GROUP THEORY

DR. PRATIKSHAN MONDAL

Department of Mathematics, Durgapur Government College, Durgapur, India
E-mail: real.analysis77@gmail.com

Semester-III, CC-6 (BSCHMTMC302), Unit-1,2,3

Binary Composition: A binary operation or law of composition on a set G is a function $\circ : G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$ in G, called the composition of a and b.

Group: A group $(G, \circ)$ is a set G together with a law of composition $(a, b) \to a \circ b$ that satisfies the following axioms:

(1) For any $a, b \in G$, the composition $a \circ b \in G$ (Closure Property).

(2) The law of composition is associative. That is,

$$(a \circ b) \circ c = a \circ (b \circ c)$$

for all $a, b, c \in G$ (Associative Property).

(3) There exists an element $e \in G$, called the identity element, such that for any element $a \in G$

$$a \circ e = e \circ a = a$$

holds (Existence of Identity).

(4) For each element $a \in G$, there exists an inverse element in G, denoted by a^{-1} , such that

$$a \circ a^{-1} = a^{-1} \circ a = e$$

holds (Existence of inverse element).

A group $(G, \circ)$ is said to be an abelian group or a commutative group if for any two elements $a, b \in G$, $a \circ b = b \circ a$ holds.

Example 1. *The integers $\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots\}$ form a group under the operation of addition. The binary operation on two integers $m, n \in \mathbb{Z}$ is just their sum. Since the integers under addition already have a well established notation, we will use the operator $+$ instead of $\circ$; that is, we shall write $m+n$ instead of $m \circ n$. The identity is 0, and the inverse of $n \in \mathbb{Z}$ is written as $-n$ instead of n^{-1}. Notice that the set of integers under addition have the additional property that $m + n = n + m$ and therefore form an abelian group.*

Remark. *Most of the time we will write ab instead of $a \circ b$; however, if the group already has a natural operation such as addition in the integers, we will use that operation. That is, if we are adding two integers, we still write $m + n$, $-n$ for the inverse, and 0 for the identity as usual. We also write $m - n$ instead of $m + (-n)$. It is often convenient to describe a group in terms of an addition or multiplication table. Such a table is called a* **Cayley table***.*

Example 2. *The integers mod n form a group under addition modulo n. Consider $\mathbb{Z}_5$, consisting of the equivalence classes of the integers $[0], [1], [2], [3]$, and $[4]$. We define the group operation on $\mathbb{Z}_5$ by modular addition. We write the binary operation on the group additively; that is, we write $[m] + [n]$. The element $[0]$ is the identity of the group and each element in $\mathbb{Z}_5$ has an inverse. For instance, $[2] + [3] = [3] + [2] = [0]$. Figure given below is a Cayley* *table for $\mathbb{Z}_5$. It can also be shown that $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$ is a group under the binary operation of addition mod n.*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

Example 3. *Not every set with a binary operation is a group. For example, if we let modular multiplication be the binary operation on $\mathbb{Z}_n$, then $\mathbb{Z}_n$ fails to be a group. The element $[1]$ acts as a group identity since $[1] \cdot [k] = [k] \cdot [1] = [k]$ for any $[k] \in \mathbb{Z}_n$; however, a multiplicative inverse for $[0]$ does not exist since $[0] \cdot [k] = [k] \cdot [0] = [0]$ for every $[k] \in \mathbb{Z}_n$. Even if we consider the set $\mathbb{Z}_n \setminus \{[0]\}$, we still may not have a group. For instance, let $[2] \in \mathbb{Z}_6$. Then $[2]$ has no multiplicative inverse since*

$$\begin{array}{ll} [0] \cdot [2] = [0] & [1] \cdot [2] = [2] \\ [2] \cdot [2] = [4] & [3] \cdot [2] = [0] \\ [4] \cdot [2] = [2] & [5] \cdot [2] = [4] \end{array}$$

Example 4. *We use $M_2(\mathbb{R})$ to denote the set of all 2×2 matrices. Let $GL_2(\mathbb{R})$ be the subset of $M_2(\mathbb{R})$ consisting of invertible matrices; that is, a matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $GL_2(\mathbb{R})$ if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$, where I is the 2×2 identity matrix. For A to have an inverse is equivalent to requiring that the determinant of A be non-zero; that is, $\det(A) = ad - bc \neq 0$. The set of invertible matrices forms a group called the* **general linear group**.

The identity of the group is the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

The inverse of $A \in GL_2(\mathbb{R})$ is

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

The product of two invertible matrices is again invertible. Matrix multiplication is associative, satisfying the other group axiom. For matrices it is not true in general that $AB = BA$; hence, $GL_2(\mathbb{R})$ is another example of a nonabelian group.

Example 5. *Let $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ and $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ where $i^2 = -1$. Then the relations $I^2 = J^2 = K^2 = -1$, $IJ = K, JK = I, KI = J, JI = -K, KJ = -I$, and $IK = -J$ hold. The set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is a group called the* **quaternion group**. *Notice that Q_8 is non-commutative.*

Example 6. *Let $\mathbb{C}^*$ be the set of all non-zero complex numbers. Under the operation of multiplication $\mathbb{C}^*$ forms a group. The identity is 1. If $z = a + bi$ is a non-zero complex* *number, then*

$$z^{-1} = \frac{a-bi}{a^2+b^2}$$

is the inverse of z. It is easy to see that the remaining group axioms hold.

A group has finite order, if it contains a finite number of elements; otherwise, the group is said to be of infinite order. The order of a finite group is the number of elements that it contains. If G is a group containing n elements, we write $|G| = n$ or $o(G) = n$. The group $\mathbb{Z}_5$ is a finite group of order 5; the integers $\mathbb{Z}$ form an infinite group under addition, and we sometimes write $|\mathbb{Z}| = \infty$.

Example 7. *Let $S = \{e, a, b, c\}$ and let $*$ be the binary composition defined on S by $e * a = a * e = a, e * b = b * e = b, e * c = c * e = c, e * e = a * a = b * b = c * c = e, a * b = b * a = c, c * a = a * c = b, b * c = c * b = a$. Then $(S, *)$ is an abelian group. This group is known as Klein's 4-group and is denoted by V_4. It is to be noted that each element of V_4 is self inverse.*

Example 8. *For $a, b \in \mathbb{Z}$, let $a \circ b = a + b + 1$. Prove that $(\mathbb{Z}, \circ)$ is an abelian group.*

Closure property: Let $a, b \in \mathbb{Z}$. Then $a + b + 1 \in \mathbb{Z}$ i.e., $a \circ b \in \mathbb{Z}$. That $\circ$ is closed in $\mathbb{Z}$.

Associative property: Let $a, b, c \in \mathbb{Z}$.

$$a \circ (b \circ c) = a \circ (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$$

$$(a \circ b) \circ c = (a + b + 1) \circ c = (a + b + 1) + c + 1 = a + b + c + 2$$

Existence of identity: let $e \in \mathbb{Z}$ be such that $a \circ e = e \circ a = a$.

Now

$$a \circ e = a \Longrightarrow a + e + 1 = a \Longrightarrow e = -1$$

$$e \circ a = e + a + 1 = -1 + a + 1 = a$$

Therefore e is the identity element of $\mathbb{Z}$.

Existence of inverse: Let $a \in \mathbb{Z}$. Suppose that there is $b \in \mathbb{Z}$ such that $a \circ b = b \circ a = e$.

Now,

$$a \circ b = e \Longrightarrow a + b + 1 = -1 \Longrightarrow b = -2 - a$$

$$b \circ a = b + a + 1 = -2 - a + a + 1 = -1 = e$$

Hence $b = -2 - a$ is the inverse of a.

Commutative property: Let $a, b \in \mathbb{Z}$. Then

$$a \circ b = a + b + 1 = b + a + 1 = b \circ a$$

Hence $(\mathbb{Z}, \circ)$ is an abelian group.

Example 9. *Let X be a no-empty set and let $P(X)$ denote the set of subsets of X. Examine if $P(X)$ is a group under the composition defined by*

(i) $A * B = A \cap B,\ A, B \in P(X)$.

(ii) $A \circ B = A \cup B,\ A, B \in P(X)$.

(iii) $A \bullet B = A \Delta B = (A - B) \cup (B - A),\ A, B \in P(X)$.

Solution: *(i) It is easy to verify that closure, associative property is satisfied in $P(X)$ under $*$. It is also easy to verify that X is the identity element of $P(X)$ with respect to $*$. However, it is clear that for $\phi \in P(X)$, there is no element A in $P(X)$ such that $\phi * A = X$, the identity element. Hence ϕ does not have any inverse with respect to $*$ and so $(P(X), *)$ is not a group.*

(ii) It is easy to verify that closure, associative property is satisfied in $P(X)$ under $\circ$. It is also easy to verify that ϕ is the identity element of $P(X)$ with respect to $\circ$. However, it is

clear that for $X \in P(X)$, there is no element A in $P(X)$ such that $X \circ A = \phi$, the identity element. Hence X does not have any inverse with respect to $\circ$ and so $(P(X), \circ)$ is not a group.

(iii) It easy to verify that closure and associative properties hold good in $P(X)$ under $\bullet$. Note that ϕ is the identity element in $P(X)$ with respect to $\bullet$. Also for any $A \in P(X)$, it is clear that $A \bullet A = \phi$ and hence A is the inverse of itself. Also for any two elements $A, B \in P(X)$, we have $A \bullet B = B \bullet A$. Hence $(P(X), \bullet)$ is a commutative group.

Example 10. *Prove that the set $H = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}$ forms a group with respect to matrix multiplication.*

Solution. *It is obvious that $H \neq \phi$, as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$.*

Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be two elements in H. Then

$$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix}.$$

Note that

$$(ac - bd)^2 + (ad + bc)^2 = (a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2) = (a^2 + b^2)(c^2 + d^2) = 1.$$

Therefore $AB \in H$ and closure property is verified. It is not very difficult to verify associative property. Note that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element in H. Now let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in H$. Then the inverse of A is given by $A^{-1} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

It is also easy to verify that $AB = BA$ for all $A, B \in H$.

Example 11. *Let $S = \{1, 2, 3\}$ be a set of order 3. A permutation on S is a bijective mapping on S i.e., a bijective mapping from $f : S \to S$. Let G be the set of all permutations on S. Then*

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2),$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3), f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3), f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$$

defines the set of all permutations on S. Then $G = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ forms a group under the composition "composition of mappings". It can be shown easily that G is not abelian (verify!). The group G is known as **symmetric group of degree** 3 *and is denoted by* $\mathbf{S_3}$*. Note that order of the group S_3 is* 6.

As you know that $(1\ 2\ 3)$ is called a 3-cycle. A 2-cycle is called a transposition. Every permutation can be written as a composition of transpositions. For example, $(1\ 2\ 3) = (1\ 3) \circ (1\ 2)$.

A permutation is called **even** *if it can be written as a composition of even number of transpositions otherwise it is called an odd permutation. Therefore $(1\ 3\ 2)$ is an even permutation. The identity permutation is an even permutation. It is to be noted that S_3 contains* 3 *even permutation and* 3 *odd permutations. The set A_3 of all even permutations, i.e., $A_3 = \{f_0, f_1, f_2\}$, forms a group with respect to the same composition which is defined in S_3. The group A_3 is called* **alternating group**. *Note that $o(A_3) = 3 = \frac{o(S_3)}{2}$. It is also to be noted that A_3 is an abelian group.*

In a similar way, it can be shown that S_n, the set of all permutations on a set of n symbols $\{1, 2, \cdots, n\}$, forms a group under the composition "composition of mappings" and the set A_n of all even permutations forms a group under the same composition. It is also to be noted that $o(S_n) = n!$ and $o(A_n) = \frac{n!}{2}$.

Basic Properties of Groups:

Theorem 12. *The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.*

Proof. Suppose that e and e' are both identities in G. Then $eg = ge = g$ and $e'g = ge' = g$ for all $g \in G$. We need to show that $e = e'$. If we think of e as the identity and e' an element of G, then $ee' = e'$; but if we consider e' is an identity and e an element of G, then $ee' = e$. Combining these two equations, we have $e = ee' = e'$. □

Theorem 13. *If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.*

Proof. Inverses in a group are also unique. If g' and g'' are both inverses of an element g in a group G, then $gg' = g'g = e$ and $gg'' = g''g = e$. We want to show that $g' = g''$, but

$$g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''.$$

□

Theorem 14. *Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Let $a, b \in G$. Then

$$abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e.$$

Similarly,

$$b^{-1}a^{-1}ab = e.$$

But by the previous theorem, inverses are unique; hence, $(ab)^{-1} = b^{-1}a^{-1}$. □

Theorem 15. *Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.*

Proof. Observe that $a^{-1}(a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a, we have

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$

□

It makes sense to write equations with group elements and group operations. If a and b are two elements in a group G, does there exist an element $x \in G$ such that $ax = b$? If such an x does exist, is it unique? The following proposition answers both of these questions positively.

Theorem 16. *If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.*

This theorem tells us that the right and left cancellation laws are true in groups. We leave the proof as an exercise.

Theorem 17. *Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.*

Proof. Suppose that $ax = b$. We must show that such an x exists. We can multiply both sides of $ax = b$ by a^{-1} to find $x = ex = a^{-1}ax = a^{-1}b$.

To show uniqueness, suppose that x_1 and x_2 are both solutions of $ax = b$; then $ax_1 = b = ax_2$. So $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$. The proof for the existence and uniqueness of the solution of $xa = b$ is similar. □

We can use exponential notation for groups just as we do in ordinary algebra. If G is a group and $g \in G$, then we define $g^0 = e$. For $n \in \mathbb{N}$, we define

$$g^n = g \cdot g \cdots g$$

and

$$g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1}.$$

Theorem 18. *In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,*

1. $g^m g^n = g^{m+n}$ *for all* $m, n \in \mathbb{Z}$*;*
2. $(g^m)^n = g^{mn}$ *for all* $m, n \in \mathbb{Z}$*;*
3. $(gh)^n = \left(h^{-1}g^{-1}\right)^{-n}$ *for all* $n \in \mathbb{Z}$*. Furthermore, if* G *is abelian, then* $(gh)^n = g^n h^n$*.*

We will leave the proof of this theorem as an exercise. Notice that $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian. If the group is $\mathbb{Z}$ or $\mathbb{Z}_n$, we write the group operation additively and the exponential operation multiplicatively; that is, we write ng instead of g^n. The laws of exponents now become

1. $mg + ng = (m + n)g$ for all $m, n \in \mathbb{Z}$;
2. $m(ng) = (mn)g$ for all $m, n \in \mathbb{Z}$;
3. $m(g + h) = mg + mh$ for all $m, n \in \mathbb{Z}$. It is important to realize that the last statement can be made only because $\mathbb{Z}$ and $\mathbb{Z}_n$ are commutative groups.

Problem 1. *For any two elements a, b in a group G and for any integer n, prove that $(aba^{-1})^n = ab^n a^{-1}$.*

Problem 2. *Let G be a group and $a \in G$. Define a mapping $f_a : G \to G$ by $f_a(x) = a \circ x$ for all $x \in G$. Prove that f_a is a bijection. Show that the set $S = \{f_a : a \in G\}$ is a group with respect to the binary composition $f_a * f_b = f_{a \circ b}$ for all $f_a, f_b \in S$.*

Problem 3. *If each element in a group be its own inverse, prove that the group is abelian.*

Solution. *Let G be a group. By hypothesis, $a = a^{-1}$ for all $a \in G$. Let $a, b \in G$. Then $ab \in G$ and therefore, $a = a^{-1}, b = b^{-1}$ and $ab = (ab)^{-1}$. Hence*

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

This is true for all $a, b \in G$ and hence G is abelian.

Problem 4. *If in a group G, $a^2 = e$ for all $a \in G$, then prove that G is abelian.*

Solution. *Let $a \in G$. So $a^{-1} \in G$. Then by hypothesis, $a^2 = e$ and so*

$$a^{-1}a^2 = a^{-1}e \text{ or, } a = a^{-1}.$$

This is true for all $a \in G$. Hence by the above result G is an abelian group.

Problem 5. *Prove that a group $(G, \circ)$ is abelian if and only if $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$ for all $a, b \in G$.*

Solution. *Let us first assume that G is abelian. Then*

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

for all $a, b \in G$.

Conversely, let $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$ for all $a, b \in G$. We claim that G is abelian.

Let $a, b \in G$. Then $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$. Taking inverse of both side, we get

$$\left((a \circ b)^{-1}\right)^{-1} = \left(a^{-1} \circ b^{-1}\right)^{-1}$$

$$or,\ ab = \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} = ba.$$

This is true for all $a, b \in G$. Hence G is abelian.

Definition 19. Order of an element: *Let G be a group and let $a \in G$. Then we say that a has order n or a is of order n if n is the smallest positive integer such that $a^n = e$, e being the identity element of G. We write $o(a) = n$ to denote that the order of the element is n.*

It is to be noted that $o(e) = 1$, e is the identity element of G.

It is very important to note that if $a^n = e$, then $o(a) \leq n$.

However if there is no such positive integer exists, then we say that the order of the element is infinite.

Example 20. *Let us consider the set S of all cube roots of unity i.e., $S = \{1, \omega, \omega^2\}$. Then it is an easy exercise to show that $(S, \cdot)$ is an abelian group. In this group, we have $o(\omega) = 3, o(\omega^2) = 3$.*

Example 21. *In Example 2 we have shown that $\mathbb{Z}_5$ is an abelian under the addition modulo 5, in notation $+_5$. In this group, $o(\bar{1}) = 5, o(\bar{2}) = 5, o(\bar{3} = 5, \bar{4} = 5$.*

If we consider the group $(\mathbb{Z}_6, +_6)$, then $o(\bar{1}) = 6, o(\bar{2}) = 3, o(\bar{3}) = 2, o(\bar{4}) = 3, o(\bar{5}) = 6$.

Example 22. *In Example 7, $o(a) = o(b) = o(c) = 2$.*

Example 23. *In Example 11, $o(f_1) = 3, o(f_2) = 3, o(f_3) = o(f_4) = o(f_5) = 2$.*

Example 24. *In Example 9 (iii), order of all non-zero element is 2.*

Example 25. *In Example 1, order of all non-identity element is infinite.*

Theorem 26. *Let G be a group and let $a \in G$. Then the following statements hold good:*

(i) *$o(a) = o(a^{-1})$.*

(ii) *if $o(a) = n$ and $a^m = e$, then n divides m.*

(iii) *if $o(a) = n$, then the elements $e, a, a^2, \cdots, a^{n-1}$ are all distinct.*

Proof. (i) **Case 1:** Let $o(a)$ be finite and let $o(a) = n$. Then n is the smallest positive integer such that $a^n = e$, where e is the identity element of G. Now,

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e$$

which implies that $o(a^{-1}) \leq n$. If possible suppose that $o(a^{-1}) = k < n$. Then $(a^{-1})^k = e$ which implies that $a^{-}k = e$. This implies that $a^k = e$ which is a contradiction to the hypothesis. hence we must have $o(a^{-1}) = n = o(a)$.

Case 2: Let $o(a)$ be infinite. We claim that $o(a^{-1})$ is also infinite. If possible suppose that $o(a^{-1}) = n$. Then as before, we get $a^n = e$ which contradicts our hypothesis. Hence our claim is established.

(ii) Let $o(a) = n$ and $a^m = e$. Then n is the smallest positive integer such that $a^n = e$, the identity element of G. Then we must have $n \leq m$ and so by division algorithm, there exists $q, r \in \mathbb{Z}$ such that

$$m = nq + r$$

with $0 \leq r < n$. We claim that $r = 0$. If not, then $0 < r < n$. Then

$$e = a^m = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$$

which is contradiction to the fact that $o(a) = n$. Hence we must have $r = 0$ which yield that $m = nq$. Hence n divides m.

(iii) Let $o(a) = n$. If possible, let the elements $e, a, a^2, \cdots, a^{n-1}$ are not all distinct. So we have $a^r = a^s$ for some r, s with $0 \leq r < s \leq n-1$. This implies that

$$a^{s-r} = e$$

and $0 < s - r < n$ which is a contradiction to the hypothesis. Hence the result follows. □

Example 27. *Let G be a group. Let $a \in G$ be such that $a^2 = e$. Then we have either (i) $a = e$ or (ii) $o(a) = 2$.*

Example 28. *Let G be a finite group. We claim that each element of G is of finite order.*

Let $a \in G$. Then the elements $e, a, a^2, a^3, \cdots$ are all in G, by closure property. Since G is a finite group, these elements cannot be distinct. So we must have $a^r = a^s$ for some integers r, s with $0 \leq r < s$ which implies that $a^{s-r} = e$ and $s - r$ is a positive integer. Hence $o(a) \leq s - r$, a finite number. This is true for all $a \in G$. Hence the result follows.

Note. *However the converse of Example 28 may not hold in general. In Example 9(iii), we have noted that each non-identity element is of order 2, but the group is of infinite order.*

Again in Example 1, we have already noted that each non-zero element is of infinite order. In this case the order of the group if also infinite.

Theorem 29. *Let G be a group and $a \in G$. If $o(a) = n$, then $o(a^k) = \frac{n}{gcd(k,n)}$.*

Proof. Let $o(a) = n$. Then n is the smallest positive integer such that $a^n = e$, e being the identity element of G. Now let $o(a^k) = m$. Then $a^{mk} = e$. From Theorem 26 (ii) it follows that n divides mk.

Let $gcd(k, n) = d$. Then we find two integers u, v with $gcd(u, v) = 1$ and $k = du$ and $n = dv$. Therefore

$$n|(mk) \implies (dv)|(mdu) \implies v|(mu) \implies v|m \text{ since } gcd(u, v) = 1.$$

We claim that $m|v$. Note that

$$(a^k)^v = a^{kv} = a^{duv} = a^{nu} = (a^n)^u = e$$

which implies that $m|v$ (applying again Theorem 26 (ii)). Hence we have $m = v = \frac{n}{d} = \frac{n}{gcd(k,n)}$. Hence the theorem follows. □

Example 30. *If b is an element of a group G and $o(b) = 20$, find the order of the element (i) b^6 (ii) b^8 (iii) b^{15}.*

(i) Here $o(b^6) = \frac{20}{gcd(6,20)} = 10$.

(ii), (iii) are left as an exercise.

Example 31. *Find the number of elements of order 10 in $(\mathbb{Z}_{30}, +)$.*

Note that $o(\bar{1}) = 30$ in $(\mathbb{Z}_{30}, +)$. Let $o(\bar{k}) = 10$. Then by the above theorem,

$$o(\bar{k}) = o(k\bar{1}) = \frac{30}{gcd(k, 30)}.$$

So by hypothesis,

$$\frac{30}{gcd(k, 30)} = 10 \implies gcd(k, 30) = 3 \implies gcd\left(\frac{k}{3}, 10\right) = 1 \implies \frac{k}{3} = 1, 3, 7, 9$$

which implies that

$$k = 3, 9, 21, 27.$$

Hence number of elements of order 10 *in* $(\mathbb{Z}_{30}, +)$ *is* 4 *and are given by* $\overline{3}, \overline{9}, \overline{21}, \overline{27}$.

Problem 6. *Find the number of elements of order* 5 *in the group (i)* $(\mathbb{Z}_{30}, +)$ *(ii)* $(\mathbb{Z}_{20}, +)$.

Example 32. *Let* G *be a group and let* $a, b \in G$*. If* $o(a) = 3$ *and if* $aba^{-1} = b^2$*, find* $o(b)$ *if* $b \neq e$*,*

Let $o(a) = 3$ *and let* $aba^{-1} = b^2$*. Then*

$$(aba^{-1})(aba^{-1}) = b^4 \implies ab^2a^{-1} = b^4 \implies a(aba^{-1})a^{-1} = b^4 \implies a^2ba^{-2} = b^4.$$

Now,

$$(a^2ba^{-2})(a^2ba^{-2}) = b^8 \implies a^2b^2a^{-2} = b^8 \implies a^2(aba^{-1})a^{-2} = b^8 \implies b = b^8$$

which implies that $b^7 = e$*. Hence* $o(b) = 7$*, since* $b \neq e$*.*

Definition 33. *Let* $(G, \circ)$ *be a group and* H *be a non-empty subset of* G*. If* H *itself form a group with respect to the same composition as defined in* G*, then* $(H, \circ)$ *is called a subgroup of the group* $(G, \circ)$*.*

Example 34. *Let* $(G, \circ)$ *be a group and let* e *be the identity element of* G*. As* G *is a subset of itself, it is a subgroup of* $(G, \circ)$*. This subgroup of* $(G, \circ)$ *is called the* **improper** *subgroup of* $(G, \circ)$*.*

Also the singleton set $\{e\}$ *is a subgroup of* $(G, \circ)$*. This subgroup* $(\{e\}, \circ)$ *is called the* **trivial** *subgroup of* $(G, \circ)$*. Any other subgroups of* $(G, \circ)$ *are called non-trivial proper subgroup of* $(G, \circ)$*.*

Example 35. *Note that* $(\mathbb{Q}, +)$ *is a group and* $\mathbb{Z}$ *is a non-empty subset of* $(\mathbb{Q}, +)$*. As* $(\mathbb{Z}, +)$ *itselt forms a group, so by definition* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$*.*

It is also to be noted that $(\mathbb{Q} \setminus \{0\}, \cdot)$ *is a group and* $\mathbb{Q} \setminus \{0\}$ *is a non-empty subset of* $\mathbb{Q}$*. But* $(\mathbb{Q} \setminus \{0\}, \cdot)$ *is not a subgroup of* $(\mathbb{Q}, +)$*.*

Theorem 36. *Let* $(H, \circ)$ *be a subgroup of* $(G, \circ)$*. Then*

(i) *the identity element of* $(H, \circ)$ *and* $(G, \circ)$ *are the same.*

(ii) *if* $a \in H$*, then the inverse of* a *in* $(H, \circ)$ *is the same as the inverse of* a *in* $(G, \circ)$*.*

Proof. (i) Let e_H be the identity element of the group $(G, \circ)$ and let e_G be the same in $(G, \circ)$. Then for any $h \in H$, we have

$$e_H \circ h = h \circ e_H = h$$

As $H \subset G$, the element h is also in G and therefore

$$e_G \circ h = h \circ e_G = h.$$

Then

$$e_H \circ h = e_G \circ h \implies e_H = e_G$$

by right cancellation law.

(ii) Let $a \in H$. Let b and c be the inverse of a in $(G, \circ)$ and $(H, \circ)$ respectively. Then

$$a \circ b = b \circ a = e_G$$

$$a \circ c = c \circ a = e_H$$

But by (i), $e_G = e_H$ and so $a \circ b = a \circ c$. Hence by cancellation law, we get $b = c$. □

Theorem 37. *Let $(G, \circ)$ be a group and let H be a non-empty subset of G. Then H is a subgroup of $(G, \circ)$ if and only if (i) $a, b \in H \implies a \circ b \in H$ and (ii) $a \in H \implies a^{-1} \in H$.*

Proof. Let us first suppose that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then by definition $(H, \circ)$ itself form a group and the conditions (i) and (ii) are obviously satisfied.

Conversely, let the conditions hold good. Condition (i) guarantees that H is closed under $\circ$. Since associative property is a hereditary property and $H \subset G$, it is clearly satisfied in H with respect to $\circ$.

Now, let $a \in H$. Then by (ii), $a^{-1} \in H$ and therefore by (i), we have $aa^{-1} = e \in H$. This shows that $(H, \circ)$ is itself a group and hence by definition it is a subgroup of $(G, \circ)$. □

Theorem 38. *Let $(G, \circ)$ be a group and let H be a non-empty subset of G. Then H is a subgroup of $(G, \circ)$ if and only if $a, b \in H \implies a \circ b^{-1} \in H$.*

Proof. Let us first suppose that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then by definition $(H, \circ)$ itself form a group. Let $a, b \in H$. Then $a, b^{-1} \in H$ and hence by closure property $a \circ b^{-1} \in H$.

Conversely, let the condition holds i.e., for any $a, b \in H \implies a \circ b^{-1} \in H$.

Let $a \in H$. Then $a \circ a^{-1} = e \in H$. Therefore, H contains the identity element e.

Now for $a \in H$, we have $e \circ a^{-1} = a^{-1} \in H$. Therefore, inverse of each element exists in H.

Let $a, b \in H$. Then we have $a, b^{-1} \in H$ and hence $a \circ b = a \circ (a^{-1})^{-1} \in H$. Therefore, $\circ$ is closed in H.

Since H is a subset of G and $\circ$ is associative on G, it follows that $\circ$ is associative on H. □

Theorem 39. *Let G be a group and H be a non-empty finite subset of G. Then H is subgroup of G if and only if for any $a, b \in H \implies ab \in H$.*

Proof. Let H be a subgroup of G. Then H is itself a group and hence the condition holds good.

Conversely, let the condition holds.

Let $a \in H$. Then $a, a^2, a^3, \cdots$ are all in H. By hypothesis, H is a finite set. Therefore, the elements $a, a^2, a^3, \cdots$ cannot be all distinct. So we must have

$$a^r = a^s$$

for some positive integers r, s with $r \geq s$. This yield that

$$a^{r-s} = e$$

and hence $e \in H$. Note also that, since $r - s \geq 1$, we have $r - s - 1 \geq 0$. From this it follows that

$$a^{r-s-1}a = a^{r-s} = aa^{r-s-1} = e$$

and hence $a^{-1} = a^{r-s-1} \in H$. Also H satisfies closure and associative properties. Hence H is a subgroup of G. □

Problem 7. *Let $H = \{x \in \mathbb{C} : x^{2021} = 1\}$. Prove that H is a subgroup of $\mathbb{C} \setminus \{0\}$ under multiplication.*

Solution. *It is to be observed that $o(H) = 2021$ and that the group $(\mathbb{C} \setminus \{0\}, \cdot)$ is abelian. Now let $a, b \in H$. Then $a^{2021} = 1$ and $b^{2021} = 1$ and therefore*

$$(ab)^{2021} = a^{2021}b^{2021} = 1$$

which implies that $ab \in H$. Hence by Theorem 39, we have H is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$.

Note. *Theorem 39 need not be true if H is assumed to be an infinite set. For example, let $G = \mathbb{Z}$ be the group with respect to addition. Let $H = \mathbb{N}$. It is to be noted that H is closed under addition but is not a subgroup of G.*

Example 40. *Let G be a group. Let us consider the set*

$$H = \{x \in G : xg = gx \text{ for all } g \in G\}.$$

Then clearly, H is non-empty as $e \in G$ where e is the identity element of G. We claim that H is a subgroup of G.

Let $a, b \in H$. Then $ag = ga$ and $bg = gb$ holds for all $g \in G$.

Now,

$$bg = gb \Longrightarrow b^{-1}(bg)b^{-1} = b^{-1}gbb^{-1} \Longrightarrow gb^{-1} = b^{-1}g$$

for all $g \in G$. Therefore, for all $g \in G$, we have

$$\begin{aligned}(ab^{-1})g &= a(b^{-1}g)\\ &= a(gb^{-1})\\ &= (ag)b^{-1}\\ &= g(ab^{-1})\end{aligned}$$

which implies that $ab^{-1} \in H$ and consequently, H is a subgroup of G. The subgroup H is called the centre of the group G and is denoted by $Z(G)$.

For example, if we take $G = V_4$, the Klein's 4-group, then

$$Z(V_4) = V_4.$$

Now if we take $G = S_3$, then $Z(S_3) = \{e\}$.

Example 41. *Let G be a group and let $a \in G$. Let us consider the set*

$$H = \{x \in G : xa = ax\}.$$

We claim that H is a subgroup of G.

Let $x, y \in H$. Then $ax = xa$ and $ay = ya$. Therefore, $ay^{-1} = y^{-1}a$. Now,

$$\begin{aligned}a(xy^{-1}) &= (ax)y^{-1}\\ &= (xa)y^{-1}\\ &= x(ay^{-1})\\ &= x(y^{-1}a)\\ &= (xy^{-1})a\end{aligned}$$

which implies that $xy^{-1} \in H$. Hence H is a subgroup of G.

The subgroup H is called the **centraliser** *of the element a and is denoted as $C(a)$. It is also obvious that $Z(G) \subset C(a)$ and $Z(G)$ is a subgroup of $C(a)$.*

Theorem 42. *Let H and K be two subgroups of a group G. Then $H \cap K$ is a subgroup of G.*

Proof. It is clear that $e \in H \cap K$, e being the identity element of G and hence $H \cap K \neq \phi$. Let $a, b \in H \cap K$. Then

$$\begin{aligned}a, b \in H \cap K &\Longrightarrow a, b \in H \text{ \& } a, b \in K\\ &\Longrightarrow ab^{-1} \in H \text{ \& } ab^{-1} \in K\\ &\Longrightarrow ab^{-1} \in H \cap K\end{aligned}$$

which implies that $H \cap K$ is a subgroup of G. □

Note. *The above theorem need not hold if you replace $\cap$ by $\cup$ i.e., the union of two subgroups of a group need not be a subgroup of the group. For example, let us consider the Klein's* 4*-group V_4 (See Example 7). Let us take $H = \{e, a\}$ and $K = \{e, b\}$. Then H and K are two subgroups of V_4. But $H \cup K = \{e, a, b\}$ is not a subgroup of V_4, since $a, b \in H \cup K$ but $c = ab \notin H \cup K$.*

However we have the following theorem:

Theorem 43. *Let G be a group and let H, K be two subgroups of G. Then $H \cup K$ is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.*

Proof. Let us first suppose that $H \cup K$ be a subgroup of G. We have to prove that either $H \subset K$ or $K \subset H$. Suppose that our claim is not true. Then $H \not\subset K$ and $K \not\subset H$. So there is an element $a \in K$ such that $a \notin H$ and another element $b \in H$ but $b \notin K$. Therefore, $a, b \in H \cup K$ and since $H \cup K$ is a subgroup of G, we have $ab \in H \cup K$. Then $ab \in H$ or $ab \in K$.

If $ab \in H$. Then $b \in H$ and $ab \in H$ implies that $abb^{-1} = a \in H$ - a contradiction.

If $ab \in K$. Then $a \in K$ and $ab \in K$ implies that $a^{-1}ab = b \in K$ - a contradiction.

Therefore ab neither belongs to H nor to K and hence $ab \notin H \cup K$ - a contradiction. This contradiction confirms that our assumption is wrong and hence we have either $H \subset K$ or $K \subset H$.

Conversely, let us suppose that either $H \subset K$ or $K \subset H$. Then either $H \cup K = K$ or $H \cup K = H$ and hence in both the cases $H \cup K$ is a subgroup of G. □

Problem 8. *In a group G, a is the only element of a fixed order n. Then show that $a \in Z(G)$.*

Solution. *Let $o(a) = n$. Let $x \in G$. Consider the element $xax^{-1} \in G$. We claim that $o(xax^{-1}) = n$. First note that*

$$\begin{aligned}(xax^{-1})^n &= (xax^{-1})(xax^{-1}) \cdots (xax^{-1})\\ &= xa^nx^{-1}\\ &= xex^{-1}\\ &= e\end{aligned}$$

where e being the identity element of G. Therefore, $o(xax^{-1}) \leq n$. Let $o(xax^{-1}) = k < n$. Then

$$(xax^{-1})^k = e \Longrightarrow xa^kx^{-1} = e \Longrightarrow a^k = xx^{-1} = e$$

which is a contradiction to the fact that $o(a) = n$. Therefore we must have $o(xax^{-1}) = n$. Now by hypothesis, we have

$$xax^{-1} = a \Longrightarrow xa = ax.$$

This is true for all $x \in G$. Hence $a \in Z(G)$.

Problem 9. *Let a and b be two elements in a group G. Show that $o(ab) = o(ba)$.*

Solution. *It is to be noted from the above problem that $o(a) = o(xax^{-1})$ for all $x \in G$. It is also to be noted that*

$$ab = b^{-1}(ba)b = b^{-1}(ba)(b^{-1})^{-1}.$$

Hence $o(ab) = o(ba)$.

Problem 10. *Let G be an abelian group. Prove that the subset $H = \{g \in G : g = g^{-1}\}$ is a subgroup of G.*

Solution. *First note that $e \in H$ as $e = e^{-1}$ where e is the identity element of G. Therefore $H \neq \phi$. Let $x, y \in H$. Then $x = x^{-1}$ and $y = y^{-1}$. Then $xy^{-1} = x^{-1}y = yx^{-1} = (xy^{-1})^{-1}$ and hence $xy^{-1} \in H$. This shows that H is a subgroup of G.*

Problem 11. *Let $(G, \circ)$ be a group and $(H, \circ)$ be a subgroup of $(G, \circ)$. Let $x, y \in G$. Define a relation ρ on G by "$x\rho y$ if and only if $x \circ y^{-1} \in H$". Prove that ρ is an equivalence relation on G.*

Solution. Reflexive: *Since $x \circ x^{-1} = e \in H$ for all $x \in G$, it follows that $x\rho x$ holds for all $x \in G$. Hence ρ is reflexive.*

Symmetric: *Let $x, y \in G$ be such that $x\rho y$ holds. Then $x \circ y^{-1} \in H$. Since H is a subgroup of G, we have $y \circ x^{-1} = (x \circ y^{-1})^{-1} \in H$. This yields that $y\rho x$. Hence ρ is symmetric.*

Transitive: *Let $x, y, z \in G$ be such that $x\rho y$ and $y\rho z$. Then $x \circ y^{-1} \in H$ and $y \circ z^{-1} \in H$ and therefore, $x \circ z^{-1} = (x \circ y^{-1}) \circ (y \circ z^{-1}) \in H$. This implies that $x\rho z$ and hence ρ is transitive. Consequently, ρ is an equivalence relation on G.*

Problem 12. *Let $(G, \circ)$ be a group and H be a non-empty subset of G. A relation ρ defined on G by "$a\rho b$ if and only if $a \circ b^{-1} \in H$ for $a, b \in G$, is an equivalence relation on G. Prove that $(H, \circ)$ is a subgroup of $(G, \circ)$.*

Solution. *Let $a \in H$. Then $a \in G$ and since ρ is reflexive, $a\rho a$ holds. That is $e = a \circ a^{-1} \in H$. This shows that H contains identity element.*

Let $a, b \in H$ so that $a, b \in G$. Since $a = a \circ e^{-1} \in H$ and $b = b \circ e^{-1} \in H$, it follows that $a\rho e$ and $b\rho e$ holds. Since ρ is symmetric, we have $e\rho b$ holds. Then by transitivity of ρ, we get $a\rho b$ holds i.e., $a \circ b^{-1} \in H$. This proves that H is a subgroup of G.

Problem 13. *Let G be a group. Show that $Z(G) = \bigcap\limits_{a \in G} C(a)$.*

Solution. *We have already noted that $Z(G) \subset C(a)$ for all $a \in G$ and hence $Z(G) \subset \bigcap\limits_{a \in G} C(a)$. Now, let $x \in \bigcap\limits_{a \in G} C(a)$. Then $x \in C(a)$ for all $a \in G$ and hence $ax = xa$ for all $a \in G$. This implies that $x \in Z(G)$ and the result follows.*

Problem 14. *Let G be a group and let $a \in G$. Prove that $C(a) = C(a^{-1})$.*

Solution. *Let $x \in C(a)$. Then $ax = xa$ which implies that $xa^{-1} = a^{-1}x$. Therefore, $x \in C(a^{-1})$ and hence $C(a) \subset C(a^{-1})$. Converse part is similar.*

Problem 15. *Suppose that a group contains elements a, b such that $o(a) = 4, o(b) = 2$ and $a^3b = ba$. Find $o(ab)$.*

Solution. *Note that*

$$(ab)^2 = abab = a(ba)b = a(a^3b)b = a^4b^2 = e$$

which implies that $o(ab) = 1$ or 2. But $o(ab) = 1$ implies that $ab = e \implies a = b^{-1} = b$ - impossible. Hence $o(ab) = 2$.

Problem 16. *Consider the elements $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ from $SL(2, \mathbb{R})$. Find $o(A), o(B)$ and $o(AB)$. Is the result surprising?*

Solution. *It can be shown that $o(A) = 4, o(B) = 3$ but $o(AB) = \infty$.*

Problem 17. *Suppose a is an element in a group G such that $o(a) = 5$. Prove that $C(a) = C(a^3)$.*

Solution. *We first show that $C(a) \subset C(a^3)$. For this, let $x \in C(a)$. Then $ax = xa$ and therefore*

$$a^3x = a^2xa = a(ax)a = a(xa)a = (ax)a^2 = (xa)a^2 = xa^3$$

which shows that $x \in C(a^3)$. So, $C(a) \subset C(a^3)$.

For the reverse inclusion, observe that $a^6 = a$. Let $y \in C(a^3)$ and then

$$ya = ya^6 = (ya^3)a^3 = a^3(ya^3) = a^3(a^3y) = a^6y = ay$$

which implies that $y \in C(a)$ and consequently, $C(a^3) \subset C(a)$. Hence the result follows.

Definition 44. *Let $(G, \circ)$ be a group. If there is an element $a \in G$ such that each element $b \in G$ can be expressed as $b = a^n$ (or, in additive notation na) for some $n \in \mathbb{Z}$, then a is said to be a* **generator** *of the group $(G, \circ)$. In this case we write $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ (or, $\{na : n \in \mathbb{Z}\}$) and read as a generates the group G.*

Example 45. *Let us consider the group $(\mathbb{Z}, +)$ (See Example 1). Note that 1 is a generator of the group and therefore $\mathbb{Z} = \langle 1 \rangle$. It is also to be noted that -1 is also a generator of $\mathbb{Z}$. It can also be easily checked that $\mathbb{Z}$ has only two generators.*

Example 46. *Let us now consider Klein's 4-group V_4 (See Example 7). No element of V_4 generates the group.*

Definition 47. Cyclic group: *A group $(G, \circ)$ is said to be a* **cyclic** *group if it is generated by an element $a \in G$. In this case we write $G = \langle a \rangle$.*

Theorem 48. *If a is a generator of a cyclic group G, then so is a^{-1}.*

Proof. Let $G = \langle a \rangle$. We claim that $G = \langle a^{-1} \rangle$. Since $a^{-1} \in G$, it is clear from closure property that

$$\langle a^{-1} \rangle \subset G.$$

Let $x \in G$. Then $x \in \langle a \rangle$ and therefore $x = a^n$ for some $n \in \mathbb{Z}$. Note that $x = a^n = (a^{-1})^{-n} \in \langle a^{-1} \rangle$, since $-n \in \mathbb{Z}$. This implies that $G \subset \langle a^{-1} \rangle$. Hence $G = \langle a^{-1} \rangle$ and the theorem follows. □

Note. *If a group G has only one generator, say a, then we must have $a = a^{-1}$. This implies that $a^2 = e$. Hence we have either $G = \{e\}$ or $G = \{e, a\}$.*

Theorem 49. *Every cyclic group is abelian.*

Proof. Let G be a cyclic group generated by a i.e., $G = \langle a \rangle$. Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$. Then

$$xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx.$$

This is true for all $x, y \in G$. Hence the result follows. □

Note. *However the converse of the above theorem need not be true i.e., an abelian group is not necessarily cyclic. For example, Kleins 4-group V_4 (Example 7) is abelian but not cyclic.*

We now prove the following theorems which has a broad application:

Theorem 50. *Let G be a finite cyclic group generated by a. Then $o(G) = n$ if and only if $o(a) = n$.*

Proof. Let us first suppose that $o(G) = n$. We claim that $o(a) = n$.

Since $a \in G$, we have $e, a, a^2, \cdots$ are elements of G. Since G is finite, the elements $e, a, a^2, \cdots$ cannot be distinct. So we have $a^r = a^s$ for some $r, s \in \mathbb{Z}$ with $r > s$. This implies that $a^{r-s} = e$ and hence $o(a)$ is finite. Let $o(a) = k$. Then by Theorem 26 (iii), the elements $e, a, a^2, \cdots, a^{k-1}$ are all distinct.

Let $H = \{e, a, a^2, \cdots, a^{k-1}\}$. It is clear that $H \subset G$. Now let $x \in G$. Then $x = a^m$ for some $m \in \mathbb{Z}$. Therefore by division algorithm, there are integers q, r such that $m = kq + r$ where $0 \leq r < k$. Now,

$$x = a^m = a^{kq+r} = (a^k)^q a^r = ea^r = a^r.$$

Since $0 \leq r < k$ and $x = a^r$, it follows that $x \in H$. Hence $G \subset H$ and consequently, $G = H$. Since $o(G) = n$, it follows that $k = n$ and hence $o(a) = k = n$.

Conversely, let $o(a) = n$. We claim that $o(G) = n$. By hypothesis, $G = \langle a \rangle$. In a similar way, it can be shown that

$$G = \{e, a, a^2, \cdots, a^{n-1}\}.$$

Hence $o(G) = n$. □

Theorem 51. *Let G be a cyclic group generated by a. Then G is infinite if and only if $o(a)$ is infinite.*

Proof. Apply above theorem. □

Theorem 52. *A finite group G of order n is cyclic if and only if there is an element $b \in G$ such that $o(b) = n$.*

Proof. Let G be a cyclic group of order n. Then there is an element $a \in G$ such that $G = \langle a \rangle$. Then by Theorem 50, it follows that $o(a) = n$. Taking $b = a$, the result follows.

Conversely, suppose that G is a finite group of order n and there exists an element $b \in G$ such that $o(b) = n$. Then by Theorem 26 (iii), the elements $e, b, b^2, \cdots, b^{n-1}$ are all distinct. Also $e, b, b^2, \cdots, b^{n-1}$ are all in G. Since $o(G) = n$ and $e, b, b^2, \cdots, b^{n-1}$ are all distinct elements of G, it follows that $G = \{e, b, b^2, \cdots, b^{n-1}\}$. We claim that $G = \{b^n : n \in \mathbb{Z}\}$. It is obvious that $G \subset \{b^n : n \in \mathbb{Z}\}$.

Since $b \in G$, it follows that $e, b, b^2, \cdots$ are all in G i.e., $\{b^n : n \in \mathbb{Z}\} \subset G$ and hence $G = \langle b \rangle$. This completes the proof. □

Theorem 53. *Let $G = \langle a \rangle$ of order $n > 1$. Then for a positive integer r, a^r is also a generator of G if and only if r is less than n and prime to n.*

Proof. By hypothesis, $G = \{e, a, a^2, \cdots, a^{n-1}\}$. Let a^r be a generator of the group G for some positive integer $r \in \{1, 2, \cdots, n-1\}$. Then by Theorem 50, $o(a^r) = n = o(a)$. Also by Theorem 29, we have

$$o(a^r) = \frac{o(a)}{gcd(r, n)}.$$

Hence $gcd(r, n) = 1$ which implies that r is less than n and prime to n.

Conversely, suppose that r is less than n and prime to n. Then for $r \in \{1, 2, \cdots, n-1\}$, we have

$$o(a^r) = \frac{o(a)}{gcd(r, n)} = o(a) = n.$$

Hence by Theorem 52, it follows that a^r is also a generator of G. □

Let us recall the Euler's ϕ function defined on $\mathbb{N}$. We have $\phi(1) = 1$ and $\phi(n)$ equals to the number of positive integers less than n and prime to n. For example, $\phi(4) = 2$ etc. From the above theorem, we have the following important result:

Corollary 54. *Number of generators of a finite cyclic group of order n is $\phi(n)$.*

Theorem 55. *Every subgroup of cyclic group is cyclic.*

Proof. Let G be a cyclic group generated by a and H be a subgroup of G. We claim that H is a cyclic group.

If $H = G$ or $H = \{e\}$ where e is the identity element of G, then there is nothing to prove. So let us suppose that H a non-trivial proper subgroup of G.

Let $x \in H$. Then $x \in G$ and so $x = a^m$ for some integer m. Since H is a subgroup of G, we have $x^{-1} = a^{-m} \in H$. Since either m or $-m$ is a positive integer, it follows that H contains an element which is a positive power of a. Then by well ordering property, let m be the smallest positive integer such that $a^m \in H$. We claim that H is a cyclic group generated by a^m i.e, $H = \langle a^m \rangle$.

Since $a^m \in H$, it follows that $\langle a^m \rangle \subset H$. For the reverse inclusion, let $x \in H$. Then $x \in G$ and hence $x = a^p$ for some integer p. Now by division algorithm, there are integers q, r such that

$$p = mq + r$$

where $0 \leq r < m$. We claim that $r = 0$. If not, then $0 < r < m$ and therefore

$$a^r = a^{p-mq} = a^p a^{-mq}$$

which implies that $a^r \in H$ and $0 < r < m$ - a contradiction to the fact that a^m is the smallest positive integer such that $a^m \in H$. Hence our claim that $r = 0$ is true. Then $p = mq$ and so

$$x = a^p = a^{mq} = (a^m)^q \in \langle a^m \rangle.$$

This shows that $H \subset \langle a^m \rangle$ and hence $H = \langle a^m \rangle$. This completes the proof. □

Let us now take an example to see that every proper subgroup of a group is cyclic but the group is not cyclic.

Example 56. *Let $G = V_4$ (see Example 7). It is to be noted that every proper subgroup of G is cyclic. But G is not cyclic.*

Theorem 57. *A cyclic group of prime order has no non-trivial proper subgroup.*

Proof. Let G be a cyclic group of prime order p generated by a. Let H be a subgroup of G. Then H is also a cyclic group. Let $H = \langle a^m \rangle$ where m is smallest positive integer such that $a^m \in H$. Note that $a^p = e \in H$ where e is the identity element of G. Then proceeding as in Theorem 55 we can show that $p = mq$ for some some $q \in \mathbb{Z}$. This shows that m divides p which implies that $m = 1$ or p. If $m = 1$, then $H = \{e\}$ and if $m = p$, then $H = G$. Hence the theorem. □

Theorem 58. *A cyclic group of order n has exactly one subgroup of order d for each positive divisor d of n.*

Proof. Let $G = \langle a \rangle$ and let $o(G) = n$. Then $o(a) = n$ and $G = \{e, a, a^2, \cdots, a^{n-1}\}$.

Note that the trivial subgroup $\{e\}$ is the only subgroup of order 1, where e is the identity element of G. Also G itself is the only subgroup of order n. Let us now take a positive divisor d of n such that $1 < d < n$. Then there is a positive integer q such that $n = dq$. Then $1 < q < n$. Note that $a^q \in G$ and $o(a^q) = \frac{n}{gcd(q,n)} = \frac{n}{q} = d$. Let $H = \langle a^q \rangle$. Then H is a cyclic subgroup of G of order d.

We now show that H is the only subgroup of G of order d. On the contrary, let us suppose that K be another subgroup of G of order d. Then $K = \langle a^p \rangle$ for some $p \in \mathbb{Z}$ and therefore $o(a^p) = d$. Note also that

$$o(a^p) = \frac{n}{gcd(p,n)} \implies gcd(p,n) = \frac{n}{d} = q.$$

Then $p = sq$ for some $s \in \mathbb{N}$. Therefore, $a^p = a^{sq} = (a^q)^s \in \langle a^q \rangle = H$. Hence $K = \langle a^p \rangle \subset H$. Since $o(H) = o(K) = d$, it follows that $H = K$ and the proof is complete. □

Problem 18. *If G be a cyclic group of prime order p, prove that every non-identity element of G is a generator of G.*

Solution. *Let $G = \langle a \rangle$ be a cyclic group of prime order p. Let $a^r, 1 \leq r < p$ be a non-identity element of G. Then*

$$o(a^r) = \frac{o(a)}{gcd(r,p)} = o(a) = p = o(G).$$

Hence a^r is a generator of G. Hence the result follows.

Example 59. *Find all generators of $\mathbb{Z}_{22}$.*

Solution. *First note that $o(\mathbb{Z}_{22}) = 22$ and $\mathbb{Z}_{22} = \langle \overline{1} \rangle$. An element $\overline{m} \in \mathbb{Z}_{22}$ is a generator of $\mathbb{Z}_{22}$ if and only if $o(\overline{m}) = 22$. Now if $\overline{m}$ is a generator of $\mathbb{Z}_{22}$, then*

$$o(\overline{m}) = \frac{o(\overline{1})}{gcd(m,22)} \implies gcd(m,22) = 1 \implies m = 1,3,5,7,9,11,13,15,17,19,21.$$

Hence $\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{21}$ are the generators of $\mathbb{Z}_{22}$.

Example 60. *Let $G = \langle a \rangle$ be a cyclic group such that $o(a) = 16$. Find all the generators of the subgroup of order 8.*

Solution. *First recall that G has exactly one subgroup H of order 8, since $8|16$. Since G is cyclic, H is also cyclic. Note that*

$$o(a^2) = \frac{o(a)}{gcd(2,16)} = \frac{16}{2} = 8.$$

Hence we can assume that $H = \langle a^2 \rangle$.

Now, let $(a^2)^m$ is another generator of H. Then $o((a^2)^m) = 8$ which implies that

$$\frac{o(a^2)}{gcd(m,8)} = 8 \implies gcd(m,8) = 1 \implies m = 1,3,5,7.$$

Hence a^2, a^6, a^{10}, a^{14} are the only generators of H.

Note. *Let $G = \langle a \rangle$. Let $r, s \in \mathbb{N}$. Then $H = \langle a^r \rangle \cap \langle a^s \rangle$ is a subgroup of G and $H = \langle a^{lcm(r,s)} \rangle$.*

Example 61. *Describe the subgroup $8\mathbb{Z} \cap 12\mathbb{Z}$.*

Solution. *It is clear that $8\mathbb{Z} = \langle 8 \rangle$ and $12\mathbb{Z} = \langle 12 \rangle$. Then by the above note $8\mathbb{Z} \cap 12\mathbb{Z} = \langle lcm(8,12) \rangle = \langle 24 \rangle$.*

Example 62. *Let $G = \langle a \rangle$. Let H be the smallest subgroup of G that contains a^m and a^n. Prove that $H = \langle a^{gcd(m,n)} \rangle$.*

Solution. *Let $d = gcd(m,n)$. Since G is cyclic, it follows that H is also cyclic. Let k be the smallest positive integer such that $H = \langle a^k \rangle$. Then $k|m$ and $k|n$ and therefore $k|gcd(m,n) = d$. Thus $a^d \in H$ and so $\langle a^d \rangle \subset H$.*

Also $d|m$ and $d|n$. Therefore, $a^m \in \langle a^d \rangle$ and $a^n \in \langle a^d \rangle$. Since H is the smallest subgroup of G that contains both a^m, a^n, it follows that $\langle a^d \rangle \subset H$. Hence we have $H = \langle a^d \rangle$.

Problem 19. *Let $G = \langle a \rangle$. Find the smallest subgroup of G containing a^8 and a^{12}.*

Solution. *By the previous example, the smallest subgroup containing a^8 and a^{12} is given by $\langle a^{gcd(8,12)} \rangle = \langle a^4 \rangle$.*

Problem 20. *Find the smallest subgroup containing 32 and 40.*

Solution. *Recall that $\mathbb{Z} = \langle 1 \rangle$. Then the smallest subgroup containing 32 and 40 is given by $\langle gcd(32, 40) \rangle = \langle 8 \rangle$.*

Problem 21. *Let G be a group and $a \in G$. If $o(a) = n$, then show that $o(a^k) = o(a^{n-k})$, $1 \leq k \leq n$.*

Problem 22. *Let $G = \langle a \rangle$. Suppose that G has a non-trivial finite subgroup. Prove that G is a finite group.*

Solution. *Let $H \neq \{e\}$ be a finite subgroup of G, where e is the identity element of G. Note that H is cyclic. So there exists a smallest positive integer m such that $H = \langle a^m \rangle$. Since $o(H)$ is finite, let $o(H) = k$. Then $(a^m)^k = e$ and therefore $a^{mk} = e$ which implies that $o(a)$ is finite. Since $o(G) = o(a)$, it follows that $o(G)$ is finite and the result follows.*

Problem 23. *Let $G = \langle a \rangle$ be an infinite cyclic group. Prove that G has only two generators a and a^{-1}.*

Solution. *Let b be a generator of $G = \langle a \rangle$ i.e., $G = \langle b \rangle$. Then $b \in \langle a \rangle$ and so $b = a^m$ for some $m \in \mathbb{Z}$. Again, since $a \in \langle b \rangle$, we have $a = b^k$ for some $k \in \mathbb{Z}$. Therefore,*

$$a = b^k = (a^m)^k = a^{mk}.$$

Since a is of infinite order, it follows that $mk = 1$ and hence we have $m = k = 1$ or $m = k = -1$. Hence we have $b = a$ or $b = a^{-1}$.

Problem 24. *Give an example of an infinite group G such that G has a non-trivial finite subgroup H.*

Solution. *Let us consider the group $G = (\mathbb{C} - \{0\}, \cdot)$ i.e., the group of all non-zero complex numbers under multiplication. Then G is an infinite group.*

Now, let $H = \{x \in \mathbb{C} - \{0\} : x^3 = 1\}$. Then $H \subset G$ is a group under multiplication of order 3 and hence a finite subgroup of G.

Problem 25. *Let G be a non-trivial group with no non-trivial proper subgroup. Prove that G is finite group of prime order.*

Solution. *Let a be a non-identity element of G. Then $\langle a \rangle$ is a non-trivial subgroup of G. Then by hypothesis, we have $G = \langle a \rangle$ i,e., G is a cyclic group generated by a.*

Now we claim that $o(G)$ is finite. If $o(G)$ is infinite, then $\langle a^2 \rangle$ is a non-trivial proper subgroups of G - a contradiction. Hence $o(G)$ must be finite. Finally, we claim that $o(G)$ is a prime. If not, then $o(G) = mn$ for some positive integers m, n such that $m, n \neq 1$. Since G is cyclic and $m|mn$, it follows from Theorem 58 that G has a subgroup of order m - a contradiction. Hence $o(G)$ is a prime number.

Problem 26. *In a group G, the elements a and b commute and $gcd(o(a), o(b)) = 1$. Show that $o(ab) = o(a) \cdot o(b)$.*

Solution. *Let $o(a) = m$ and $o(b) = n$. Let $o(ab) = k$. Then we have $a^m = b^n = (ab)^k = e$, where k is the identity element of G. Now*

$$\begin{aligned}(ab)^{mn} &= a^{mn}b^{mn}\\ &= ee = e\end{aligned}$$

which implies that $k|mn$.

Now

$$\begin{aligned}(ab)^k = e &\implies a^k b^k = e\\ &\implies a^k = b^{-k}\\ &\implies a^{nk} = b^{-nk} = e\end{aligned}$$

which implies that $m|nk$. Since $gcd(m, n) = 1$, it follows that $m|k$.

Also

$$\begin{aligned}(ab)^k = e &\implies a^k b^k = e\\ &\implies b^k = a^{-k}\\ &\implies b^{mk} = a^{-mk} = e\end{aligned}$$

which implies that $n|mk$. Since $gcd(m, n) = 1$, it follows that $n|k$.

Therefore $mn|k$ and consequently, $mn = k$. Hence $o(ab) = k = mn = o(a) \cdot o(b)$.

Problem 27. *If G be a finite group of even order, then prove that G has atleast one element of order 2.*

Solution. *Let G be a finite group of even order. We know that e, the identity element of G, is the only element of order 1. Let us consider the set $S = \{a \in G : a \neq a^{-1}\}$. If $S = \phi$, then all the non-identity elements of G are of order 2 and we are done.*

Suppose that $S \neq \phi$. Then observe that if $a \in S$, then $a^{-1} \in S$ also. This shows that S contains an even number of elements. Note that $e \notin S$. Then $S \cup \{e\}$ contains an odd number of elements of G and hence is a proper subset of G. This implies that there exists atleast one element $a \in G$ such that $a \notin S \cup \{e\}$. Hence $a \neq e$ and $a = a^{-1}$ i.e., $a \neq e$ and $a^2 = e$. This shows that a is an element of order 2. Hence the result follows.

Problem 28. *If an abelian group G of order 10 contains an element of order 5, prove that G must be a cyclic group.*

Solution. *Since G is a group of even order, it follows from Exercise 27 that G has an element, say a, of order 2. By hypothesis, G has an element b of order 5. Then $gcd(o(a), o(b)) = 1$. Since G is abelian, we have $ab = ba$. Hence from Exercise 26, it follow that $o(ab) = o(a) \cdot o(b) = 10$. This shows that G has an element ab of order 10. Thus, by Theorem 52, G is a cyclic group.*

Problem 29. *Let G be a cyclic group of order 30 generated by a. Find the subgroup H of G of order 6. Find the generators of H.*

Solution. *Note that $o(a) = 30$. Now,*

$$o(a^5) = \frac{o(a)}{gcd(5, 30)} = \frac{30}{5} = 6.$$

Hence a^5 is an element of G of order 6. Then $H = \langle a^5 \rangle$ is a subgroup of G of order 6. Let $(a^5)^k$ be a generator of H. Then

$$o((a^5)^k) = \frac{o(a^5)}{gcd(k,6)} \Longrightarrow 6 = \frac{6}{gcd(k,6)} \Longrightarrow gcd(k,6) = 1.$$

Therefore, $k = 1, 5$. Hence the generators of H are a^5 and a^{25}.

Definition 63. Left Cosets: *Let G be a group and H be a subgroup of G. Then for any $a \in G$, the set $aH = \{ah : h \in H\}$ is called the left coset of H in G. Similarly, the set $Ha = \{ha : h \in H\}$ is called the right coset of H in G.*

Example 64. *Let $G = S_3$ and let $H = \{f_0, f_4\}$ (see Example 11). Then the left cosets are*

$$\begin{aligned} f_0H &= H \\ f_3H &= \{f_3, f_3f_4\} = \{f_3, f_1\} = f_1H \\ f_4H &= H \\ f_5H &= \{f_5, f_5f_4\} = \{f_5, f_2\} = f_2H. \end{aligned}$$

Therefore the distinct left cosets of H in G are $H = \{f_0, f_4\}, f_1H = \{f_1, f_3\}, f_2H = \{f_2, f_5\}$. It is to be noted that $H \cup f_1H \cup f_2H = S_3$.

We now find all the right cosets of H in G.

$$\begin{aligned} Hf_0 &= H \\ Hf_3 &= \{f_3, f_4f_3\} = \{f_3, f_2\} = Hf_2 \\ Hf_4 &= H \\ Hf_5 &= \{f_5, f_4f_5\} = \{f_5, f_1\} = Hf_1. \end{aligned}$$

Therefore the distinct right cosets of H in G are $H = \{f_0, f_4\}, Hf_1 = \{f_1, f_5\}, Hf_2 = \{f_2, f_3\}$. It is to be noted that $H \cup Hf_1 \cup Hf_2 = S_3$.

It is to be noted that $f_1H \neq Hf_1$ and $f_2H \neq f_2H$. It is also very important to note that the set of all distinct left cosets $\Big\{\{f_0, f_4\}, \{f_1, f_3\}, \{f_2, f_5\}\Big\}$ is different from the set of all distinct right cosets $\Big\{\{f_0, f_4\}, \{f_1, f_5\}, \{f_2, f_3\}\Big\}$.

Now let us take another subgroup $K = \{f_0, f_1, f_2\}$. Find all the left cosets as well as all the right cosets of K in G. Find if there is same distinction as in the previous one.

Example 65. *Let us consider the group $G = V_4$ (see Example 7). Let $H = \{e, a\}$. Then the left cosets of H in G are*

$$\begin{aligned} eH &= aH = H \\ bH &= \{b, c\} = cH \end{aligned}$$

Therefore the set of all distinct left cosets of H in G are H, bH. Note that $H \cup bH = V_4$.

Theorem 66. *Let G be a group and let H be a subgroup of G. Then the following statements hold good:*

(a) *$hH = H$ if and only if $h \in H$.*

(b) *If $a \in G - H$, then $H \cap aH = \phi$.*

(c) *If $a, b \in G$, then either $aH = bH$ or $aH \cap bH = \phi$.*

(d) *For $a, b \in G$, $aH = bH$ if and only if $a^{-1}b \in H$.*

(e) *Any two left cosets of H in G have the same cardinality.*

(f) *The relation defined on G by "$a\rho b$ if and only if $a^{-1}b \in H$" for $a, b \in G$ is an equivalence relation.*

Proof. (a) Let $hH = H$. Then $h = he \in hH = H$.

Conversely, let $h \in H$. We claim that $hH = H$. Let $x \in hH$. Then $x = hh'$ for some $h' \in H$. Since both $h, h' \in H$, it follows that $x = hh' \in H$. Hence $hH \subset H$.

Let $y \in H$. Since H is itself a group, so by Theorem 17 there exists an element $h_1 \in H$ such that $hh_1 = y$. This implies that $y = hh_1 \in hH$ and therefore, $H \subset hH$. Hence we have $hH = H$.

(b) If possible, suppose that $H \cap aH \neq \phi$. Let $x \in H \cap aH$. Then $x \in H$ and $x \in aH$. So there exists $h \in H$ such that $x = ah$ which implies that $a = xh^{-1} \in H$ - a contradiction. Hence the result follows.

(c) Let $a, b \in G$. Then aH and bH are two left cosets of H in G. Therefore, $aH \cap bh \neq \phi$ or $aH \cap bH = \phi$.

Let $aH \cap bH \neq \phi$. Let $x \in aH = bH$. So there exist elements $h_1, h_2 \in H$ such that $x = ah_1$ and $x = bh_2$. Then $ah_1 = bh_2$ which yields that $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$. We claim that $aH = bH$.

Let $p \in aH$. Then for some $h_3 \in H$, we have

$$p = ah_3 = bh_2h_1^{-1}h_3 = bh_4$$

where $h_4 = h_2h_1^{-1}h_3 \in H$. This implies that $p \in bH$ and therefore $aH \subset bH$.

Now let $q \in bH$. Then there exists $h_6 \in H$ such that $q = bh_6$. Then

$$q = bh_6 = ah_1h_2^{-1}h_6 = ah_7$$

where $h_7 = h_1h_2^{-1}h_6 \in H$. This shows that $bH \subset aH$. Hence $aH = bH$.

(d) Let $aH = bH$. Then $b = be \in bH = aH$ and so there is $h \in H$ such that $b = ah$. Therefore, $a^{-1}b = h \in H$.

Conversely, let $a^{-1}b \in H$. Then $a^{-1}b = h'$ for some $h' \in H$ and so $b = ah' \in aH$. Since $b = be \in bH$, it follows that $b \in aH \cap bH \neq \phi$. Hence by part (c), $aH = bH$.

(e) Let aH and bH be two left cosets of H in G. Define a mapping $f : aH \to bH$ by

$$f(ah) = bh$$

for all $ah \in aH$. We show that f is bijective.

Let $f(ah_1) = f(ah_2)$ for $ah_1, ah_2 \in aH$. Then $bh_1 = bh_2$ which implies that $h_1 = h_2 \implies ah_1 = ah_2$. Hence f is injective.

Let $bh \in bH$. Then by definition of the mapping, we get $f(ah) = bh$ and $ah \in aH$. Hence f is surjective and consequently, f is bijective. Therefore aH and bH have the same cardinality.

(f) **Reflexive:** For any $a \in G$, we have $a^{-1}a = e \in H$. Therefore $a\rho a$ holds for all $a \in G$. So ρ is reflexive.

Symmetric: Let $a, b \in G$ be such that $a\rho b$ holds. Then $a^{-1}b \in H$. Since H is a group, $(a^{-1}b)^{-1} \in H$ i.e., $b^{-1}a \in H$ which implies that $b\rho a$ holds. Therefore ρ is symmetric.

Transitive: Let $a, b, c \in G$ be such that $a\rho b$ and $b\rho c$ holds. Then $a^{-1}b \in H$ and $b^{-1}c \in H$ and therefore

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H.$$

This shows that $a\rho c$ holds and therefore ρ is transitive. Hence ρ is an equivalence relation. □

Note. *Let us now find the equivalence class of an element $a \in G$ under the equivalence relation defined in (f).*

$$\begin{aligned} cl(a) &= \{x \in G : a\rho x\} \\ &= \{x \in G : a^{-1}x \in H\} \\ &= \{x \in G : x \in aH\} = aH. \end{aligned}$$

This shows that $cl(a) = aH$ for all $a \in G$. Since the set of all equivalence classes defines a partition of the set, it follows that the set of all distinct left cosets of H in G forms a partition of G,

Note. *All the above properties established for left cosets are also true for right cosets and can be established in a similar way and hence can be left as an exercise.*

Now we are in a position to prove the famous **Lagrange's theorem** on groups.

Theorem 67. *Order of every subgroup of a* **finite** *group divides the order of the group.*

Proof. Let G be a finite group and let H be a subgroup of G. Let $o(G) = n$. Then the number of distinct left cosets of H in G is also finite. Let $a_H, a_H, \cdots, a_kH$ deonte the distinct left cosets of H in G. Then by the above note, $\{a_H, a_H, \cdots, a_kH\}$ form a partition of G i.e., $G = \bigcup_{i=1}^{k} a_iH$ and $a_iH \cap a_jH = \phi$ for all i, j with $i \neq j$. This implies that

$$o(G) = \sum_{i=1}^{k} o(a_iH).$$

By Theorem 66 (e), $o(a_iH) = o(a_jH)$ for all i, j with $i \neq j$. Since H is itself a left coset of H in G, it follows that $o(a_iH) = o(H)$ for all $i = 1, 2, \cdots, k$. Hence

$$o(G) = \sum_{i=1}^{k} o(H) = k \cdot o(H)$$

which implies that $o(H)$ divides $o(G)$. □

Note. *From the above theorem, we see that $o(G) = k \cdot o(H)$ and therefore $\frac{o(G)}{o(H)} = k$ =the number of distinct left cosets of H in G. The number of distinct left cosets of H in G is called the index of H in G and is denoted by $[G : H]$. Hence by Lagrange's theorem, we see that for a finite group G*

$$[G : H] = k = \frac{o(G)}{o(H)}.$$

There are a large number of important result which follows from Lagrange's theorem. Here we present a few of them.

Theorem 68. *A group G of prime order p is cyclic.*

Proof. Let $a \in G$ be a non-identity element of G. Consider $H = \langle a \rangle$. Then H is a subgroup of G with $o(H) > 1$. By Lagrange's theorem, we have $o(H)|o(G) = p$. Since p is a prime and $o(H) > 1$, we must have $o(H) = p$. Again since $H \subset G$ and $o(H) = o(G)$, we have $G = H = \langle a \rangle$. Hence G is a cyclic group generated by a. □

Note. *From the proof of the above theorem, it follows that every non-identity element of G is a generator of G and hence number of generator of a group of prime order p is $p - 1$.*

Theorem 69. *Let G be a finite group and let $a \in G$. Then $o(a)|o(G)$. Hence $a^{o(G)} = e$, where e is the identity element of G.*

Proof. Let $H = \langle a \rangle$. Then H is a subgroup of G and $o(H) = o(a)$. Then by Lagrange's theorem, $o(H)|o(G)$ i.e., $o(a)|o(G)$.

For the last part, let $o(a) = m$ i.e., $a^m = e$. Since $m|o(G)$, we have $o(G) = mk$ for some $k \in \mathbb{Z}$. Hence

$$a^{o(G)} = a^{mk} = (a^m)^k = e.$$

□

In view of the above theorem, it seems to happen that in an infinite group all the elements are of infinite order. However this is not true in general. There are infinite groups each element of which has finite order (see Example 9). The following problem provides another example of an infinite group having the same property.

Problem 30. *Let* $S = \bigcup_{n\in\mathbb{N}} \{x \in \mathbb{C} : x^n = 1\} = \{x \in \mathbb{C} : x^n = 1, n \in \mathbb{N}\}$*. Show that* S *is an infinite group under the usual multiplication of complex numbers in which each element has finite order.*

Theorem 70. *If* p *be a prime and* a *be an integer such that* p *is not a divisor of* a*, then* $a^{p-1} \equiv 1(mod\ p)$*.*

Proof. Let us first choose $a \in \{1, 2, \cdots, p-1\}$. Consider the group $(\mathbb{Z}_p - \{\overline{0}\}, \cdot_p)$ where $\cdot_p$ denotes the multiplication modulo p. Note that $o(\mathbb{Z}_p - \{\overline{0}\}) = p - 1$ and $\overline{a} \in \mathbb{Z}_p - \{\overline{0}\}$. Then $(\overline{a})^{p-1} = \overline{1}$, $\overline{1}$ being the identity element of $\mathbb{Z}_p - \{\overline{0}\}$. This implies that $a^{p-1} \equiv 1(mod\ p)$.

We now take take $a \in \{1, 2, \cdots, p-1\}^c$ i.e., a is a negative integer or a positive integer greater than p. Then by division algorithm, there are integers q, r such that $a = pq + r$ with $0 \leq r < p$ which implies that $a \equiv r(mod\ p)$. Hence $\overline{a} = \overline{r}$. Since $1 \leq r < p$, it follows from above that $r^{p-1} \equiv 1(mod\ p)$. Since $\overline{a} = \overline{r}$, it follows that $a^{p-1} \equiv 1(mod\ p)$. □

However the converse of the Lagrnage's theorem may not be true i.e., if G be a group of finite order and if $d|o(G)$, there G may not have a subgroup of order d.

Example 71. *Let us look at the following table. The following table represents the Cayley table for the Alternating group* A_4 *having* 12 *elements say,* $\alpha_1 = (1), \alpha_2 = (12)(34), \alpha_3 = (13)(24), \alpha_4 = (14)(23), \alpha_5 = (123), \alpha_6 = (243), \alpha_7 = (142), \alpha_8 = (134), \alpha_9 = (132), \alpha_{10} = (143), \alpha_{11} = (234), \alpha_{12} = (124)$.

$\circ$	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
α_1	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
α_2	α_2	α_1	α_4	α_3	α_6	α_5	α_8	α_7	α_{10}	α_9	α_{12}	α_{11}
α_3	α_3	α_4	α_1	α_2	α_7	α_8	α_5	α_6	α_{11}	α_{12}	α_9	α_{10}
α_4	α_4	α_3	α_2	α_1	α_8	α_7	α_6	α_5	α_{12}	α_{11}	α_{10}	α_9
α_5	α_5	α_8	α_6	α_7	α_9	α_{12}	α_{10}	α_{11}	α_1	α_4	α_2	α_3
α_6	α_6	α_7	α_5	α_8	α_{10}	α_{11}	α_9	α_{12}	α_2	α_3	α_1	α_4
α_7	α_7	α_6	α_8	α_5	α_{11}	α_{10}	α_{12}	α_9	α_3	α_2	α_4	α_1
α_8	α_8	α_5	α_7	α_6	α_{12}	α_9	α_{11}	α_{10}	α_4	α_1	α_3	α_2
α_9	α_9	α_{11}	α_{12}	α_{10}	α_1	α_3	α_4	α_2	α_5	α_7	α_8	α_6
α_{10}	α_{10}	α_{12}	α_{11}	α_9	α_2	α_4	α_3	α_1	α_6	α_8	α_7	α_5
α_{11}	α_{11}	α_9	α_{10}	α_{12}	α_3	α_1	α_2	α_4	α_7	α_5	α_6	α_8
α_{12}	α_{12}	α_{10}	α_9	α_{11}	α_4	α_2	α_1	α_3	α_8	α_6	α_5	α_7

From the above table, we see that A_4 contains 8 elements of order 3 and are $\alpha_5, \cdots, \alpha_{12}$. We claim that A_4 has no subgroup of order 6. Let H be a subgroup of A_4 of order 6. Let a be an element in A_4 of order 3. Since $[A_4 : H] = 2$, the left cosets H, aH, a^2H cannot be all distinct. Now $H = aH$ implies that $a \in H$. If $aH = a^2H$, then $a^2H = a^3H = H$. Therefore, in rest of the cases, we have $a^2H = H$ and therefore, $H = a^3H = aH$ which again implies that $a \in H$. Hence in case we find the $a \in H$. Since a was taken arbitrarily from A_4, it follows that H contains all the 8 elements of A_4-which is a contradiction. Hence A_4 does not have a subgroup of order 6.

Problem 31. *Prove that every group of order < 6 is commutative.*

Solution. *If G be a group of order 1, then $G = \{e\}$, where e is the identity element of G. Then $G = \langle e \rangle$ and hence commutative.*

If $o(G) = 2, 3, 5$, then G is a group of prime order and hence cyclic by Theorem 68. Then by theorem 49, G is commutative.

Now let G be a group of order 4. Then the order of the elements of G are $1, 2$ or 4. If G has an element of order 4, then G is a cyclic group and hence commutative.

Let G has no element of order 4. Then all the non-identity element of G has order 2. Let $a, b \in G$. Then $ab \in G$. Therefore, $o(a) = o(b) = o(ab) = 2$ and so $a = a^{-1}, b = b^{-1}$ and $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. This is true for all $a, b \in G$. Hence G is commutative.

Example 72. *Let H be a normal subgroup of a group G. Let G/H denote the set of all left (or right) cosets of H in G i.e., $G/H = \{aH : a \in G\}$. We show that G/H forms a group under the operation $aH \circ bH = abH$.*

Before that, we first show that the operation $\circ : G/H \times G/H \to G/H$ is well defined. For this, let $(aH, bH), (a'H, b'H) \in G/H \times G/H$ be such that $(aH, bH) = (a'H, b'H)$. Then $aH = a'H$ and $bH = b'H$. Then $a = a'h_1$ and $b = b'h_2$ for some $h_1, h_2 \in H$. We claim that $abH = a'b'H$.

$$\begin{aligned} aH \circ bH = abH &= a'h_1b'h_2H \\ &= a'h_1b'H \\ &= a'h_1Hb' \\ &= a'Hb' \\ &= a'b'H = a'H \circ b'H \end{aligned}$$

Hence the binary operation $\circ$ is well-defined. It is easy to see that eH is the identity element in G/H and $a^{-1}H$ is the inverse of $aH \in G/H$. Rest of the properties are easy to verify. Hence $(G/H, \circ)$ is a group. This group is called the **factor group** *or* **quotient group**.

In addition, if G is commutative, then the quotient group G/H is commutative and if $G = \langle a \rangle$ is a cyclic group generated by a, then $G/H = \langle aH \rangle$ is also a cyclic group. But the converse is not true. For example, consider $G = S_3$ and $H = \{f_0, f_1, f_2\}$. Then H is a normal subgroup of G. Note that $o\left(G/H\right) = \frac{o(G)}{o(H)} = 2$ and hence G/H is cyclic as well as commutative, but S_3 is neither cyclic nor commutative.

Problem 32. *Let P and Q are subgroups of a group G such that $o(o(P), o(Q)) = 1$. Prove that $P \cap Q = \{e\}$.*

Solution. *Note that $P \cap Q$ is a subgroup of P and Q. Then $o(P \cap Q) | o(P)$ as well as $o(P \cap Q) | o(Q)$. This implies that $o(P \cap Q) = 1$ and hence $P \cap Q = \{e\}$.*

Problem 33. *Let G be a group of order pq where p and q are distinct primes. Prove that every proper subgroup of G is cyclic.*

Problem 34. *Prove that a non-commutative group of order 10 must have a subgroup of order 5.*

Solution. *Let G be a group of order 10. Then the order of elements of G are $1, 2, 5,$ or 10. Since G is non-commutative, G cannot have an element of order 10.*

If possible suppose that G has no element of order 5. Then all the non-identity elements of G are of order 2.

Let $a, b \in G$. Then $ab \in G$. By hypothesis, $o(a) = o(b) = o(ab) = 2$ which implies that $a = a^{-1}, b = b^{-1}$ and

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

This shows that G is commutative - a contradiction. Hence we must have an element in G of order 5.

Problem 35. *Prove that a group of order 27 must have a subgroup of order 3.*

Solution. *Let G be a group of order 27. Then the order of the elements of G are $1, 3, 9,$ or 27. If G has an element of order 27, then G is a cyclic group and hence by Theorem 58, G has a subgroup of order 3 as $3|27$.*

If G has an element of order 9, say a, then $o(a^3) = 3$ and hence $H = \langle a^3 \rangle$ is a subgroup of order 3.

If G contains an element of order 3, then $H = \langle a \rangle$ is a subgroup of G of order 3.

Thus, in any of the above cases, G has a subgroup of order 3.

Problem 36. *Prove that a non-abelian group of order 8 must have an element of order 4.*

Problem 37. *Let G be a group of order 15 and let A, B be two subgroups of G of order $3, 5$ respectively. Prove that $G = AB$.*

Solution. *It is to be noted that $A \cap B = \{e\}$. Then $o(A \cap B) = \frac{o(A) \cdot o(B)}{o(A \cap B)} = \frac{3 \cdot 5}{1} = 15$. Therefore $AB \subset G$ and $o(AB) = o(G)$. This implies that $G = AB$.*

Problem 38. *Prove that the total number of subgroups of a finite cyclic group of order n is the number of positive divisors of n.*

Solution. *Let G be a cyclic group of order n. Then all the subgroups of G are also cyclic. Hence G has only cyclic subgroups. By Theorem 58, for each positive divisor d of n G has a unique subgroup of order d. Hence the total number of subgroups of a finite cyclic group of order n is the number of positive divisors of n.*

Problem 39. *Let H and K be two subgroups of a group G such that $o(H) = o(K) = p$ where p is a prime. Show that $H \cap K = \{e\}$.*

Deduce that if G has exactly m distinct subgroups of prime order p, then the total number of elements of order p is $m(p-1)$.

Problem 40. *Let G be a cyclic group of order 12 generated by a and H be the subgroup of G generated by a^4. Show that the distinct left cosets of H in G are H, aH, a^2H, a^3H. Verify that $H \cup a^2H$ is a also a subgroup of G.*

Problem 41. *Let G be an infinite cyclic group generated by a i.e., $G = \langle a \rangle$ and let H be the subgroup generated by a^s i.e., $H = \langle a^s \rangle$, where s is a positive integers > 1. Prove that $H, aH, a^2H, \cdots, a^{s-1}H$ is a complete list of distinct left cosets of H in G.*

Problem 42. *Suppose that G is an abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.*

Solution. *Since $o(G)$ is odd, therefore G cannot have any element of order 2. Thus, each non-identity element x of G has an inverse with $x \neq x^{-1}$. So we can write the elements of G as $e, a_1, a_1^{-1}, a_2, a_2^{-1}, \cdots, a_n, a_n^{-1}$ and hence the product of all these elements must be e, the identity element of G.*

Problem 43. *Let $o(G) = pq$, where p, q are distinct primes. If G has only one subgroup of order p and only one subgroup of order q, then prove that G is cyclic.*

Solution. *Let H be the subgroup of G of order p and let K be the subgroup of G order q. Then $H \cup K$ has $p+q-1 < pq$ elements. Let $a \in G$ be such that $a \notin H \cup K$. By Lagrange's theorem $o(a) = p, q,$ or pq. If $o(a) = p$, then $\langle a \rangle$ is a subgroup of G of order p and by hypothesis, $H = \langle a \rangle$. This implies that $a \in H$ - a contradiction. In a similar way, $o(a) \neq q$. Hence we must have $o(a) = pq$ and consequently, G is a cyclic group.*

Problem 44. *Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all $g \in G$, where e is the identity element of G.*

Problem 45. *Let G be a group of order 33. Show that G has an element of order 3.*

Solution. *The possible orders of the elements of G are $1, 3, 11,$ or 33. If there is an element $x \in G$ such that $o(x) = 33$, then $o(x^{11}) = 3$ and we are done. Suppose that there is no element of G of order 33. Then every non-identity element of G has order 3 or 11. Now note that number of elements of order 11 in G is a multiple of $\phi(11) = 10$ i.e., there $0, 10, 20,$ or 30 elements of order 11. Since identity element is of order 1, we have found atmost 31 elements of G. Hence we must have an element of order 3.*

We have already noted that for some subgroups of a group, left cosets and right cosets coincide and for some subgroups this is not true.

Definition 73. Normal subgroup: *A subgroup H of a group G is said to be a* **normal subgroup** *of G if $aH = Ha$ for all $a \in G$. In this case write $H \Delta G$.*

It is very easy to verify that the trivial subgroup and the improper subgroup of a group are normal subgroups.

Theorem 74. *Every subgroup of a commutative group is normal.*

Proof. Let G be a commutative group and let H be a subgroup of G. Let $a \in H$. Then, since $ab = ba$ for all $a, b \in G$, we have

$$aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$$

which implies that $H \Delta G$. □

Example 75. *Let G be a group and let H be a subgroup of G such that $[G : H] = 2$. Prove that $H \Delta G$.*

Proof. Since $[G : H] = 2$, there are two distinct left cosets as well as two distinct right cosets. Let $x \in G$. If $x \in H$, then $xH = H = Hx$. Now let $x \in G - H$. Then xH is a left coset other than H and Hx is a right coset other than H. Hence we must have $xH = Hx$. Hence the result follows. □

Theorem 76. Test for normality: *Let H be a subgroup of G. Then $H \Delta G$ if and only if for any $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$.*

Proof. Let us first suppose that $H\Delta G$. Then $gH = Hg$ for all $g \in G$.

Let $x \in G$ and $h \in H$. Then $xh \in xH = Hx$. So there exists $h' \in H$ such that $xh = h'x \Longrightarrow xhx^{-1} = h' \in H$.

Conversely, let for any $g \in G$ and for any $h \in H$, we have $ghg^{-1} \in H$. We show that $H\Delta G$.

Let $g \in G$. Let $x \in gH$. Then for some $h_1 \in H$, we have

$$x = gh_1 = gh_1g^{-1}g \in Hg$$

as $gh_1g^{-1} \in H$. This implies that $gH \subset Hg$.

Now, let $y \in Hg$. So there exists $y = h_2g$ for some $h_2 \in H$. Now

$$y = h_2g = gg^{-1}h_2g = gg^{-1}h_2(g^{-1})^{-1} \in gH$$

as $g^{-1} \in G$ and $g^{-1}h_2(g^{-1})^{-1} \in H$. This shows that $Hg \subset gH$. Consequently, $gH = Hg$. This is true for all $g \in G$. Hence $H\Delta G$. □

Note. *The above theorem can also be viewed as:*
$H\Delta G$ if and only if $gHg^{-1} \subset H$ for all $g \in G$.

Example 77. *Let G be a group. Then $Z(G)\Delta G$.*

We apply the above theorem to prove this.

Let $g \in G$ and $h \in Z(G)$. Then

$$ghg^{-1} = gg^{-1}h = h \in Z(G)$$

which implies that $ghg^{-1} \in Z(G)$ for all $g \in G$. Hence $Z(G)\Delta G$.

Theorem 78. *Intersection of two normal subgroups of a group G is also a normal subgroup of G.*

Proof. Let H and K be two normal subgroups of a group G. We claim that $H \cap K$ be a normal subgroup of G. We have already proved that $H \cap K$ is a subgroup of G (see Theorem 42).

Now, let $g \in G$ and $h \in H \cap K$. Then $h \in H$ and $h \in K$. Therefore, $ghg^{-1} \in H$ and $ghg^{-1} \in K$. Hence $ghg^{-1} \in H \cap K$ and therefore, $H \cap K$ is a normal subgroup of G. □

Problem 46. *Let H be a subgroup of a group G and $[G : H] = 2$. Prove that $x^2 \in H$ for all $x \in G$. Deduce that A_4 has no subgroup of order 6.*

Solution. *By hypothesis, $H\Delta G$. Therefore the quotient group G/H exists and is of order 2 i.e., $o(G/H) = 2$. Now for any $x \in G$, we have $(xH)^2 = H$, the identity element of G/H which implies that $x^2H = H \Longrightarrow x^2 \in H$. Hence the first part follows.*

For the second part, Let H be a subgroup of $G = A_4$ of order 6. Then $[G : H] = 2$. Then by first part, we have $x^2 \in H$ for all $x \in G = A_4$.

Now note that A_4 has 12 elements of which α_1 is the identity element (see Example 71). Also

$$\alpha_1^2 = \alpha_2^2 = \alpha_3^2 = \alpha_4^2 = \alpha_1.$$

$$\alpha_5^2 = \alpha_9, \alpha_6^2 = \alpha_{11}, \alpha_7^2 = \alpha_{12}, \alpha_8^2 = \alpha_{10}, \alpha_9^2 = \alpha_5, \alpha_{10}^2 = \alpha_8, \alpha_{11}^2 = \alpha_6, \alpha_{12}^2 = \alpha_7.$$

Hence there are more than 6 squares belongs to H - a contradiction to the fact that $o(H) = 6$. Hence $G = A_4$ cannot have a subgroup of order 6.

Readers are requested to compare the following result with the Example 64.

Problem 47. *Let H be a subgroup of a group G such that every left coset of H is also a right coset of H in G. Prove that $H\Delta G$.*

Solution. *Let $a \in G$. Then by hypothesis, there exists an element $b \in G$ such that $aH = Hb$. Note that $a = ae \in aH = Hb$. Also $a = ea \in Ha$. Therefore, $a \in Ha \cap Hb$. Since any two right cosets are either disjoint or equal, we get $Ha = Hb = aH$. This is true for all $a \in G$ and hence $H\Delta G$.*

Problem 48. *Let H be a subgroup of a group G such that the product of any two left cosets of H is a left coset of H. Prove that $H\Delta G$.*

Solution. *Let $a \in G$. Then by hypothesis, there exists $b \in G$ such that $aHa^{-1}H = bH$. Now, $e = aea^{-1}e \in aHa^{-1}H = bH$. So there exists an element $h \in H$ such that $e = bh$ which implies that $b = h^{-1} \in H$. Hence we have $aHa^{-1}H = H$ and therefore,*

$$aHa^{-1} \subset aHa^{-1}H = H.$$

This proves that $H\Delta G$.

Problem 49. *Let $G = GL(2, \mathbb{R})$ and let H be the group of all 2×2 real orthogonal matrices. Prove that H is not a normal subgroup of G.*

Solution. *Let $A = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \in G$ and let $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in H$. Then $B^T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and*

$$BB^T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which shows that B is orthogonal and so $B \in H$. Also note that $A^{-1} = \frac{1}{3}\begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix}$. Now,

$$\begin{aligned} ABA^{-1} &= \frac{1}{3}\begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix} \\ &= \frac{1}{3}\begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} = C \quad \text{say.} \end{aligned}$$

Then $C^T = \begin{pmatrix} 1 & 0 \\ -4 & -1 \end{pmatrix}$ and therefore,

$$CC^T = \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -4 & -1 \end{pmatrix} = \begin{pmatrix} 17 & 4 \\ 4 & 1 \end{pmatrix}$$

and therefore C is not orthogonal matrix and hence $ABA^{-1} \notin H$. This proves that H is not a normal subgroup of G.

Problem 50. *Let M and N be two normal subgroups of a group G such that $M \cap N = \{e\}$. Prove that $mn = nm$ for all $m \in M$ and for all $n \in N$.*

Solution. *Let $m \in M$ and $n \in N$. Since $N\Delta G$, we have $mnm^{-1} \in N$ and therefore, $mnm^{-1}n^{-1} \in N$. Again, since $M\Delta G$, we have $nm^{-1}n^{-1} \in M$. Since $m \in M$, we have $mnm^{-1}n^{-1} \in M$. This shows that $mnm^{-1}n^{-1} \in M \cap N = \{e\}$. Therefore,*

$$mnm^{-1}n^{-1} = e \Longrightarrow mn(nm)^{-1} = e \Longrightarrow mn = nm.$$

This is true for all $m \in M$ and for all $n \in N$.

Problem 51. *Let G be a group and $a \in G$ in which $(ab)^3 = a^3b^3$ for all $a, b \in G$. Prove that $H = \{x^3 : x \in G\}$ is a normal subgroup of G.*

Solution. *Let* $a, b \in H$*. Then there exists* $p, q \in G$ *such that* $a = p^3, y = q^3$*. Then*

$$ab^{-1} = p^3q^{-3} = (pq^{-1})^3 \quad \text{by hypothesis.}$$

Since $pq^{-1} \in G$*, then* $(pq^{-1})^3 = ab^{-1} \in H$*, it follows that* H *is a subgroup of* G*.*

Now let $g \in G$*. Then*

$$gag^{-1} = gp^3g^{-1} = (gpg^{-1})^3$$

and since $gpg^{-1} \in G$*, it follows that* $gag^{-1} \in H$*. This is true for all* $g \in G$ *and for all* $a \in H$*. Hence* $H\Delta G$*.*

Problem 52. *Let* G *be a group and* $a \in G$*. Prove* $\langle a \rangle$ *is a normal subgroup of* $C(a)$*.*

Solution. *Let* $g \in C(a)$ *and let* $h \in \langle a \rangle$*. Then* $h = a^m$ *for some* $m \in \mathbb{Z}$*. Then*

$$ghg^{-1} = ga^mg^{-1} = gg^{-1}a^m = a^m \in \langle a \rangle$$

which shows that $\langle a \rangle$ *is a normal subgroup of* $C(a)$*.*

Problem 53. *Let* G *be a group of order* 8 *and let* x *be an element of* G *of order* 4*. Prove that* $x^2 \in Z(G)$*.*

Solution. *Let* $H = \langle x \rangle = \{e, x, x^2, x^3\}$*. Let* $g \in G$*. Consider the element* gx^2g^{-1}*. Then* $o(gx^2g^{-1}) = o(x^2) = 2$*.*

Now note that $H\Delta G$*. Then* $gx^2g^{-1} \in H$*. It is also to be noted that* x^2 *is the only element of* H *of order* 2*. Hence we must have*

$$gx^2g^{-1} = x^2 \Longrightarrow gx^2 = x^2g.$$

This is true for all $g \in G$*. Hence* $x^2 \in Z(G)$*.*

Problem 54. *If every cyclic subgroup of a group* G *is normal in* G*, prove that every subgroup of* G *is normal in* G*.*

Solution. *Let every cyclic subgroup of a group* G *be normal in* G*. Let* H *be a subgroup of* G*. Let* $h \in H$*. Then* $h \in G$*. Then by hypothesis,* $\langle h \rangle$ *is normal in* G *as it is a cyclic subgroup of* G*. Then for any* $g \in G$*, we have* $ghg^{-1} \in \langle a \rangle \subset H$*. Hence* $H\Delta G$*.*

Example 79. *Let* G *be a group. If* H *is the only subgroup of* G *of a fixed order, then* $H\Delta G$*.*

Solution. *Let* H *be a subgroup of* G *and let* $o(H) = n$*. Let* $g \in G$*. Consider the set* $gHg^{-1} = \{ghg^{-1} : h \in H\}$*. Clearly,* $gHg^{-1} \neq \phi$ *as* $e = geg^{-1} \in gHg^{-1}$*.*

Let $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$*. Then*

$$gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$$

as $h_1h_2^{-1} \in H$*. Hence* gHg^{-1} *is a subgroup of* G*.*

We claim that $o(gHg^{-1}) = o(H)$*. Define a mapping* $f : H \to gHg^{-1}$ *by* $f(h) = ghg^{-1}$ *for all* $h \in H$*. Let* $h_1, h_2 \in H$*. Then*

$$\begin{aligned} & f(h_1) = f(h_2) \\ \Longleftrightarrow\ & gh_1g^{-1} = gh_2g^{-1} \\ \Longleftrightarrow\ & h_1 = h_2. \end{aligned}$$

This shows that f *is well defined and injective. Definition of* f *clearly shows that* f *is surjective and hence* f *is bijective. Consequently,* $o(H) = o(gHg^{-1}$*. Then by hypothesis,* $gHg^{-1} = H$ *which implies that* $gH = Hg$*. This is true for all* $g \in G$*. Hence* $H\Delta G$*.*

Problem 55. *Prove that every subgroup of* Q_8 *is normal (see Example 5).*

Solution. *Let H be a subgroup of Q_8. Then $o(H) = 1, 2, 4,$ or 8.*

If $o(H) = 1$, then $H = \{e\}$ and $H \Delta G$.

If $o(H) = 8$, then $H = G$ and $H \Delta G$.

If $o(H) = 4$, then $[G : H] = 2$ and hence by Example 75, $H \Delta G$.

Now, let $o(H) = 2$. Then H is cyclic and must be generated by an element of Q_8 of order 2. Note that Q_8 has only one element, say -1, of order 2. Hence H is the only subgroup of Q_8 of order 2. Hence by Example 79, we have $H \Delta G$.

Problem 56. *Let G be a non-commutative group of order $2p$, p being an odd prime. Prove that there exists atleast one element of order p in G. If $o(a) = p$, prove that $\langle a \rangle$ is normal in G.*

Problem 57. *Let H be a normal subgroup of a group G such that $o(H) = 3$ and $[G : H] = 10$. If $a \in G$ and $o(a) = 3$, prove that $a \in H$.*

Solution. *Since $[G : H] = 10$ it follows that $o(G/H) = 10$. Let $a \in G$ be such that $o(a) = 3$. Note that $aH \in G/H$. Since $o(G/H) = 10$, we have*

$$(aH)^{10} = H \implies a^{10}H = H \implies aH = H \implies a \in H.$$

Problem 58. *Let G be a group and let H be a subgroup of G. If $x^2 \in H$ for all $x \in G$, then prove that $H \Delta G$.*

Solution. *Let $x^2 \in H$ for all $x \in G$. Let $g \in G$ and $h \in H$. Then*

$$ghg^{-1} = ghghh^{-1}g^{-1}g^{-1} = (gh)^2h^{-1}(g^{-1})^{-1}.$$

Since $g \in G, h \in H \subset G$, we have $gh \in G$ and hence by hypothesis, $(gh)^2 \in H$. Again $g^{-1} \in G$ and by the same property we have $(g^{-1})^2 \in H$. Hence $ghg^{-1} \in H$ and therefore $H \Delta G$.

Theorem 80. *Let G be a group and let $Z(G)$ be the centre of the group. If $G/Z(G)$ is cyclic, then G is commutative.*

Solution. *Let $G/Z(G)$ be cyclic and let $gZ(G)$ be a generator of $G/Z(G)$. We claim that G is commutative.*

Let $a, b \in G$. Then there exists integers i, j such that $aZ(G) = (gZ(G))^i = g^iZ(G)$ and $bZ(G) = (gZ(G))^j = g^jZ(G)$. So there exists $x, y \in Z(G)$ such that $a = g^ix$ and $b = g^jy$. Now,

$$ab = (g^ix)(g^jy) = g^i(xg^j)y = g^ig^j(xy) = g^ig^j(yx) = g^j(g^iy)x = (g^jy)(g^ix) = ba.$$

This is true for all $a, b \in G$. Hence G is commutative.

Note. *The contrapositive statement of the above theorem is as follows:*
"if G is non-commutative, then $G/Z(G)$ is not cyclic."

Problem 59. *Prove that a non-abelian group of order 10 must have a trivial centre.*

Solution. *Let G be a group of order 10. Then $o(Z(G)) = 1, 2, 5,$ or 10. Since G is non-abelian, so $G \neq Z(G)$ and hence $o(Z(G)) \neq 10$.*

Let $o(Z(G)) = 5$. Then $o(G/Z(G)) = \frac{o(G)}{o(Z(G))} = 2$ and therefore, $G/Z(G)$ is a cyclic group. Hence by Theorem 80, we have G is commutative - a contradiction. Thus, $o(Z(G)) \neq 5$.

In a similar way $o(Z(G)) \neq 2$. Hence we have only $o(Z(G)) = 1$ which shows that $Z(G) = \{e\}$. Hence the result follows.

Example 81. *Prove that $Z(S_3) = \{e\}$.*

Solution. *Note that $o(Z(S_3)) = 1, 2,$ or 3.*

If $o(Z(S_3)) = 2$, then $o(S_3/Z(S_3)) = 3$, a prime number. Therefore, $S_3/Z(S_3)$ is cyclic and hence by Theore 80, S_3 is commutative - a contradiction.

If $o(Z(S_3)) = 3$, then $o(S_3/Z(S_3)) = 2$, a prime number. Therefore, $S_3/Z(S_3)$ is cyclic and hence again by Theore 80, S_3 is commutative - a contradiction.

We have only one possibility and therefore $o(Z(S_3)) = 1$ and the result follows.

Problem 60. *Find the order of $\overline{5} + \langle\overline{6}\rangle$ in the quotient group $\mathbb{Z}_{18}/\langle\overline{6}\rangle$.*

Solution. *Let $G = \mathbb{Z}_{18}$ and let $H = \langle\overline{6}\rangle = \{\overline{0}, \overline{6}, \overline{12}\}$. Then $o(H) = 3$ since $o(\overline{6}) = 3$. Then $G/H = \{\overline{0}+H, \overline{1}+H, \overline{2}+H, \overline{3}+H, \overline{4}+H, \overline{5}+H\}$. Then it is easy to verify that $(\overline{5}+H) = 6$.*

Problem 61. *Let G be a finite group and $H\Delta G$. Prove that for each $g \in G$, the order of the element $gH \in G/H$ divides $o(g)$.*

Solution. *Let $g \in G$ be such that $o(g) = k$. Now, let $o(gH) = n$. We claim that $n|k$. Now*

$$(gH)^k == g^k H = H.$$

Then by Theorem 26(ii), we have $n|k$ i.e., $o(gH)|o(g)$.

Problem 62. *Suppose that G is a non-abelian group of order p^3, p being a prime number. Prove that $o(Z(G)) = 1$ or p.*

Solution. *Note that $o(Z(G)) = 1, p, p^2,$ or p^3.*

If $o(Z(G)) = p^3$, then $G = Z(G)$ which is impossible.

If $o(Z(G)) = p^2$, then $o(G/Z(G)) = \frac{p^3}{p^2} = p$ and hence $G/Z(G)$ is a cyclic group. Then by Theorem 80, we have G is commutative - a contradiction.

Hence we have $o(Z(G)) = 1$ or p.

Definition 82. Simple group: *A group G is said to be a simple group if it has no non-trivial proper normal subgroup.*

For example, a group of prime order is simple, as it has no non-trivial proper subgroups and no non-trivial proper normal subgroups.

Example 83. *Let G be a group and $H\Delta G$. Define $N(H) = \{x \in G : xHx^{-1} = H\}$. We claim that $N(H)$ is a subgroup of G.*

Let $a, b \in N(H)$. Then $aHa^{-1} = H$ and $bHb^{-1} = H \Longrightarrow b^{-1}Hb = H$. Then

$$(ab^{-1}H(ab^{-1})^{-1} = a(b^{-1}Hb)a^{-1} = aHa^{-1} = H$$

which implies that $ab^{-1} \in N(H)$. Hence $N(H)$ is a subgroup of G.

Definition 84. Normaliser of a subgroup: *Let G be a group and $H\Delta G$. Then the subgroup $N(H) = \{x \in G : xHx^{-1} = H\}$ is called the normaliser of H in G.*

Problem 63. *Let G be a group and H be a subgroup of G. Prove that*

(a) *$H\Delta N(H)$.*

(b) *$H\Delta G$ if and only if $N(H) = G$.*

(c) *$N(H)$ is the largest subgroup of G in which H is normal i.e., if $H\Delta K$, where K is a subgroup of G, then $K \subset N(H)$.*

Solution. *(a) Let $g \in N(H)$ and $h \in H$. Then $gHg^{-1} = H$. We claim that $ghg^{-1} \in H$. This is trivially true from the definition i.e., $ghg^{-1} \in gHg^{-1} = H$. Hence $H\Delta G$.*

(b) If $N(H) = G$, then from part (a), it follows that $H\Delta G$.

Conversely, let $H \Delta G$. Then for all $g \in G$, we have $gH = Hg$ i.e., $gHg^{-1} = H$ which implies that $g \in N(H)$. Therefore, $G \subset N(H)$.

It is clear that $N(H) \subset G$. Thus $G = N(H)$.

(c) Let K be a subgroup of G such that $H \Delta K$. Then for all $k \in K$, we have $kH = Hk$ which implies that $k \in N(H)$. This shows that $K \subset N(H)$. Hence the result follows.

Definition 85. *Let G be a group. Let $a \in G$. An element $b \in G$ is said to be a* **conjugate** *of a if there exists an element $c \in G$ such that $b = cac^{-1}$.*

Example 86. Conjugacy relation in a group: *Let G be a group. Define a relation ρ on G by : for $a, b \in G$, $a\rho b$ if and only if b is a conjugate of a. Then ρ is an equivalence relation on G.*

Reflexive: *For any $g \in G$, $g = ege^{-1}$. Thus for all $g \in G$, g is a conjugate of g.*

Symmetry: *Let $a, b \in G$ be such that $a\rho b$. Then there exists an element $c \in G$ such that $b = cac^{-1}$. This implies that $a = c^{-1}bc$ which implies that $b\rho a$.*

Transitive: *Let $a, b, c \in G$ be such that $a\rho b$ and $b\rho c$. So there exists $x, y \in G$ such that $b = xax^{-1}$ and $c = yby^{-1}$. This implies that $c = yxax^{-1}y^{-1} = (yx)a(yx)^{-1}$. Since $xy \in G$, it follows that $c\rho a$.*

Hence ρ is an equivalence relation on G. This relation on G is called **conjugacy relation** *or* **conjugacy** *on G.*

Definition 87. Conjugacy class: *The equivalence class of an element a in G with respect to the above equivalence relation is called the conjugacy class of a and is denoted by $[a]$. Therefore, $b \in [a]$ if and only if there is an element $c \in G$ such that $b = cac^{-1}$ i.e., the elements of $[a]$ are of the form cac^{-1} for $c \in G$.*

Theorem 88. *The number of conjugates of a is equal to the index of $C(a)$ in G i.e., $o([a]) = [G : C(a)]$.*

Proof. Let $a \in G$. Let $\mathcal{F}$ denote the set of all distinct left cosets of $C(a)$ in G. Then $o(\mathcal{F}) = [G : C(a)]$. Note that $bab^{-1} \in [a]$ for all $b \in G$. We now define a mapping $f : \mathcal{F} \to [a]$ by $f(bC(a)) = bab^{-1}$ for all $bC(a) \in \mathcal{F}$. We show that f is an well defined bijective mapping.

Let $b, c \in G$. Then

$$\begin{aligned} & bC(a) = cC(a) \\ \iff & c^{-1}b \in C(a) \\ \iff & (c^{-1}b)a = a(c^{-1}b) \\ \iff & bab^{-1} = cac^{-1}. \end{aligned}$$

Therefore f is an well defined injective mapping. It is obvious that f is surjective and hence bijective. Consequently, $o([a]) = o(\mathcal{F}) = [G : C(a)]$. □

Theorem 89. *Let G be a finite group. Then*

$$o(G) = \sum_a [G : C(a)]$$

where the summation is over a complete set of distinct conjugacy class representatives.

Proof. From Example 86, it follows that $G = \bigcup_a [a]$, where the union runs over a complete set of distinct conjugacy class representatives. Since the distinct conjugacy classes are mutually disjoint, we have

$$o(G) = \sum_a o([a]) = \sum_a [G : C(a)]$$

by Theorem 88. □

Problem 64. *Let G be a group and $a \in G$. Prove that $a \in Z(G)$ if and only if $C(a) = G$.*

Solution. *First, let $a \in Z(G)$. We always have $C(a) \subset G$. Now for any $g \in G$, we have $ga = ag$ which implies that $g \in C(a)$ and therefore $G \subset C(a)$. Hence $C(a) = G$.*

Conversely, let $C(a) = G$. Let $g \in G$. Then $g \in C(a)$ and so $ga = ag$. This is true for all $g \in G$. Hence $a \in Z(G)$.

Theorem 90. *Let G be a finite group. Then*

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} [G : C(a)]$$

where $Z(G)$ denotes the centre of G and the summation runs over a complete set of distinct conjugacy class representatives, which do not belongs to $Z(G)$.

Proof. We have from Problem 67, $a \in Z(G) \iff G = C(a) \iff [G : C(a)] = 1$. Therefore

$$o(Z(G)) = \sum_{a \in Z(G)} [G : C(a)].$$

We have from Theorem 89 that

$$o(G) = \sum_{a} [G : C(a)]$$

where the summation is over a complete set of distinct conjugacy class representatives. This implies that

$$o(G) = \sum_{a \in Z(G)} [G : C(a)] + \sum_{a \notin Z(G)} [G : C(a)] = o(Z(G)) + \sum_{a \notin Z(G)} [G : C(a)]$$

where the summation runs over a complete set of distinct conjugacy class representatives, which do not belongs to $Z(G)$. □

Note. *For a finite group G, the equation*

$$o(G) = \sum_{a \in Z(G)} [G : C(a)] + \sum_{a \notin Z(G)} [G : C(a)] = o(Z(G)) + \sum_{a \notin Z(G)} [G : C(a)]$$

where the summation runs over a complete set of distinct conjugacy class representatives, which do not belongs to $Z(G)$ is called the **(conjugacy) class equation***. Let us now an example.*

Example 91. *Let us take $G = S_3$. Note that $Z(S_3) = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$ i.e., $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$ is self-conjugate.*

Now, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

which implies that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Since order of an element and its conjugates are the same, no element of order 2 is conjugate to an element of order 3. Hence $\left[\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$.

In a similar way, we have another conjugacy class $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$.

Then S_3 has three conjugacy classes $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$ and $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$.

Therefore the class equation is given by

$$\begin{aligned} o(S_3) &= o(Z(G)) + \left[S_3 : C(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix})\right] + \left[S_3 : C(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix})\right] \\ 6 &= 1 \quad + \quad 2 \quad + \quad 3. \end{aligned}$$

Problem 65. *Let G be a finite group and $a \in G$ be such that a has only two conjugates. Prove that $C(a)$ is a normal subgroup of G.*

Solution. *From Theorem 88, we have $[G : C(a)] = o([a])$. By hypothesis, $o([a]) = 2$. Hence $[G : C(a)] = 2$ and hence by Example 75 we have $C(a)$ is a normal subgroup of G.*

Problem 66. *Let G be a finite group that has only two conjugate classes. Show that $o(G) = 2$.*

Solution. *Let $o(G) = n$. Let $a \in G$ be such that $a \neq e$. Then $G = [e] \cup [a]$. Since $o([e]) = 1$, $o([a]) = n - 1$. Hence, $n - 1 = o([a]) = [G : C(a)]$ divides $o(G) = n$. This is possible only if $n - 1 = 1 \Longrightarrow n = 2$.*

Problem 67. *Let G be a group and $a \in G$. Prove that $a \in Z(G)$ if and only if $[a] = \{a\}$.*

Solution. *Let $a \in Z(G)$. Then $ag = ga$ for all $g \in G$. Therefore, $gag^{-1} = a$ for all $g \in G$ which implies that $[a] = \{a\}$.*

Conversely, suppose that $[a] = \{a\}$. Then $gag^{-1} = a$ for all $g \in G$ and so $ga = ag$ for all $g \in G$. This implies that $a \in Z(G)$.

Theorem 92. *If G be a group of order p^2, where p is a prime then G is abelian.*

Proof. By Lagrange's theorem, $o(Z(G))|o(G)$. Then Since $o(G) = p^2$, we have $o(Z(G)) > 1$. So we have $o(Z(G)) = p$, or p^2.

Let $o(Z(G)) = p$. Then $o(G/Z(G)) = p$ and so $G/Z(G)$ is a cyclic group. Then by Theorem 80, we have G is commutative.

Let $o(Z(G)) = p^2$. Then $Z(G) = G$ and hence G is commutative. □

Problem 68. *Find the conjugacy classes in Q_8 and write down the class equation.*

Solution. *We have $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. It is to be noted that $Z(Q_8) = \{-1, 1\}$. Observe that for any $x \in Q_8$,*

$$\begin{aligned} (-x)y(-x)^{-1} &= -1 \cdot x \cdot y(-1 \cdot x)^{-1} \\ &= -1 \cdot x \cdot y \cdot x^{-1} \cdot -1 \\ &= xyx^{-1} \end{aligned}$$

It can be shown that $[I] = \{-I, I\}, [J] = \{-J, J\}, [K] = \{-K, K\}$. Hence the class equation of Q_8 is

$$\begin{aligned} o(Q_8) &= o(Z(Q_8)) + [Q_8 : C(I)] + [Q_8 : C(J)] + [Q_8 : C(K)] \\ 8 &= 2 \quad + \quad 2 \quad + \quad 2 \quad + \quad 2. \end{aligned}$$

Problem 69. *Find the conjugacy classes in D_4 and write down the class equation.*

Note. *To find the conjugacy classes of S_3, we first construct the Cayley table as follows:*

Let $a, b \in S_3$ be such that $o(a) = 3$ and $o(b) = 2$. Then it can be easily shown that

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b			e		
ab	ab				e	
a^2b	a^2b			a^2		e

Let us now fill up the empty cells. For, the element ba, we have one of the following possibilities:

$$ba = a \text{ or, } ba = a^2 \text{ or, } ba = ab \text{ or, } ba = a^2b.$$

It is clear that $ba \neq a, ba \neq a^2$. If $ba = ab$, then $bab = ab^2 = a$ and therefore, $abab = a^2$ which implies that

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

- a contradiction. Hence we must have $ba = a^2b$.

For the element ba^2, we have

$$ba^2 = a \text{ or, } ba^2 = a^2 \text{ or, } ba^2 = ab.$$

It is also clear that $ba^2 \neq a$ and $ba^2 \neq a^2$. Hence we must have $ba^2 = ab$.

For the element bab, we have only two possibilities

$$bab = a \text{ or, } bab = a^2.$$

If $bab = a$, then $abab = a^2$ - a contradiction as shown earlier. So we have $bab = a^2$.

Finally, for the element ba^2b has only one possibility i.e., $ba^2b = a$.

We now find out the elements related to the element ab. Note that

$$aba = a(a^2b) = b, aba^2 = a(ab) = a^2b, abb = a, ab(a^2b) = a(ab)b = a^2.$$

Similarly, the elements of the last row will be as follows:

$$a^2ba = a^2(a^2b) = ab, a^2ba^2 = a^2(ab) = b, a^2b(ab) = a^2(a^2) = a.$$

Hence the complete table will be looked like as follows:

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

We now find out the complete list of distinct conjugacy classes:

$$\begin{aligned}[e] &= \{eee^{-1}, aea^{-1}, a^2e(a^2)^{-1}, beb^{-1}, abe(ab)^{-1}, a^2be(a^2b)^{-1}\}\\ &= \{e\}.\end{aligned}$$

$$\begin{aligned}[a] &= \{eae^{-1}, aaa^{-1}, a^2a(a^2)^{-1}, bab^{-1}, aba(ab)^{-1}, a^2ba(a^2b)^{-1}\}\\ &= \{a, a, a, bab, aba^2b, a^2ba^3b\}\\ &= \{a, a, a, a^2bb, a(ab)b, a^2bb\}\\ &= \{a, a, a, a^2, a^2, a^2\}\\ &= \{a, a^2\} = [a^2].\end{aligned}$$

$$\begin{aligned}[b] &= \{ebe^{-1}, aba^{-1}, a^2b(a^2)^{-1}, bbb^{-1}, abb(ab)^{-1}, a^2bb(a^2b)^{-1}\}\\ &= \{b, aba^2, a^2ba, b, a(ab), a^2(a^2b)\}\\ &= \{b, a(ab), a^2(a^2b), b, a^2b, ab\}\\ &= \{b, a^2b, ab, b, a^2b, ab\}\\ &= \{b, ab, a^2b\} = [ab] = [a^2b].\end{aligned}$$

Hence from Problem 67, it follows that $Z(S_3) = \{e\}$. Therefore, the class equation for S_3 is given by

$$o(S_3) = o(Z(G)) + \sum_{a\notin Z(G)} o([a]) = 1 + o([a]) + o([b]) = 1 + 2 + 3.$$