UNIT 3 SUBGROUPS

Structure

3.1 INTRODUCTION

You have studied the algebraic structures of integers, rational numbers, real numbers and, finally, complex numbers. You have noticed that, not only is $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, but the operations of addition and multiplication coincide in these sets.

In this unit you will study more examples of subsets of groups which are groups in their own right. Such structures are rightfully named subgroups. In Sec. 3.3 we will discuss some of their properties also.

In Sec. 3.4 we will see some cases in which we obtain a group from a few elements of the group. In particular, we will study cases of groups that can be built up by a single element of the group.

Do study this unit carefully because it consists of basic concepts which will be used again and again in the rest of the course.

Objectives

After reading this unit, you should be able to

- define subgroups and check if a subset of a given group is a subgroup or not;
- check if the intersection, union and product of two subgroups is a subgroup;
- describe t h structure and properties of cyclic groups.

3.2 SUBGROUPS

You may have already noted that the groups $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ and $(\mathbb{R},+)$ are contained in the bigger group $(\mathbb{C},+)$ of complex numbers, not just as subsets but as groups. Ail these are examples of subgroups, as you will see.

Definition : Let $(G,*)$ be a group. A non-empty subset H of G is called a **subgroup** of G if

i) $a * b \in H \ \forall\, a, b \in H$, i.e., $*$ is a binary operation on H,

ii) $(H,*)$ is itself a group.

So, by definition, $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$.

Now, if $(H, *)$ is a subgroup of $(G,*)$, can the identity element in $(H,*)$ be different from the identity element in $(G,*)$? Let us see. If h is the identity of $(H,*)$, then, for any $a \in H$, $h * a = a * h = a$. However, $a \in H \subseteq G$. Thus, $a * e = e * a = a$, where e is the identity in G. Therefore, $h * a = e * a$.

By right cancellation in $(G,*)$, we get $h = e$.

Thus, whenever $(H, *)$ is a subgroup of $(G,*)$, $e \in H$.

Now you may like to try the following exercise.

E 1) If $(H, *)$ is a subgroup of $(G,*)$, does $a^{-1} \in H$ for every $a \in H$?

E 1 and the discussion before it allows us to make the following remark.

Remark 1: $(H,*)$ is a subgroup of $(G, *)$ if and only if

i) $e \in H$,

ii) $a, b \in H \Rightarrow a * b \in H$,

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

We would also like to make an important remark about notation here.

Remark 2 : If $(H,*)$ is a subgroup of $(G,*)$, **we shall** just **say that H is a subgroup of *G*,** provided that there is no confusion about the binary operations. We will also denote this fact by $H \leq G$.

Now we discuss an important necessary and sufficient condition for a subset to be a subgroup.

Theorem 1 : Let H be a **non-empty** subset of a group G. Then H is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof : Firstly, let us assume that $H \leq G$. Then, by Remark 1, $a, b \in H \Rightarrow a, b^{-1} \in H$ $\Rightarrow ab^{-1} \in H$.

Conversely, since $H \neq \phi$, $\exists\, a \in H$. But then, $aa^{-1} = e \in H$.

Again, for any $a \in H$, $ea^{-1} = a^{-1} \in H$.

Finally, if $a, b \in H$, then $a, b^{-1} \in H$. Thus, $a\,(b^{-1})^{-1} = ab \in H$, i.e.,

H is closed under the binary operation of the group.

Therefore, by Remark 1, H is a subgroup.

Let us look at some examples of subgroups now. While going through these you may realise the fact that **a subgroup of an abelian group is abelian.**

Example 1 : Consider the group $(C^*, .)$. Show that

$S = \{ z \in C \mid |z| = 1 \}$ is a subgroup of C^*.

Solution : $S \neq \phi$, since $1 \in S$. Also, for any $z_1, z_2 \in S$,

$$\left|z_1 z_2^{-1}\right| = \left|z_1\right| \left|z_2^{-1}\right| = \left|z_1\right| \frac{1}{\left|z_2\right|} = 1.$$

Hence, $z_1 z_2^{-1} \in S$. Therefore, by Theorem 1, $S \leq C^*$.

Example 2: Consider $G = M_{2\times 3}(C)$, the set of all 2 x 3 matrices over C. Check that $(G,+)$ is an abelian group. Show that

$$S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \middle| \; a, b, c \in C \right\} \text{ is a subgroup of G.}$$

Solution : We define addition on *G* by

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} p & q & r \\ s & t & u \end{bmatrix} = \begin{bmatrix} a+p & b+q & c+r \\ d+s & e+t & f+u \end{bmatrix}.$$

You can see that + is a binary operation on *G*. $O = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is the additive identity and

$\begin{bmatrix} -a & -c \\ -d & -f \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \in G$.

Since, $a + b = b + a \;\forall\; a, b \in C$, + is also abelian.

Therefore, $(G,+)$ is an abelian group.

$H \leq (G,+) \Leftrightarrow$
$H \neq \phi$ and
$a - b \in H \; \forall \; a, b \in H.$

Now, since $O \in S$, $S \neq \phi$. Also. for

$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & & \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & & \end{bmatrix} \in$ S, we see that

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} - \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \blacksquare S.$$

$\therefore$ S I G.

Example 3 : Consider the set of all invertible 3×3 matrices over $\mathbf{R}$, $GL_3(R)$. That is, $A \in GL_3(\mathbf{R})$ iff det (A) $\neq 0$. Show that $SL_3(R) = (A \in GL_3(\mathbf{R}) \mid \det(A) = I)$ is a subgroup of $(GL_3(\mathbf{R}),.)$.

Solution : The 3x3 identity matrix is in $SL_3(\mathbf{R})$. Therefore, $SL_3(\mathbf{R}) \neq \phi$.
Now, for A, B $\in SL_3(\mathbf{R})$,

det (AB^{-1}) = det (A) $\det(B^{-1})$ = det (A) $\frac{1}{\det(B)}$ = 1, since det (A) = 1 and det (B) =I.

$\therefore$ $AB^{-1} \in SL_3(\mathbf{R})$
$\therefore$ $SL_3(\mathbf{R})$ I $GL_3(\mathbf{R})$.
Try the following exercise now.

E 2) Show that for any group G, {e} arid G are subgroups of G.
((e) is called the trivial subgroup.)

The next example is very important, and you may use it quite often.

Example 4 : Any non-trivial subgroup of $(\mathbf{Z}, +)$ is of the form $m\mathbf{Z}$, where $m \in N$ and $m\mathbf{Z} = \{ mt \mid t \in Z \} = \{ 0, \pm m, \pm 2m, \pm 3m, \ldots\ldots \}$.

Solution : We will first show that $m\mathbf{Z}$ is a subgroup of Z. Then we will show that if H is a subgroup of Z, $H \neq \{0\}$, then $H = m\mathbf{Z}$, for some $m \in N$.

Now, $0 \in m\mathbf{Z}$. Therefore, $m\mathbf{Z} \neq \phi$. Also, for mr, $ms \in m\mathbf{Z}$, mr–ms = m(r–s) $\in m\mathbf{Z}$. Therefore, $m\mathbf{Z}$ is a subgroup of Z.

Note that m is the least **positive integer in** $m\mathbf{Z}$.

Now, let $H \neq \{0\}$ be a subgroup of Z and $S = \{ i \mid i > 0, i \in H \}$.

Since H # {0), there is a non-zero integer k in H. If $k > 0$, then $k \in$ S. If $k < 0$, then $(-k) \in$ S, since $(-k) \in$ H and $(-k) > 0$.

Hence, $S \neq \phi$.

Clearly, $S \subseteq N$. Thus, by the well-ordering principle (Sec. I.6.1) S has a least element, say s. That is, s is the least positive integer that belongs to H.

Now $s\mathbf{Z} \subseteq$ H . Why ? Well, consider any element $st \in s\mathbf{Z}$.
If t = 0, then $st = 0 \in$ H.
If $t > 0$, then st = s + s + ... + s (t times) $\in$ H.
If $t < 0$, then st = (–s) + (–s) + ...+ (–s) (–t times) $\in$ H.

Therefore, $st \in H \; \forall \; t \in Z$. That is, $s\mathbf{Z} \subseteq$ H.

Now, let $m \in$ H. By the division algorithm (see Sec. 1.6.2), m = ns + r for some n, $r \in Z$, $0 \leq r <$ s. Thus, r = m – ns. But H is a subgroup of Z and m, $ns \in$ H. Thus, r $\in$ H. By **minimality** of s in S, we must have $r = 0$, **i.e.**, m = ns. Thus, $H \subseteq s\mathbf{Z}$.

So we have proved that $H = s\mathbf{Z}$.

Before going to the next example, let us see what the nth roots of unity are, that is, for which complex numbers z is $z^n = 1$.

From the appendix to Unit 2, you know that the polar form of a non-zero complex number $z \in \mathbb{C}$ is $z = r(\cos\theta + i \sin\theta)$, where $r = |z|$ and θ is an argument of z. Moreover, if θ_1 is an argument of z_1 and θ_2 that of z_2, then $\theta_1 + \theta_2$ is an argument of $z_1 z_2$. Using this we will try to find the nth roots of 1, where $n \in N$.

If $z = r(\cos\theta + i \sin\theta)$ is an nth root of 1, then $z^n = 1$.

Thus, by De Moivre's theorem,

$1 = z^n = r^n (\cos n\theta + i \sin n\theta)$, that is,

$\cos(0) + i \sin(0) = r^n (\cos n\theta + i \sin n\theta)$. ..... (1)

Equating the modulus of both the sides of (1), we get $r^n = 1$, i.e., $r = 1$.

On comparing the arguments of both sides of (1), we see that $0 + 2nk$ ($k \in Z$) and $n\theta$ are arguments of the same complex number. Thus, $n\theta$ can take any one of the values $2\pi k$, $k \in Z$. Does this mean that as k ranges over Z and θ ranges over $\frac{2nk}{n}$ we get distinct nth roots of 1? Let us find out. Now, $\cos\frac{2nk}{n} + i \sin\frac{2\pi k}{n} = \cos\frac{2\pi m}{n} + i \sin\frac{2\pi m}{n}$ if and only if $\frac{2nk}{n} - \frac{2nm}{n} = 2nt$ for some $t \in Z$. This will happen iff $k = m + nt$, i.e., $k \equiv m \pmod n$. Thus, corresponding to every r in Z, we get an nth root of unity, $z = \cos\frac{2\pi r}{n} + i \sin\frac{2\pi r}{n}$, $0 \le r < n$; and these are all the nth roots of unity.

For example, if $n = 6$, we get the 6th roots of 1 as z_0, z_1, z_2, z_3, z_4 and z_5, where $z_j = \cos\frac{2\pi j}{6} + i \sin\frac{2\pi j}{6}$, $j = 0, 1, 2, 3, 4, 5$. In Fig. 1 you can see that all these lie on the unit circle (i.e., the circle of radius one with centre (0,0)). They form the vertices of a regular hexagon.

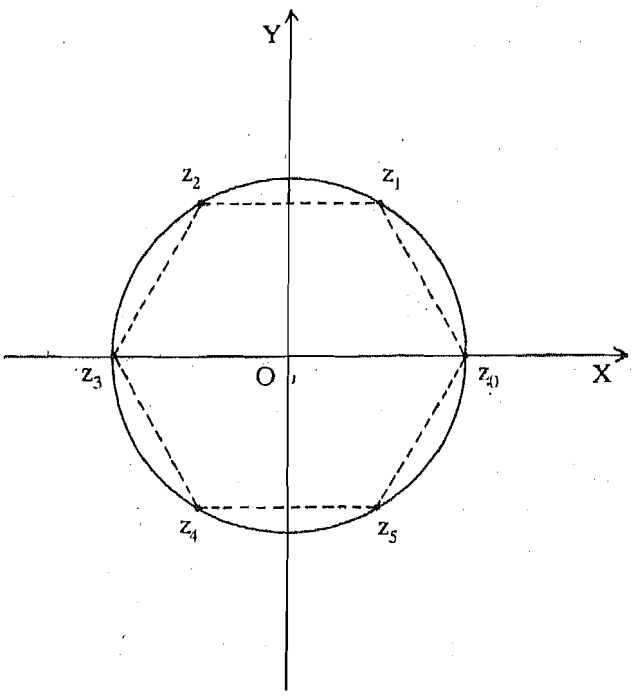

Fig. 1: 6th roots of unity

Now, let $\omega = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ Then all the nth roots of 1 are $1, w, w^2, \ldots\ldots, \omega^{n-1}$, since $\omega^j = \cos\frac{2\pi j}{n} + i \sin\frac{2\pi j}{n}$ for $0 \le j \le n-1$ (using De Moivre's theorem).

ω is the Greek letter omega.

Let $U_n = \{1, \omega, w^2, \ldots, \omega^{n-1}\}$. The following exercise shows you an interesting property of the elements of U_n.

E 3) If $n > 1$ and $w = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, then show that

$1 + \omega + \omega^2 + \omega^3 + \ldots\ldots + \omega^{n-1} = 0$.

Now we are in a position to obtain a finite subgroup of $\mathbb{C}^*$.

Example 5 : Show that $U_n \leq (\mathbb{C}^*, .)$.

Solution : Clearly, $U_n \neq \phi$. Now, let $\omega^i, \omega^j \in U_n$.

Then, by the division algorithm, we can write $i+j = qn + r$ for $q, r \in Z$, $0 \leq r \leq n-1$. But then $\omega^i . \omega^j = \omega^{i+j} = \omega^{qn+r} = (\omega^n)^q . \omega^r = \omega^r \in U_n$, since $\omega^n = 1$. Thus, U_n is closed under multiplication.

Finally, if $\omega^i \in U_n$, then $0 \leq n-i \leq n-1$ and $\omega^i . \omega^{n-i} = \omega^n = 1$, i.e., ω^{n-i} is the inverse of ω^i for all $1 \leq i < n$. Hence, U_n is a subgroup of $\mathbb{C}^*$.

Note that U_n is a finite group of order n and is a subgroup of an infinite group, $\mathbb{C}^*$. So, for every natural number n we have a finite subgroup of order n of $\mathbb{C}^*$.

Before ending this section we will introduce you to a subgroup that you will use off and on.

Definition : The centre of a group G, denoted by $Z(G)$, is the set
$Z(G) = \{g \in G \mid xg = gx \ \forall\ x \in G\}$.

Thus, $Z(G)$ is the set of those elements of G that commute with every element of G.

For example, if G is abelian, then $Z(G) = G$.

We will now show that $Z(G) \leq G$.

Theorem 2 : The centre of any group G is a subgroup of G.

Proof: Since $e \in Z(G)$, $Z(G) \neq \phi$. Now,

$a \in Z(G) \Rightarrow ax = xa \ \forall\ x \in G.$
$\Rightarrow x = a^{-1} xa \ \forall\ x \in G$, pre-multiplying by a^{-1}.
$\Rightarrow xa^{-1} = a^{-1} x \ \forall\ x \in G$, post-multiplying by a^{-1}.
$\Rightarrow a^{-1} \in Z(G)$.

Also, for any $a, b \in Z(G)$ and for any $x \in G$,
$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.
$\therefore ab \in Z(G)$.

Thus, $Z(G)$ is subgroup of G.

The following exercise will give you some practice in obtaining the centre of a group.

E 4) Show that $Z(S_3) = [I]$.
(Hint : Write the operation table for S_3.)

Let us now discuss some properties of subgroups.

3.3 PROPERTIES OF SUBGROUPS

Let us start with showing that the relation 'is a subgroup of' is transitive. The proof is very simple.

Theorem 3 : Let G be a group, H be a subgroup of G and K be a subgroup of H. Then K is a subgroup of G.

Proof : Since $K \leq H$, $K \neq \phi$ and $ab^{-1} \in K \ \forall\ a, b \in K$. Therefore, $K \leq G$.

Let us look at subgroups of Z, in the context of Theorem 3.

Example 6: In Example 4 we have seen that my subgroup of Z is of the form mZ for some $m \in N$. Let mZ and kZ be two subgroups of Z. Show that mZ is a subgroup of kZ iff $k \mid m$.

Solution : We need to show that $mZ \subseteq kZ \Leftrightarrow k \mid m$. Now $mZ \subseteq kZ \Rightarrow m \in mZ \subseteq kZ$
$\Rightarrow m \in kZ \Rightarrow m = kr$ for some $r \in Z \Rightarrow k \mid m$.

Conversely, suppose $k \mid m$.

Then, m = kr for some r ∈ **Z**. Now consider any **n** ∈ **mZ**, and let t ∈ Z such that n = mt.
Then n = mt = (kr) t = k(rt) ∈ **kZ** .
Hence, **mZ** ⊆ **kZ**.
Thus, **mZ** I **kZ** iff k | m.

Now, you may like to try the next exercise.

E 5) Which subgroups of **Z** is **9Z** a subgroup of?

We will now discuss the behaviour of subgroups under the operations of intersection and union.

Theorem 4 : If H and K are two subgroups of a group **G**, then H ∩ K is also a subgroup of G.

Proof : Since e ∈ H and e ∈ K, where e is the identity of G, e ∈ H ∩ K.

Thus, H ∩ K ≠ ϕ.

Now, let a, b ∈ H ∩ K. By Theorem 1 , it is enough to show that $ab^{-1} \in H \cap K$. Now, since a, b ∈ H, $ab^{-1} \in$ H. Similarly, since a, b ∈ K, $ab^{-1} \in$ K. Thus, $ab^{-1} \in H \cap K$.
Hence, H ∩ K is a subgroup of G.

The whole argument of Theorem 4 remains valid if we take a family of subgroups instead of just two subgroups. Hence, we have the following result.

Theorem 4′ : If $\{H_i\}_{i \in I}$ is a family of subgroups of a group G, then $\bigcap_{i \in I} H_i$ is also a subgroup of G.

Now, do you think the union of two (or more) subgroups is again a subgroup? Consider the two subgroups **2Z** and **3Z** of **Z**. Let S = **2Z** U 32. Now, 3 ∈ 32 ⊆ S, **2** ∈ 22 ⊆ S, but 1 = 3–2 is neither in **2Z** nor in 3Z. Hence, S is not a subgroup of (**Z**, +). Thus, if A and B are subgroups of G, AUB need not be a subgroup of G. But, if A ⊆ B, then AUB = B is a subgroup of G. The next exercise says that this is the only situation in which AUB is a subgroup of G.

E 6) Let A and B be two subgroups of a group G. Prove that AUB is a subgroup of G iff A ⊆ B or B ⊆ A.

(Hint : Suppose A ⊄ B and B ⊄ A. Take a ∈ A\B and b ∈ B\A. Then show that ab ∉ AUB. Hence, AUB ≤ G. Note that proving this amounts to proving that AUB ≤ G ⇒ A ⊆ B or B ⊆ A.)

'≤' denotes 'is not a subgroup of.

Let us now see what we mean by the product of two subsets of a group G.

Definition : Let G be a group and A, B be non-empty subsets of G.

The product of A and B is the set AB = { ab | a ∈ **A**, b ∈ B).

For example, (2Z) (**3Z**) = { (2m) (3m) | m, **n** ∈ Z }
= { **6mn** | m, n ∈ **Z** }
= 62.

In this example we find that the product of two subgroups is a subgroup. But is that always so? Consider the group

S_3 = {I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}, and its subgroups H = {I, (1 2) } and K = {I, (1 3)).

(Remember, (1 2) is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and (1 2 3) is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.)

Now HK $= \{ I \circ I, I \circ (1\ 3), (1\ 2) \circ I, (1\ 2) \circ (1\ 3)\}$
$= \{ I, (1\ 3), (1\ 2), (1\ 3\ 2)\}$

HK is not a subgroup of G, since it is not even closed under composition. (Note that $(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \notin$ HK.)

So, when will the product of two subgroups be a subgroup? The following result answers this question.

Theorem 5 : Let H and K be subgroups of a group G. Then HK is a subgroup of G if and only if HK = KH.

Proof : Firstly, assume that HK $\leq$ G. We will show that HK = KH. Let hk $\in$ HK. Then $(hk)^{-1} = k^{-1} h^{-1} \in$ HK, since HK $\leq$ G.

Therefore, $k^{-1} h^{-1} = h_1 k_1$ for some $h_1 \in$ H, $k_1 \in$ K. But then $hk = (k^{-1} h^{-1})^{-1}$
$= k_1^{-1} h_1^{-1} \in$ KH. Thus, HK $\subseteq$ KH.

Now, we will show that KH $\subseteq$ HK. Let kh $\in$ KH. Then $(kh)^{-1} = h^{-1} k^{-1} \in$ HK. But HK $\leq$ G. Therefore, $((kh)^{-1})^{-1} \in$ HK, that is, kh $\in$ HK. Thus, KH $\subseteq$ HK.

Hence, we have shown that HK = KH.

Conversely, assume that HK = KH. We have to prove that HK $\leq$ G. Since $e = e^2 \in$ HK, HK $\neq \phi$. Now, let a, b $\in$ HK. Then a = hk and b = $h_1 k_1$ for some h, $h_1 \in$ H and k, $k_1 \in$ K. Then $ab^{-1} = (hk)\ (k_1^{-1}\ h_1^{-1}) = h\ [\ (kk_1^{-1})\ h_1^{-1}]$.

Now, $(kk_1^{-1})\ h_1^{-1} \in$ KH = HK, Therefore, $\exists\ h_2 k_2 \in$ HK such that $(kk_1^{-1})h_1^{-1} = h_2 k_2$.

Then, $ab^{-1} = h(h_2 k_2) = (hh_2)k_2 \in$ HK.

Thus, by Theorem 1, HK $\leq$ G.

The following result is a nice corollary to Theorem 5.

Corollary : If H and K are subgroups of an abelian group G, then HK is a subgroup of G.

Try the following exercise now.

E 7) Is AB a subgroup of S_4, where A = { I, (1 4)) and B = {I, (1 2)}?

The next topic that we will take up is generating sets.

3.4 CYCLIC GROUPS

In this section we will briefly discuss generating sets, and then talk about cyclic groups in detail.

Let ***G*** be any group and S a subset of G. Consider the family $\mathcal{F}$ of all subgroups of G that contain S, that is,

$\mathcal{F} = \{ H \mid H \leq G \text{ and } S \subseteq H\}$.

We claim that $\mathcal{F} \neq \phi$. Why? Doesn't G $\in \mathcal{F}$? Now, by Theorem 4', $\bigcap_{H \in \mathcal{F}} H$ is a subgroup of ***G***.

Note that

i) $S \subseteq \bigcap_{H \in \mathcal{F}} H$.

ii) $\bigcap_{H \in \mathcal{F}} H$ is the smallest subgroup of G containing S. (Because if K is a subgroup of G containing S, then K $\in \mathcal{F}$. Therefore, $\bigcap_{H \in \mathcal{F}} H \subseteq$ K.)

These observations lead us to the following definition.

Definition : If S is a subset of a group G, then the smallest subgroup of G containing S is called **the subgroup generated by the set S,** and is written as $\langle S \rangle$.

Thus, $\langle S \rangle = \cap \{ H \mid H \leq G, S \subseteq H\}$.

If S = ϕ, then $\langle S \rangle = \{e\}$.

If $\langle S \rangle$ = G, then we say that ***G*** is **generated by the set S,** and that S is a **set of generators of *G*.**

If the set S is finite, we say that G is **finitely generated.**

Before giving examples, we will give an alternative way of describing $\langle S \rangle$. This definition is much easier to work with than the previous one.

Theorem 6 : If S is a non-empty subset of a group G, then

$\langle S \rangle = \{ a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \mid a_i \in S \text{ for } 1 \leq i \leq k, n_1, \ldots, n_k \in \mathbf{Z} \}$.

Proof :Let $A = \{ a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \mid a_i \in S \text{ for } 1 \leq i \leq k, n_1, \ldots, n_k \in \mathbf{Z} \}$.

Since $a_1, \ldots, a_k \in S \subseteq \langle S \rangle$ and $\langle S \rangle$ is a subgroup of G, $a_i^{n_i} \in \langle S \rangle$

$\forall$ i = 1, ..., k. Therefore, $a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \in \langle S \rangle$, i.e., $A \subseteq \langle S \rangle$.

Now , let us see why $\langle S \rangle \subseteq A$. We will show that **A** is a subgroup containing S. Then, by the definition of $\langle S \rangle$, it will follow that $\langle S \rangle \subseteq A$.

Since any $a \in S$ can be written as $a = a^1$, $S \subseteq A$.

Since $S \neq \phi$, $A \neq \phi$.

Now let $x, y \in A$. Then $x = a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}$,

$y = b_1^{m_1} b_2^{m_2} \ldots b_r^{m_r}$, $a_i, b_j \in S$ for $1 \leq i \leq k$, $1 \leq j \leq r$.

Then $xy^{-1} = (a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}) (b_1^{m_1} b_2^{m_2} \ldots b^{m_r})^{-1}$

$= (a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}) (b_r^{-m_r} \ldots b_1^{m_1}) \in A$.

Thus, by Theorem 1, **A** is a subgroup of G. Thus, **A** is a subgroup of G containing S. And hence, $\langle S \rangle \subseteq A$.

This shows that $\langle S \rangle = A$. ·

Note that, if (G, +) is a group generated by S, then any element of ***G*** is of the form $n_1 a_1 + n_2 a_2 + \ldots + n_r a_r$, where $a_1, a_2, \ldots, a, \in S$ and $n_1, n_2, \ldots, n_r \in Z$.

For example, $\mathbf{Z}$ is generated by the set of odd integers $S = \{ \pm 1, f3, \pm 5, \ldots \}$. Let us see why. Let $m \in Z$. Then $m = 2^r s$ where $r \geq 0$ and $s \in S$. Thus, $m \in \langle S \rangle$. And hence, $\langle S \rangle = \mathbf{Z}$.

Try the following exercises now.

E 8) Show that $S = \{1\}$ generates Z.

E 9) Show that a subset S of N generates the group Z of all integers iff there exist $s_1, \ldots, s_k$ in S and $n_1, \ldots, n_k$ in Z such that $n_1 s_1 + \ldots + n_k s_k = 1$.
(Hint : Apply Theorem 6.)

E 10) Show that if S generates a group G and $S \subseteq T \subseteq G$, then $\langle T \rangle = G$.

E 10 shows that a group can have many generating sets. E 8 gives an example of a group that is generated by only one element. We give such a group a special name.

Definition : **A** group G is called a **cyclic group** if $G = \langle \{a) \rangle$ for some $a \in G$. We usually write $\langle \{a) \rangle$ as $\langle a \rangle$.

Note that $\langle a \rangle = \{ a^n \mid n \in \mathbf{Z} \}$.

A subgroup H of a group G is called a **cyclic subgroup** if it is a cyclic group. Thus, $\langle (1\ 2) \rangle$ is a cyclic subgroup of S_3 and $2\ 2 = \langle 2 \rangle$ is a cyclic subgroup of **Z.**

We would like to make the following remarks here.

Remark 3 : i) If $K \leq G$ and $a \in K$, then $\langle a \rangle \subseteq K$. This is because $\langle a \rangle$ is the smallest subgroup of G containing a.

ii) All the elements of $\langle a \rangle = \{ a^n \mid n \in \mathbf{Z} \}$ may or may not be distinct. For example, take $a = (1\ 2) \in S_3$.
Then $\langle (1\ 2) \rangle = \{ I, (1\ 2) \}$, since $(1\ 2)^2 = I$, $(1\ 2)^3 = (1\ 2)$, and so on.

Fig! 2: Felix Klein
(1849—1925)

Now you can try the following simple exercises.

E 11) Show that if G # {e}, then $G \neq \langle e \rangle$.

E 12) Show that $\langle a \rangle = \langle a^{-1} \rangle$ for any $a \in G$.

We will now prove a nice property of cyclic groups.

Theorem 7 : Every cyclic group is abelian.

Proof : Let $G = \langle a \rangle = \{ a^n \mid n \in Z \}$. Then, for any x, y in G, there exist m, $n \in \mathbb{Z}$ such that $x = a^m$, $y = a^n$. But, then, $xy = a^m . a^n = a^{m+n} = a^{n+m} = a^n . a^m = yx$. Thus, xy = yx for all x, y in G.

That is. G is abelian.

Note that Theorem 7 says that every cyclic group is abelian. But this does not mean that every abelian group is cyclic. Consider the following example.

Example 7 : Consider the set $K_4 = \{e, a, b, ab\}$ and the binary operation on K_4 given by the table.

•	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

The table shows that $(K_4, .)$ is a group.

This group is called the **Klein 4-group,** after the pioneering German group theorist Felix Klein.

Show that K_4 is abelian but not cyclic.

Solution : From the table we can see that K_4 is abelian. If it were cyclic, it would have to be generated by e, a, b or ab. Now, $\langle e \rangle = \{e\}$. Also, $a^1 = a$, $a^2 = e$, $a'' = a$, and so on.

Therefore, $\langle a \rangle = \{ e, a \}$. Similarly, $\langle b \rangle = \{ e, b \}$ and $\langle ab \rangle = \{ e, ab \}$.

Therefore, K_4 can't be generated by e, a, b or ab.

Thus, K_4 is not cyclic.

Use Theorem 7 to solve the following exercise.

E **13)** Show that S_3 is not cyclic.

Now let us look at another nice property of cyclic groups.'

Theorem 8 : Any subgroup of a cyclic group is cyclic.

Proof : Let $G = \langle x \rangle$ be a cyclic group and H be a subgroup.

If $H = \{e\}$, then $H = \langle e \rangle$, and hence, H is cyclic.

Suppose $H \neq \{e\}$. Then $\exists\, n \in Z$ such that $x^n \in H$, $n \neq 0$. Since H is a subgroup, $(x^n)^{-1} = x^{-n} \in H$. Therefore, there exists a positive integer m (i.e., n or –n) such that $x^m \in H$. Thus, the set $S = \{ t \in N \mid x^t \in H \}$ is not empty. By the well-ordering principle (see Sec. 1.6.1.) S has a least element, say k. We will show that $H = \langle x^k \rangle$.

Now, $\langle x^k \rangle \subseteq H$, since $x^k \in H$.

Conversely, let x^n be an arbitrary element in H. By the division algorithm $n = mk + r$ where $m, r \in Z$, $0 \leq r \leq k-1$. But then $x^r = x^{n-mk} = x^n . (x^k)^{-m} \in H$, since $x^n, x^k \in H$. But k is the

least positive integer such that $x^k \in H$. Therefore, x^r can be in H only if $r = 0$. And then, $n = mk$ and $x^n = (x^k)^m \in < x^k >$. Thus, $H \subseteq < x^k >$. Hence, $H = < x^k >$, that is, H is cyclic.

Using Theorem 8 we can immediately prove what we did in Example 4.

Now, Theorem 8 says that every subgroup of a cyclic group is cyclic. But the converse is not true. That is, we can have groups whose proper subgroups are all cyclic, without the group being cyclic. We give such an example now.

Consider the group S_3, of all permutations on 3 symbols. Its proper subgroups are

$A = <I>$
$B = <(1\ 2)>$
$C = <(1\ 3)>$
$D = <(2\ 3)>$
$E = <(1\ 2\ 3)>$.

As you can see, all these are cyclic. But, by E 13 you know that S_3 itself is not cyclic.

Now we state a corollary to Theorem 8, in which we write down the important point made in the proof of Theorem 8.

Corollary : Let $H \neq \{e\}$ be a subgroup of $< a >$. Then $H = < a^n >$, where n is the least positive integer such that $a^n \in H$.

Try the following exercises now.

H is a proper subgroup of G if $H \subsetneq G$.

E 14) Show that any non-abelian group must have a proper subgroup other than $\{e\}$.

E 15) Obtain all the subgroups of Z_4, which you know is $<\bar{1}>$.

Let us now see what we have done ill this unit.

3.5 SUMMARY

In this unit we have covered the following points.

1) The definition and examples of subgroups.
2) The intersection of subgroups is a subgroup.
3) The union of two subgroups H and K is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.
4) The product of two subgroups H and K is a subgroup if and only if HK = KH.
5) The definition of a generating set.
6) A cyclic group is abelian, but the converse need not be true.
7) Any subgroup of a cyclic group is cyclic, but the converse need not be true.

3.6 SOLUTIONS/ANSWERS

E 1) Yes, because H is a group in its own right.

E 2) $\{e\} \neq \phi$. Also $ee^{-1} = e \in \{e\}$. $\therefore$, by Theorem 1, $\{e\} \leq G$.
$G \neq \phi$. Also for any $x \in G$, $x^{-1} \in G$. $\therefore$, for a, $b \in G$,
$a, b^{-1} \in G$. $\therefore ab^{-1} \in G$. $\therefore G \leq G$.

E 3) Since $\omega^n = 1$, $(1-\omega^n) = 0$, i.e.,
$(I - a)(1 + \omega + \omega^2 + ... + \omega^{n-1}) = 0$.
Since $\omega \neq 1$, $1 + \omega + \omega^2 + ... + \omega^{n-1} = 0$.

E 4) From E 14 of Unit 2 recall the elements of S_3. On writing the operation table for S_3 you will find that only I commutes with every permutation in S_3.

E 5) The divisors of 9 are 1, 3 and 9.
Thus, $9\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, $3\mathbb{Z}$ and itself only.

E 6) We know that if $A \subseteq B$ or $B \subseteq A$, then AUB is A or B, and hence, is a subgroup of G.
Conversely, we will assume that $A \not\subseteq B$ and $B \not\subseteq A$, and conclude that $AUB \not\leq G$.
Since $A \not\subseteq B$, $\exists\ a \in A$ such that $a \notin B$.
Since $B \not\subseteq A$, $\exists\ b \in B$ such that $b \notin A$.
Now, if $ab \in A$, then $ab = c$, for some $c \in A$.
Then $b = a^{-1}c \in A$, a contradiction. $\therefore ab \notin A$. Similarly, $ab \notin B$. $\therefore ab \notin AUB$.
But $a \in AUB$ and $b \in AUB$. So, $AUB \not\leq G$.

E 7) $AB = \{ I, (1\ 4), (1\ 2), (1\ 2\ 4) \}$.
But, $(1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin AB$. $\therefore$ $AB \not\leq S_4$.

E 8) For any $n \in \mathbb{Z}$, $n = n.1 \in <\{1\}>$. $\therefore \mathbb{Z} = <\{1\}>$.

E 9) Firstly, suppose $\mathbb{Z} = <S>$. Then $1 \in <S>$. $\therefore \exists\ s_1, ...s_k \in S$ and $n_1,.....,n_k \in \mathbb{Z}$ such that $n_1s_1 + ... + n_ks_k = 1$.
Conversely, suppose $\exists\ s_1, ...,s_k \in S$ and $n_1, ..., n_k \in \mathbb{Z}$ such that $n_1s_1 + n_2s_2 + ...+ n_ks_k = 1$.
Then, for any $n \in \mathbb{Z}$, $n = n.1 = nn_1s_1 + ... + nn_ks_k \in <S>$.
$\therefore \mathbb{Z} = <S>$.

E 10) We know that $G = <S>$. Therefore, for any $g \in G$,
$\exists\ s_1, ... s_k \in S$ and $n_1.....n_k \in \mathbb{Z}$ such that
$g = s_1^{n_1} .....s_k^{n_k}$. Since $S \subseteq T$, $s_i \in T\ \forall\ i = 1, ... k$.
$\therefore$ by Theorem 6, we see that $G = <T>$.

E 11) Since $G \neq \{e\}$, $\exists\ a \neq e$ in G. Since $a \neq e$, $a \neq e^r$ for any $r \in \mathbb{Z}$. $\therefore a \notin <e>$.
$\therefore G \neq <e>$.

E 12) We will show that $<a> \subseteq <a^{-1}>$ and $<a^{-1}> \subseteq <a>$.
Now, any element of $<a>$ is $a^n = (a^{-1})^{-n}$, for $n \in \mathbb{Z}$.
$\therefore a^n \in <a^{-1}>$. $\therefore <a> \subseteq <a^{-1}>$.
Similarly, $<a^{-1}> \subseteq <a>$.
$\therefore <a> = <a^{-1}>$.

E 13) Since S_3 is not abelian (e.g., $(1\ 3) \circ (1\ 2) \neq (1\ 2) \circ (1\ 3)$), by Theorem 7, S_3 can't be cyclic.

E 14) Let G be a non–abelian group. Then $G \neq \{e\}$. Therefore, $\exists\ a \in G$, $a \neq e$. Then $<a> \leq G$. $G \neq <a>$, since G is non-abelian. $\therefore <a> \not\leq G$.

E 15) Since $\mathbb{Z}_4$ is cyclic, all its subgroups are cyclic.
Thus, its subgroups are $\mathbb{Z}_4$, $<\bar{2}>$, $<\bar{3}>$ and $\{\bar{0}\}$.