3.5. Subgroups

Definition. Let G be a set with a binary operation $*$ defined on it. Let $S \subseteq G$. If for each $a, b \in S$, $a * b$ (computed in G) is in S, we say that S is **closed** with respect to the *binary operation* "$*$".

Examples

1. $(\mathbf{Z}, +)$ is a group. The set $\mathbf{E}$ of all even integers is closed under $+$ and further $(\mathbf{E}, +)$ is itself a group.

2. The set of G of all non-singular 2×2 matrices form a group under matrix multiplication. Let H be the set of all matrices of the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. H is subset of G. Also H itself is a group under matrix multiplication.

Definition. A subset H of group G is called a **subgroup** of G if H forms a group with respect to the binary operation in G.

Examples.

1. Let G be any group. Then $\{e\}$ and G are subgroups of G. They are called **improper subgroups** of G.

2. $(\mathbf{Q}, +)$ is a subgroup of $(\mathbf{R}, +)$ ad $(\mathbf{R}, +)$ is a subgroup of $(\mathbf{C}, +)$.

3. In $(\mathbf{Z}_8, \oplus)$, let $H_1 = \{0, 4\}$ and $H_2 = \{0, 2, 4, 6\}$. The Cayley tabels for H_1 and H_2 are given by

$\oplus$	0	4
0	0	4
4	4	0

$\oplus$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

It is easily seen that H_1 and H_2 are closed under $\oplus$ and $(H_1, \oplus)$ and $(H_2, \oplus)$ are groups. Hence H_1 and H_2 are subgroups of $\mathbf{Z}_8$.

4. $\{1, -1\}$ is a subgroup of $(\mathbf{R}^*, \cdot)$.

5. $\{1, i, -1, -i\}$ is a subgroup of $(\mathbf{C}^*, \cdot)$.

6. For any integer n we define

   $n\mathbf{Z} = \{nx / x \in \mathbf{Z}\}$. Then $(n\mathbf{Z}, +)$ is a subgroup of $(\mathbf{Z}, +)$.

   For, let $a, b \in n\mathbf{Z}$. Then $a = nx$ and $b = ny$ where $x, y \in \mathbf{Z}$.

   Hence $a + b = n(x + y) \in n\mathbf{Z}$. Hence $n\mathbf{Z}$ is closed under $+$.

   $0 \in n\mathbf{Z}$ is the identity element.

   Inverse of nx is $-nx = n(-x) \in n\mathbf{Z}$.

   Hence $(n\mathbf{Z}, +)$ is a group.

7. In the symmetric group S_3, $H_1 = \{e, p_1, p_2\}$;

   $H_2 = \{e, p_3\}$; $H_3 = \{e, p_4\}$; and

   $H_4 = \{e, p_5\}$ are subgroups.

8. A_n is a subgroup of S_n (by theorem 3.14).

9. The set of permutations $\{e, p_1, p_2, p_3\}$ wh

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

   is a subgroup of S_4.

Note. In all the above the examples we see that th identity element in the subgroup is the same as th identity element of the group.

Theorem 3.15. Let H be a subgroup of G. Then

(a) the identity element of H is the same as tha of G.

(b) for each $a \in H$ the inverse of a in H is th same as the inverse of a in G.

Proof. (a) Let e and e' be the identities of G and H respectively.
Let $a \in H$. Now,

$$e'a = a \text{ (since } e' \text{ is the identity of } H)$$
$$= ea \text{ (since } e \text{ is the identity of } G \text{ and } a \in G)$$
$$\therefore \quad e'a = ea.$$
$$\therefore \quad e' = e \text{ (by cancellation law).}$$

(b) Let a' and a'' be the inverse of a in G and H respectively. Since by (a), G and H have the same identity element e, we have $a'a = e = a''a$. Hence by cancellation law $a' = a''$.

Theorem 3.16. A subset H of a group G is a subgroup of G iff

(i) it is closed under the binaty operation in G.

(ii) The identity e of G is in H.

(iii) $a \in H \Rightarrow a^{-1} \in H$.

Proof. Let H be a subgroup of G. The result follows immediately from theorem 3.15.

Conversely let H be a subset of G satisfying conditions (i), (ii) and (iii). Then, obviously H itself is a group with respect to the binary operation in G.

Therefore H is a subgroup of G.

Theorem 3.17. A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof. Let H be a subgroup of G. Then $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Conversely let H be a non-empty subset of G such that $a, b \in H \Rightarrow ab^{-1} \in H$.

Since $H \neq \Phi$, there exists an element $a \in H$.

Hence $aa^{-1} \in H$. Thus $e \in H$

Also since $e, a \in H$, $ea^{-1} \in H$. Hence $a^{-1} \in H$.

Now, let $a, b \in H$. Then $a, b^{-1} \in H$

Hence $a(b^{-1})^{-1} = ab \in H$. Thus H is closed under the binary operation in G.

Hence by theorem 3.16 H is a subgroup of G.

Note. If the operation is $+$ then H is a subgroup of G iff $a, b \in H \Rightarrow a - b \in H$.

Theorem 3.18. Let H be a non-empty finite subset of G. If H is closed under the operation in G then H is a subgroup of G.

Proof. Let $a \in H$.

Since H is closed $a, a^2, a^3, \ldots\ldots, a^n \ldots$ are all elements of H.

But since H is finite the elements $a, a^2, a^3, \ldots\ldots$ cannot all be distinct.

Hence let $a^r = a^s, r < s$. Then $a^{s-r} = e \in H$.

Now, let $a \in H$. We have proved that $a^n = e$ for some n. Hence $aa^{n-1} = e$. Hence $a^{-1} = a^{n-1} \in H$.

Thus H is a subgroup of G.

Note. The above theorem is not true if H is infinite. For example, $\mathbf{N}$ is an infinite subset of $(\mathbf{Z}, +)$ and $\mathbf{N}$ is closed under addition. However $\mathbf{N}$ is not a subgroup of $(\mathbf{Z}, +)$.

Theorem 3.19. If H and K are subgroups of a group G then is $H \cap K$ is also a subgroup of G.

Proof. Clearly $e \in H \cap K$ and hence $H \cap K$ is non-empty. Now let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$.

$\therefore$ $ab^{-1} \in H \cap K$. Hence by theorem 3.17, $H \cap K$ is a subgroup of G.

Note.

1. It can be similarly proved that the intersection of any number of subgroups of G is again a subgroup of G.
2. The union of two subgroups of a group need not be a subgroup. For example, $2\mathbf{Z}$ and $3\mathbf{Z}$ are subgroups of $(\mathbf{Z}, +)$ but $2\mathbf{Z} \cup 3\mathbf{Z}$ is not a subgroup of $\mathbf{Z}$ since $3, 2 \in 2\mathbf{Z} \cup 3\mathbf{Z}$ but $3 + 2 = 5 \notin 2\mathbf{Z} \cup 3\mathbf{Z}$.

Theorem 3.20. The union of two subgroups of a group G is a subgroup iff one is contained in the other.

Proof. Let H and K be two subgroups of G such that one is contained in the other. Hence either $H \subseteq K$ or $K \subseteq H$.

$\therefore$ $H \cup K = K$ or $H \cup K = H$. Hence $H \cup K$ is a subgroup of G.

Conversely, suppose $H \cup K$ is a subgroup of G. We claim that $H \subseteq K$ or $K \subseteq H$.

Suppose that H is not contained in K and K is not contained in H. Then there exist elements a, b such that

$$a \in H \quad \text{and} \quad a \notin K \qquad \ldots (1)$$

$$b \in K \quad \text{and} \quad b \notin H \qquad \ldots (2)$$

Clearly $a, b \in H \cup K$. Since $H \cup K$ is a subgroup of G, $ab \in H \cup K$. Hence $ab \in H$ or $ab \in K$.

Case (i) Let $ab \in H$. since $a \in H, a^{-1} \in H$.

Hence $a^{-1}(ab) = b \in H$ which is a contradiction to (2).

Case (ii) Let $ab \in K$. Since $b \in K, b^{-1} \in K$.

Hence $(ab)b^{-1} = a \in K$ which is a contradiction to (1). Hence our assumption that H is not contained in K and K is not contained in H is false.

$\therefore$ $H \subseteq K$ or $K \subseteq H$.

Definition. Let A and B be two subsets of a group G. We define $AB = \{ab / a \in A, b \in B\}$.

Note. If A and B are two subgroups of G, AB need not be a subgroup of G.

In S_3, consider $A = \{e, p_3\}$ and $B = \{e, p_4\}$. Clearly A and B are subgroups of S_3.

Also $AB = \{ee, ep_4, ep_3, p_3p_4\} = \{e, p_4, p_3, p_2\}$.

Now, $p_4p_2 = p_5 \notin AB$.

Hence AB is not a subgroup of S_3.

Theorem 3.21. Let A and B be two subgroups of a group G. Then AB is a subgroup of G iff $AB = BA$.

Proof. Let AB be a subgroup of G.

We claim that $AB = BA$.

Let $x \in AB$. Since AB is a subgroup of G, $x^{-1} \in AB$.

Let $x^{-1} = ab$ where $a \in A$ and $b \in B$.

$\therefore \quad x = (ab)^{-1} = b^{-1}a^{-1}$.

Since A and B are subgroups of G, $a^{-1} \in A$ and $b^{-1} \in B$.

$\therefore \quad x \in BA$. Hence $AB \subseteq BA$ ... (1)

Now, let $x \in BA$. Then $x = ba$ where $b \in B$ and $a \in A$.

$\therefore \quad x^{-1} = (ba)^{-1} = a^{-1}b^{-1} \in AB$.

Now, since AB is a subgroup and $x^{-1} \in AB$, we have $x \in AB$,

$\therefore \quad BA \subseteq AB$. ... (2)

From (1) and (2) we get $AB = BA$.

Conversely, let $AB = BA$. We claim that AB is a subgroup of G. Clearly $e \in AB$ and hence AB is non-empty. Now let $x, y \in AB$. Then $x = a_1b_1$ and $y = a_2b_2$ where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

$\therefore \quad xy^{-1} = (a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$.

Now, $b_2^{-1}a_2^{-1} \in BA$. Since $BA = AB$,

$b_2^{-1}a_2^{-1} \in AB$.

$\therefore \quad b_2^{-1}a_2^{-1} = a_3b_3$ where $a_3 \in A$ and $b_3 \in B$.

$\therefore \quad xy^{-1} = a_1b_1a_3b_3$.

Now $b_1a_3 \in BA$. Since $BA = AB$, $b_1a_3 \in AB$.

$\therefore \quad b_1a_3 = a_4b_4$ where $a_4 \in A$ and $b_4 \in B$.

$\therefore \quad xy^{-1} = a_1(a_4b_4)b_3 = (a_1a_4)(b_4b_3) \in AB$.

$\therefore \quad AB$ is a subgroup of G.

Corollary. If A and B are subgroups of an abelian group G, then AB is a subgroup of G.

Proof. Let $x \in AB$. Then $x = ab$ where $a \in A$ and $b \in B$. Since G is abelian, $ab = ba$.

$\therefore \quad x \in BA$. Hence $AB \subseteq BA$.

Similarly $BA \subseteq AB$.

$\therefore \quad AB = BA$.

Hence AB is a subgroup of G.

Solved problems

Problem 1. Let $a \in \mathbf{R}^*$. Let $H = \{a^n / n \in \mathbf{Z}\}$. Then H is a subgroup of $\mathbf{R}^*$.

Solution. Clearly H is non-empty.

Now, let $x, y \in H$.

Then $x = a^s$ and $y = a^t$ where $s, t \in \mathbf{Z}$.

$\therefore \quad xy^{-1} = a^s(a^t)^{-1} = a^{s-t} \in H$.

Hence H is a subgroup of $\mathbf{R}^*$.

Problem 2. Let H denote the set of all permutations in S_n fixing the symbol 1. Then H is a subgroup of S_n.

Solution. Clearly $e \in H$ and hence H is non-empty. Let $\alpha, \beta \in H$. Then α and β fix the symbol 1. Now β fixes the symbol $1 \Rightarrow \beta^{-1}$ fixes the symbol 1. Hence $\alpha\beta^{-1}$ fixes the symbol 1. Hence $\alpha\beta^{-1} \in H$.

Thus H is a subgroup of S_n.

Problem 3. Let G be the set of all 2×2 matrices with entries from $\mathbf{R}$. Then G is a group under matrix addition.

Let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbf{R} \right\}$. Then H is a subgroup of G.

Solution. Let $A, B \in H$.

Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

Now, $A - B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

$$= \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in H.$$

Hence H is a subgroup of G.

Problem 4. Let G be a group.

Let $H = \{a/a \in G \text{ and } ax = xa \text{ for all } x \in G\}$. (ie) H is the set of all elements which commute with every other element. Show that H is a subgroup of G.

Solution. Clearly $ex = xe = x$ for all $x \in G$.

Hence $e \in H$, so that H is non empty.

Now, let $a, b \in H$.

Then $ax = xa$ and $bx = xb$ for all $x \in G$.

Now,

$$\begin{aligned} bx = xb &\Rightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1} \\ &\Rightarrow (b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1}) \\ &\Rightarrow exb^{-1} = b^{-1}xe \\ &\Rightarrow xb^{-1} = b^{-1}x. \qquad \ldots (1) \end{aligned}$$

$$\begin{aligned} \therefore \quad (ab^{-1})x &= a(b^{-1}x) \\ &= a(xb^{-1}) \qquad \text{(by (1))} \\ &= (ax)b^{-1} \\ &= (xa)b^{-1} \qquad (\text{since } ax = xa) \\ &= x(ab^{-1}). \end{aligned}$$

Thus ab^{-1} commutes with every element of G.

$\therefore$ $ab^{-1} \in H$ and hence H is a subgroup of G.

Note. The above subgroup of G is called the **centre** of G and is denoted by $Z(G)$.

Problem 5. Let G be a group and let a be a fixed element of G.

Let $H_a = \{x/x \in G \text{ and } ax = xa\}$

(ie) H_a is the set of all elements in G which commute with a.

Show that H_a is a subgroup of G.

Solution. Clearly $ea = ae = a$.

Hence $e \in H_a$ so that H_a is non-empty.

Now, let $x, y \in H_a$.

Then $ax = xa$ and $ay = ya$.

Now, $ay = ya \Rightarrow y^{-1}a = ay^{-1}$. (as in the pervious problem) $\ldots (1)$

$$\begin{aligned} \text{Hence } a(xy^{-1}) &= (ax)y^{-1} \\ &= (xa)y^{-1} \qquad (\text{since } ax = xa) \\ &= x(ay^{-1}) \\ &= x(y^{-1}a) \qquad \text{(by (1))} \\ &= (xy^{-1})a. \end{aligned}$$

Hence xy^{-1} commutes with a.

$\therefore$ $xy^{-1} \in H_a$ and hence H_a is a subgroup of G.

Note. H_a is called the **normaliser** of a in G.

Exercises

1. Show that $\{a + bi/a, b \in \mathbf{Z}\}$ is a subgroup of $(\mathbf{C}, +)$.
2. Determine which of the following are subgroups of $(\mathbf{C}, +)$
   (a) $\mathbf{R}$ (b) $\{a + b\sqrt{-5}/a, b \in \mathbf{N}\}$
   (c) $\{z/|z| = a\}$ (d) $\{z/\text{real part of } z \text{ is } 0\}$
   (e) $\{1, i, -1, -i\}$.
3. Let G_1 and G_2 be two groups. Let e_1 and e_2 be the identity elements of G_1 and G_2 respectively. Let $G_1 \times G_2$ be the direct product of these groups. Let $H = \{(e_1, y)/y \in G_2\}$ and $K = \{(x, e_2)/x \in G_1\}$. Show that H and K are subgroups of $G_1 \times G_2$.
4. Prove that $H = \{(1, b)/b \in \mathbf{R}\}$ is a subgroup of the group G given in example 26 of 3.1.

5. Let G be a group and let H be the centre of G. Show that $H = G$ iff G is abelian.
6. Show that the centre of S_3 is $\{e\}$.

   (Hint. For each $a \in S_3$ and $a \neq e$, find another element $b \in S_3$ such that $ab \neq ba$).
7. Show that a proper subgroup of a non-abelian group can be abelian.

   (Hint. Consider any proper subgroup of S_3).
8. Show that any subgroup of an abelian group is abelian.
9. Let S and N be subgroups of G such that $S \cap N = \{e\}$ and $S \cup N = G$. Prove that either $S = G$ or $N = G$.
10. Find as many subgroups as you can in

    (a) V_4 (b) the group of symmetries of a square

    (c) $\mathbf{Z}_6$ (d) $\mathbf{Z}$

3.6. Cyclic Groups

Definition. Let G be a group. Let $a \in G$.

Then $H = \{a^n / n \in \mathbf{Z}\}$ is a subgroup of G (verify). H is called the **cyclic subgroup of G generated by** a and is denoted by $\langle a \rangle$.

Examples

1. In $(\mathbf{Z}, +)$, $\langle 2 \rangle = 2\mathbf{Z}$ which is the group of even integers.
2. In the group $G = (\mathbf{Z}_{12}, \oplus)$, $\langle 3 \rangle = \{0, 3, 6, 9\}$. $\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbf{Z}_{12}$.
3. In the group $G = \{1, i - 1, -i\}$. $\langle i \rangle = \{i, i^2, i^3 \ldots\} = \{i, -1, -i, 1\} = G$.

Definition. Let G be a group and let $a \in G$. a is called a **generator** of G if $\langle a \rangle = G$.

A group G is **cyclic** if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Note. If G is a cyclic group generated by an element a, then every element of G is of the form a^n for some $n \in \mathbf{Z}$.

Examples

1. $(\mathbf{Z}, +)$ is a cyclic group. 1 is a generator of this group. -1 is also a generator of this group. Thus a cyclic group can have more than one generator.
2. $(n\mathbf{Z}, +)$ is a cyclic group. n and $-n$ are generators of this group.
3. $(\mathbf{Z}_8, \oplus)$ is a cyclic group. 1, 3, 5, 7 are all generators of this group.
4. $(\mathbf{Z}_n, \oplus)$ is a cyclic group for all $n \in \mathbf{N}$; 1 is a generator of this group. In fact if $m \in \mathbf{Z}_n$ and $(m, n) = 1$ then m is a generator of this group.
5. $G = \{1, i, -1, -i\}$ is a cyclic group under usual multiplication; i is a generator, $-i$ is also a generator of G. However -1 is not a generator of G since $\langle -1 \rangle = \{1, -1\} \neq G$.
6. $G = \{1, \omega, \omega^2\}$ where $\omega \neq 1$ is a cube root of unity is a cyclic group. ω and ω^2 are both generators of this group.
7. In the group $G = (\mathbf{Z}_7, -\{0\}, \odot)$, 3 and 5 are both generators. Here 2 is not a generator of G since $\langle 2 \rangle = \{2, 4, 1\} \neq G$.
8. Let A be a set containing more than one element. Then $(\wp(A), \Delta)$ is not cyclic; for let $B \in \wp(A)$ be any element. Then $B \Delta B = \Phi$ so that $\langle B \rangle = \{B, \Phi\} \neq \wp(A)$.
9. $(\mathbf{R}, +)$ is not a cyclic group since for any $x \in \mathbf{R}$, $\langle x \rangle = \{nx / n \in \mathbf{Z}\} \neq \mathbf{R}$.

Exercises

Determine which of the following groups are cyclic. If it is cyclic find all the generators of the group.

1. $(6\mathbf{Z}, +)$. 2. $(\mathbf{Q}, +)$.
3. The set of all n^{th} roots of unity under multiplication.
4. The group of symmetries of an equilateral triangle.
5. The group of symmetries of a rectangle.

6. The group of symmetries of a square.
7. $\{2^n / n \in \mathbf{Z}\}$ under usual multiplication.
8. $(\mathbf{Z}_4, \oplus)$ 9. $(\mathbf{R}^*, \cdot)$
10. $(\mathbf{Z}_{11} - \{0\}, \odot)$
11. $G = \{e, p_1, p_2, p_3, p_4\}$ where

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

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \text{ and}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Answers.

1, 3, 7, 8, 10 and 11 are cyclic.

Theorem 3.22. Any cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group.

Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbf{Z}$.

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

$\therefore$ G is abelian.

Theorem 3.23. A subgroup of cyclic group is cyclic.

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

Clearly every element of H is of the form a^n for some integer n.

Let m be the smallest positive integer such that $a^m \in H$. We claim that a^m is a generator of H.

Let $b \in H$. Then $b = a^n$ for some $n \in \mathbf{Z}$.

Let $n = mq + r$ where $0 \leq r < m$.

Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$.

$$\therefore \quad a^r = (a^m)^{-q} b. \qquad \ldots (1)$$

Now, $a^m \in H$. Since H is a subgroup, $(a^m)^{-q} \in H$.

Also $b \in H$.

By (1), $a^r \in H$ and $0 \leq r < m$.

But m is the least positive integer such that $a^n \in H$.

$\therefore$ $r = 0$. Hence $b = a^n = a^{qm} = (a^m)^q$.

$\therefore$ Every element of H is a power of a^m.

$\therefore$ $H = \langle a^m \rangle$ and hence H is cyclic

Exercises

1. Prove that if a is a generator of a cyclic group G then a^{-1} is also a generator of G.
2. Prove that any subgroup of $(\mathbf{Z}, +)$ is of the form $n\mathbf{Z}$ for some integer n.
3. Find the number of elements in the following cyclic subgroups.
   (a) $\langle 2 \rangle$ in $(\mathbf{Z}_{18}, \oplus)$ (b) $\langle 18 \rangle$ in $(\mathbf{Z}_{30}, \oplus)$
   (c) $\langle 5 \rangle$ in $(\mathbf{Z}_{80}, \oplus)$ (d) $\langle i \rangle$ in $\mathbf{C}^*$
4. Show that every proper subgroup of V_4 is cyclic. (However V_4 is not cyclic).
5. Show that every proper subgroup of S_3 is cyclic.
6. Give the multiplication table for the cyclic subgroup of S_5 generated by

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

7. Determine which of the following statements are true and which are false.
   (a) For any fixed integer n, $\{kn + 1/k \in \mathbf{Z}\}$ is a subgroup of $(\mathbf{Z}, +)$.
   (b) Every cyclic group is abelian.
   (c) Every abelian group is cyclic.
   (d) Every element of a cyclic group is a generator of the group.
   (e) $(\mathbf{Z}, +)$ is a cyclic group.
   (f) $(\mathbf{Q}, +)$ is a cyclic group.
   (g) S_3 is a cyclic group.
   (h) A_3 is a cyclic group.
   (i) $(\mathbf{Z}_n, \oplus)$ is a cyclic group.
   (j) $(\mathbf{Z}_n, -\{0\}, \odot)$ is a cyclic group.

(k) Any group of order 3 is cyclic.

(l) Any group of order 4 is cyclic.

(m) Given any positive integer n, there exists a cyclic group with n elements.

(n) Every group has cyclic subgroups.

(o) Every subgroup of a cyclic group is cyclic.

(p) If every proper subgroup of a group G is cyclic then G is cyclic.

(q) Every cyclic group has more than one generator.

Answers.

3. (a) 9 (b) 5 (c) 16 (d) 4

7. (b), (e), (h), (i), (k), (m), (n) and (o) are true.

3.7. Order of an Element

1. Consider the group S_3 given in 3.4

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$p_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_2.$$

$$p_1^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

In this case 3 is the least positive integer such that $p_1^3 = e$. Also $\langle p_1 \rangle = \{e, p_1, p_2\}$ is a subgroup of S_3 of order 3.

2. Consider $(\mathbf{R}^*, \cdot)$. From the sequence of elements $2, 2^2, 2^3, \ldots 2^n, \ldots\ldots$ In this case there is no positive integer n such that $2^n = 1$ and $\langle 2 \rangle$ contains infinite numbers of elements.

Definition. Let G be a group and let $a \in G$. The least positive integer n (if it exists) such that $a^n = e$ is called the **order** of a. If there is no positive integer n such that $a^n = e$, then the order of a is said to be infinite.

In example 1, p_1 is of order 3 and 2 is of infinite order in example 2.

In $(\mathbf{C}^*, \cdot)$, i is an element of order 4.

Exercises

1. Show that in any group G, e is the only element of order 1.
2. Find the order of -1 and 3 in $(\mathbf{Z}, +)$.
3. Find the order of -1 and 3 in $(\mathbf{R}^*, \cdot)$.
4. Find the order of -1 and $-i$ in $(\mathbf{C}^*, \cdot)$.
5. Find the order of 2 and 3 in $(\mathbf{Z}_8, \oplus)$.
6. Show that in V_4 the order of every element other than the identity is 2.
7. Show that in $(\mathbf{Z}, +)$ the order of every element other than 0 is infinite.
8. Show that in $(\wp(S), \Delta)$ the order of every element other than Φ is 2.
9. Show that in $(\mathbf{C}^*, \cdot)$ for every positive integer n there exists an element of order n.

Answers.

2. infinite
3. order of -1 is 2 and order of 3 is infinite.
4. order of -1 is 2 and order of $-i$ is 4.
5. order of 2 is 4 and order of 3 is 8.

Theorem 3.24. Let G be a group and $a \in G$. Then the order of a is the same as the order of the cyclic group generated by a.

Proof. Let a be an element of order n. Then $a^n = e$. We claim that $e, a, a^2, \ldots, a^{n-1}$ are all distinct.

Suppose $a^r = a^s$ where $0 < r < s < n$.

Then $a^{s-r} = e$ and $s - r < n$ which contradicts the definition of the order of a. Hence $e, a, a^2, \ldots, a^{n-1}$ are n distinct elements and $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ which is of order n.

If a is of infinite order, the sequence of elements $a, a^2, \ldots, a^n, \ldots$ are all distinct and are in $\langle a \rangle$. Hence $\langle a \rangle$ is an infinite group.

Theorem 3.25. In a finite group every element is of finite order.

Proof. Let $a \in G$. If a is of infinite order, then $\langle a \rangle$ is an infinite subgroup of G, which is a contradiction since G is finite. Hence the order of a is finite.

Remark. The converse of the above theorem is not true. (ie) if G is a group in which every element is of finite order then the group G need not be finite. For example, if S is any infinite set, then $(\wp(S), \Delta)$ is an infinite group. In this group $A \Delta A = \Phi$ for every $A \in \wp(S)$ so that the order of every element other than Φ is 2.

Theorem 3.26. Let G be a group and a be an element of order n in G. Then $a^m = e$ iff n divides m.

Proof. Suppose $n|m$. Then $m = nq$ where $q \in \mathbf{Z}$.

$\therefore \quad a^m = a^{nq} = (a^n)^q = e^q = e.$

Conversely, let $a^m = e$.

Let $m = nq + r$ where $0 \leq r < n$.

$\therefore \quad a^m = a^{nq+r} = a^{nq} a^r = e a^r = a^r.$

$\therefore \quad a^r = e$ and $0 \leq r < n$.

Now, since n is the smallest positive integer such that $a^n = e$, we have $r = 0$. Hence $m = nq$.

Therefore $n|m$.

Theorem 3.27. Let G be a group and $a, b \in G$.

Then

(i) order of a = order of a^{-1}.

(ii) order of a = order of $b^{-1}ab$.

(iii) order of ab = order of ba.

Proof. **(i)** Let a be an element of order n.

Then $a^n = e$.

$\therefore \quad (a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$

Now, if possible let $0 < m < n$ and $(a^{-1})^m = e$.

$\therefore \quad (a^m)^{-1} = e$. Hence $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(a^{-1})^n = e$.

$\therefore$ The order of a^{-1} is n.

(ii) We shall first prove that for any positive integer r.

$$(b^{-1}ab)^r = b^{-1}a^r b. \qquad \ldots (1)$$

(1) is trivialy true if $r = 1$,

Now, suppose that (1) is true for $r = k$ so that $(b^{-1}ab)^k = b^{-1}a^k b$.

Then

$$\begin{aligned}(b^{-1}ab)^{k+1} &= (b^{-1}ab)^k (b^{-1}ab). \\ &= (b^{-1}a^k b)(b^{-1}ab). \\ &= b^{-1}a^{k+1}b.\end{aligned}$$

Hence by induction (1) is true for all positive integers.

Now, let a be an element of order n. Then $a^n = e$.

$$\begin{aligned}\therefore \quad (b^{-1}ab)^n &= b^{-1}a^n b \quad \text{(by (1))} \\ &= b^{-1}eb = e.\end{aligned}$$

Now, if possible, let $0 < m < n$ and $(b^{-1}ab)^m = e$.

$\therefore \quad b^{-1}a^m b = e$. Hence $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(b^{-1}ab)^n = e$.

$\therefore$ The order of $b^{-1}ab$ is n.

(iii)

$$\begin{aligned}\text{The order of } ab &= \text{the order of } a^{-1}(ab)\, a \text{ (by (ii))} \\ &= \text{the order of } ba.\end{aligned}$$

Theorem 3.28. Let G be a group and let a be an element of order n in G. Then the order of a^s, where $0 < s < n$, is n/d where d is the g.c.d of n and s.

Proof. Let $(n/d) = k$ and $(s/d) = l$ so that k and l are relatively prime.

Now, $(a^s)^k = a^{sk} = a^{ldk} = a^{ln} = (a^n)^l = e$.

Further if m is any positive integer such that $(a^s)^m = e$ then $a^{sm} = e$.

Since order of a is n, we have $n|sm$.

$\therefore \quad kd|ldm$. Hence $k|lm$

But k and l are relatively prime.

Hence k/m so that $m \geq k$.

Thus k is the least positive integer such that $(a^s)^k = e$.

$\therefore$ order of $a^s = k = n/d$.

Corollary 1. The order of any power of a cannot exceed the order of a.

Corollary 2. Let G be a finite cyclic group of order n generated by an element a. Then a^s generates a cyclic group of order n/d where d is the g.c.d of n and s.

Corollary 3. Let G be a finite cyclic group of order n generated by an element a. a^s is a generator of G iff s and n are relatively prime. *Hence the number of generators of a cyclic group of order n is* $\phi(n)$ where $\phi(n)$ is the number of positive integers less than n and relatively prime to n.

For example, consider the group $(\mathbf{Z}_{12}, \oplus)$.

$\phi(12) = 4$. Hence the group has exactly 4 generators and they are 1, 5, 7 and 11.

Solved Problems

Problem 1. If G is a finite group with even number of elements then G contains at least one element of order 2.

Solution. a is an element of order 2 $\Leftrightarrow a^2 = e$

$\Leftrightarrow a^{-1} = a$.

Hence it is enough if we prove that there exists an element different from e in G whose inverse is itself.

Let $S = \{a/a \in G, a \neq a^{-1}\}$.

Clearly $a \in S \Rightarrow a^{-1} \in S$ and $a \neq a^{-1}$.

Hence S contains an even number of elements.

Also $e \notin S$.

Hence $S \cup \{e\}$ contains an odd number of elements. Since the order of the group is even, there exists at least one element $a \notin S \cup \{e\}$. Clearly $a = a^{-1}$.

Problem 2. The order of a permutation p is the *l.c.m.* of the lengths if its disjoint cycles.

Solution. Let $p = c_1 c_2 \ldots, c_r$ where the c_i's are mutually disjoint cycles of lengths l_i. Now, let $p^m = e$.

Since product of disjoint cycles is commutative, $e = p^m = (c_1 c_2 \ldots c_r)^m = {c_1}^m c_2^m \ldots c_r^m$.

Now, since the elements moved by one cycle are left fixed by all the other cycles, $c_1^m = c_2^m = \ldots, c_r^m = e$.

Now, $c_1^m = e \Rightarrow l_1 | m$ since the order of $c_1 = l_1$.

Similarly $l_2, l_3, \ldots, l_r$ divide m.

Thus m is a common multiple of $l_1, l_2, \ldots, l_r$.

$\therefore$ The order of p is the least such m which is obviously the *l.c.m* of $l_1, l_2, \ldots, l_r$.

Problem 3. If a is a generator of the cyclic group G and if there exist two unequal integers m and n such that $a^m = a^n$, prove that G is a finite group.

Solution. Since m and n are unequal we may assume that $m > n$.

Hence $m - n$ is a positive integer.

Also $a^m = a^n \Rightarrow a^{m-n} = e$.

$\therefore$ Order of a is finite.

$\therefore$ $G = \langle a \rangle$ is a finite group (by theorem 3.24)

Exercises

1. Show that a group G of order n is cyclic iff G contains an element of order n.
2. Find the number of generators of the cyclic groups of orders 8, 24 and 60.
3. Let p and q be prime numbers. Find the number of generators of Z_{pq}.
4. Find the number of generators of Z_p, where p is prime.
5. Find two elements a, b in a group such that
   (a) order of $ab \neq$ (order of a) (order of b).
   (b) order of $ab =$ (order of a) (order of b).
6. Find the order of the following permutations.
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$
   (c) (12345) (67) (1657)
   (d) (12) (23) (345) (1456).
7. Find all the elements of finite order in the following groups.
   (a) $(\mathbf{Z}, +)$

(b) $(\mathbf{R}^*, .)$

(c) $(\wp(S), \Delta)$

8. Determine which of the following are true and which are false.

   (a) In a finite group the order of every element is finite.

   (b) If in a group every element is of finite order then the group is finite.

   (c) In an infinite group the order of every element is infinite.

   (d) The order of e is zero.

   (e) The order of every element of $(\mathbf{R}^*, .)$ is finite.

Answers.

2. 4, 8 and 16.
6. (a) 4 (b) 4 (c) 7 (d) 6
7. (a) 0 (b) 1 and -1 (c) All elements.
8. (a) T (b) F (c) F (d) F (e) F

3.8. Cosets and Lagrange's Theorem

Consider S_3. Let $H = \{e, p_3\}$. H is a subgroup of S_3. This subgroup does not contain the elements p_1, p_2, p_4 and p_5. Let us now perform the binary operation between p_1 and each element of H. We denote the resultant set by the symbol $p_1 H$.

Thus $p_1 H = \{p_1 e, p_1 p_3\} = \{p_1, p_4\}$.

Now, the element p_2 belongs neither to H nor to $p_1 H$. Therefore, we now perform the binary operation between p_2 and the elements of H.

Thus $p_2 H = \{p_2 e, p_2 p_3\} = \{p_2, p_5\}$. The union of the three sets H, $p_1 H$, $p_2 H$ gives all the elements of S_3 (ie) $S_3 = H \cup p_1 H \cup p_2 H$. Further H, $p_1 H$ and $p_2 H$ are mutually disjoint. Hence $\{H, p_1 H, p_2 H\}$ is a partition of S_3.

Definition. Let H be a subgroup of a group G. Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called the **left coset** of H defined by a in G.

Similarly $Ha = \{ha / h \in H\}$ is called the **right coset** of H defined by a.

Examples.

1. Let us determine the left cosets of $(5\mathbf{Z}, +)$ in $(\mathbf{Z}, +)$. Here the operation is $+$.
   $0 + 5\mathbf{Z} = 5\mathbf{Z}$ is itself a left coset.
   Another left coset is $1 + 5\mathbf{Z} = \{1 + 5n / n \in \mathbf{Z}\}$. We notice that this left coset contains all integers having remainder 1 when divided by 5.
   Similarly

   $$2 + 5\mathbf{Z} = \{2 + 5n / n \in \mathbf{Z}\}$$
   $$3 + 5\mathbf{Z} = \{3 + 5n / n \in \mathbf{Z}\}.$$
   and $$4 + 5\mathbf{Z} = \{4 + 5n / n \in \mathbf{Z}\}.$$

   These are all the left cosets of $(5\mathbf{Z}, +)$. Here also we note that all the left cosets are mutually disjoint, and their union is $\mathbf{Z}$. In other words the collection of all left cosets forms a partition of the group.

2. Consider $(\mathbf{Z}_{12}, \oplus)$. Then $H = \{0, 4, 8\}$ is a subgroup of G.
   The left cosets of H are given by

   $$0 + H = \{0, 4, 8\} = H$$
   $$1 + H = \{1, 5, 9\}$$
   $$2 + H = \{2, 6, 10\}$$
   and $$3 + H = \{3, 7, 11\}$$

   We notice that

   $$4 + H = \{4, 8, 0\} = H \quad \text{and}$$
   $$5 + H = \{5, 9, 1\} = 1 + H \quad \text{etc.}$$

Exercises.

1. Find all the left cosets of $(n\mathbf{Z}, +)$ in $(\mathbf{Z}, +)$.
2. Find all the left cosets of $\{0, 3, 6, 9\}$ in $(\mathbf{Z}_{12}, \oplus)$.
3. Find all the left cosets of $\{1, 6\}$ in $(\mathbf{Z}_7 - \{0\}, \odot)$.

Theorem 3.29. Let G be a group and H be a subgroup of G. Then

(i) $a \in H \Rightarrow aH = H$

(ii) $aH = bH \Rightarrow a^{-1}b \in H$.

(iii) $a \in bH \Rightarrow a^{-1} \in Hb^{-1}$.

(iv) $a \in bH \Rightarrow aH = bH$.

Proof.

(i) Let $a \in H$. We claim that $aH = H$.

Let $x \in aH$. Then $x = ah$ for some $h \in H$.

Now, $a \in H$ and $h \in H \Rightarrow ah = x \in H$ (since H is a subgroup).

Hence $aH \subseteq H$.

Let $x \in H$. Then $x = a(a^{-1}x) \in aH$.

Hence $H \subseteq aH$. Thus $H = aH$.

Conversely, let $aH = H$. Now $a = ae \in aH$.

$\therefore \quad a \in H$.

(ii) Let $aH = bH$.

$\therefore \quad a^{-1}(aH) = a^{-1}(bH)$.

$\therefore \quad H = (a^{-1}b)H$.

$\therefore \quad a^{-1}b \in H$ (by i).

Conversely let $a^{-1}b \in H$.

Then $a^{-1}bH = H$ (by i).

$\therefore \quad aa^{-1}bH = aH$ and hence $bH = aH$.

(iii) Let $a \in bH$. Then $a = bh$ for some $h \in H$.

$\therefore \quad a^{-1} = (bh)^{-1} = h^{-1}b^{-1} \in Hb^{-1}$.

Converse can be similarly proved.

(iv) Let $a \in bH$. We claim that $aH = bH$.

Let $x \in aH$. Then $x = ah_1$ for some $h_1 \in H$.

Also

$a \in bH \Rightarrow a = bh_2$ for some $h_2 \in H$. . . . (1)

$\therefore \quad x = (bh_2)h_1) = b(h_2h_1) \in bH$.

$\therefore \quad aH \subseteq bH$.

Now, let $x \in bH$. Then $x = bh_3$ for some $h_3 \in H$.

Also from (1), $b = ah_2^{-1}$.

$\therefore \quad x = ah_2^{-1}h_3 \in aH$.

$\therefore \quad bH \subseteq aH$. Hence $aH = bH$.

Conversely, let $aH = bH$.

Then $a = ae \in aH$.

$\therefore \quad a \in bH$.

Theorem 3.30. Let H be a subgroup of G. Then

(i) any two left cosets of H are either identical or disjoint.

(ii) union of all the left cosets of H is G.

(iii) the number of elements in any left coset aH is the same as the number of elements in H.

Proof.

(i) Let aH and bH be two left cosets.

Suppose aH and bH are not disjoint.

We claim that $aH = bH$.

Since aH and bH are not disjoint;

$aH \cap bH \neq \Phi$.

$\therefore \quad$ There exists an element $c \in aH \cap bH$.

$\therefore \quad c \in aH$ and $c \in bH$.

$\therefore \quad aH = cH$ and $bH = cH$ (by (iv) of Theorem 3.29).

$\therefore \quad aH = bH$.

(ii) Let $a \in G$. Then $a = ae \in aH$.

$\therefore \quad$ Every element of G belongs to a left coset of H.

$\therefore \quad$ The union of all the left cosets of H is G.

(iii) The map $f : H \to aH$ defined by $f(h) = ah$ is clearly a bijection. Hence every left coset has the same number of elements as H.

Note 1. This theorem shows that the collection of all left cosets forms a partition of the group.

Note 2. The above result is true if we replace left cosets by right cosets. In what follows, the results we prove for left cosets are also true for right cosets.

Remark. Let H be a subgroup of G. We define a relation in G as follows. Define $a \sim b \Leftrightarrow a^{-1}b \in H$.

Then $\sim$ is an equivalence relation.

For, $a^{-1}a = e \in H$. Hence $a \sim a$.

Hence $\sim$ is reflexive.

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H.$$
$$\Rightarrow b^{-1}a \in H \Rightarrow b \sim a.$$
$$\therefore \quad a \sim b \Rightarrow b \sim a.$$

Hence $\sim$ is symmetric.

Now,

$$a \sim b \text{ and } b \sim c \Rightarrow a^{-1}b \in H \text{ and } b^{-1}c \in H$$
$$\Rightarrow (a^{-1}b)(b^{-1}c) \in H$$
$$\Rightarrow a^{-1}c \in H$$
$$\Rightarrow a \sim c.$$

Hence $\sim$ is transitive.

Thus $\sim$ is an equivalence relation.

Now, we claim that equivalence class $[a] = aH$.

Let $b \in [a]$. Then $b \sim a$.

$\therefore \quad a^{-1}b \in H.$

$\therefore \quad a^{-1}b = h$ for some $h \in H$.

$\therefore \quad b = ah$. Hence $b \in aH$.

$\therefore \quad [a] \subseteq aH$.

Also,

$$b \in aH \Rightarrow b = ah \quad \text{for some} \quad h \in H.$$
$$\Rightarrow a^{-1}b = h \in H.$$
$$\Rightarrow a \sim b$$
$$\Rightarrow b \in [a].$$

Thus the left cosets of H in G are precisely the equivalence classes determined by $\sim$. Hence the left cosets form a partition of G. This gives another proof of Theorem 3.30.

Theorem 3.31. Let H be a subgroup of G. The number of left cosets of H is the same as the number of right cosets of H.

Proof. Let L and R respectively denote the set of left and right cosets of H. We define a map $f : L \to R$ by $f(aH) = Ha^{-1}$.

f is well defined. For $aH = bH. \Rightarrow a^{-1}b \in H$
$$\Rightarrow a^{-1} \in Hb^{-1}$$
$$\Rightarrow Ha^{-1} = Hb^{-1}$$

f *is* $1-1$. For,

$$f(aH) = f(bH)$$
$$\Rightarrow Ha^{-1} = Hb^{-1}$$
$$\Rightarrow a^{-1} \in Hb^{-1}$$
$$\Rightarrow a^{-1} = hb^{-1} \text{ for some } h \in H.$$
$$\Rightarrow a = bh^{-1}$$
$$\Rightarrow a \in bH$$
$$\Rightarrow aH = bH.$$

f *is onto*. For, every right coset Ha has a pre-image under f namely $a^{-1}H$.

Hence f is a bijection from L to R. Hence the number of left cosets is the same as the number of right cosets.

Definition. Let H be a subgroup of G. The number of distinct left (right) cosets of H in G is called the **index** of H in G and is denoted by $[G : H]$.

Example. In $(\mathbf{Z}_8, \oplus)$, $H = \{0, 4\}$ is a subgroup. The left cosets of H are given by

$$0 + H = \{0, 4\} = H$$
$$1 + H = \{1, 5\}.$$
$$2 + H = \{2, 6\}.$$
$$3 + H = \{3, 7\}.$$

These are the four distinct left cosets of H.

Hence the index of the subgroup H is 4.

Note that $[\mathbf{Z}_8 : H] \times |H| = 4 \times 2 = 8 = |\mathbf{Z}_8|$.