi(g_1Kg_2)$$

$$= \phi(g_1g_2K)$$

$$= \phi(g_1g_2)$$

$$\phi(g_1 \quad = \phi(g_1)\phi(g_2)$$

$\varphi(g_1K g_2K) = \varphi(g_1K)\ \varphi(g_2K)$

$\therefore$ φ is homomorphism.

$\therefore$ Then $\frac{G}{K} \approx \varphi(G)$

$\frac{G}{\text{Ker}\varphi} \approx \phi(G)$

Hence the proof

$\sim$ —

UNIT-5

RING HOMOMORPHISM

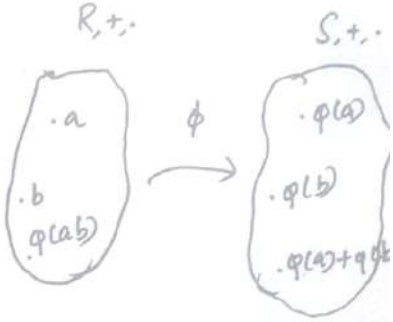
Defn: Ring homomorphism:

A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operation.

ie for all a, b in R.

$$\phi(a+b) = \phi(a) + \phi(b)$$

and $$\phi(ab) = \phi(a) \cdot \phi(b).$$



Ring Isomorphism:

A ring homomorphism homomorphism that is both one-to-one and onto is called a ring isomorphism.

Example :-1.

For any positive integer n the mapping $k \to k \bmod n$ is a ring homomorphism from Z onto Z_n. This mapping is called the natural homomorphism from Z to Z_n

(ii) $\langle Z, +, \cdot \rangle$ and $\langle Z_n, +_n, \times_n \rangle$ are two Ring.

$$\phi : Z \to Z_n \text{ as}$$

$$\phi(x) = x \bmod n \quad \forall x \in Z$$

Let $x, y \in Z$ to show

1. $\phi(x+y) = \phi(x) + \phi(y)$
2. $\phi(xy) = \phi(x) \times \phi(y)$.

$$\phi(x+y) = (x+y) \bmod n$$

$$= (x \bmod n + y \bmod n) \bmod n$$

$$= x \bmod n + y \bmod n$$

$$= \phi(x) + \phi(y)$$

$$\phi(xy) = (xy) \bmod n$$

$$= [(x \bmod n).(y \bmod n)] \bmod n$$

$$= x \bmod n \cdot y \bmod n$$

$$= \phi(x) \times \phi(y)$$

∴ Hence ϕ is Ring homomorphism.

Example -2

The mapping $a+bi \to a-bi$ is a ring isomorphism from the complex numbers onto the complex numbers.

(ii) $\langle \mathbb{C}, +, \cdot \rangle$ be a ring.

$\phi : \mathbb{C} \to \mathbb{C}$ as

$\phi(a+ib) = a-ib \quad \forall a,b \in R$

$\phi(z) = \bar{z}$ where $z = a+ib \in \mathbb{C}$.

Let $z_1, z_2 \in \mathbb{C}$ (ii) $z_1 = a+ib$
$z_2 = c+id$.

to show,

1. $\phi(z_1+z_2) = \phi(z_1) + \phi(z_2)$
2. $\phi(z_1 z_2) = \phi(z_1) \cdot \phi(z_2)$

1. $\phi(z_1+z_2) = \phi(a+ib+c+id)$

$= \phi(a+c) + i(b+d)$

$= (a+c) - i(b+d)$

$= a-ib+c-id$

$\phi(z_1+z_2) = \phi(z_1) + \phi(z_2)$

2. $\phi(z_1 \cdot z_2) = \phi[(a+ib)(c+id)]$

$= \phi(ac-bd+i(ad+bc))$

$= \phi(ac-bd+i(ad+bc))$

$= ac-bd-i(ad+bc)$

$= ac-bd-iad-ibc$

$= ac-iad-bd-ibc$

$= a(c-id) - ib(c-id)$

$= (a-ib)\ (c-id)$

$\varphi(z_1 \cdot z_2) = \varphi(z_1) \cdot \varphi(z_2)$

$\therefore \varphi$ is a Ring homomorphism isomorphism

PROPERTIES OF RING HOMOMORPHISMS

Let ϕ be a homomorphism from a ring R to a ring S. Let A be a subring of R and B an ideal of S.

Property - 1.

For any $r \in R$ and any positive integer n, $\varphi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.

Proof:

Given $\phi : R \to S$ is homomorphism.

We know that $2+2+2+2 = 4(2)$

$4+4+4+4+4 = 5(4)$

Use this,

$\varphi(nr) = \varphi(r+r+r+\ldots r \text{ (n times)})$

$= \varphi(r) + \varphi(r) + \varphi(r) + \ldots \varphi(r)$ n times

$\therefore \boxed{\phi(nr) = n\phi(r)}$

The we have to prove

$$\phi(r^n) = [\phi(r)]^n$$

Proof:

$$\phi(r^n) = \phi(r \times r \times r \times \ldots \ldots r \text{ (n times)}$$

$$= \phi(r) \times \phi(r) \times \phi(r) \times \ldots \phi(r) \text{ n times.}$$

$$\therefore \boxed{\phi(r^n) = [\phi(r)]^n}$$

Property - 2

$\phi(A) = \{\phi(a) : a \in A\}$ is a subring of S

Proof:

Given $\phi : R \to S$ is homomorphism

A is subring of R.

We have to show that $\phi(A)$ is a subring of S (i.e) $\phi(A) = \{\phi(a) : a \in A\}$

To show that $\phi(A)$ is a subring we have to show that:

1. $\phi(A)$ is non-empty
2. if $a', b' \in \phi(A) \Rightarrow a' - b' \in \phi(A)$
3. if $a', b' \in \phi(A) \Rightarrow a'b' \in \phi(A)$

1. We know that 0 of A always maps to 0' of A.

$$\Rightarrow \phi(0) = 0'$$

$\Rightarrow \phi(A)$ contains $0'$

$\Rightarrow \phi(A)$ is non empty and $\phi(A) \subseteq S$ —①

2. Let $a', b' \in \phi(A)$

since $\phi : R \to S$ $\exists\ a, b \in A$

s.t $\phi(a) = a'$, $\phi(b) = b'$

$$a' - b' = \phi(a) - \phi(b)$$
$$= \phi(a-b)$$
$$\in (A)$$

{$\because a \in A, b \in A$ and A is subring $(a-b) \in A$.

$\therefore a' - b' \in \phi(A)$.

3. $a', b' \in \phi(A)$

$\Rightarrow$ a and b such that $\phi(a) = a'$, $\phi(b) = b'$

$$\therefore \phi(a'b') = \phi(a)\,\phi(b)$$
$$= \phi(ab)$$
$$\therefore \phi(a'b') \in \phi(A)$$ {$\because$ A is an ideal}

and other properties of Ring homomorphisms as follows.

* If A is an ideal and ϕ is onto S,

then $\phi(A)$ is an ideal.

* $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.

* If R is commutative, then $\phi(R)$ is commutative.

* If R has a unity 1, $S \neq \{0\}$ and ϕ is onto, then $\phi(1)$ is the unity of S.

* ϕ is an isomorphism iff ϕ is onto and

$$\ker \phi = \{r \in R \mid \phi(r) = 0\} = 0.$$

* If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

The proof of these properties are similar to properties of homomorphism.

Theorem: (Kernels Are Ideals.)

Let ϕ be a homomorphism from a ring S. Then $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem: (First Isomorphism theorem for Rings.)

Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker \phi$ to $\phi(R)$,

given by $r + \ker\phi \longrightarrow \phi(r)$ is an isomorphism.

In symbols,

$$R/\ker\phi \approx \phi(R).$$

Theorem: Ideals Are Kernels.

Every ideal of a ring R is the kernal of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \longrightarrow r+A$ from R to R/A.

Theorem: Homomorphism from z to a Ring with Unity

Statement

Let R be a ring with unity e. The mapping $\phi : z \to R$ given by $n \to ne$ is a ring homomorphism

Proof:

Given the mapping $\phi : z \to R$ and $n \to ne$

$$\therefore \phi(n) \to ne.$$

Let $m, n \in z$. To show that addition is preserved. we consider three cases.

(i) First suppose that both m and n are non-negative (ie) $m \geq 0$ and $n \geq 0$

Then $\varphi(m+n) = (m+n)e$

$= e+e+e \ldots\ldots +e$ {$(m+n)$ times

$= \underbrace{(e+e+e+\ldots+e)}_{m \text{ times of } e} + \underbrace{(e+e+e+\ldots+e)}_{n \text{ times of } e.}$

$= me + ne$

$\varphi(m+n) = \varphi(m) + \varphi(n)$

Case-ii Suppose that both m and n are negative

(ie) $m < 0$ and $n < 0$.

Then,

$\phi(m+n) = (m+n)e$

$= (-m-n)(-e)$

$= (-m)(-e)+(-n)(-e)$

$= me + ne$

$\phi(m+n) = \varphi(m) + \varphi(n)$

Case-iii) Suppose that one of m and n is non-negative and the other is negative,

(ie) $m \geq 0$, $n < 0$

$\Rightarrow \phi(m+n) = (m+n)e$

$= \underbrace{(e+e+\ldots+e)}_{m \text{ times}} - \underbrace{(e+e+\ldots+e)}_{-n \text{ times}}$

$$= me + (-n)(-e)$$

$$= me + ne$$

$$\phi(m+n) = \phi(m) + \phi(n)$$

So, ϕ preserved addition.

Now the multiplication can be handled in a single case the aid of previous proof.

i.e. $(ma)(nb) = (mn)(ab)$

for all integers m and n.

Thus $\phi(mn) = (mn)e$

$$= (me)(ne)$$

$$= \phi(m) \cdot \phi(n)$$

So ϕ is preserves multiplication as well.

Hence the proof.

~!~

THE FIELD OF QUOTIENTS

Theorem: (Field of Quotients)

Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

Proof:

Let S be the set of all formal symbols of the form $\frac{a}{b}$ where $a, b \in D$ and $b \neq 0$.

Define an equivalence relation $\equiv$ on S by

$$\frac{a}{b} \equiv \frac{c}{d}$$

if $ad = bc$

Now, let F be the equivalence classes of S under the relation $\equiv$ and denote the equivalence class that contains $\frac{x}{y}$ by $[x/y]$.

We define addition and multiplication on F by

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = [(ad+bc)/bd]$$

and

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = [ac/bd]$$

(noticed that here we need the fact that D is an integral domain to ensure that multiplication is closed: that is, $bd \neq 0$ whenever $b \neq 0$ and $d \neq 0$).

Since there are many representations of any particular element of F, we must to show that these two operation are well defined.

To do this, suppose that,

$$[a/b] = [a'/b'] \text{ and } [c/d] = [c'/d']$$

So that,

$$ab' = a'b \text{ and } cd' = c'd.$$

It then follows that,

$$\begin{aligned}(ad+bc)\,b'd' &= adb'd' + bcb'd \\ &= (ab')dd' + (cd')bb' \\ &= (a'b)dd' + (c'd)bb' \\ &= a'd'bd + b'c'bd \\ &= (a'd' + b'c')\,bd\end{aligned}$$

Thus, by definition, we have

$$[(ad+bc)/bd] = [(a'd'+b'c')/b'd']$$

and, therefore, addition is well defined.

We leave the verification that multiplication is well defined. That F is a field is straight forward. Let 1 denote the unity of D.

Then $[0/1]$ is the additive identity of F.

The additive inverse of $[a/b]$ is $[-a/b]$;

The multiplicative inverse of $[a/b]$ is $[b/a]$.

The remaining field properties can be checked easily.

Finally, the mapping $\phi : D \to F$ given by $x \to [x/1]$ is ring isomorphism from D to $\phi(D)$.

Hence the proof.

~ i ~