Discrete Structures and Theory of Logic

Unit-2

Dharmendra Kumar(Associate Professor)
Department of Computer Science and Engineering
United College of Engineering and Research, Prayagraj

Group Theory

1 Group

Binary operation
Let G be a non empty set. If f:$G \times G \to$ G, then f is said to be binary operation defined on set G.
Thus, a binary operation on G is a function that assign each ordered pairs of elements of G to an element of G.
Algebraic structure
A non-empty set together with one or more than one binary operations is called an algebraic structure.
Example: (N,+), (Z,+), (R,+) and (R,+,*) are all the algebraic structures.

1.1 Definition of group

An algebraic structure (G,o), where G is a set and o is a binary operator defined on the set G, is called a group if it satisfies following properties:-
(1) Closure property:
For all a,b $\in$ G, aob $\in$ G.
(2) Associative property:
For all a,b,c $\in$ G, ao(boc) = (aob)oc.
(3) Existence of identity property:
For all a $\in$ G, $\exists$ e $\in$ G, such that aoe = eoa = a.
Element e is said to be identity element of the group G.
(4) Existence of inverse property:
For all a $\in$ G, $\exists$ b $\in$ G, such that aob = e = boa.
Element b is said to be inverse of an element a.

1.2 Abelian group

A group (G,o) is said to be an abelian group if it satisfies the following property:-
aob = boa, $\forall$ a,b $\in$ G.
Note: If aob = boa, $\forall$ a,b $\in$ G, then this is known as commutative property.

1.3 Groupoid

An algebraic structure (G,o) is said to be groupoid if it satisfies only closure property.

1.4 Semigroup

An algebraic structure (G,o) is said to be semigroup if it satisfies closure and associative property.

1.5 Monoid

An algebraic structure (G,o) is said to be monoid if it satisfies closure, associative and existence of identity property.

1.6 Some examples

Example: Is (R,+) a group, where R is a set of real numbers?
Solution: (R,+) will be a group if it satisfies all the four properties of the group.
Closure property
Consider any two real numbers a and b. Clearly a+b will also be a real number. Therefore, (R,+) satisfies closure property.
Associative property
Consider three real numbers 10, 15, 2/3.
10+(20+(2/3)) = 10+(62/3) = 92/3.
(10+20)+2/3 = 30+2/3 = 92/3. Clearly, 10+(20+(2/3)) = (10+20)+2/3. Therefore, a+(b+c) = (a+b)+c, for all a,b,c $\in$ R. Therefore, (R,+) satisfies associative property.
Identity property
Clearly, 0 is a real number such that 0+a = a, $\forall$ a $\in$ R.
Therefore, 0 is the identity element. Therefore, (R,+) satisfies identity property.
Inverse property
Consider an element a $\in$ R. Clearly, a+(-a) = 0, therefore inverse of a is -a. Similarly, for any real number a, -a will be its inverse. Therefore, (R,+) satisfies inverse property.
Since (R,+) satisfies all the four properties of the group, therefore (R,+) is a group.

Example: Is (R',*) a group, where R' = R-{0} ?
Solution:
Closure property
Consider any two non-zero real numbers a and b. Clearly a*b will also be a real number. Therefore, (R',*) satisfies closure property.
Associative property
Consider three real numbers 10, 0.5, 2.
10*(0.5*2) = 10*1 = 10.
(10*0.5)*2 = 5*2 = 10. Clearly, 10*(0.5*2) = (10*0.5)*2 . Therefore, a*(b*c) = (a*b)*c, for all a,b,c $\in$ R'. Therefore, (R',*) satisfies associative property.
Identity property
Clearly, 1 is a real number such that 1*a = a, $\forall$ a $\in$ R'.
Therefore, 1 is the identity element. Therefore, (R',*) satisfies identity property.
Inverse property
Consider an element a $\in$ R'. Clearly, there exists a non-zero real number 1/a such that a*(1/a) = 1, therefore inverse of a is 1/a. Similarly, for any real number a, 1/a will be its inverse. Therefore, (R',*) satisfies inverse property.
Since (R',*) satisfies all the four properties of the group, therefore (R',*) is a group.

Example: Is (Z^+,+) a group, where Z^+ denotes set of positive integers?
Solution:
Since the sum of any two positive integers is also a positive integers, therefore it satisfies closure property.
Similarly, the sum of any three positive integers in any way will be same. therefore it

satisfies associative property.
Since the operation is addition, therefore identity element is 0. Clearly $0 \in Z^+$, therefore it satisfies identity property.
But the inverse of any positive integer a will be -a. and -a $\notin Z^+$. Therefore, inverse property is not satisfied. Hence, $(Z^+,+)$ is not a group.

Example: Prove that the four roots of unity 1, -1, i, , -i form an abelian multiplicative group.
Solution: First we construct composition table of it. The composition table of it is the following:-
From table, all entries in this table are belong into the given set. Therefore, closure

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

property is satisfied.
Clearly, associative operation is also satisfied, because the operation is multiplication.
In the table, row 1 indicate that element 1 is identity element.
Clearly, $(1)^{-1} = 1$, $(-1)^{-1}$ = -1, $(i)^{-1}$ = -i, $(-i)^{-1}$ = i. Since each element has inverse, therefore inverse property is satisfied.
Clearly, a*b = b*a, therefore commutative property is also satisfied. Since all the five properties of abelian group is satisfied, therefore this is a multiplicative group.

Example: Show that the set of all positive rational numbers form an abelian group under the operation defined by aob = (ab)/2.
Solution:
Closure property
Consider any two positive rational numbers a and b.
Since aob = (ab)/2. Clearly (ab)/2 will be a positive rational number. Therefore, it satisfies closure property.
Associative property
Consider three positive rational numbers a, b, c.
ao(boc) = ao(bc/2) = (abc)/4
(aob)oc = ((ab)/2)oc = (abc)/4
Clearly, ao(boc) = (aob)oc, for all a,b,c $\in$ R. Therefore, it satisfies associative property.
Identity property
Let e the identity element. Therefore, aoe = a $\Rightarrow$ (ae)/2 = a $\Rightarrow$ e = 2. Therefore, 2 is an identity element. Therefore, (it satisfies identity property.
Inverse property
Consider, a is positive rational number. Let b is an inverse of a.
Therefore, aob = e = 2 $\Rightarrow$ (ab)/2 = 2 $\Rightarrow$ b = 4/a. Therefore inverse of a is 4/a. Therefore, it satisfies inverse property.
Now, aob = (ab)/2 = (ba)/2 = boa. Therefore, it satisfies commutative property.
Since it satisfies all the five properties of an abelian group, therefore it is an abelian group.

1.7 Order of a group

The order of a group(G,o) is the number of elements of G, when G is finite. If G is infinite, then the order will be infinite.
Example: Show that the set {1,2,3,4,5} is not a group under addition and multiplication modulo 6 operation.
Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table 1: Composition table under $+_6$ operation

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Table 2: Composition table under $\times_6$ operation

Closure property is not satisfied under both operation, because 0 entry belongs into table which is not the element of set. Therefore, the set {1,2,3,4,5} is not a group under addition and multiplication modulo 6 operation.

Example: Prove that the set {0,1,2,3,4} is a finite abelian group of order 5 under addition modulo 5 operation.
Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From table, closure property is satisfied, because all entries of table belongs into set {0,1,2,3,4}. Since operation is addition, therefore associative property is satisfied. Clearly from table, identity element is 0. And each element has a inverse i.e. $(0)^{-1} = 0$, $(1)^{-1} = 4$, $(2)^{-1} = 3$, $(3)^{-1} = 2$, $(4)^{-1} = 1$. Commutative property is also satisfied because aob = boa, for all a,b.
Therefore, this set is an abelian group under operation $+_5$.

1.8 Left cancellation law

For a,b,c $\in$ G, aob = aoc $\Leftrightarrow$ b = c.

1.9 Right cancellation law

For a,b,c $\in$ G, boa = coa $\Leftrightarrow$ b = c.

1.10 Some examples

Example: In a group (G,o), prove the following:-
(a) $(a^{-1})^{-1}$ = a
(b) $(aob)^{-1} = b^{-1}oa^{-1}$
Solution:
(a) Since a^{-1} is the inverse of a, therefore aoa^{-1} = e .....(1)
Since a $\in$ G, therefore a^{-1} is also belong into G. Since $a^{-1} \in$ G, therefore inverse of it will also belong.
Using inverse property, $(a^{-1})^{-1}oa^{-1}$ = e .....(2)
Using (1) and (2), $(a^{-1})^{-1}oa^{-1} = aoa^{-1}$
By right cancellation law, we get $(a^{-1})^{-1}$ = a
It is proved.
(b) Consider a,b $\in$ G. Therefore, its inverses are a^{-1} and b^{-1}.
Since a,b $\in$ G, therefore aob also belong into G.
Now, $b^{-1}oa^{-1}$ will be inverse of aob if (aob)o $(b^{-1}oa^{-1})$ = e.
Now, (aob)o $(b^{-1}oa^{-1})$ = ao(bo$(b^{-1}oa^{-1})$) using associative property
= ao((bob^{-1})oa^{-1})) using associative property
= ao(eoa^{-1}) since b^{-1} is the inverse of b
= aoa^{-1} using identity property
= e since a^{-1} is the inverse of a
Therefore, $(aob)^{-1} = b^{-1}oa^{-1}$

Example: Prove that in a group (G,o), if a^2 = a, then a = e, for a $\in$ G and e is the identity element of G.
Solution:
Since a^2 = a $\Rightarrow$ aoa = aoe
$\Rightarrow$ a = e using left cancellation law.

Example: Show that if every element of a group (G,o) be its own inverse, then it is an abelian group. Is the converse true?
Solution:
First part:
Consider two elements a,b $\in$ G. Since each element has its own inverse, therefore $a^{-1} = a$ and $b^{-1} = b$.
To show that the group (G,o) is abelian, we have to show that aob = boa.
Since a,b $\in$ G, therefore aob also belong into G. Since each element has its own inverse, therefore $(aob)^{-1} = aob$
We know that $(aob)^{-1} = b^{-1}oa^{-1}$, therefore $b^{-1}oa^{-1}$ = aob $\Rightarrow$ boa = aob (Since $a^{-1} = a$ and $b^{-1} = b$)
Therefore the group is abelian.
Second part:
In this part, we have to check if a group is abelian then each element has its own inverse. This part is not true. We are giving justification of it below.
Consider an abelian group (Z,+). Clearly in this group, inverse of any element a will be

-a, which is not equal to a. Therefore, converse part not true.

1.11 Exercise

1. If (G,o) is an abelian group, then for all a,b ∈ G, show that $(aob)^n = a^n o b^n$.
2. Write down the composition tables for $(Z_7, +_7)$ and $(Z_7^*, \times_7)$, where $Z_7^* = Z_7 - \{0\}$.

1.12 Order of an element

The order of an element **a** in a group (G,o) is the smallest positive integer n such that a^n = e, where e is the identity element of G.
If no such integer exists, then we say a has infinite order.

Example: Let G = {1,-1,i,-i} be a multiplicative group. Find the order of every element.
Solution: In this group, the identity element, e = 1. Therefore,
$(1)^1 = 1$ (That is e.), therefore order of 1 = 1.
$(-1)^1$ = -1, $(-1)^2 = 1$, therefore order of -1 = 2.
$(i)^1$ = i, $(i)^2$ = -1, $(i)^3$ = -i, $(i)^4 = 1$, therefore order of i = 4.
$(-i)^1$ = -i, $(-i)^2$ = -1, $(-i)^3$ = i, $(-i)^4 = 1$, therefore order of -i = 4.

Example: Find the order of every element in the multiplicative group G=$\{a, a^2, a^3, a^4, a^5, a^6 = e\}$.
Solution: In this group, the identity element, e = a^6. Therefore,
$(a)^6$ = e, therefore order of a = 6.
$(a^2)^1 = a^2$, $(a^2)^2 = a^4$, $(a^2)^3 = a^6$ = e, therefore order of $a^2 = 3$.
$(a^3)^1 = a^3$, $(a^3)^2 = a^6$ = e, therefore order of $a^3 = 2$.
$(a^4)^1 = a^4$, $(a^4)^2 = a^8 = a^6 o a^2 = eoa^2 = a^2$,
$(a^4)^3 = a^12 = a^6 o a^6$ = eoe = e, therefore order of $a^4 = 3$.
$(a^5)^1 = a^5$, $(a^5)^2 = a^10 = a^6 o a^4 = eoa^4 = a^4$,
$(a^5)^3 = a^15 = a^6 o a^6 o a^3 = eoeoa^3 = a^3$
$(a^5)^4 = a^20 = a^6 o a^6 o a^6 o a^2 = eoeoeoa^2 = a^2$
$(a^5)^5 = a^25 = a^6 o a^6 o a^6 o a^6 o a = eoeoeoeoa$ = a
$(a^5)^6 = a^30 = a^6 o a^6 o a^6 o a^6 o a^6 = eoeoeoeoe$ = e
Therefore, the order of $a^5 = 6$.
$(a^6)^1 = a^6$ = e, therefore order of $a^6 = 1$.

1.13 Cyclic group

A group (G,o) is said to be a cyclic group if there exists an element a∈G such that every element of G can be written as some power of a, that is a^n for some integer n. a is said to be the generator of G.
Example: Show that the set of integers with respect to + operation is cyclic group.
Solution: A group will be cyclic if there exists a generator in the group.
Consider an element 1 of this group.

$(1)^1 = 1$
$(1)^2 = 1+1 = 2$
$(1)^3 = 1+1+1 = 3$
$(1)^4 = 1+1+1+1 = 4$
Clearly 1, 2, 3, 4 are expressed in the power of 1. Similarly, we can expressed all the positive integers in the power of 1.
Now, $(1)^{-1}$ = -1
$(1)^{-2} = (1^{-1})^2 = (-1)^2$ = -1+(-1) = -2
$(1)^{-3} = (1^{-1})^3 = (-1)^3$ = -1+(-1)+(-1) = -3
$(1)^{-4} = (1^{-1})^4 = (-1)^4$ = -1+(-1)+(-1)+(-1) = -4
Clearly -1, -2, -3, -4 are expressed in the power of 1. Similarly, we can expressed all the negative integers in the power of 1.
Now, $(1)^0 = 0$
Clearly, all the integers are expressed in the powers of 1. Therefore, 1 is the generator of this group. Since generator exists, therefore the group is cyclic.

Example: Is $(G,+_6)$ a cyclic group, where G = {0,1,2,3,4,5}.
Solution: We have to find generator in this group.
Consider an element 1 of this group.
Now, $(1)^1 = 1$
$(1)^2 = 1+_61 = 2$
$(1)^3 = 1+_61+_61 = 3$
$(1)^4 = 1+_61+_61+_61 = 4$
$(1)^5 = 1+_61+_61+_61+_61 = 5$
$(1)^6 = 1+_61+_61+_61+_61+_61 = 0$
Clearly all the elements of G are expressed in the power of 1, therefore 1 is a generator of G. Since generator exists, therefore the group is cyclic.

Example: Is the multiplicative group $\{1, \omega, \omega^2\}$, a cyclic group?
Solution: Consider an element ω of G.
Now, $(\omega)^1 = \omega$
$(\omega)^2 = \omega^2$
$(\omega)^3 = \omega^3 = 1$
Clearly all the elements of G are expressed in the power of ω, therefore ω is a generator of G. Since generator exists, therefore the group is cyclic.

Example: Show that every cyclic group is an abelian group.
Solution: Consider (G,o) is a cyclic group. Since (G,o) is cyclic, therefore generator exists. Let it's generator is a.
Consider two elements b,c ∈ G. It can be expressed in the power of a. Let b = a^i and c = a^j.
Now, boc = $a^i o a^j$
$= a^{i+j}$
$= a^{j+i}$ (since set of integers with respect to addition operation is an abelian)
$= a^j o a^i$
= cob
That is, boc = cob
Therefore group (G,o) is an abelian. Now, we can say, every cyclic group is an abelian

group.

Example: Show that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.
Solution: Since a is a generator of G, therefore each elements of G can be epressed in the power of a.
Consider any element b $\in$ G such that b = a^i. If we can epressed b in the power of a^{-1}, then a^{-1} will be also generator of G.
Now, b = $a^i = (a^{-1})^{-i}$. Clearly b is expressed in the power of a^{-1}, therefore a^{-1} is also generator of G.

Example: How many generators are there of the cyclic group G of order 8?
Solution: Since the group is cyclic, therefore there exists generator in this group. Let a is a generator.
Therefore, G=$\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$.
Now, consider an element a^2.
$(a^2)^1 = a^2$
$(a^2)^2 = a^4$
$(a^2)^3 = a^6$
$(a^2)^4 = a^8 =$ e
$(a^2)^5 = a^10 = a^2$
Clearly elements a^1, a^3, a^5, a^7 are not expressed in the power of a^2. Therefore a^2 is not generator.
Now, consider an element a^3.
$(a^3)^1 = a^3$
$(a^3)^2 = a^6$
$(a^3)^3 = a^9 =$ a
$(a^3)^4 = a^12 = a^4$
$(a^3)^5 = a^15 = a^7$
$(a^3)^6 = a^18 = a^2$
$(a^3)^7 = a^21 = a^5$
$(a^3)^8 = a^24 = a^8 =$ e
Clearly all the elements of G are expressed in the power of a^3, therefore a^3 is a generator of G.
Now, consider an element a^4.
$(a^4)^1 = a^4$
$(a^4)^2 = a^8 =$ e
$(a^4)^3 = a^12 = a^4$
Clearly elements a^1,a^2, a^3, a^5,a^6, a^7 are not expressed in the power of a^4. Therefore a^4 is not a generator.
Now, consider an element a^5.
$(a^5)^1 = a^5$
$(a^5)^2 = a^10 = a^2$
$(a^5)^3 = a^15 = a^7$
$(a^5)^4 = a^20 = a^4$
$(a^5)^5 = a^25 = a$
$(a^5)^6 = a^30 = a^6$
$(a^5)^7 = a^35 = a^3$

$(a^5)^8 = a^40 = a^8 = e$
Clearly all the elements of G are expressed in the power of a^5, therefore a^5 is a generator of G.
Similarly, we can show that a^7 is a generator and a^6 is not generator.
Therefore the generators of this group are a, a^3, a^5, a^7. Total number of generators is 4.

Example: Show that the group ({ 1,2,3,4,5,6}, $\times_7$) is cyclic. How many generators of this group?
Solution:
Consider the element 3 of this group.
$(3)^1 = 3$
$(3)^2 = 3\times_7 3 = 2$
$(3)^3 = 3\times_7 3\times_7 3 = 6$
$(3)^4 = 3\times_7 3\times_7 3\times_7 3 = 4$
$(3)^5 = 3\times_7 3\times_7 3\times_7 3\times_7 3 = 5$
$(3)^6 = 3\times_7 3\times_7 3\times_7 3\times_7 3\times_7 3 = 1$
Clearly all the elements of G are expressed in the power of 3, therefore 3 is a generator of G.
Since generator exists, therefore the group is cyclic.
Another generator will be 5. Because,
$(5)^1 = 5$
$(5)^2 = 5\times_7 5 = 4$
$(5)^3 = 5\times_7 5\times_7 5 = 6$
$(5)^4 = 5\times_7 5\times_7 5\times_7 5 = 2$
$(5)^5 = 5\times_7 5\times_7 5\times_7 5\times_7 5 = 3$
$(5)^6 = 5\times_7 5\times_7 5\times_7 5\times_7 5\times_7 5 = 1$
No other elements will be generator. Therefore number of generators is 2 i.e. 3 and 5.

1.14 Subgroup

Let (G,o) be a group and H is a subset of G. (H,o) is said to be a subgroup of (G,o) if (H,o) is also a group by itself.

Note: (G,o) and ({e},o) are the improper subgroups or trivial subgroups of (G,o).

Example: Is the subset {1,-1} a subgroup of multiplicative group {1, -1, i, -i}?
Solution: We have to check all the properties of group is satisfied with in set {1,-1} under multiplication operation.
Now, 1*1 = 1, 1*-1 = -1, and -1*(-1) = 1. Clearly the results of these operation are 1 and -1. And both elements belong in to given subset {1,-1}. Therefore closure property is satisfied.
Since {1,-1} is subset of set {1,-1,i,-i}, therefore associative property is satisfied with in {1,-1}.
Clearly 1 is identity element and it is belong into {1,-1} , therefore existence of identity property is also satisfied.
Now, 1*1 = 1, and -1*(-1) = 1. Therefore, inverse of 1 is 1 and inverse of -1 is -1. Since each element has its inverse, therefore subset {1,-1} is satisfied inverse property.
Clearly, this subset satisfies all the property, therefore this is group. And it will also be

subgroup of {1,-1,i,-i}.

Example: Is the set of even integers a subgroup of additive group of integers?
Solution: Let I be the set of integers and H be the set of even integers.
If we add any two even integers, then we get also an integer. Therefore, addition operation satisfies closure property with in H.
Since H is a subset of I, therefore associative property is also satisfied in H.
Clearly 0 is an identity element and it also belong into H, therefore, identity property is also satisfied in H.
Consider an element a∈H. Clearly, a+(-a) = 0, therefore -a is the inverse of a. And -a is also belong into H. Therefore, inverse property is satisfied in H.
Clearly, this subset satisfies all the property, therefore this subset H is group. And it will also be subgroup of I.

1.15 Some theorems

Theorem: The identity of a subgroup is the same as that of the group.
Proof: Let H be the subgroup of G and e and e' are the identity elements of G and H respectively.
Let a ∈ H. Then
aoe' = a .....(1)
Since a ∈ H ⇒ a∈ G, therefore
aoe = a .....(2)
from (1) and (2), aoe' = aoe
⇒ e' = e (using left cancellation law)
Therefore, the identity of a subgroup is the same as that of the group.

Theorem: The inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.
Proof: Let H be a subgroup of G..
Let a ∈ H. Let b and c are the inverses of element a in H and g respectively. Therefore,
aob = e' .....(1)
and aoc = e .....(2)
From previous theorem, e' = e
Therefore, aob = aoc
⇒ b = c (using left cancellation law)
Therefore, the inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Theorem: A non-empty subset H of a group G is a subgroup of G iff
(a) a ∈ H, b ∈ H ⇒ aob ∈ H.
(b) a ∈ H ⇒ a^{-1} ∈ H, where a^{-1} is the inverse of a in G.
Proof:
Necessary part:
Suppose H is a subgroup of G.
Since H is a subgroup of G, therefore closure property is satisfied within H.
So, a ∈ H, b ∈ H ⇒ aob ∈ H. Clearly part (a) is proved.

Let a $\in$ H. Since H $\subseteq$ G, therefore a $\in$ G. Let a^{-1} is the inverse of a in G. Since the inverse of an element in subgroup and group is same, therefore $a^{-1} \in$ H. Clearly, part (b) is also proved.

Sufficient part:

Suppose given two statements (a) and (b) are true.

Using statement (a), closure property is satisfied within H.

Since H is a subset of G and G is a group, therefore associative property is also satisfied within H.

Using statement (b), if a $\in$ H then $a^{-1} \in$ H. therefore inverse property is also satisfied within H.

Now, consider a $\in$ H $\Rightarrow$ a $\in$ H and $a^{-1} \in$ H (since inesr property is satisfied)

$\Rightarrow$ ao$a^{-1} \in$ H (using statement (a))

$\Rightarrow$ e $\in$ H, where e is an identity element.

Therefore, identity property is also satisfied within H. Clearly, all the four properties of group is satisfied within H. Therefore, H is a subgroup of G.

Theorem: The necessary and sufficient condition for a non-empty subset H of a group (G,o) to be a subgroup is

a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$

Where b^{-1} is the inverse of b in G.

Proof:

Necessary part:

Suppose H is a subgroup of G.

Let a$\in$ H and b $\in$ H. Since H is subgroup, therefore $b^{-1} \in$ H using inverse property.

Now, a$\in$ H and $b^{-1} \in$ H. By using closure property, ao$b^{-1} \in H$. Therefore the given statement is proved.

Sufficient part:

Suppose a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$ .....(1)

Now, we have to show that H is a subgroup of G.

Identity property:

a$\in$H , a$\in$H $\Rightarrow$ ao$a^{-1} \in H$ (using statement (1))

$\Rightarrow$ e $\in H$

Here, e is the identity element. Therefore, identity property is satisfied within H.

Inverse property:

Now, e $\in H$, a$\in$H $\Rightarrow$ eo$a^{-1} \in H$ (using statement (1))

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

Therefore, inverse property is satisfied within H.

Associative property:

Since H $\subseteq$ G, therefore associative property is also satisfied within H, because G is a group.

Closure property:

consider a$\in$H, b$\in$H $\Rightarrow$ a$\in$H, $b^{-1} \in$H

$\Rightarrow$ ao$(b^{-1})^{-1} \in H$ (using statement (1))

$\Rightarrow$ aob $\in$ H

Therefore, closure property is satisfied within H.

Clearly all the four properties are satisfied within H, therefore H is a subgroup of G.

It is proved.

Example: Let G = { .....,$3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3$,.....} be the multiplicative group. Let H = {1,3,$3^2, 3^3$,.....}. Is H a subgroup of G.
Solution: Clearly H is a subset of G, therefore it may be subgroup.
If a∈H, b∈H ⇒ a$ob^{-1} \in H$ is satisfied for each elements a,b ∈ H, then H will be subgroup.
Consider a = 3 and b= 3^3.
Now, aob^{-1} = 3o$(3^3)^{-1}$
= 3o3^{-3}
= 3^{-2}
Clearly this element i.e. $3^{-2} \notin$ H, therefore H is not subgroup of G.

Theorem: The intersection of any two subgroups of a group (G,o) is again a subgroup of (G,o).
Proof: Let (H_1,o) and (H_2,o) are the two subgroups of (G,o).
Let a ∈ $H_1 \cap H_2$ and b ∈ $H_1 \cap H_2$
⇒ (a ∈ H_1 and a ∈ H_2) and (b ∈ H_1 and b ∈ H_2)
⇒ (a ∈ H_1 and b ∈ H_1) and (a ∈ H_2 and b ∈ H_2)
⇒ a$ob^{-1} \in H_1$ and a$ob^{-1} \in H_2$ (Since H_1 and H_2 are subgroups.)
⇒ a$ob^{-1} \in H_1 \cap H_2$
Therefore, $H_1 \cap H_2$ is also a subgroup.

Example: The union of two subgroups is not necessarily a subgroup.
Solution: Let G be the additive group of integers.
H_1 = { .....,-6,-4,-2,0,2,4,6,.....} and H_2 = { .....,-9,-6,-3,0,3,6,9,.....} are both subgroups of G. But $H_1 \cup H_2$ is not subgroup.

1.16 Coset

Let H be subgroup of G and let a ∈ G. Then set {aoh ! h ∈ H} is called the left coset generated by a and H and is denoted by aH. And right coset is denoted by Ha = {hoa ! h ∈ H}.

1.17 Index of a subgroup in a group

If H is a subgroup of a group G, then the number of distinct right(or left) cosets of H in G is called the index of H in G and it is denoted by [G:H].

Example: Let G be the additive group of integers i.e. G = { .....-3,-2,-1,0,1,2,3,4,.....}. Let H = { .....,-9,-6,-3,0,3,6,9,.....} be the subgroup of G. Determine the index of H in G.
Solution: The index of H in G = The number of left cosets of H in G.
Now, we calculate all distinct left cosets.
0+H = H = { .....,-9,-6,-3,0,3,6,9,.....}.
1+H = {.....,-8,-5,-2,1,4,7,10,.....}
2+H = {....., -7,-4,-1,2,5,8,11,.....}
3+H = { .....,-9,-6,-3,0,3,6,9,.....}.
4+H = {.....,-8,-5,-2,1,4,7,10,.....}
Clearly the number of distinct left cosets is 3. Therefore, the index of H in G = 3.

1.18 Normal Subgroup

A subgroup H of G is said to be normal subgroup of G if Ha = aH, $\forall$ a $\in$ G.

Theorem: A subgroup H of G is normal iff $g^{-1}hg \in$ H, $\forall$ h $\in$ H, g$\in$ G.
Proof:
First part: Let H be a normal subgroup of G.
Let h $\in$ H, $g \in$ G. Since H is normal subgroup, therefore $gH = Hg$.
Now,$hg \in Hg \Rightarrow$ h$g \in gH$ (since $gH = Hg$)
$\Rightarrow g^{-1}hg \in (g^{-1}g)H$
$\Rightarrow g^{-1}hg \in$ eH
$\Rightarrow g^{-1}hg \in$ H
Now, it is proved.
Second part: Suppose $g^{-1}hg \in$ H, $\forall$ h $\in$ H, $g \in$ G .....(1)
Now, we have to show that $gH = Hg$.
Let $hg \in Hg$. $\Rightarrow (gg^{-1})hg \in Hg$
$\Rightarrow g(g^{-1}hg) \in Hg$
$\Rightarrow gh' \in$ Hg (using (1))
$\Rightarrow gh' \in$ gH
$\Rightarrow g(g^{-1}hg) \in gH$
$\Rightarrow hg \in gH$
Therefore, $Hg \subseteq gH$ .....(2)
Now, let $gh \in gH$. $\Rightarrow (g^{-1})^{-1})hg^{-1}g \in gH$
$\Rightarrow h'g \in gH$ (using (1))
$\Rightarrow h'g \in Hg$
$\Rightarrow (g^{-1})^{-1})hg^{-1}g \in Hg$
$\Rightarrow gh \in Hg$
Therefore, $gH \subseteq Hg$ .....(3)
From (2) and (3), $gH = Hg$, $\forall$ $g \in$ G.
Therefore, H is normal subgroup of G. Now, it is proved.

Example: If H is a subgroup of G such that $a^2 \in$ H for every a$\in$ G, then prove that H is a normal subgroup of G.
Solution: Let a $\in$ G. Then $a^2 \in$ H.
We know that if $a^{-1}ba \in$ H, then H is normal subgroup, for b $\in$ H.
Here, b = a^2, therefore, $a^{-1}ba = a^{-1}a^2a = a^2 =$ b
Since, b $\in$ H, therefore $a^{-1}ba \in$ H. Hence, H is a normal subgroup.

1.19 Lagrange's theorem

Statement: The order of each subgroup of a finite group G is a divisor of the order of the group.

Proof: Let H be any subgroup of order m of a finite group G of order n.
Consider all the left cosets of H in G.
Let H = $\{h_1, h_2, h_3, ..., h_m\}$. Then the left cosets of H i.e aH also consists of m

elements i.e. aH = $\{ah_i \text{ ! } 1 \leq i \leq m\}$.
Clearly, each cosets of H in G consists of m distinct elements. Since G is a finite group, therefore the number of distinct left cosets is also finite. Let this be k. Therefore,

km = n

$\Rightarrow$ m is a divisor of n.

It is proved.

1.20 Exercise

1. Consider the group G = {1, 2, 3, 4, 5, 6} under multiplication modulo 7.
   (a) Find the multiplication table of G.
   (b) Find $2^{-1}, 3^{-1}, 6^{-1}$.
   (c) Find the orders and subgroups generated by 2 and 3.
   (d) Is G cyclic?
2. Let Z be the group of integers with binary operation $*$ defined by $a * b$ = a + b - 2 , for all a,b $\in$ Z . Find the identity element of the group $(Z, *)$.
3. What do you mean by cosets of a subgroup? Consider the group Z of integers under addition and the subgroup H = {. . . ., -12, -6, 0, 6 12, ... } considering of multiple of 6.
   (a) Find the cosets of H in Z.
   (b) What is the index of H in Z.
4. Prove or disprove that intersection of two normal subgroups of a group G is again a normal subgroup of G.
5. Let $(A, *)$ be a monoid such that for every x in A , $x * x$ = e, where e is the identity element . Show that $(A, *)$ is an abelian group.
6. Let H be a subgroup of a finite group G. Prove that order of H is a divisor of order of G.
7. Prove that every group of prime order is cyclic.

2 Permutation group

2.1 Permutation

Let A be a finite set. Then a function f: A $\rightarrow$ A is said to be a permutation of A if f is bijective.

Degree of permutation The number of distinct elements in the finite set A is called the degree of the permutation.

Suppose A = $\{a_1, a_2, a_3, ..., a_n\}$. Then the notation of permutation will be of the following type:-

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & ..... & a_n \\ f(a_1) & f(a_2) & f(a_3) & ..... & f(a_n) \end{pmatrix}$$

2.2 Equality of two permutations

Let f and g be two permutations defined on the set A.

f = g iff f(a) = g(a), $\forall$ a $\in$ A.

Example: f = $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, g = $\begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$

Clearly f = g because image of each element is same.

2.3 Identity permutation

If each element of a permutation is replaced by itself, then it is called an identity permutation.

Example: Identity permutation defined on set A = {a,b,c} is

$$\text{I} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

2.4 Product of permutations or Composition of permutations

The product of two permutations f and g of same degree is denoted by fog or fg, meaning first perform f and then perform g.

Example: If f = $\begin{pmatrix} a_1 & a_2 & \ldots\ldots\ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots\ldots\ldots & b_n \end{pmatrix}$, g = $\begin{pmatrix} b_1 & b_2 & \ldots\ldots\ldots\ldots & b_n \\ c_1 & c_2 & \ldots\ldots\ldots\ldots & c_n \end{pmatrix}$

Then fg = $\begin{pmatrix} a_1 & a_2 & \ldots\ldots\ldots\ldots & a_n \\ c_1 & c_2 & \ldots\ldots\ldots\ldots & c_n \end{pmatrix}$

Note 1: fg $\neq$ gf.

Therefore, the product of two permutations is not commutative.

Note 2: The product of permutations is associative.

2.5 Inverse permutation

Consider a permutation $f = \begin{pmatrix} a_1 & a_2 & \ldots\ldots\ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots\ldots\ldots & b_n \end{pmatrix}$

Then the inverse of this permutation will be $f^{-1} = \begin{pmatrix} b_1 & b_2 & \ldots\ldots\ldots\ldots & b_n \\ a_1 & a_2 & \ldots\ldots\ldots\ldots & a_n \end{pmatrix}$

Total number of permutations

If n is the degree of the permutation, then the number of permutations of degree n is n!.

If S_n be the set of all permutations of degree n, then S_n is said to be symmetric set of permutations of degree n.

2.6 Permutation group or symmetric group

An algebraic structure $(S_n, *)$ is said to be permutation group, where the operation * is the composition or product of permutations and set S_n is symmetric set of permutations of degree n. This group is also called symmetric group.

2.7 Cyclic permutation

A permutation which replaces n objects or elements cyclically is called a cyclic permutation of degree n.

Example: Permutation f = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
It is written as (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3)
The number of elements in a cycle is said to be its length.

Disjoint cycle; Two cycles are said to be disjoint if there is no common element in both the cycles.
Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles.

Example: Permutation f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

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

Transposition A cyclic permutation with length 2 is said to be transposition.
Ex.: (1 2), (4 5) are transpositions.

Even or odd permutation
A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

Example: Find out following permutations are even or odd.
(1) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$, (2) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$
Solution:
(1) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$

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

Clearly, this permutation is expressed as 3 number of transpositions, therefore this permutation is odd permutation.
(2) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

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

Clearly, this permutation is expressed as 4 number of transpositions, therefore this permutation is even permutation.

3 Homomorphism and Isomorphism of groups

3.1 Group homomorphism

Let (G_1, o_1) and (G_2, o_2) be the two groups and f is function from G_1 to G_2. f is said to be group homomorphism from G_1 to G_2 if $\forall$ a,b$\in G_1$,

f(ao_1b)= f(a)o_2f(b).

3.2 Group Isomorphism

A group homomorphism f is said to be group isomorphism if f is bijective.

3.3 Group automorphism

An isomorphism is said to be automorphism if both groups are same i.e. $G_1 = G_2$.

3.4 Kernel of homomorphism

The kernel of homomorphism f of a group G_1 to G_2 is the set of all elements of G_1 mapped on the identity element of G_2 by f. That is,
ker(f) = { a$\in G_1$! f(a) = e_2, where e_2 is the identity element of G_2}

Example: Let (G_1, o_1) = (Z,+) and (G_2, o_2) = ({1,-1},$\times$) are two groups.
f: Z $\to$ {1,-1} such that

$$\text{f(x)} = \begin{cases} 1 & , \ if\ n\ is\ even \\ -1 & , \ if\ n\ is\ odd \end{cases}$$

Find out f is a group homomprphism and isomorphism. And also find kernel of f.
Solution: Consider two integers a and b belong into Z. There will be four case for the sum a+b.
Case 1: when both a and b are even.
f(a+b) = 1 = 1 $\times$ 1 = f(a)$\times$f(b)
Case 2: when both a and b are odd.
f(a+b) = 1 = (-1) $\times$ (-1) = f(a)$\times$f(b)
Case 3: when a is even and b is odd.
f(a+b) = -1 = 1 $\times$ (-1) = f(a)$\times$f(b)
Case 4: when a is odd and b is even.
f(a+b) = -1 = (-1) $\times$ 1 = f(a)$\times$f(b)
Clearly, in all the four cases, f(a+b) = f(a)$\times$f(b)
Therefore, f is homomorphism.
Now, we have to check function is bijective or not.
Clearly, function not one-one. Because all even numbers mapped to 1 and all odd numbers mapped to -1. Therefore, this function is not bijective.
Hence the function is not isomorphism.
Now, ker(f) = The set of all even integers. Because all even integers are mapped on to identity element 1 of G_2.

Example: Let (G_1, o_1) = (R,+) and $(G_2, o_2) = (R^+,\times)$ are two groups.
f: $G_1 \to G_2$ defined by f(x) = 2^x.
Find out f is a group homomorphism and isomorphism.

Solution: Consider any two elements a and b of R.
Now, f(a+b) = $2^{(a+b)}$
$= 2^a \times 2^b$
= f(a)×f(b)
Clearly, f(a+b) = f(a)×f(b). Therefore f is homomorphism.
Clearly, for each distinct real number a, there will be distinct positive real number 2^a. Therefore the function is one-one.
Clearly, the function is onto because each element of R^+ is the image of some element of R.
Therefore the function f is bijective. Hence the function is isomorphism.

Theorem: Let (G_1, o_1) and (G_2, o_2) are two groups and let f be a homomorphism from G_1 to G_2. Then, prove the following:-
(1) f(e_1) = e_2, where e_1 is the identity of G_1 and e_2 is the identity of G_2.
(2) f(a^{-1}) = $(f(a))^{-1}$, $\forall a \in G_1$
(3) If H is a subgroup of G_1, then f(H) = {f(h) ! h ∈ H} is a subgroup of G_2.
Proof: (1) f(e_1) = f(e_1 o_1 e_1) = f(e_1) o_2 f(e_1)
⇒ f(e_1) = f(e_1) o_2 f(e_1) .....(1)
Since f(e_1) is the element of G_2, therefore using identity property
e_2 o_2 $f(e_1)$ = f(e_1) .....(2)
From (1) and (2), f(e_1)o_2f(e_1) = $e_2 o_2 f(e_1)$
⇒ f(e_1) = e_2 (using right cancellation law)
It is proved.
(2) f(e_1) = f(a o_1 a^{-1}) = $f(a)$ o_2 $f(a^{-1})$
⇒ f(e_1) = $f(a)$ o_2 $f(a^{-1})$ .....(3)
Now, $f(a)$ o_2 $(f(a))^{-1}$ = e_2 .....(4)
From part (1), we know that f(e_1) = e_2 , therefore from (3) and (4)
$f(a)$ o_2 $f(a^{-1})$ = $f(a)$ o_2 $(f(a))^{-1}$
⇒ f(a^{-1}) = $(f(a))^{-1}$ (using left cancellation law)
It is proved.
(3) Let h is subgroup of G_1.
a∈H, b∈H ⇒ ao_1b^{-1} ∈ H
Now, we have to show that f(H) is a subgroup of G_2.
Since a,b∈ H, therefore f(a), f(b) ∈ f(H).
f(a)∈ f(H), f(b)∈ f(H) ⇒ a∈H, b∈H
⇒ a o_1 b^{-1} ∈ H
⇒ f(a o_1 b^{-1}) ∈ f(H)
⇒ $f(a)$ o_2 $f(b^{-1})$ ∈ f(H)
⇒ $f(a)$ o_2 $(f(b))^{-1}$ ∈ f(H) (using part (2),f(a^{-1}) = $(f(a))^{-1}$)
Therefore, f(H) is a subgroup of G_2.
It is proved.

3.5 Factor or Quotient group

If H is a normal subgroup of group G, then the set of all left cosets of G forms a group with respect to the multiplication of left coset defined as (aH)(bH) = (ab)H, called the factor group of G by H. It is denoted by G/H.
G/H = { gH ! g ∈ G }

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_14	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

4 Exercise

1. In the symmetric group S_3, find all those elements a and b such that
   (a) $(a * b)^2 \neq a^2 * b^2$
   (b) $a^2 = \text{e}$
   (c) $a^3 = \text{e}$
2. Show that in a group (G,o), if for any a,b $\in$ G, $(aob)^2 = a^2ob^2$, then (G,o) must be abelian.
3. Show that every cyclic group of order n is isomorphic to the group $(Z_n,\ +_n)$.
4. Find all the subgroups of following groups:-
   (a) $(Z_{12},\ +_{12})$
   (b) $(Z_5,\ +_5)$
   (c) $(Z_7^*,\ \times_7)$
   (d) $(Z_{11}^*,\ \times_{11})$

5 Exercise's solution

1. Let $p_1, p_2, p_3, p_4, p_5, p_6$ are the elements of S_3.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

   The composition table for S_3 with respect to multiplication operation is the following:-

   (a) In this part, we have to find elements a and b of S_3 which satisfy equation (1).
   $(a * b)^2 \neq a^2 * b^2$ ..... (1)
   Consider, a = p_2 and b = p_3.
   Now, LHS = $(a * b)^2 = (p_2 * p_3)^2 = p_5^2 = p_6$
   RHS = $a^2 * b^2 = p_2^2 * p_3^2 = p_1 * p_1 = p_1$
   Clearly, $(a * b)^2 \neq a^2 * b^2$ for a = p_2 and b = p_3.

Similarly, Consider, a = p_2 and b = p_4.
Now, LHS = $(a * b)^2 = (p_2 * p_4)^2 = p_6^2 = p_5$
RHS = $a^2 * b^2 = p_2^2 * p_4^2 = p_1 * p_1 = p_1$
Clearly, $(a * b)^2 \neq a^2 * b^2$ for a = p_2 and b = p_4.

Similarly, following pairs of a and b are also satisfied.
a = p_2 and b = p_5
a = p_2 and b = p_6
a = p_3 and b = p_4
a = p_3 and b = p_5
a = p_3 and b = p_6
a = p_4 and b = p_5
a = p_4 and b = p_6

(b) In this part, we have to find element a of S_3 which satisfy equation (2).
a^2 = e .....(2)
Here, the identity element is e = p_1.
Consider, a = p_1
$a^2 = p_1^2 = p_1$ = e
Therefore, a = p_1 satisfy the equation (2).
Similarly, a = p_2, p_3, p_4 also satisfy the equation (2).

(c) In this part, we have to find element a of S_3 which satisfy equation (3).
a^3 = e .....(3)
Here, the identity element is e = p_1.
Consider, a = p_1
$a^3 = p_1^3 = p_1$ = e
Therefore, a = p_1 satisfy the equation (3).
Similarly, a = p_5, p_6 also satisfy the equation (3).

2. Given $(aob)^2 = a^2ob^2$, for a,b ∈ G.
It imply that (aob)o(aob) = (aoa)o(bob)
⇒ ao(bo(aob)) = ao(ao(bob)) (using associative law)
⇒(bo(aob)) = (ao(bob)) (using left cancellation law)
⇒(boa)ob = (aob)ob (using associative law)
⇒ (boa) = (aob)(using right cancellation law)
Therefore, the group (G,o) is an abelian group.

3. Let cyclic group(G,o) of order n be generated by an element a ∈ G. So the elements of G are $a, a^2, a^3, ..., a^n = e$.
Define g : $Z_n \to G$ such that g([1]) = a. [1] is the generator of $(Z_n, +_n)$. Then g([j]) = a^j, for all j = 0,1,2,3,.....,n-1.
Clearly this function is bijective because each element j is mapped to unique element a^j.
Now, g([j]+[k]) = $a^{[j]+[k]}$
= $a^{[j]}oa^{[k]}$
= g[j] o g[k]
Clearly, g([j]+[k]) = g[j] o g[k]

Therefore, g is homoomorphism. Since g is bijective and homomorphism, so g is isomorphism.
Therefore, every cyclic group of order n is isomorphic to the group $(Z_n, +_n)$.

4. In this question, we have to find all the subgroups of given groups. In these questions, Z_n = {0,1,2,3,4,.....,n-1} and $+_n$ and $\times_n$ are addition and multiplication modulo n operations.
According to Lagrange's theorem, order of each subgroup is the divisor of the order of the group. We will use this theorem to find all the subgroups.

   (a) Here group is $(Z_{12}, +_{12})$. Therefore Z_{12} = {0,1,2,3,4,5,6,7,8,9,10,11}. Clearly, the order of this group is 12. Using Lagrange's theorem, the number of subgroups of Z_{12} = number of positive divisors of 12.
   The positive divisors of 12 are 1,2,3,4,6,12. Since the number of divisors is 6, therefore number of subgroups will be 6 with orders 1,2,3,4,6,12. These subgroups are the following:-
   Now, H_1 = {0}, this is a subgroup with order 1.
   H_2 = {0,6}, this is a subgroup with order 2.
   H_3 = {0,4,8}, this is a subgroup with order 3.
   H_4 = {0,3,6,9}, this is a subgroup with order 4.
   H_5 = {0,2,4,6,8,10}, this is a subgroup with order 6.
   H_6 = {0,1,2,3,4,5,6,7,8,9,10,11}, this is a subgroup with order 12.

   (b) Here group is $(Z_5, +_5)$. Therefore Z_5 = {0,1,2,3,4}. Clearly, the order of this group is 5. The positive divisors of 5 are 1,5. Since the number of divisors is 2, therefore number of subgroups will be 2 with orders 1,5. These subgroups are the following:-
   H_1 = {0}, this is a subgroup with order 1.
   H_2 = {0,1,2,3,4}, this is a subgroup with order 5.

   (c) Here group is $(Z_7^*, \times_7)$. Therefore Z_7^* = {1,2,3,4,5,6}. Clearly, the order of this group is 6. The positive divisors of 6 are 1,2,3,6. Since the number of divisors is 4, therefore number of subgroups will be 4 with orders 1,2,3,6. These subgroups are the following:-
   H_1 = {1}, this is a subgroup with order 1.
   H_2 = {1,6}, this is a subgroup with order 2.
   H_3 = {1,2,4}, this is a subgroup with order 3.
   H_4 = {1,2,3,4,5,6}, this is a subgroup with order 6.

   (d) Here group is $(Z_{11}^*, \times_{11})$. Therefore Z_{11}^* = {1,2,3,4,5,6,7,8,9,10}. Clearly, the order of this group is 10. The positive divisors of 10 are 1,2,5,10. Since the number of divisors is 4, therefore number of subgroups will be 4 with orders 1,2,5,10. These subgroups are the following:-
   H_1 = {1}, this is a subgroup with order 1.
   H_2 = {1,10}, this is a subgroup with order 2.
   H_3 = {1,3,4,5,9}, this is a subgroup with order 5.
   H_4 = {1,2,3,4,5,6,7,8,9,10}, this is a subgroup with order 10.

Ring and Field

6 Ring

6.1 Definition

An algebraic structure (R, +, .), where R is a set and + and . are two binary operators defined on set R, is said to be ring if it satisfies following properties:-
(1) (R, +) is an abelian group.
(2) (R, .) is a semigroup.
(3) Distributive property must hold i.e. a.(b+c) = a.b + a.c and (b+c).a = b.a + c.a, $\forall$ a,b,c $\in$ R.

6.2 Commutative ring

A ring R is said to be commutative ring if it satisfies commutative property with respect second operation i.e.
a.b = b.a, $\forall$ a,b $\in$ R.

6.3 Ring with unity

A ring R is said to be ring with unity if it contains identity element with respect to second operation that is . operation.
Note: We will denote here identity element with respect to first operation by 0 and identity element with respect to second operation by 1.

Example: Show that the set Z of integers under addition and multiplication is commutative ring with unity.
Solution: (Z, +, .) is a ring if it satisfies all the properties of ring.
First we have to show that (Z,+) is an abelian group.
Closure property: We know that the addition of any two integers is also an integers. So, Z is closed under addition operation.
Associative property: We know that the addition of any three integers in any way is equal, therefore we can say, a+(b+c) = (a+b)+c, $\forall$ a,b,c $\in$ Z.
Therefore, Z satisfies associative property.
Existence of identity property: Let a $\in$ Z. Clearly, 0 $\in$ Z such that a+0 = a = 0+a. Therefore, 0 is an identity element. So, it satisfies identity property.
Existence of inverse property: Let a $\in$ Z. Clearly, -a $\in$ Z such that a+(-a) = 0. Therefore, -a is an additive inverse of any element a. So, it satisfies inverse property under addition operation.
Commutative property: Clearly, a+b = b+a, $\forall$ a,b $\in$ Z. So, Z satisfies commutative property with respect to addition operation.
Therefore, (Z,+) is an abelian group.

Now, we have to show that (Z, .) is a semigroup.
Closure property: We know that the multiplication of any two integers is also an integers. So, Z is closed under multiplication operation.
Associative property: We know that the multiplication of any three integers in any way is equal, therefore we can say, a.(b.c) = (a.b).c, $\forall$ a,b,c $\in$ Z.
Therefore, Z satisfies associative property.
Therefore, (Z, .) is a semigroup.
Now, we have to show **distributive property** is satisfied.
Clearly, for any three integers a,b,c; followings are satisfied:-
(i) a.(b+c) = a.b + a.c
(ii) (b+c).a = b.a + c.a
Therefore, distributive property is satisfied in (Z, +, .).
Therefore, (Z, +, .) is a ring.

Example: The set Z_n = {0,1,2,3,.....,n-1} under addition and multiplication modulo n is a commutative ring with unity.
Solution: $(Z_n, +_n, \times_n)$ is a ring if it satisfies all the properties of ring.
First we have to show that $(Z, +_n)$ is an abelian group.
Closure property: Consider a,b $\in$ Z_n. Clearly, a$+_n$b = c $\in$ Z_n. Therefore, Z_n is closed under addition modulo n operation.
Associative property: Clearly, if we compute $a +_n (b +_n c)$ and $(a +_n b) +_n c)$ then both value will be same. Therefore we can say, $a +_n (b +_n c) = (a +_n b) +_n c)$, $\forall$ a,b,c $\in$ Z_n).
Therefore, Z_n satisfies associative property.
Existence of identity property: Let a $\in$ Z_n. Clearly, 0 $\in$ Z_n such that a$+_n$0 = a = 0$+_n$a. Therefore, 0 is an identity element. So, it satisfies identity property.
Existence of inverse property: Let a $\in$ Z_n. Clearly, n-a $\in$ Z_n such that a$+_n$(n-a) = 0. Therefore, n-a is an additive modulo n inverse of any element a. So, it satisfies inverse property under addition operation.
Commutative property: Clearly, a$+_n$b = b$+_n$a, $\forall$ a,b $\in$ Z_n. So, Z_n satisfies commutative property with respect to addition modulo n operation.
Therefore, $(Z_n, +_n)$ is an abelian group.
Now, we have to show that $(Z_n, \times_n)$ is a semigroup.
Closure property: Consider a,b $\in$ Z_n. Clearly, a$\times_n$b = c $\in$ Z_n. Therefore, Z_n is closed under multiplication modulo n operation.
Associative property: Clearly, if we compute $a \times_n (b \times_n c)$ and $(a \times_n b) \times_n c)$ then both value will be same. Therefore we can say, $a \times_n (b \times_n c) = (a \times_n b) \times_n c)$, $\forall$ a,b,c $\in$ Z_n).
Therefore, Z_n satisfies associative property.
Therefore, $(Z_n, \times_n)$ is a semigroup.
Now, we have to show **distributive property** is satisfied.
Clearly, for any three elements a,b,c Z_n; followings are satisfied:-
(i) a$\times_n$(b$+_n$c) = a$\times_n$b $+_n$ a$\times_n$c
(ii) (b$+_n$c)$\times_n$a = b$\times_n$a $+_n$ c$\times_n$a
Therefore, distributive property is satisfied in $(Z_n, +_n, \times_n)$.
Therefore, $(Z_n, +_n, \times_n)$ is a ring.
Now, if this ring satisfies commutative property and identity property with respect to multiplication modulo n operation, then it is said to be commutative ring with unity.

Commutative property: Clearly, a$\times_n$b = b$\times_n$a, $\forall$ a,b $\in Z_n$. So, Z_n satisfies commutative property with respect to multiplication modulo n operation.
Existence of identity property: Let a $\in Z_n$. Clearly, 1 $\in Z_n$ such that a$\times_n$1 = a = 1$\times_n$a. Therefore, 1 is an identity element. So, it satisfies identity property with respect to multiplication modulo n operation.
Therefore, this ring $(Z_n, +_n, \times_n)$ is commutative ring with unity.

6.4 Elementary properties of a ring

Let a,b,c $\in$ R, then

1. a.0 = 0.a = 0
2. a.(-b) = (-a).b = -(a.b)
3. (-a).(-b) = a.b
4. a.(b-c) = a.b - a.c and (b-c).a = b.a - c.a

Proof: (1) a.0 +a.a = a.(0+a)
= a.a
= 0 + a.a
using right cancellation law, a.0 = 0
Similarly, 0.a +a.a = (0+a).a
= a.a
= 0 + a.a
using right cancellation law, 0.a = 0
Therefore, a.0 = 0.a = 0
(2) a.(-b) + a.b = a.(-b+b)
= a.0
= 0
therefore, a.(-b) = -(a.b)
Similarly, (-a).b + a.b = (-a+a).b
= 0.b
= 0
Therefore, (-a).b = -(a.b)
Therefore, a.(-b) = (-a).b = -(a.b)
(3) (-a).(-b) = -((-a).b) = -(-(a.b)) = a.b
(4) a.(b-c) = a.(b+(-c))
= a.b + a.(-c)
= a.b - a.c
Similarly, (b-c).a = (b+(-c)).a
= b.a + (-c).a
= b.a - c.a

Example: If R is a ring such that a^2 = a, $\forall$ a $\in$ R, prove that
(1) a+a = 0 , $\forall$ a $\in$ R i.e. each element of R is its own additive inverse.
(2) a+b = 0 $\Rightarrow$ a = b
(3) R is a commutative ring.

Solution:
(1) $(a+a)^2$ = a+a
$\Rightarrow$ $a^2+a^2+a^2+a^2$ = a+a
$\Rightarrow$ a+a+a+a = a+a
$\Rightarrow$ a+a = 0 using cancellation law
It is proved.
(2) a+b = 0 $\Rightarrow$ a+b = a+a (using part (1))
$\Rightarrow$ b = a (using cancellation law)
It is proved.
(3) $(a+b)^2$ = a+b
$\Rightarrow$ $a^2+ab+ba+b^2$ = a+b
$\Rightarrow$ a + ab + ba + b = a + b
$\Rightarrow$ ab + ba = 0 (using cancellation law)
$\Rightarrow$ ab = ba (using part (2))
Therefore, R is commutative ring. Now, It is proved.

7 Field

7.1 Definition

An algebraic structure (F, +, .), where F is a set and + and . are two binary operators defined on set F, is said to be field if it satisfies following properties:-
(1) (R, +) is an abelian group.
(2) (R' , .) is an abelian group, where R' = R-{0}.
(3) Distributive property must hold i.e. a.(b+c) = a.b + a.c and (b+c).a = b.a + c.a, $\forall$ a,b,c $\in$ F.

Example: The ring of rational numbers (Q , +, .) is a field.
Solution: Since (Q , +, .) is a ring therefore we have to show only second property of field i.e. (Q',.) is an abelian.
Since (Q , +, .) is ring therefore (Q',.) is a semigroup. Now, we hae to find identity element and inverse.
Clearly 1 is an identity element.
Consider an element a $\in$ Q'. clearly the inverse of a is 1/a. Therefore inverse property is also satisfied.
If a,b $\in$ Q' then a.b = b.a, therefore commutative property is satisfied. Since all the properties of an abelian group is satisfied within Q'. Therefore, (Q',.) is an abelian group.
Therefore, (Q , +, .) is a field.

Example: (R,+,.) is a field.

7.2 Ring with zero divisors

If a and b are two non-zero elements of a ring R such that a.b = 0, then a and b are divisors of 0(or o divisors). In particular, a is a left divisor of 0 and b is right divisor of 0.

Example: The ring of integers do not have zero divisors. Because there exist no two non-zero integers such that their product is zero.

7.3 Ring homomorphism

Let (R, +, .) and (S, $\oplus, \odot$) be rings. A mapping f: R $\rightarrow$ S is called a ring homomorphism from (R, +, .) to (S, $\oplus, \odot$) if for any a,b $\in$ R,
f(a+b) = f(a)$\oplus$ f(b) and f(a.b) = f(a)$\odot$ f(b)

7.4 Boolean ring

A ring R is said to be boolean ring if a^2 = a, $\forall$ a $\in$ R. **Example:** Show that a Boolean ring is always commutative.

Solution: It is proved in the previous example.

Example: If (R, +, .) is a ring with unity, then show that, for all a $\in$ R,
(i) (-1).a = -a
(ii) (-1).(-1) = 1
Solution:
(i) a + (-1).a = 1.a + (-1).a
= (1+(-1)).a
= 0.a
= 0
$\Rightarrow$ -a = (-1).a
(ii) (-1).(-1) = -((-1).1) = -(-(1.1)) = -(-(1)) = 1 (since $(a^{-1})^{-1}$ = a)

Example: Explain Boolean ring with suitable example.
Solution: A ring R is said to be boolean ring if a^2 = a, $\forall$ a $\in$ R.
Example of Boolean ring is $(Z_2, +_2, \times_2)$ because
Z_2 = {0,1} and $0^2 = 0 \times_2 0 = 0$, $1^2 = 1 \times_2 1 = 1$.

Note: $(Z_n, +_n, \times_n)$ is a field iff n is prime number.

Example: Determine all values of x from the given field which satisfies the given equation:-
(i) x + 1 = -1 over Z_2, Z_3, Z_5 *and* Z_7
(ii) 2x + 1 = 2 over Z_3, *and* Z_5
(iii) 5x + 1 = 2 over Z_5
Solution:
(i) Consider field Z_2. Z_2 = {0,1}. Now, we have to find which values of Z_2 satisfies following x + 1 = -1.
Here, -1 indicate the additive inverse of 1.Clearly, in this field, additive inverse of 1 is 1, therefore the given equation is modified as x + 1 = 1.
Clearly x = 0 satisfies this equation.
Consider field Z_3. Z_3 = {0,1,2}. In this field, additive inverse of 1 is 2, therefore the given equation is modified as x + 1 = 2.

Clearly x = 1 satisfies this equation.
Consider field Z_5. Z_5 = {0,1,2,3,4}. In this field, additive inverse of 1 is 4, therefore the given equation is modified as x + 1 = 4.
Clearly x = 3 satisfies this equation.
Consider field Z_7. Z_7 = {0,1,2,3,4,5,6}. In this field, additive inverse of 1 is 6, therefore the given equation is modified as x + 1 = 6.
Clearly x = 5 satisfies this equation.
(ii) Consider field Z_3. Z_3 = {0,1,2}. Now, we have to find which values of Z_3 satisfies following 2x + 1 = 2.
Clearly x = 2 satisfies this equation.
Consider field Z_5. Z_5 = {0,1,2,3,4}. Now, we have to find which values of Z_5 satisfies following 2x + 1 = 2.
Clearly x = 3 satisfies this equation.
(iii) Consider field Z_5. Z_5 = {0,1,2,3,4}. Now, we have to find which values of Z_5 satisfies following 5x + 1 = 2.
Clearly there is no x in Z_5 which satisfies this equation.

7.5 Exercise

1. Show that $(Z_7, +_7, \times_7)$ is a commutative ring with identity.

2. We are given the ring ({a,b,c,d}, +, .), whose operations are given by the following table:-

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

.	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	a

   Is it commutative ring? Does it have an identity? what is the zero of this ring? Find the additive inverse pf each of its elements.

3. Show that $(I, \oplus, \odot)$ is a commutative ring with identity, where the operations $\oplus$ and $\odot$ are defined, for any a,b $\in$ I as a$\oplus$b = a+b-1 and a$\odot$b = a+b-ab.

4. Prove that $(R, +, *)$ is a ring with zero divisors, where R is 2x2 matrix and + and $*$ are usual addition and multiplication operations.