Unit 4 (Algebraic structures)

§ Binary operation on a set: Let G be a non-empty set. Then $G \times G = \{(a,b) : a \in G, b \in G\}$. If $f : G \times G \longrightarrow G$, then f is said to be a binary operation on the set G. The image of the ordered set pair (a,b) under the function f is denoted by afb. Often we use symbols $+, \times, \cdot, \circ, *$ etc. to denote binary operation on a set.

Thus $(+)$ will be a binary operation on G iff

$a+b \in G, \forall a,b \in G$ and $a+b$ is unique.

Similarly, $*$ will be a binary operation on G iff

$a*b \in G, \forall a,b \in G$ and $a*b$ is unique.

A binary operation on a set G is sometimes also called binary composition.

Example: Addition is a binary operation on the set N of natural numbers. The sum of two natural numbers is also a natural number. Therefore N is closed with respect to addition i.e $a+b \in N \ \forall a,b \in N$.

Subtraction is not a binary operation on N. we have $4-7 = -3 \notin N$ whereas $4 \in N$, $7 \in N$. Thus N is not closed with respect to subtraction. But subtraction is a binary operation on the set of integers I. we have $a-b \in I \ \forall a,b \in I$.

§ Algebraic Structure: A non-empty set G equipped with one or more binary operations is called an algebraic structure.

Suppose $*$ is a binary operation on G. Then $(G,*)$ is an algebraic structure.

$(N,+)$, $(I,+)$ $(I,-)$, $(R,+,\cdot)$ are all algebraic structures.

Unit 4 (Algebraic structures)

§. **Binary operation on a set:** Let G be a non-empty set. Then $G \times G = \{(a,b) : a \in G, b \in G\}$.

If $f : G \times G \longrightarrow G$, then f is said to be a binary operation on the set G. The image of the ordered set pair (a,b) under the function f is denoted by afb. Often we use symbols $+, \times, \cdot, \circ, *$ etc. to denote binary operation on a set.

Thus '$+$' will be a binary operation on G iff

$a+b \in G, \forall a, b \in G$ and $a+b$ is unique.

Similarly, '$*$' will be a binary operation on G iff

$a * b \in G, \forall a, b \in G$ and $a * b$ is unique.

A binary operation on a set G is sometimes also called binary composition.

Example: Addition is a binary operation on the set N of natural numbers. The sum of two natural numbers is also a natural number. Therefore N is closed with respect to addition i.e $a+b \in N \ \forall a, b \in N$.

Subtraction is not a binary operation on N. we have $4-7 = -3 \notin N$ whereas $4 \in N$, $7 \in N$. Thus N is not closed with respect to subtraction. But subtraction is a binary operation on the set of integers I. we have $a-b \in I \ \forall a, b \in I$.

§. **Algebraic Structure:** A non-empty set G equipped with one or more binary operations is called an algebraic structure.

Suppose $*$ is a binary operation on G. Then $(G, *)$ is an algebraic structure.

$(N, +)$, $(I, +)$ $(I, -)$, $(R, +, \cdot)$ are all algebraic structures.

§. Group. (Definition)

Let G be a non-empty set equipped with a binary operation denoted by • ie $a \cdot b$ or more conveniently ab represents the element of G obtained by applying the said binary operation between the elements a and b of G taken in that order. Then this algebraic structure $(G, \cdot)$ is a group, if the binary operation • satisfies the following postulates:

1. Closure property ie, $ab \in G \ \forall \ a, b \in G$
2. Associativity ie. $(ab)c = a(bc) \ \forall \ a, b, c \in G$
3. Existence of identity. There exists an element $e \in G$ such that $ea = a = ae \ \forall a \in G$.

The element e is called the identity.

4. Existence of inverse: Each element of G possesses inverse. In other words, $a \in G \Rightarrow$ there exists an element $b \in G$ such that $ba = e = ab$. The element b is then called the inverse of a and we write $b = a^{-1}$. Thus a^{-1} is an element of G such that $a^{-1}a = e = aa^{-1}$.

Abelian group or Commutative group. Definition

A group G is said to be abelian or commutative if in addition to the above four postulates the following postulate is also satisfied.

5. Commutativity: ie $ab = ba \ \forall \ a, b \in G$.

§. Finite and Infinite groups: Order of a finite group

If in a group G the underlying set G consists of a finite number of distinct elements, then the group is called a finite group, otherwise an infinite group. The number of elements in a finite group is called the order of the group. An infinite group is said to be of infinite order

We shall denote the order of a group G by the symbol $O(G)$.

Q: Show that the four fourth roots of unity namely $1, -1, i, -i$ form a group with respect to multiplication.

Sol Let $G = \{1, -1, i, -i\}$. To show that multiplication is a composition in G, we form the composition table.

Multiplication (×)	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(I) **Closure property:** Since all the entries in the composition table are elements of the set G, G is closed with respect to multiplication. Hence G is closed with respect to multiplication.

(II) **Associativity:** $a(bc) = (ab)c$ for all values of a, b, c in G.

For example, $1[(-1)i] = -i = [1(-1)]i$

(III) **Identity element:** $1 \in G$ is the identity element as $1 \cdot a = a \cdot 1 = a$. It can be seen from the first row and first column of the table.

[IV] **Inverse:** Inverses of $1, -1, i$ and $-i$ are $1, -1, -i$ and i respectively and all those belong to G.

(V) **Commutative law:** $ab = ba$ for all a, b in G.

From the composition table it is clear that elements in each row are the same as the elements in the corresponding column so that $ab = ba$.

Hence G is a group (abelian) with respect to multiplication.

For Practice

Q: Show that the set $G = \{1, \omega, \omega^2\}$, where ω is an imaginary cube root of unity is a group with respect to multiplication.

Q: Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition and multiplication modulo 6.

Example: Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = (ab)/2$

Solution: Let Q_+ denote the set of all positive rational numbers. We define an operation $*$ on Q_+ as follows:

$$a * b = (ab)/2 \quad \forall\ a, b \in Q_+$$

To show that $(Q_+, *)$ is a group.

(1) **Closure property:** Since for every $a, b \in Q_+$, $(ab)/2$ is also in Q_+, therefore Q_+ is closed with respect to the operation $*$.

(2) **Associativity:** Let $a, b, c \in Q_+$. Then

$$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{[ab/2]c}{2} = \frac{a[(bc)/2]}{2} = a * \frac{bc}{2} = a*(b*c)$$

(3) **Existence of identity:** The number e will be the identity element if $e \in Q_+$ and if

$$e * a = a = a * e \quad \forall\ a \in Q_+.$$

Now $e*a = a \Rightarrow (ea)/2 = a \Rightarrow (a/2)(e-2) = 0 \Rightarrow e = 2$, since $a \in Q_+ \Rightarrow a \neq 0$

Now, $2 \in Q_+$ and we have $2*a = (2a)/2 = a = a*2 \quad \forall\ a \in Q_+$

$\therefore$ 2 is the identity element.

(4) **Existence of inverse:** Let a be any element of Q_+. If the number b is to be the inverse of a, then we must have

$$b*a = e = 2 \Rightarrow \frac{ba}{2} = 2 \Rightarrow b = 4/a$$

Now, $a \in Q_+ \Rightarrow \frac{4}{a} \in Q_+$.

we have $\left(\frac{4}{a}\right)*a = \left[\left(\frac{4}{a}\right)a\right]/2 = 2 = a * \frac{4}{a}$

Therefore $4/a$ is the inverse of a. Thus each element of Q_+ is inversible.

(5) **Commutativity:** Since for every $a, b \in Q_+$, $\frac{ab}{2}$ is also in Q_+.

Let $a, b \in Q_+$. Then $a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$

Hence $(Q_+, *)$ is an abelian group

§. Subgroup: A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a composition in H and for this composition H itself is a group.

Now every set is a subset of itself. Therefore if G is a group, then G itself is a subgroup of G. Also if e is the identity of G, then the subset of G containing only one element i.e. e is also a subgroups of G. These two are subgroups of any group. They are called trivial or improper subgroups. A subgroup other than these two is called a proper subgroup.

Note: (i) The identity of a subgroup is the same as that of the group.

(ii) The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group

§ Some examples of subgroups

(i) The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$

(ii) The additive group of even integers is a subgroup of the additive group of all integers.

Theorem: A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a \in H, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in G.

Proof: The condition is necessary: Suppose H is a subgroup of G. Then H must be closed with respect to multiplication i.e. the composition in G. Therefore $a \in H, b \in H \Rightarrow ab \in H$.

Let $a \in H$ and let a^{-1} be the inverse of a in G. Then the inverse of a in H is also a^{-1}.

Since H itself is a group, therefore each element of H must possess inverse. Therefore

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

The conditions are sufficient

Since $a \in H, b \in H \Rightarrow ab \in H$. Therefore H is closed with respect to multiplication.

Associativity: The elements of H are also the elements of G. The composition of G is associative. Therefore the same composition must also be associative in H.

Existence of Identity. The identity of the subgroup is the same as the identity of the group.

Now $a \in H \Rightarrow a^{-1} \in H$ (from the given condition (ii))

Further $a \in H, a^{-1} \in H \Rightarrow a a^{-1} \in H$ [from the given condition (i)]

$\therefore$ the identity e is an element of H.

Existence of Inverse: since $a \in H \Rightarrow a^{-1} \in H$, therefore each element of H possesses inverse. Hence H itself is a group for the composition in G. So H is a subgroup of G.

5. Order of an element of a group. Definition

Suppose G is a group and the composition has been denoted multiplicatively. By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that

$$a^n = e \quad \text{(the identity of G)}$$

If there exists no positive integer n such that $a^n = e$, then we say that a is of infinite order or of zero order.

We shall use the symbol $O(a)$ to denote the order of a.

In any group the identity element e is always of order one and it is the only element of order one.

Theorem: If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof: Let H_1 and H_2 be any two subgroups of G. Then $H_1 \cap H_2 \neq \phi$, since at least the identity element e is common to both H_1 and H_2.

In order to prove that $H_1 \cap H_2$ is a subgroup it is sufficient to prove that

$a \in H_1 \cap H_2,\ b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

Both H_1 and H_2 are subgroups, therefore

$a \in H_1,\ b \in H_1 \Rightarrow ab^{-1} \in H_1 \cap H_2$

$a \in H_2,\ b \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Finally, $ab^{-1} \in H_1,\ ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Thus we have shown that $a \in H_1 \cap H_2,\ b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is a subgroup of G.

Note: The union of two subgroups is not necessarily a subgroup.

For example, let G be the additive group of integers. [i.e $G = \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$]

Then $H_1 = 2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$H_2 = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

are both subgroups of G.

we have $H_1 \cup H_2 = \{\ldots, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$

Obviously $H_1 \cup H_2$ is not closed with respect to addition as $2 \in H_1 \cup H_2,\ 3 \in H_1 \cup H_2$ but $2+3$ i.e. $5 \notin H_1 \cup H_2$ because neither 5 is neither in H_1 nor in H_2. Therefore $H_1 \cup H_2$ is not a subgroup of G.

However, $H_1 \cap H_2 = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}$ is a subgroup of G.

If we take $H_3 = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = 4\mathbb{Z}$ of G, then $H_1 \cup H_3 = H_1$ and H_1 is a subgroup of G. Therefore union of two subgroups is a subgroup iff one is contained in the other.

Theorem: (An important characteristic property of a subgroup)

A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that

$a \in H, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.

Proof: The condition is necessary: Suppose H is a subgroup of G. Let $a \in H$, $b \in H$.

Now each element of H must possesses inverse because H itself is a group.

$\therefore b \in H \Rightarrow b^{-1} \in H$

Further H must be closed with respect to multiplication ie. the composition in G.

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

The condition is sufficient: Now it is given that

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

we are to prove that H is a subgroup of G.

~~(i) Closure Property:~~

(i) Existence of Identity: we have

$a \in H, a \in H \Rightarrow aa^{-1} \in H$ (by given condition)

$\Rightarrow e \in H$

Thus the identity e is an element of H.

(ii) Existence of inverse: Let a be any element of H. Then by the given condition we have

$e \in H, a \in H \Rightarrow ea^{-1} \in H$

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

Thus each element of H possesses inverse.

(iii) Closure Property: Let $a, b \in H$. Then as shown above $b \in H \Rightarrow b^{-1} \in H$.

Therefore applying the given condition, we have

$a \in H, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$

$\therefore$ H is closed with respect to the composition in G.

(iv) Associativity: The elements of H are also the elements of G. The composition in G is associative. Therefore it must also be associative in H.

Hence H itself is a group for the composition in G. Therefore H is a subgroup of G.

Q: Show that if a, b are any two elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Sol Suppose G is abelian

Then $(ab)^2 = (ab)(ab)$

$= a(ba)b$

$= a(ab)b$ [$\because G$ is abelian $\Rightarrow ab = ba$]

$= (aa)(bb)$

$(ab)^2 = a^2b^2$

Conversely, let a, b be any two elements of G.

Then $(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ [by left cancellation law]

$\Rightarrow (ba)b = (ab)b$ [by Right cancellation law]

$\Rightarrow ba = ab$

$\Rightarrow G$ is abelian.

Q: Find the order of every element in the multiplicative group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Sol The given cyclic group is of order 6 and a is a generator of G.

We have $O(a) = O(G) = 6$

Now we know that if $O(a) = n$ and p is prime to n, then $O(a^p) = n = O(a)$

Since 5 and 6 are relatively prime, therefore $O(a^5) = O(a) = 6$

The element $a^6 = e$ is the identity of the group G and so $O(a^6) = 1$

Now it remains to find the orders of a^2, a^3 and a^4.

We have $(a^2)^1 = a^2$, $(a^2)^2 = a^4 \neq e$, $(a^2)^3 = a^6 = e \Rightarrow O(a^2) = 3$

$(a^3)^1 = a^3$, $(a^3)^2 = a^6 = e \Rightarrow O(a^3) = 2$

$(a^4)^1 = a^4$, $(a^4)^2 = a^8 = a^6 \cdot a^2 = a^2 \neq e$, $(a^4)^3 = a^{12} = (a^6)^2 = e^2 = e \Rightarrow O(a^4) = 3$

Thus $O(a) = 6$, $O(a^2) = 3$, $O(a^3) = 2$, $O(a^4) = 3$, $O(a^5) = 6$, $O(a^6) = 1$

§. Cyclic groups. Definition:

A group G is called cyclic if, for some $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. The element a is then called a generator of G.

There may be more than one generators of a cyclic group. If G is a cyclic group generated by a, then we shall write $G = \{a\}$ or $G = (a)$. The elements of G will be of the form

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots\ldots$$

of course they are not necessarily all distinct.

Example 1. The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic. We can write $G = \{i, i^2, i^3, i^4\}$. Thus G is a cyclic group and i is a generator. Also we can write $G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$

Thus $-i$ is also a generator of G.

Example 2. The multiplicative group $\{1, \omega, \omega^2\}$ is cyclic. The generators are ω and ω^2.

§. Some properties of cyclic groups.

Theorem 1. Every cyclic group is an abelian group.

Proof: Let $G = \{a\}$ be a cyclic group generated by a. Let x, y be any two elements of G. Then there exists integers r and s such that $x = a^r$, $y = a^s$.

Now $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = yx$

Thus we have $xy = yx \ \forall\, x, y \in G$. Therefore G is abelian.

Theorem 2. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof: Let $G = \{a\}$ be a cyclic group generated by a. Let a^r be any element of G, where r is some integer. We can write $a^r = (a^{-1})^{-r}$. Since $-r$ is also an integer, therefore each element of G is generated by a^{-1}. Thus a^{-1} is also a generator of G.

Q: Show that the group $(\{1,2,3,4,5,6\}, \times_7)$ is cyclic. How many generators it has?

Sol Let us denote the given group by G

$\therefore \quad G = (\{1,2,3,4,5,6\}, \times_7)$

To prove G is cyclic: We know that a group G is said to be cyclic if there exists an element $a \in G$ such that $O(a) = 6$ i.e. equal to the order of the group G and a will be a generator of G.

We see that $O(3) = 6$ because $3^1 = 3$, $3^2 = 3 \times_7 3 = 2$, $3^3 = (3 \times_7 3) \times_7 3 = 6$, $3^4 = 6 \times_7 3 = 4$

$3^5 = 4 \times_7 3 = 5$, $3^6 = 5 \times_7 3 = 1$ i.e. the identity element

So, G is cyclic and 3 is a generator of G. We can write

$$G = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$$

Now 5 is prime to 6, therefore 5 is also a generator of G.

No. of generators $= \phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3)$ $\quad [\phi(p) = p-1,\ p \text{ is prime}]$

$= (2-1)(3-1)$

$= 2$

Q: How many generators are there of the cyclic group G of order 8?

Sol Let a be a generator of G. Then $O(a) = 8$, we can write $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

We know that if a cyclic group G is generated by an element a of order n, then a^m is a generator of G if and only if the greatest common divisor of m and n is 1 i.e. if and only if m and n are relatively prime.

Since 7 is prime to 8, therefore a^7 is also a generator of G.

5 is prime to 8, therefore a^5 is also a generator of G.

3 is prime to 8, therefore a^3 is also a generator of G.

Since 2 and 8, 4 and 8, 6 and 8, 8 and 8 are not relatively prime, therefore none of the elements a^2, a^4, a^6 and $a^8 = e$ can be a generator of G.

Thus there are only four generators of G i.e. a, a^3, a^5, a^7

Direct Method- No. of generators of group $G = \phi(8) = \phi(2^3)$ $\quad [\phi(p^n) = p^n - p^{n-1}$ if p is prime$]$

$= 2^3 - 2^{3-1}$

$= 8 - 4 = 4$

§. Cosets. Definition:

Suppose G is a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G generated by a. Similarly, the set $aH = \{ah : h \in H\}$ is called left coset of H in G generated by a.

Obviously Ha and aH are both subsets of G.

If e is the identity element of G, then $He = H = eH$. Therefore H itself is a right as well a left coset.

Note: If the composition in the group G has been denoted additively then the right coset of H in G generated by a is defined as

$$H + a = \{h + a : h \in H\}$$

Similarly the left coset $a + H = \{a + h : h \in H\}$

Example: Let G be the additive group of integers i.e.

$$G = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\cdots\}$$

Let H be the subgroup of G obtained on multiplying each element of G by 3.

Then $H = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\cdots\}$

Since the group G is abelian, any right coset will be equal to the corresponding left coset. Let us form the right cosets of H in G.

we have $0 \in G$ and $H + 0 = H = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\cdots\}$

Again $1 \in G$ and $H + 1 = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\cdots\}$

Then $2 \in G$ and $H + 2 = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\cdots\}$

we see that the right cosets H, $H+1$ and $H+2$ are all distinct and moreover these are disjoint ie. have no element common.

Now $3 \in G$ and $H + 3 = \{\cdots, -6, -3, 0, 3, 6, 9, 12, \cdots\cdots\}$

we see that $H + 3 = H$. Also we observe that $3 \in H$.

Again $4 \in G$ and $H + 4 = \{\cdots, -5, -2, 1, 4, 7, 10, 13, \cdots\}$

we see that $H+4 = H+1$. Also we observe that $4 \in H+1$.

Similarly the right coset $H+5$ coincides with $H+2$, $H+6$ with H, $H+(-1)$ with $H+2$, $H+(-2)$ with $H+1$ and so on.

Thus we get only three distinct right cosets ie. H, $H+1$, $H+2$.

Obviously $G = H \cup (H+1) \cup (H+2)$.

Lagrange's theorem

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

Proof: Let G be a group of a finite order n. Let H be a subgroup of G and let $o(H) = m$.

Suppose $h_1, h_2, h_3, \ldots, h_m$ are the m members of H.

Let $a \in G$. Then Ha is a right coset of H in G and we have

$$Ha = \{h_1 a, h_2 a, \ldots, h_m a\}$$

Ha has m distinct elements (members), since $h_i a = h_j a \Rightarrow h_i = h_j$

Therefore each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are distinct ie. they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say equal to k. The union of these k distinct right cosets of H in G is equal to G. Thus

if $Ha_1, Ha_2, \ldots, Ha_k$

are the k distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$$

$\Rightarrow$ the number of elements in G = the number of elements in Ha_1 + the number of elements in Ha_2 + $\ldots$ + the number of elements in Ha_k

[$\because$ two distinct right cosets are mutually distinct]

$\Rightarrow o(G) = km \Rightarrow n = km$

$\Rightarrow k = \frac{n}{m} \Rightarrow m$ is a divisor of n.

$\Rightarrow o(H)$ is a divisor of $o(G)$

Hence the theorem.

9. Normal Subgroup. Definition

A subgroup H of a group G is said to be a normal subgroup of G if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$.

From this definition we can immediately conclude that H is a normal subgroup of G if and only if $xHx^{-1} \subseteq H \ \forall x \in G$.

Theorem: 1 A subgroup H of a group G is normal if and only if $xHx^{-1} = H \ \forall x \in G$.

Proof. Let $xHx^{-1} = H \ \forall x \in G$. Then $xHx^{-1} \subseteq H \ \forall x \in G$.

Therefore H is a normal subgroup of G.

Converse: Let H be a normal subgroup of G.

Then $xHx^{-1} \subseteq H \ \forall x \in G$ ---- (1)

Also $x \in G \Rightarrow x^{-1} \in G$. Therefore we have

$x^{-1}H(x^{-1})^{-1} \subseteq H \ \forall x \in G$

$\Rightarrow x^{-1}Hx \subseteq H \ \forall x \in G$

$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \ \forall x \in G$

$\Rightarrow H \subseteq xHx^{-1} \ \forall x \in G$ ---(2)

From (1) & (2), we conclude that $xHx^{-1} = H$ for all $x \in G$.

Theorem 2 The intersection of any two normal subgroups of a group is a normal subgroup.

Proof. Let H and K be two normal subgroups of a group G. Since H and K are subgroups of G, therefore $H \cap K$ is also a subgroup of G. Now to prove that $H \cap K$ is a normal subgroup of G. Let x be any element of G and n be any element of $H \cap K$. We have

$n \in H \cap K \Rightarrow n \in H, \ n \in K$

Since H is a normal subgroup of G, therefore $x \in G, n \in H \Rightarrow xnx^{-1} \in H$.

Similarly $xnx^{-1} \in K$.

Now, $xnx^{-1} \in H, xnx^{-1} \in K \Rightarrow xnx^{-1} \in H \cap K$.

Thus we have $x \in G, n \in H \cap K \Rightarrow xnx^{-1} \in H \cap K$.

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

§. Permutations:

Definition: Suppose S is a finite set having n distinct elements. Then a one-one mapping of S onto itself is called a permutation of degree n.

The number of elements in the finite set S is known as the degree of permutation

§. Symbol for a permutation: Let $S = \{a_1, a_2, a_3, \ldots, a_n\}$ be a finite set having n distinct elements. If $f: S \longrightarrow S$ and f is one-one onto, then f is a permutation of degree n.

Let $f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$, $\ldots$, $f(a_n) = b_n$ where $\{b_1, b_2, \ldots, b_n\} = \{a_1, a_2, \ldots, a_n\}$

ie $b_1, b_2, \ldots, b_n$ is nothing but some arrangement of the n elements of S.

we find it convenient to introduce a two line notation to write this permutation.

In this notation we write

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix} \text{ ie.}$$

each element in the second row is the f-image of the element of the first row lying directly above it.

§ Equality of two permutations: Two permutations f and g of degree n are said to be equal if we have $f(a) = g(a)$ $\forall a \in S$

e.g. if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

are two permutations of degree 4, then we have $f = g$.

§. Total number of distinct permutations of degree n. If S is a finite set having n distinct elements, then we shall have $n!$ distinct arrangements of the elements of S. Therefore there will be $n!$ distinct permutations of degree n.

If S_n be the set consisting of all permutations of degree n, then the set S_n will have $n!$ distinct elements. This set S_n is called the symmetric set of permutations of degree n.

Thus, $S_n = \{f : f \text{ is a permutation of degree } n\}$.

The set S_3 of all permutations of degree 3 will have 3! i.e. 6 elements. Obviously,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

or, $S_3 = \{ I, (12), (13), (23), (123), (132) \}$

∫. Symmetric Group: The set S_n of all permutations on n symbols is a finite group of order $n!$ with respect to composite of mappings as the operation. For $n \leq 2$, this group is abelian and for $n > 2$ it is always non-abelian.

This group is called the symmetric group of degree n or the symmetric group of order $n!$.

§ Group Homomorphism:

Homomorphic mapping: (Definition)

Suppose G and G' are two groups, the composition in each being denoted multiplicatively. A mapping f of G into G' is said to be a homomorphic mapping or (a homomorphism) of G into G' if

$$f(ab) = f(a)\,f(b) \quad \forall\, a, b \in G$$

Note: If f is a homomorphic mapping of a group G onto the group G' so that $f(G) = G'$, then the group G' is called a homomorphic image of the group G.

Theorem: Let f be a homomorphic mapping of a group G into a group G'. Then we have the following important properties:

(i) The f-image of the identity e of G is the identity of G' ie. f(e) is the identity of G'

Proof: Let e be the identity of G and e' be the identity of G'.

Let a be any element of G. Then $f(a) \in G'$.

Now, $e' f(a) = f(a)$ [$\because$ e' is the identity of G']

$= f(ea)$ [$\because$ e is the identity of G]

$= f(e)\,f(a)$ [$\because$ f is a homomorphism]

Now in the group G', we have

$e' f(a) = f(e)\,f(a)$

$\Rightarrow e' = f(e)$ [by right cancellation law in G']

$\therefore f(e)$ is the identity of G'.

(ii) The f-image of the inverse of an element a of G is the inverse of the f-image of a ie. $f(a^{-1}) = [f(a)]^{-1}$

Proof: Suppose e is the identity of G and e' is the identity of G'. Then

$f(e) = e'$.

Now let a be any element of G. Then $a^{-1} \in G$. and $aa^{-1} = e$. we have

$$e' = f(e)$$
$$= f(aa^{-1})$$
$$= f(a)\, f(a^{-1}) \quad [\because f \text{ is composition preserving}]$$

Therefore $f(a^{-1})$ is the inverse of $f(a)$ in the group G'. Thus

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

§. Ring: Suppose R is a non-empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '·' respectively ie. for all $a, b \in R$ we have $a+b \in R$ and $a \cdot b \in R$. Then this algebraic structure $(R, +, \cdot)$ is called a ring if the following postulates are satisfied:

A1. Addition is associative ie $(a+b)+c = a+(b+c)$ $\forall\ a, b, c \in R$

A2. Addition is commutative ie. $a+b = b+a$, $\forall\ a, b \in R$

A3. There exists an element denoted by '0' in R such that $0+a = a$ $\forall\ a \in R$

A4. To each element a in R, there exists an element $-a$ in R such that $(-a)+(a) = 0$

M5. Multiplication is associative, ie. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall\ a, b, c \in R$

M6. Multiplication is distributive with respect to addition ie. for all a, b, c in R,

$a \cdot (b+c) = (a \cdot b) + (a \cdot c) = a \cdot b + a \cdot c$ } Left distributive law

and $(b+c) \cdot a = b \cdot a + c \cdot a$ } Right distributive law

Since addition is commutative in R, therefore we shall have $0 \in R$ such that $0+a = a+0$ $\forall\ a \in R$.

Also if $a \in R$, then we shall have $(-a)+a = 0 = a+(-a)$

Thus R will be an abelian group with respect to addition. The element $0 \in R$ will be the additive identity. It is called zero element of the ring.

Since in a group the identity element is unique, therefore every ring will possesses a unique zero element and it will be the identity element for addition composition. We shall always denote this element by the symbol 0.

→ In a ring every element will possess a unique inverse for addition composition. We shall denote the additive inverse of a by the symbol $-a$.

We shall defined $a-b = a+(-b)$

→ Both cancellation laws will hold good for addition in R ie for all a,b,c in R

$a+b = a+c \Rightarrow b=c$ and $b+a = c+a \Rightarrow b=c$

→ If in a ring we have $a+b=0$, then $a=-b$ and $b=-a$

§. Ring with unity: If in a ring R there exists an element denoted by 1 such that $1\cdot a = a = a\cdot 1$ $\forall a \in R$, then R is called a ring with element. The element $1 \in R$ is called the unit element of the ring. Obviously 1 is the multiplicative identity of R. Thus if a ring possesses multiplicative identity, then it is a ring with unity.

§. Commutative ring: If in a ring R, the multiplication composition is also commutative ie. if we have $a\cdot b = b\cdot a$ $\forall a,b \in R$, then R is called a commutative ring.

§. Elementary Properties of a ring:

If R is a ring, then for all $a, b \in R$

(i) $a0 = 0a = 0$

(ii) $a(-b) = -(ab) = (-a)b$

(iii) $(-a)(-b) = ab$

(iv) $a(b-c) = ab-ac$

(v) $(b-c)a = ba-ca$

Proof: (i) we have $a0 = a(0+0)$ [$\because 0+0=0$]

$= a0+a0$ [by left distributive law]

$\therefore 0+a0 = a0+a0$ [$\because a0 \in R$ and $0+a0=a0$]

Now R is a group with respect to addition, therefore by applying right cancellation law in R, we have

$0 = a0$ #

Similarly, we have $0a = (0+0)a$

$= 0a + 0a$ (by Right distributive law)

$\therefore 0 + 0a = 0a + 0a$ $(\because 0 + 0a = 0a)$

$\Rightarrow 0 = 0a$

(ii) we have $a[(-b)+b] = a0$ $[\because -b+b=0]$

$\Rightarrow a(-b) + ab = 0$ [by using left distributive law and the result (i)]

$\Rightarrow a(-b) = -ab$, [since in a ring R, $a+b=0 \Rightarrow a=-b$]

Similarly, we have $(-a+a)b = 0b \Rightarrow (-a)b + ab = 0 \Rightarrow (-a)b = -(ab)$

(iii) we have $(-a)(-b) = -[(-a)b]$, since $a(-b) = -ab = -[-(ab)]$ since $(-a)b = -(ab)$

$= ab$, [since R is a group with respect to addition and in a group we have $-(-a) = a$]

(iv) we have $a(b-c) = a[b+(-c)] = ab + a(-c)$ [by Left distributive law]

$= ab + [-ac]$ $[\because a(-c) = -(ac)]$

$= ab - ac$

(v) we have $(b-c)a = [b+(-c)a] = ba + (-c)a$ (by Right distributive law)

$= ba + [-(ca)]$

$= ba - ca$

§ Examples of ring:

(i) The set I of all integers is a ring with respect to addition and multiplication of integers as two ring operations. The ring is called the ring of integers.

(ii) The set Q of all rational numbers is a commutative ring with unity, the addition and multiplication of rational numbers being the two ring compositions.

§. Field Definition: A ring R with at least two elements is called a field if it (i) is commutative (ii) has unity (iii) is such that each non-zero element possesses multiplicative inverse.

Examples (i) The ring of rational numbers $(Q, +, \cdot)$ is a field since it is a commutative ring with unity and each non-zero element is invertible.

(ii) The rings of real numbers and complex numbers are also examples of fields.