Discrete Mathematics

III-CS/IS and I-MCA

LECTURE NOTES

(B. E OF VTU)

VTU-EDUSAT Programme-17

Dr. V. Lokesha
Professor of Mathematics
DEPARTMENT OF MATHEMATICS
ACHARYA INSTITUTE OF TECNOLOGY
Soldevanahalli, Bangalore – 90

DISCRETE MATHEMATICS

Content

	CHAPTER
UNIT VII	Groups

Groups :

This unit will cover:

- Algebraic structures
- Some particular groups
- Subgroups
- Cyclic groups

  -Order of an element of a group
- Coset decomposition of a group

  -Lagrange's theorem.
- Homomorphism; Isomorphism

Introduction:

Group theory is a central branch of pure Mathematics, with many applications.

• The group axioms are very simple, yet they give rise to a very rich theory. There are many non-isomorphic examples. Groups govern many interesting structures in and out of mathematics, including field extensions (Galois theory), geometric objects and differential equations (Lie theory) and elementary particles (the Standard Model). The study of groups splits naturally into two, often overlapping, approaches.

Methods for solving the quadratic equations were known to the ancient Greeks. Then in the sixteenth century advances were made toward solving cubic and quartic polynomial equations where the coefficients were rational numbers. Continuing with polynomials of fifth and higher degree, both Leonhard Euler and Joseph Louis Lagrange(1736 – 1813) attempted to solve the general quintic. Lagrange realized there had to be a connection between the degree n of a polynomial equation and the permutation group s_n.

In mathematics, a **group** is an algebraic structure consisting of a set together with an operation

that combines any two of its elements to form a third element. To qualify as a group, the set and the operation must satisfy four conditions called the group axioms, namely closure, associativity,

identity and invertibility. Many familiar mathematical structures such as number systems obey these axioms: for example, the integers endowed with the addition operation form a group.

However, the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

The concept of a group arose from the study of polynomial equations, starting with Évariste Galois in the 1830s. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870.

Modern group theory—a very active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups. In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely (its group representations), both from a theoretical and a computational point of view. A particularly rich theory has been developed for finite groups, which culminated with the monumental classification of finite simple groups announced in 1983. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become a particularly active area in group theory

J Stillwell, one finds that the group concept and infact the actual word “group” first appears in Galios’ work Memoire sur les conditions deresolubilite des equations par radicaux, published in 1831.

Following the accomplishments of Galios group theory affected many areas of mathematics. During the late nineteenth century the German mathematician Felix Klein attempted to codify all existing geometries according to the group of transformations under which the properties of the geometry is invariant

Many other mathematicians such as Augustin Louis Cauchy, Arthur Cayley, Ludwig Sylow, Richard Dedekind and Leopald Kronecker contributed to the further development of certain types of groups.

Let S be a non-empty set. A function from S x S S is called a binary operation.

This function assigns to every ordered pair a unique element of S. Order of this function is 2.

In general, for any positive integer n a function from S x S x …. x S S is called an n-ary

operation.

Notations to be remembered:

1.	*	a binary operator.
2.	G	a non empty set.
3.	a, b, c ∈ G	elements of the non empty set G.
4.	a * b	closure law under the binary operator *.
5.	a*(b*c)=(a*b)*c	Associative law under the binary operator *.
6.	a*e = e*a = a	The existence of an identity under the binary operator * where, e is the identity element.
7.	$a*a^{-1} = a^{-1}*a = e$	Existence of inverses under the binary operator * where a^{-1} is the inverse element.
8.	a*b = b*a	Commutative law under the binary operator *.

Applications:

1. Group theory has extensive applications in Mathematics, Science and Engineering. any algebraic structures such as fields and vector spaces may be defined concisely in terms of groups.
2. Group theory provides an important tool for studying symmetry, since the symmetries of any object form a group.
3. Groups are thus essential abstractions in branches of physics involving symmetry principles such as relativity, quantum mechanics, and particle physics.

Furthermore, their ability to respect geometric transformations in chemistry, computer graphics, and other fields

GROUPS: let G be a non empty set and * be a binary operation on G. then G is called a group under the operation * if the following conditions

1. a*b belong to G for all a,b belongs to G.(i.e., G is closed under *)
2. (a*b)*c = a*(b*c) for all a,b,c belongs to G. (i.e., * is associative)
3. There is an element e belongs to G such that a*e = e*a =a for all a belongs to G (e is an identity element under *).
4. For every a belongs to G, there is an element a' belongs to G such that a*a' = a'*a =e.(

here a' is inverse of a under * and is denoted by $\bar{a}$

To simplify the notation, we write ab for a*b when there is no ambiguity. Likewise we write for a*a.

A group G under * will be denoted by (G,*) or just G.

A group G is said to be commutative or abelian if ab=ba for all a,b ∈G.

A group (G,*) is said to be a finite group of order n if G is a finite set with = . Then we write o(G)=n.

A group (G,*), where G is not a finite set, is called an infinite group.

Ex: 1. The set Z of all integers is closed under the usual addition operation + which is associative. We check a+0=0+a=a for all a ∈Z. therefore, 0 is an identity element in Z under +. Further, with each a ∈Z, there is –a, such that a + (-a) = (-a) + a = 0. Therefore for any a ∈ Z, -a is an inverse under +. These shows that (Z, +) is a group. This group is an infinite group; it is also an abelian group.

Ex: 2. We have noted that the usual multiplication × is a binary operation on Z, which is associative. Also a×1 = 1×a = a for all a ∈Z. therefore, 1 is an identity element in Z under ×. However, for an element a 1 in Z, there exists no element a' in Z such that a×a' = a'×a=1. Therefore (Z, ×) is not a group.

Examples of Commutative Groups:

- The integers, under addition, are a commutative group.
- The positive real numbers, under multiplication, are a commutative group.
- The set of complex numbers without 0, under multiplication, are a commutative group.
- Real/complex invertible matrices, under multiplication are a non-commutative group.

The rotation matrices, under multiplication, are a non-commutative group. (Except in 2D when they are commutative

An algebraic system < S, * > in which the operator * is ***associative*** is called a **semigroup.**

If * is commutative then < S, * > is called a ***commutative*** or **abelian semigroup**

Ex : < Z, + >, < R, x >, < P(S), U >

Let < S, * > be a semigroup. If S contains an ***identity*** element with respect to * then < S, * > is called a **monoid.**

Ex : < Z + > e = 0

< R, x > e = 1

< P(S), U > e = Ø

< P(S), > e = S

Let < S, * > be a semigroup and let T be a subset of S. Then < T, * > is called a **subsemigroup** of < S, * > if T is closed under the operation *.

Similarly, Let < S, * > be a monoid and let T be a subset of S. Then < T, * > is called a **submonoid** of < S, * > if T is closed under the operation * and e T.

Theorem-1: In a group, there exists only one identity element.

Proof: suppose that are two identity elements in group G. since is an identity element in G, we have = = for all a in G. this is true for a= because in G. this means that = = since is an identity element in G, a similarly we have = =

Therefore = = =

This shows that are not different. This means that G has only one identity element.

Theorem-2: in a group G, every element has only one inverse.

Proof: let e be the identity element in G. suppose a' and a'' are inverse of an element a in G. then

a' = a'e (because x = xe for al x in G)

= a'(aa'') (because a'' is an inverse of a)

=(a'a)a'' (associative)

= ea'' (because a' is an inverse of a)

= a''

Thus, a’ and a’’ cannot be different.

Theorem-3: let G be a group and let a,b,x be elements of G. then

I. Xa = xb implies a=b (left cancellation property)
II. ax = bx implies a= b (right cancellation property)

Some other properties of a group

From the uniqueness of identity and inverse of G we can prove the following properties for elements of G.

- **$(a^{-1})^{-1} = a$**
- **$(ab)^{-1} = b^{-1} a^{-1}$**
- **xa = xb implies a = b (left cancellation)**
- **ax = bx implies a = b (right cancellation)**
- **ax = b has unique solution $x = a^{-1}b$**
- **ya = b has unique solution $y = ba^{-1}$**

Example:

1. Let G be the set of real numbers not equal to -1 and * be defined by a*b = a+b+ab. Prove that (G, *) is an abelian group.

Proof: When a - 1 and b - 1, we note that a+b+ab -1
Therefore * is a binary operation on G. the definition of * itself indicates that * is commutative.
For any a,b,c in G, we have

A*(b*c)= a*(b+c+bc)
= a+ b+c+bc+a{ b+c+bc}
= a+b+c+ab+bc+ac+abc
= {(a+b+ab)+c}+{(a+b+ab)c}
= (a+b+ab)*c
= (a*b)*c

Thus, * is associative

For any a in G, we have

a*0 = a+0+a.0= a = 0+a+0.a= 0*a

thus, 0 is the identity I G under *.

For any a in G, if we put a’ = -a/(1+a), then a’ in G and

$A*a' = a+a'=aa'=a - a/(1+a) - a^2/(1+a) = 0 = a'*a$

Thus, $a' = -a/(1+a)$ in G is the inverse of a, under *.

The above facts show that (G,*) is an abelian group.

Problems :

1. Let G be the set of all non-zero real numbers and let a*b= (ab)/2. Show that (G, *) is an abelian group.
2. Let G be the set of real numbers not equal to -1 and * be defined by a+b = a+b+ab. Prove that (G, *) is an abelian group.
3. Prove that a group G in which every element is its own inverse is abelian.
4. In a group G having more than one element, if $x^2 = x$ for every $x \in G$, prove that G is abelian.
5. Prove that a group G is abelian if and only if $(ab)^2=a^2b^2$,for all $a , b \in G$
6. Prove that a group G is abelian if and only if $(ab)^{-1}=a^{-1}b^{-1}$ for all $a , b \in G$
7. Let $(G_1,*_1)$ and $(G_2,*_2)$ be two groups. Consider the Cartesian product $G_1 \times G_2$ and, on this product, define the operation $*_3$ by $(a, b) *_3 (c, d) = (a*_1 c, b *_2 d)$. Show that $(G_1 \times G_2 , *_3)$ is a Group. If G_1 and G_2 are abelian, prove that $G_1 \times G_2$ is abelian.

Problem : If $\circ$ is an operation on Z defined by $x \circ y=x+y+1$, Prove that $(Z, \circ)$ is an abelian group.

Sol : If $x, y \in Z$ then $x+y+1 \in Z$: that is $x \circ y \in Z$.
This verifies Z is closed under the given operation $\circ$.
For any $x, y, z \in Z$

$$x \circ (y \circ z) = x \circ (y + z + 1) = \{x + (y + z + 1) +1 \}$$
$$= \{(x + y + 1)+ z +1 \}$$
$$= (x \circ y) \circ z$$

This shows that $\circ$ is associative in Z
Further, for any $x \in Z$

$$x \circ (-1) = (x-1) +1 = x \text{ and } (-1) \circ x = (-1+x) +1 = x$$

This -1 is the identity element in Z under $\circ$.
Also, For any $x \in Z$

$$x \circ \{-(x+2)\} = x-(x+2) +1 = -1 \text{ and } -(x+2) \circ x = -(x+2)+x +1 = -1$$

This shows that every $x \in Z$ has an inverse $-(x+2) \in Z$ under $\circ$.
Lastly, we note that, for any $x, y \in Z$

$$x \circ y = x + y + 1= y + x + 1 = y \circ x$$

Thus $\circ$ is commutative. The above facts prove that $(Z, \circ)$ is an abelian group

Some particular Groups:

The klein 4-group: Consider a set A = { e, a, b, c), on this set, suppose we define a binary operation described by the following table.

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It is easy to verify that A is an abelian group under the binary operation defined. We observe that *e* is the identity element in the group and every element is its own inverse.

This group which is of order 4 is known as the Klein 4-group, after the German Mathematician Felix Klein. Also refered as Quadratic group and usually denoted as V_4

Table for $(Z_6, +)$:

•	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Problem : Let $Z_6^3 = Z_6 \times Z_6 \times Z_6$. Find the order of Z_6^3 and determine the inverse of each of the element (2, 3, 4), (4, 0, 2), (5, 1, 2) in Z_6^3 .

Sol : Since $Z_6 = 6$, the order of is 6 x 6 x 6 = 216. A typical element of is (a, b, c), where $a \in Z_6$, $b \in Z_6$, $c \in Z_6$. The inverse of this element is (-a, -b, -c) = (6-a, 6-b, 6-c).

Therefore

the inverse of (2, 3, 4) is (6-2, 6-3, 6-4) = (4, 3, 2)
the inverse of (4, 0, 2) is (6-4, 0, 6-2) = (2, 6, 4)
the inverse of (5, 1, 2) is (6-5, 6-1, 6-2) = (1, 5, 4) .

Find all x in $(Z_{11}, \bullet)$ such that $x = x^{-1}$

•	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

- X=1 and x=10 are only elements $(Z_{11}, \bullet)$ which are their own inverses

$$x^2 \equiv 1 (\mathrm{mod} 11)$$

Example If S(X) is the set of bijections from any set X to itself, then (S(X), °) is a group under composition. This group is called the symmetric group or permutation group of X.

Example . A translation of the plane R^2 in the direction of the vector (a, b) is a function $f : R^2 \to R^2$ defined by f (x, y) = (x + a, y + b). The composition of this translation with a translation g in the direction of (c, d) is the function

f g: $R^2 \to R^2$, where f g(x, y) = f (g(x, y)) = f (x + c, y + d) = (x + c + a, y + d + b).

This is a translation in the direction of (c + a, d + b). It can easily be verified that the set of all translations in R^2 forms an abelian group, under composition. The identity is the identity transformation

$1_{R^2}: R^2 \to R^2$, and the inverse of the translation in the direction (a, b) is the translation in the opposite direction (−a,−b).

1. **additive group of Integers modulo n:**

   let denote the set of all these n congruence classes, i.e.
   = { 0 , 1 , 2 , … … … . − 1 }

   On this set, let us define the operation addition modulo n denoted by $\oplus_n$, by
   ⊕ = + ! "" , ∈

2. **multiplicative group of integers mod p**

   let denote the set of all these n congruence classes, i.e.
   = { 0 , 1 , 2 , … … … . − 1 }

   On this set, let us define the operation multiplication modulo n denoted by $\otimes_n$, by
   ⊗ = × ! "" , ∈

Subgroups:

A non empty subset H of a group G is called a subgroup of G whenever H itself is a group under the binary operation in G.
or
Let < G, * > be a group and let H be a subset of G. Then < H, * > is called a **subgroup** of < G, * > if

1. H is closed under the operation *.
2. Identity element e of G belongs to H.
3. For all a in H a^{-1} is in H.

Conditions (i) and (ii) are equivalent to the single condition:
(iii) $a \cdot b^{-1} \in H$ *for all* $a, b \in H$.

Improper subgroup: Any group is a subgroup of itself (called the improper subgroup)

Trivial subgroup: The set consisting of just the identity of a group is a subgroup.

Eg. <Z, +> is a subgroup of <R, +>. But <Z, x> is not a subgroup of <R, x>

Prove that the intersection of two subgroups of a group is a subgroup of the group. Is the union of two subgroup of a group is a subgroup of the group.

Solution: Let G be a group and H and K be subgroups of G. take any a,b in % ∩ '. Then a, b in H and a, b in K. therefore (∈ % (∈ ', because H and K are subgroups of G. this means that (∈ % ∩ '. Hence % ∩ ' is a subgroup of G.

Thus, the intersection of 2 subgroups of a group G is a subgroup of G.

Consider the symmetric group)∗ and 2 of its subgroup + = {,-,,∗} and + = {,-,,.} then + ∪ + = {,-,,∗,,.}. From the multiplication table for)∗ we find that ,∗,. = , . But , ∉ + ∪ + . Therefore + ∪ + is not closed under the product of permutations and consequently cannot be a group. Thus, the union of two subgroups of a group need not be a subgroup of the group.

Example : Let W_4 = {1, -1, i, - i), the set of all fourth root of unity. The operation Table for the usual multiplication on W_4 ia as shown below:

x	1	-1	*i*	-*i*
1	1	-1	*i*	-*i*
-1	-1	1	-*i*	*i*
i	*i*	-*i*	-1	1
-*i*	-*i*	*i*	1	-1

From the table, it is evident that W_4 is closed under 'x'. Since 'x' is associative in the set of complex numbers, it is associative in W_4
Further, 1 is in W_4 and is the identity element under 'x'. Also, every element of A has an inverse under x. Lastly, x is commutative.
Hence W_4 and is an abelian group under x. This group ia a finite group of order 4

Criteria for a subset to be a subgroup – 1

Theorem : H is a subgroup of G iff for all a, b in H we have a*b H and a^{-1} H.
Proof : => Let H be a subgroup of G. So H is a group by itself and hence for all a, b in H we have a*b H and a^{-1} H.
Conversely, suppose for all a, b in H if a*b H and a^{-1} H. T. S. T H is a group
(i) By Heredity associtivity holds for H as * is closed on H.
(ii) For a H we have a^{-1} H so a a^{-1} = e H.
(iii) Also for every a H we have a^{-1} H.
Thus by (i), (ii), (iii), H is a group and hence a subgroup of G.

Criteria for a subset to be a subgroup - 2

Theorem : H is a subgroup of G iff for all a, b in H we have $a*b^{-1}$ H.

Proof : => Let H be a subgroup of G. So H is a group by itself and hence for all a, b in H we have a, b^{-1} H and so $a*b^{-1}$ H.

Conversely, suppose for all a, b in H if $a * b^{-1}$ H.

(i) For a H, take b = a we have $a * a^{-1} = e$ H.

(ii) For b H, take a = e then $e * b^{-1} = b^{-1}$ H.

(iii) For a H, take b = b^{-1} => $a * (b^{-1})^{-1} = a * b$ H.

Thus by (i), (ii), (iii), H is a group and hence a subgroup of G.

Theorem : When H is finite, H is a subgroup of G if and only if, for all a, b $\in$ H, we have *ab* $\in$H

Proof : First suppose that H is a subgroup. Then H is a group in its own right. let for all a,b $\in$ H then ab$\in$ H.

Conversely, suppose that for all a,b $\in$ H, ab$\in$ H : that is suppose that H is closed under the operation in G. Since H $\subseteq$ G and associative law holds in G it holds in H as well.

Take any a$\in$ H , and consider the set, aH = {ah / h $\in$ H}

Since a$\in$ H , we have ah$\in$ H for any h$\in$ H. therefore aH $\subseteq$ H. Since H is finite, it follows that aH is also finite.

Define a function f: H $\rightarrow$ aH by f(h) =ah for all h$\in$ H. then,

f(h_1) = f(h_2) $ah_1 = ah_2$

$h_1 = h_2$

Hence f is one-to- one function from H to aH. Since H is finite, it follows that |H | = | aH |. Since aH $\subseteq$ H and |aH | = |H| , it follows that aH=H.

Since a $\in$H and H $\in$ aH, a $\in$ aH. Therefore, a = ah_1 for some h_1 $\in$H.

Since a = ae, ae = ah_1 e = h_1 thus e $\in$ H.

Since e $\in$ H-aH, e =a h^2 for some h^2 $\in$ H. Evidently, $h^2 = a^{-1}$ Thus every a $\in$ H has an inverse in H. Hence the proof.

Example: Let G be a group and let J={x$\in$G \ xy = yx for all y $\in$ G}Then prove that J is a subgroup of G.

Proof : Since e $\in$ G and ey = ye for all y $\in$G, it follows that e $\in$J. Therefore, J is not empty.

Take any a, b $\in$ J and y $\in$G, then

(ab)y = a(by) = a(yb), because b $\in$ J

= (ay)b = (ya)b, because a $\in$ J

= y(ab)

This shows that ab $\in$ J.

Next, Since ya = ay,

$a^{-1}(ya)\ a^{-1} = a^{-1}(ay)\ a^{-1}$

$(a^{-1}y)(a\ a^{-1}) = (a^{-1}a)(y\ a^{-1})$
$(a^{-1}y)e = e(y\ a^{-1})$
$a^{-1}y = y\ a^{-1}$.
This shows that $a^{-1} \in J$.
Thus when a, b $\in$ J, We have ab $\in$ J and $a^{-1} \in$J. Therefore, J is a subgroup of G.

Example: For the group z_6^3, find subgroups of order 6, 12 and 36.
Sol : The group Z_6 is of order 6 and the group $z_6^3 = z_6 \times z_6 \times z_6$ is of order $6^3 = 216$.
Every element of z_6^3 is of the form (a, b, c), where a, b, c $\in Z_6$,
We find that, for z_6^3
H1 = {(a,0,0)/ a $\in Z_6$ } is a subgroup of order 6,
H2 = {(a,b,0)/ a $\in Z_6$, b=0,3}is a subgroup of order 12,
H3 = {(a,b,0)/ a, b $\in Z_6$ } is a subgroup of order 36,
Problems :
1. Prove that H = {x $\in$ Z/ x=3y for integer y} is a subgroup of (Z, +).
2. Prove that H = {0, 2, 4} is a subgroup of (Z_6, +).
3. Prove that the subsets {1, 8} and { 1, 4, 7} of (U_6, •).
4. Prove that the intersection of two subgroups of a group is a subgroup of the group. But the union of two subgroups of a group need not be a subgroup of the group.
Ex. Symmetric group.

- **Definition. Let G be a group and let a $\in$ G. If $a^k = 1$ for some k $\geq$ 1, then the smallest such exponent k $\geq$ 1 is called the *order of a;* if no such power exists, then one says that a has *infinite order.***

Proposition. ***Let G be a group and assume that a $\in$G has finite order k. If $a^n = 1$, then k | n. In fact, {n $\in$Z : $a^n = 1$} is the set of all the multiples of k.***

Proposition *Let G be a finite group and let a $\in$ G. Then the order of a is the number of elements in $\langle a \rangle$.*

- **Definition.** If G is a finite group, then the number of elements in G, denoted by |G|, is called the ***order of G.***

Cyclic groups:

A group G is said to be cyclic if there exists an element g in G such that every element a of G is an integral power of g; i.e a is of the form 1 for some integer n. then the element g is called a generator of the group.

If g is a generator of a cyclic group G, we say that g generates G or that G is generated by g.

A cyclic group G generated by g is denoted by <g>.

Ex: let w = {1, -1, i, -i} in this group, we notice that
$1 = 2^{-}$, $-1 = 2$, $2 = 2$, $-2 = 2^{*}$
Thus, every element of the group is an integral power of the element i. hence this group is cyclic and has I as a generator. Thus, (w, .)= <i>.

A group G is said to be cyclic if there exists an element g G s.t. every element in G can be expressed as an integral power of g. Then g is called as generator of G and we write it as

$G = \langle g \rangle = \{1, g, g^2, g^3 \ldots\ldots\ldots g^n\}$

Ex. $\langle W_4 \ x \rangle = \langle i \rangle$

$\langle Z_4 + \rangle = \langle [1] \rangle$ $\langle Z^*_5 \ x \rangle = \langle [2] \rangle$

Note : Every cyclic group is abelian, but not conversely.

- **Definition.** If G is a group and $a \in G$, write
  $\langle a \rangle = \{a^n : n \in Z\} = \{$all powers of a $\}$.
  It is easy to see that $\langle a \rangle$ is a subgroup of G .
  $\langle a \rangle$ is called the *cyclic subgroup* of G generated by a. A group G is called *cyclic* if there is some $a \in G$ with $G = \langle a \rangle$; in this case a is called a *generator* of G.
  Proposition. *If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if gcd(k; n)= 1.*
  Corollary. *The number of generators of a cyclic group of order n is $\phi(n)$.*
- *If g is a generator of a cyclic group G, then inverse of g is also a generator of G.*

Example: Prove that the Klien 4-group is not cyclic.

Sol : In the Klien 4-Subgroup, every element is its own inverse. Thus, for any x in this group, we have $x^2 = e$.
Consequently, $x^n = e$ if n is even and
$x^n = ex = x$ if n is odd.
Therefore, every integral power of x is equal to e or x. this means that no element x in this group can be a generator of the group.
Thus, the Klien 4 – group is not cyclic.

Example: Prove that the group (Z_5^*, •)is a cyclic group. Find all its generators.
Sol : The elements of the group (Z_5^*, •) are the congruence classes [1], [2],[3],[4] and the operation • in (Z_5^*, •) is "multiplication modulo 5". We find the, in this group

$[2] = [2]^1$
$[3] = [8] = [2] \bullet [2] \bullet [2] = [2]^3$
$[4] = [2] \bullet [2] = [2]^2$
$[1] = [16] = [2] \bullet [2] \bullet [2] \bullet [2] = [2]^4$

Thus, in the group (Z_5^*, •) every element is an integral power of the element[2]. Therefore (Z_5^*, •) is a cyclic group with [2] as a generator. [3] is also generator because [3] is inverse of [2].

Example:

1. Prove that the group (U_9, •)is cyclic.

2. Prove that the group (Z_4, +)is cyclic. Find all its generators

Definition: A subgroup H of a group G is called a *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

Theorem: Every cyclic group is abelian, but converse is not rue.

Proof : Let G be a cyclic group and g be a generator of G. Consider any a, b ∈ G. Then a = g^m and b = g^n for some integers m and n. Hence

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba$$

This shows that G is abelian.

We note that the Klien 4-group is abelian but not cyclic. Thus an abelian group need not be cyclic.

Theorem: Every subgroup of a cyclic group is cyclic.

Proof : Let G be a cyclic group and g be a generator of G. Then every element of G is an integral power of g. Hence, if H is a subgroup of G, then every element of H is in G and therefore is an integral power of g. Let m be the smallest positive integer such that $g^n \in H$.

Take any a ∈ H. Then a = g^n for some n ∈ Z. By division algorithm, their exist integers q and r with $0 \le r < m$ such that n = qm +r. Hence

$$a = g^n = g^{qm+r} = g^{qm}g^r = (g^m)^q g^r$$

Since $g^m \in H$ and H is a subgroup. $(g^m)^q \in H$. Also a ∈ H . Therefore $g^r \in H$. Since m is the smallest positive integer such that $g^m \in H$ and since $0 \le r < m$, $g^r \in H$ is possible only if r=0. thus $n=qm$ so that

$$a = g^{qm} = (g^m)^q$$

This shows that every element a of H is an integral power of g^m. Hence, H is a cyclic group with g^m as a generator. This completes the proof.

Theorem: Every element of a group G generates a cyclic group which is a subgroup of G.

Proof : Let G be a group and a be an element of G. Consider the subset A of G defined by

$$A=\{ x \in G / x = a^n, n \in Z\}$$

That is, the subset A of G consists of all those elements of G which are integral powers of a. Evidently, a∈ A. therefore A is non empty. Take any x , y ∈ A. Then x = a^n and y = a^m for some integers m and n.

Now we find that

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

This shows that $x y^{-1}$ is an integral power of a.

Therefore, $xy^{-1} \in A$. Thus if x, y ∈ A, thus $xy^{-1} \in A$.

Therefore A is a subgroup of G. Since every element of A is an integral power of a. it follows that A is a cyclic subgroup of G.

Thus every element a of G generates a cyclic group A which is a subgroup of G.

Example: In the group $(W_4, \bullet)$ find the cyclic subgroups generated by -1 and –i.
Sol : we have $W_4 = \{1, -1, i, -i\}$.
The cyclic subgroup generated by -1.

$<-1> = \{ x \in W_4 / x = (-1)^n, n \in Z\}$
$= \{1,-1\}$, because $= \pm 1$ for all $n \in Z$

Thus $(\{1, -1\}, \bullet)$ is the cyclic subgroup of $(W_4, \bullet)$, generated by -1.
The cyclic subgroup generated by -*i*.

$< -i > = \{ x \in W_4 / x = (-i)^n, n \in Z\}$
$= \{1,-1, i, -i\} = W_4$

Thus $-i$ generates the whole of the group W_4.

Example: Find the cyclic subgroups generated by the elements [2] and [3] of the group $(Z_6, +)$.

Sol : For the group $(Z_6, +)$, we have
$Z_6 = \{[0], [1], [2], [3], [4], [5]\}$ and + is " addition modulo 6". Therefore,

$<[2]> = \{ x \in Z_6 / x = [2]^n, n \in Z\}$
$= \{ x \in Z_6 / x = n[2], n \in Z\}$, because $[X]^n = n[x]$ under +
$= \{[0], [2], [4]\}$.

$<[3]> = \{ x \in Z_6 / x = n[3], n \in Z\} = \{[0], [3]\}$.

Are the subgroups of $(Z_6, +)$ generated by [2] and [3] respectively

Theorem 1 : Let G be a group and a be an element of G. Then a is of finite order n if and only if $a^n = e$ and n is the smallest positive integer. Then $<a> = \{a, a^2, \ldots\ldots, a^n = e\}$.

Proof : First suppose that a is of finite order n. then the cyclic subgroup $<a>$ generated by a, namely

$<a> = \{a^k / k \in Z\}$

is of order n. As such, there must be repetitions in the infinite entries in $<a>$. That is $a^s = a^t$ for some positive integers s and t with $s > t$. This implies that $a^{s-t} = e$. Let m be the smallest of such integer. That is, m is the smallest positive integer such that $a^m = e$. if k is any integer, then by division algorithm, we may write $k = mq + r$ where q and r are integers such that $0 \le r < m$. Hence

$a^k = a^{qm+r} = (a^m)^q a^r = e^q a^r = a^r$

Thus, every integral power of a is equal to a^r for some positive integer r, $0 \le r < m$. Hence $<a>$ must be of the form

$<a> = \{a^0 = e, a, a^2, \ldots\ldots, a^{m-1}\} = \{a, a^2, \ldots\ldots, a^m = e\}$

we note that no two elements of $<a>$ shown here can be equal. Because if $a^u = a^v$ for $u < v \le m$, then $a^{v-u} = e$ with $v - u < m$: this is not possible since m is the smallest positive integer such that $a^m = e$.

Hence <a> contains exactly m elements as shown. But by hypothesis o(<a>)=n, Hence m=n: that is

$<a>=\{a, a^2, \ldots\ldots, a^n=e\}$
Thus $a^n = e$ is the smallest such positive integer.

Conversely,
Suppose that $a^n = e$ and n is the smallest such positive integer. Then, as above, we find that every element of $< a>$ is of the form a^r where r is the positive integer such that $0 \le r < n$; that is,
$<a> = \{a^0 = e, a, a^2, \ldots\ldots, a^{n-1}\} = \{a, a^2, \ldots\ldots, a^n = e\}$
Also, no two elements of $<a>$ shown here can be equal. Hence $o(a) = n$ or a is of order n.
This completes proof.

Example : Let G be a group and a be an element of finite order in G. Show that
(i) $o(a) = o(a^{-1})$, (ii) $o(a) = o(xax^{-1})$, $\forall\, x \in G$
(iii) $o(ab) = o(ba)$, $\forall\, b \in G$
Proof : (i)Let $o(a) = n$. Then n is the smallest positive integer such that $a^n = e$. we note that the equation $a^n = e$ is equivalent to $(a^n)^{-1} = e^{-1}$ or $(a^{-1})^n = e$. hence, n is the smallest positive integer such that $(a^{-1})^n = e$; as such,
$n = o(a^{-1})$ as well.

(ii) We first note that $\forall a, x \in G$, and any positive integer n,

$$(xax^{-1})^n = (xax^{-1})(xax^{-1}) \ldots\ldots (xax^{-1}) \text{ (n factors)}$$
$$(xax^{-1})^n = xa(x^{-1}x)a(x^{-1}x) \ldots\ldots (x^{-1}x)ax^{-1} = xa^nx^{-1}$$

Let $o(a) = n$. Then n is the smallest positive integer such that $a^n = e$. Since the equation $a^n = e$ is equivalent to
$xa^nx^{-1} = xex^{-1} = e$ or equivalently, $(xax^{-1})^n = e$. It follows that n is the smallest positive integer such that $(xax^{-1})^n = e$; as such, $n = o(xax^{-1})^n$ as well.

(iii) by the virtue of result (ii), we have
$o(ba) = o\{b^{-1}(ba)(b^{-1})^{-1}\} = o\{(b^{-1}b)(ab)\} = o(ab)$.

Theorem 2 : Let G be a group and a be an element of G. For a non-zero integer k, $a^k = e$ if and only if o(a) is finite, say n and n divides k.

Proof : First suppose that $a^k = e$. Then $a^{|k|} = e$. Thus $|k|$ is a positive integer such that $a^{|k|} = e$. If k is the smallest such positive integer, then by theorem1, $|k| = o(a)$ so that a is of n be the smallest positive integer such that $a^n = e$. then by above theorem again, a is of finite order n.

By the division algorithm, we can write $|k| = nq + r$ where q and r are integers with $0 \le r < n$. Hence

$e = a^{|k|} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$

This is possible only if r=0. Hence $|k|=nq$, or n divides k.
Conversely, suppose that o(a) is finite, say n, and k is a multiple of n. then $a^n = e$ by theorem 1 and k=qn for some integer q. hence
$a^k = e^{qn} = (a^n)^q = e$.

Theorem 3 : Let G be a group and a be an element of G with o(a) =n then, for any integer $m \neq 0$, we have $o(a^m) = n/|d|$, where greatest common divisor of m and n.

Proof : Let us set $a^m = b$. Then $b \in \langle a \rangle$. Since o(a) = n, <a> is a finite group of order n. Hence, the cyclic subgroup of <a> generated by b must be of order less than or equal to n; that is $o(b) \leq n$. let o(b) = k. Then $b^k = e$ or $a^{mk} = e$. Hence by theorem 2, mk is multiple of o(a) that is mk = qn for some integer q.

If d is the gcd of m and n, we have m=rd and n=sd, where r and s are relatively prime.
Hence, the equation mk=qn yields rk=sq from which it follows that s divides k. Now
$b^s = a^{ms} = a^{srd} = a^{rn} = (a^n)^r = e^r = e$

Since o(b) = k, it follows that k divides s. Thus, s divides k and k divides s. Hence $s = \pm k$, so that $n = \pm kd$ or $k = n/|d|$.
Hence the proof.

Example: Find the order of the elements [8] and [15] in $(Z_{18},+)$. Also, list the elements of <[8]> and <[15]> in $(Z_{18},+)$.

Sol : It is very easy to check $(Z_{18},+)$ is a cyclic group with [1] as a generator. Therefore, $o([1]) = o(Z_{18}) = 18$.
Since $[8] \in (Z_{18},+)$, we have $[8] = [1]^8$. using theorem 3, we find that

$$o([8]) = o([1]^8) = \frac{o([1])}{d_1} = \frac{18}{d_1}$$

Where d_1 is the gcd of 8 and 18. since the gcd of 8 and 18 is 2, we have $d_1 = 2$. Therefore,

$$o([8]) = 18/2 = 9$$

Similarly,

$$o([8]) = o([1]^{15}) = \frac{o([1])}{d_2} = \frac{18}{d_2}$$

Where d_2 is the gcd of 15 and 18.
since $d_2 = 3$, we have o([15]) = 18/3 = 6
We further note that , in $(Z_{18},+)$,
$\langle [8] \rangle = \{[8]^n = n[8], n=1,2,3,4,\ldots\ldots 9\}$
$= \{[8], [16], [24], [32], [40], [48], [56], [64], [72]\}$
$= \{[8], [16], [6], [14], [4], [12], [2], [10], [0]\}$

and

$<[15]> = \{[15]^n = n[15], n=1, 2, 3, 4, 5, 6\}$
$= \{[15], [12], [9], [6], [3], [0]\}.$

Example: Find all the generators of $(Z_{16}, +)$.

Sol : We first note that [1] is a generator of $(Z_{16}, +)$. Take any $[k] \in [1]^k$. by theorem 3, $[1]^{k=}$ [k] is a generator of $(Z_{16}, +)$ if and only if k is less than and relatively prime to $o(Z_{16}) = 16$. Hence the possible values of k for which [k] is a generator of $(Z_{16}, +)$. That is,
$(Z_{16}, +) = <[1]> = <[3]> = <[5]> = <[7]> = <[9]> = <[11]> = <[13]> = <[15]>$

Exerciese: Show that $(U_{14}, \bullet)$ is cyclic and find all its generators..

Example: List all the subgroups of a cyclic group G of order 16.

Sol : We Note that $0(G) = 16$ is a composite number whose divisors are 1, 2, 4, 8 and 16. Hence G has exactly one subgroup corresponding to each of these 5 divisors. If g is a generator of G, then the five subgroups of G are,

$$<z> = G, <g^2>, <g^4>, <g^8>, <g^{16}>, = \{e\}$$

Example : Find all the subgroups of $(Z_{11}, +)$.

Sol : We Note that $0(Z_{11}) = 10$ and the divisors of 10 are 1, 2, 5 and 10. Wee check that [2] is a generator of $(Z_{11}, +)$. Therefore, the subgroups of this group are

$<[2]> = Z_{11}$
$<[2]^2> = <[4]> = \{[4], [5], [9], [3], [1]\}$
$<[2]^5> = <[10]> = \{[10], [1]\}$
$<[2]^{10}> = \{[1]\}$

Example : Find all the subgroups of $(Z_{21}, +)$.

1. Show that the group (G, *) whose multiplication table is as given below is cyclic.

*	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d

f	f	a	b	c	d	e

We note that a is the identity element of G. also we find that

(* = (∗ (= 4 ∗ (= ,
(· = (* ∗ (= ∗ (=
(5 = (· ∗ (= ∗ (=
(6 = (5 ∗ (= ∗ (=

Thus, every element of G is an integral power of b. therefore (G, *) is a cyclic group with b as a generator.

Coset Decomposition

Let < G, * > be a group and let H be its subgroup. For any a G we have
aH = { a * h / h H } left coset of H
Ha = { h * a / h H } right coset of H

Note :

1. The Left and right cosets of H are subsets of G.
2. If G is abelian then aH = Ha
3. a aH and Ha, both
4. If H is a finite subgroup then |H| = |aH| = |Ha|.
5. The left and right cosets of H are not one and the same in general

Results on cosets:

Theorem : Any two left cosets are either disjoint or equal.

Proof : Let aH and bH be two left cosets of H. Suppose aH and bH are not disjoint. Let c be an element in both so $c = ah_1$ and $c = bh_2$.

This gives $a = ch_1^{-1} = (bh_2)h_1^{-1}$

Now let x ϵ aH gives x = ah for some h ϵ H.

$x = ah = (bh_2)h_1^{-1} h = b(h_2 h_1^{-1} h)$ ϵ bH.

Thus for any x ϵ aH we get x ϵ bH So aH = bH

- Let $(G, \cdot)$ be a group with subgroup H. For a, b ∈ G, we say that a is congruent to b modulo H, and write a b mod H if and only if $ab^{-1} \in H$.
- Proposition. The relation a b mod H is an equivalence relation on G. The equivalence class containing a can be written in the form Ha = {ha|h ∈ H}, and it is called a right coset of H in G.

The element a is called a representative of the coset Ha

Example. Find the right cosets of A_3 in S_3.

Solution. One coset is the subgroup itself $A_3 = \{(1), (123), (132)\}$. Take any element not in the subgroup, say (12). Then another coset is $A_3(12) = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}$. Since the right cosets form a partition of S_3 and the two cosets above contain all the elements of S_3, it follows that these are the only two cosets.

In fact, $A_3 = A_3(123) = A_3(132)$ *and* $A_3(12) = A_3(13) = A_3(23)$.

Example. Find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2, \ldots, g^{11}\}$.

Solution. H itself is one coset. Another is $Hg = \{g, g^5, g^9\}$. These two cosets have not exhausted all the elements of C_{12}, so pick an element, say g^2, which is not in H or Hg. A third coset is $Hg^2 = \{g^2, g^6, g^{10}\}$ and a fourth is $Hg^3 = \{g^3, g^7, g^{11}\}$.

Since $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$, these are all the cosets.

Problems:

1. Find the Right cosets of the following:

(i). For the Group $H = \{[0], [3]\}$, $G = (Z_6, +)$.
(ii). $H = \{[1], [3], [9]\}$ in of $G = (Z_{13}, X)$,

2. Find all the left cosets of the subgroup $\{1, -1\}$ in the Fourth roots of unity. Hence obtain a coset decomposition of fourth roots of unity under multiplication.

Every coset contains the same number of elements. We use this result to prove the famous theorem of Joseph Lagrange (1736–1813).

Lemma. There is a bijection between any two right cosets of H in G.

Proof. Let Ha be a right coset of H in G. We produce a bijection between Ha and H, from which it follows that there is a bijection between any two right cosets. Define $\psi: H \to Ha$ by $\psi(h) = ha$. Then ψ is clearly surjective. Now suppose that $\psi(h_1) = \psi(h_2)$, so that $h_1a = h_2a$. Multiplying each side by a^{-1} on the right, we obtain $h_1 = h_2$. Hence ψ is a bijection.

Theorem : Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then |H| divides |G|.

Proof. The right cosets of H in G form a partition of G, so G can be written as a disjoint union $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$ for a finite set of elements $a_1, a_2, \ldots, a_k \in G$.

By Lemma, the number of elements in each coset is |H|. Hence, counting all the elements in the disjoint union above, we see that $|G| = k|H|$. Therefore, |H| divides |G|.

- If H is a subgroup of G, the number of distinct right cosets of H in G is called the index of H in G

and is written $|G : H|$. The following is a direct consequence of the proof of Lagrange's theorem.

- Corollary. If G is a finite group with subgroup H, then |G : H| = |G|/|H|.
- Corollary. If a is an element of a finite group G, then the order of a divides the order of G.

Example: Let G be a group with subgroups H and K. If |G|=660, |K|=66 and $K \subset H \subset G$, what are the possible values of H.

Sol: By Lagrange's theorem, |H| must divide |G| =660 and |K|=66must divide |H|. Therefore 660=|H|p for some integer p>1 and |H|=66q for some integer q>1. Hence 660=66pq or pq=10 thus either p=2, and q=5, or p=5 and q=2.

Thus |H|= 66X5= 330 or |H|=66X2= 132.

Definition of Homomorphisms

If $(G, \ )$ and $(H, *)$ are two groups, the function

$f: G \to H$ is called a group homomorphism if $f(a \ b) = f(a) * f(b)$ for all $a, b \in G$.

- We often use the notation $f: (G, \ ) \to (H, *)$ for such a homomorphism. Many authors use morphism instead of homomorphism.
- A group isomorphism is a bijective group homomorphism. If there is an isomorphism between the groups $(G, \ )$ and $(H, *)$, we say that $(G, \ )$ and $(H, *)$ are isomorphic and write $(G, \ ) \cong (H, *)$.

Examples of Homomorphism's:

- The function $f: Z \to Z_n$, defined by $f(x) = [x]$ is the group homomorphism.
- Let R be the group of all real numbers with operation addition, and let R^+ be the group of all positive real numbers with operation multiplication. The function $f: R \to R^+$, defined by $f(x) = e^x$, is a homomorphism, for if $x, y \in R$, then $f(x+y) = e^{x+y} = e^x e^y = f(x) f(y)$. Now f is an isomorphism, for its inverse function $g: R^+ \% R$ is $g(x) = \ln x$. Therefore, the addiYve group R is isomorphic to the multiplicative group R^+. Note that the inverse function g is also an isomorphism:

  $g(xy) = \ln(xy) = \ln x + \ln y = g(x) + g(y)$.

Problem: Let be R the group of all real numbers with operation addition, and let R^+ be the group of all positive real numbers with operation multiplication. The function $f: R \to R^+$, defined by $f(x) = 2^x$, is a homomorphism.

Theorem on Homomorphism:

Proposition. Let $f: G \to H$ be a group homomorphism, and let e_G and e_H be the identities of G and H, respectively. Then

(i) $f(e_G) = e_H$.

(ii) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

Proof. (i) Since f is a homomorphism, $f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = f(e_G)e_H$. Hence (i) follows by cancellation in H

(ii) $f(a)\, f(a^{-1}) = f(a\, a^{-1}) = f(e_G) = e_H$ by (i). Hence $f(a^{-1})$ is the unique inverse of $f(a)$; that is $f(a^{-1}) = f(a)^{-1}$

Definition: A subgroup H of a group G is called a normal subgroup of G if $g-1hg \in H$ for all $g \in G$ and $h \in H$.

Proposition. $Hg = gH$, for all $g \in G$, if and only if H is a normal subgroup of G.

Proof. Suppose that $Hg = gH$. Then, for any element $h \in H$, $hg \in Hg = gH$. Hence $hg = gh1$ for some $h1 \in H$ and $g-1hg = g-1gh1 = h1 \in H$. Therefore, H is a normal subgroup.

Conversely, if H is normal, let $hg \in Hg$ and $g-1hg = h1 \in H$. Then $hg = gh1 \in gH$ and $Hg \subseteq gH$. Also, $ghg-1 = (g-1)-1hg-1 = h2 \in H$, since H is normal, so $gh = h2g \in Hg$. Hence, $gH \subseteq Hg$, and so $Hg = gH$.

If $f: G \to H$ is a group morphism, the kernel of f, denoted by Kerf, is defined to be the set of elements of G that are mapped by f to the identity of H. That is, $Kerf = \{g \in G | f(g) = e_H\}$

Proposition. Let $f: G \to H$ be a group morphism. Then:

(i) Kerf is a normal subgroup of G.

(ii) f is injective if and only if $Kerf = \{e_G\}$.

Proposition. For any group morphism $f: G \to H$, the image of f, $Imf = \{f(g) | g \in G\}$, is a subgroup of H (although not necessarily normal).

Theorem : Let f be a homomorphism from a group G_1 to a group G_2. Then the following are true.

1. If e_1 is the identity in G_1 and e_2 is the identity in G_2 the we have $f(e_1) = e_2$.
2. $f(a^{-1}) = (f(a))^{-1}$ for all $a \in G_1$
3. If H_1 is a subgroup of G_1 and $H_2 = f(H_1)$, then H_2 is a subgroup of G_2
4. If f is an isomorphism from G_1 onto G_2, then f^{-1} is an isomorphism from G_2 onto G_1.

Proof : 1) we have, in G_2,

$e_2 f(e_1) = f(e_1)$, because e_2 is the identity in G_2

$= f(e_1 e_1)$, because $e_1 e_1 = e_1$ in G_1

$= f(e_1)f(e_1)$, because f is a homomorphism

therefore, $e_2 = f(e_1)$ by the cancellation law

2) For $a \in G_1$ we have,

$f(a)\, f(a^{-1}) = f(aa^{-1}) = f(e_1) = e_2$

and $f(a^{-1})\, f(a) = f(a^{-1}a) = f(e_1) = e_2$

This shows that $f(a^{-1})$ is the inverse of $f(a)$ in G_2.

That is $f(a^{-1}) = [f(a)]^{-1}$

3) $H_2 = f(H_1)$ is the image of H_1 under f; this is a subset of G_2. Take any $x, y \in H_2$. Then $x = f(a), y = f(b)$ for some $a, b \in H_1$ Since H_1 is a subgroup of G_1, we have $ab^{-1} \in H_1$. Consequently,

$xy^{-1} = f(a)\,[f(b)]^{-1} = f(a)\, f(b^{-1}) = f(ab^{-1})\, f(H_1) = H_2$

Accordingly, H_2 is a subgroup of G_2

4) Since $f : G_1 \to G_2$ is an isomorphism, f is one-to-one and onto. Therefore, the function exists and is one-to-one.

Take any $x, y \in G_2$. Then $xy \in G_2$. Then there exist $ab \in G_1$ such that $x = f(a), y = f(b)$. Therefore,

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

$= f^{-1}f(ab)$, because f is a homomorphism

$= ab$, because $f^{-1}f$ is the identity function

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

This shows that $f^{-1}: G_1 \to G_2$ is a homomorphism as well. Thus f^{-1} is an isomorphism

Example 1 : Prove that $(U_9, \bullet)$ and $(Z_6, +)$ are isomorphic.

Sol : We note that $U_9 = \{[1], [2], [4], [5], [7], [8]\}$ and $(U_9, \bullet)$ is a cyclic group with $<2>$ as a generator, the operation $\bullet$ being multiplication modulo 9. also $(Z_6, +)$ is the additive group of integers modulo 6.

Define the function $f : U_9 \to Z_6$ by $f(2^k) = [k]$, $1 \le k \le 6$. then for any $2^r, 2^s \in U_9$ where $1 \le r \le 6$, $1 \le s \le 6$, we have

$f(2^r, 2^s) = f(2^{r+s}) = r+s$

$= [r] + [s]$ in Z_6

Also, for $[r], [s]$ $2^r \in U_9$, $2^s \in U_9$ and $f(2^r) = [r]$ and $f(2^s) = [s]$. There fore f is onto. Since U_9 and Z_6 are finite, f is one-to-one as well.

Thus, there exists an isomorphism from $(U_9, \bullet)$ onto $(Z_6, +)$. This proves that $(U_9, \bullet)$ and $(Z_6, +)$ are isomorphic.

Example 2: If $G = (Z_6, +)$, $H = (Z_3, +)$ and $(Z_2, +)$, prove that G and H x K are isomorphic.

Sol : Let us define the function $f : G \to H \times K$ by

$f(0) = (0, 0), f(1) = (1,1), f(2) = (2,0),$

$f(3)=(0,1), f(4)=(1,0), f(5)=(2,1)$ Then we find that no two elements of G have the same image in H x K under f. Therefore, f is a one-to-one function. We observe that G and H x K are the same finite order 6. Therefore is onto as well.

By taking $a, b \in G$, we check that

$f(a+b)=f(a)+f(b)$, in H x K

because, in H x K, $(x_1, y_1)+(x_2+y_2)=(x_1+x_2, y_1+y_2)$ and 2=0 in K. Thus $f(a)+f(b)=f(a+b)$. This proves that f is homomorphism.

Thus, there exists an isomorphism from G onto H x K. Therefore, G and H x K are isomorphic.

Example 3: For a given group G, Prove that the function

$f: G \to G$ defined by $f(a)=a^{-1}$ is isomorphic if and only if G is abelian.

Sol : Using the definition of f, we find that, for any $a, b \in G$

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

$a=b$, by the uniqueness of inverse

This shows that f is one-to-one.

Also, for any $a \in G$

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

Thus every $a \in G$, has a^{-1} as the pre image under f. Therefore, f is onto.

Further, we note that, for any $a, b \in G$

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

$=f(b)f(a)=f(a)f(b)$ if and only if G is abelian.

Thus, f is a homomorphism if and only if G is abelian.

Since f is one-to-one, it follows that f is isomorphism if and only if G is abelian.

Theorem : Let $\phi: G \to G'$ be a homomorphism and Kernel = $K=\{g \mid \phi(g)=e'\}$ Then K is an invariant subgroup of G and $G/K \approx G'$.

Proof 1 (K is a subgroup of G):

ϕ is a homomorphism:

$\therefore\ a, b \in K \to \phi(ab)=\phi(a)\phi(b)=e'e'=e' \to ab \in K$ (closure)

$\phi(ae)=\phi(a)\phi(e)=e'\phi(e)=\phi(e)$

$=\phi(a)=e' \to \phi(e)=e' \to e \in K$ (identity)

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

$=\phi(e)=e' \to a^{-1} \in K$ (inverse)

Associativity is automatic.

Proof 2 (K is a invariant):

Let $a \in K$ & $g \in G$.

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

$\to g\,a\,g^{-1} \in K$

Proof 3 ($G/K \approx G'$):

$G/K = \{ pK \mid p \in G \}$

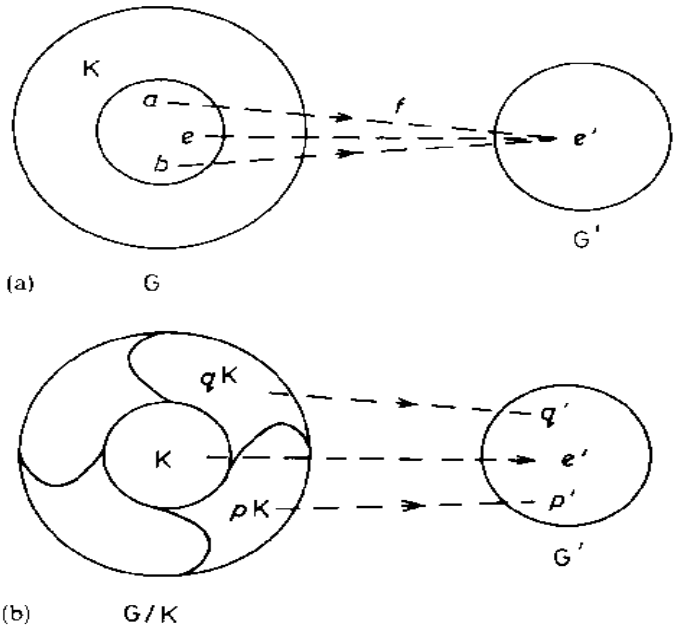
$\therefore \quad \phi(pa) = \phi(p)\phi(a) = \phi(p)e' = \phi(p) \quad \forall\ a \in K$

i.e., ϕ maps the entire coset pK to one element $\phi(p)$ in G'.

Hence, $\psi : G/K \to G'$ with $\psi(pK) = \phi(p) = \phi(q \in pK)$ is 1-1 onto.

$\psi(pK\,qK) = \psi[(pq)K] = \phi(pq) = \phi(p)\phi(q) = \psi(pK)\psi(qK)$

$\to \psi$ is a homomorphism.



a) Kernel b). $G/K \approx G'$

Conjugate Class:

Let $a \in G$, the conjugate class of a is the set

$\xi = \{ p\,a\,p^{-1} \mid p \in G \}$.

Comments:

. Members of a class are equivalent & mutually conjugate.

. Every group element belongs to 1 & only 1 class.

. e is always a class by itself.

. For matrix groups, conjugacy = similarity transform.

Theorem: Cayley

Every group of finite order n is isomorphic to a subgroup of S_n.

Exercises:

1. Let $f : G \to H$ be a homomorphism, if $a \in G$ with $o(a) = n$ and $o(f(a)) = k$, Prove that k divides n.
2. Let $f : G \to H$ be a homomorphism from G onto H. If G is abelian, Prove that H is also abelian.
3. Let $f : G \to H$ and $g : H \to K$ are homomorphisms. Prove that $g \circ f : G \to K$ defined by $(g \circ f)(x) = g\{f(x)\}$ is a homomorphism.