UNIT 8 FINITE GROUPS

Structure

8.1 INTRODUCTION

By now you are familiar with various finite and infinite groups and their subgroups. In this unit we will pay special attention to certain finite groups and discuss their structures. For example, you will see that any group of order 6 is cyclic or is isomorphic to S_3.

To be able to describe the structure of a finite group we need some knowledge of a direct product of groups. In Sec. 8.2 we will discuss external and internal direct products.

In Sec. 8.3 we discuss the uses of certain results obtained by the famous mathematician Sylow (1832-1918). These theorems, as well as a theorem by Cauchy, allow us to determine various subgroups of some finite groups.

Finally, in Sec. 8.4, we use the knowledge gained in Sec. 8.2 and Sec. 8.3 to describe the structures of several finite groups. In particular, we discuss groups of order less than or equal to 10.

With this unit we wind up our discussion of group theory. In the next block you will start studying ring theory. Of course, you will keep using what you have learnt in the first two blocks, because every ring is a group also, as you will see.

Objectives

After reading this unit, you should be able to

- construct the direct product of a finite number of groups;
- check if a group is a direct product of its subgroups;
- use Sylow's theorems to obtain the possible subgroups and structures of finite groups; classify groups of order p, p^2 or pq, where p and q are primes such that $p > q$ and $q \not| p - 1$.

8.2 DIRECT PRODUCT OF GROUPS

In this section we will discuss a very important method of constructing new groups by using given groups as building blocks. We will first see how two groups can be combined to form a third group. Then we will see how two subgroups of a group can be combined to form another subgroup.

8.2.1 External Direct Product

In this sub-section we will construct a new group from two or more groups that we already have.

Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. Consider their Cartesian product (see Sec. 1.3)
$G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$.
Can we define a binary operation on G by using the operations on G_1 and G_2? Let us try the obvious method, namely, componentwise multiplication. That is, we define the operation $*$ on G by $(a, b) * (c, d) = (a *_1 c, b *_2 d) \forall a, c \in G_1, b, d \in G_2$. . .

The way we have defined $*$ ensures that it is a binary operation.

To check that $(G, *)$ is a group, you need to solve the following exercise.

E 1) Show that the binary operation $*$ on G is associative. Find its identity element and the inverse of any element (x, y) in G.

So, you have proved that $G = G_1 \times G_2$ is a group with respect to $*$. We call G the **external** direct product of $(G_1, *_1)$ and $(G_2, *_2)$.

For example $\mathbf{R}^2$ is the external direct product of R with itself.

Another example is the direct product $(Z, +) \times (R^*, .)$ in which the operation is given by $(m, x) * (n, y) = (m + n, xy)$.
We can also define the external direct product of 3, 4 or more groups on the same lines.

Definition : Let $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ be n groups. Their external direct product is the group $(G, *)$, where
$G = G_1 \times G_2 \ldots \times G_n$ and

$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \ldots, x_n *_n y_n) \forall x_i, y_i \in G_i$.

Thus, R^n is the external direct product of n copies of R.

We would like to make a remark about notation now.
Remark 1 : Henceforth, we will assume that all the operations $*, *_1, \ldots, *_n$ are multiplication, unless mentioned otherwise. Thus, the operation on $G = G_1 \times G_2 \times \ldots \times G_n$ willbegivenby

$(a_1, \ldots, a_n) . (b_1, \ldots, b_n)$
$= (a_1 b_1, a_2 b_2, \ldots, a_n b_n) \forall a_i, b_i \in G_i$.

Now try the following exercise.

E 2) Show that $G_1 \times G_2 \simeq G_2 \times G_1$, for any two groups G_1 and G_2.

Because of E 2 we can speak of the direct product of 2 (or n) groups without bothering about their order.

Now, let G be the external direct product $G_1 \times G_2$. Consider the projection map

$\pi_1 : G_1 \times G_2 \longrightarrow G_1 : \pi_1 (x, y) = x$.

Then π_1 is a group homomorphism, since

$\pi_1 ((a, b) (c, d)) = \pi_1 (ac, bd)$
$= ac$
$= \pi_1(a, b)\ \pi_1 (c, d)$

π_1 is also onto, because any $x \in G_1$ is $\pi_1 (x, e_2)$
Now, let us look at Ker π_1.
Ker $\pi_1 = \{(x, y) \in G_1 \times G_2 \mid \pi_1 (x, y) = e_1\}$
$= \{(e_1, y) \mid y \in Gz\} = \{e_1\} \times G_2$.
$\therefore \{e_1\} \times G_2 \trianglelefteq G_1 \times G_2$.
Also, by the Fundamental Theorem of Homomorphism $(G_1 \times G_2)/(\{e_1\} \times Gz) \simeq G_1$.
We can similarly prove that $G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2$ and $(G_1 \times G_2)/(G_1 \times \{e_2\}) \simeq G_2$.

In the following exercises we give you general facts about external direct products of groups.

E 3) Show that $G_1 \times G_2$ is the product of its normal subgroups $H = G_1 \times \{e_2\}$ and $K = \{e_1\} \times G_2$.
Also show that $(G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2) = \{(e_1, e_2)\}$.

E 4) Prove that $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$, where $Z(G)$ denotes the centre of G (see Theorem 2 of Unit 3).

The direct product of finite cyclic groups is cyclic iff their orders are relatively prime.

E 5) Let A and B be cyclic groups of order m and n, respectively, where $(m, n) = 1$. Prove that $A \times B$ is cyclic of order mn.
(Hint : Define $f : Z \to Z_m \times Z$, : $f(r) = (r + mZ, r + nZ)$. Then apply the Fundamental Theorem of Homomorphism to show that $Z_m \times Z_n \simeq Z_{mn}$.

So, far we have seen the construction of $G_1 \times G_2$ from two groups G_1 and G_2. Now we will see under what conditions we can express a group as a direct product of its subgroups.

8.2.2 Internal Direct Product

Let us begin by recalling from Unit 5 that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. We are interested in the case when HK is the whole of G. We have the following definition.

Definition: Let H and K be normal subgroups of a group G. We call G the **internal direct product** of H and K if

$G = HK$ and $H \cap K = \{e\}$.

We write this fact as $G = H \times K$.

For example, let us consider the familiar Klein 4-group

$K_4 = \{e, a, b, ab\}$, where $a^2 = e$, $b^2 = e$ and $ab = ba$.

Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Then $H \cap K = \{e\}$. Also, $K_4 = HK$.

$\therefore K_4 = H \times K$.

Note that $H \simeq Z_2$ and $K \simeq Z_2$ $\therefore$ $K_4 \simeq Z2 \times Z_2$.

For another example, consider Z_{10}. It is the internal direct product of its subgroups $H = \{\bar{0}, \bar{5}\}$ and $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$. This is because

i) $Z_{10} = H + K$, since any element of Z_{10} is the sum of an element of H and an element of K, and

ii) $H \cap K = \{\bar{0}\}$.

Now, can an external direct product also be an internal direct product? Well, go back to E 3. What does it say? It says that the external product of $G_1 \times G_2$ is the internal product $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

We would like to make a remark here.

Remark 2 : Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is isomorphic to the external direct product of H and K. Therefore, when we talk of an internal direct product of subgroups we can drop the word internal, and just say 'direct product of subgroups'.

Let us now extend the definition of the internal direct product of two subgroups to that of several subgroups.

Definition: A group G is the **internal direct product** of its normal subgroups $H_1, H_2, \ldots, H_n$ if

i) $G = H_1 H_2 \ldots . H_n$, and

ii) $H_i \cap H_1 \ldots . H_{i-1} H_{i+1} \ldots . H_n = \{e\}$ $\forall i = 1, \ldots, n$.

For example, look at the group G generated by {a, b, c}, where $a^2 = e = b^2 = c^2$ and $ab = ba$, $ac = ca$, $bc = cb$. This is the internal direct product of $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$. That is $G \simeq Z_2 \times Z_2 \times Z_2$.

Now, can every group be written as an internal direct product of two or more of its proper normal subgroups? Consider Z. Suppose $Z = H \times K$, where H, K are subgroups of Z. From Example 4 of Unit 3 you know that $H = \langle m \rangle$ and $K = \langle n \rangle$ for some m, n E Z. Then mn E $H \cap K$. But if $H \times K$ is a direct product, $H \cap K = \{0\}$. So, we reach a contradiction. Therefore, Z can't be written as an internal direct product of two subgroups.

By the same reasoning we can say that Z can't be expressed as $H_1 \times H_2 \times \ldots . \times H_n$, where $H_i \leq Z$ $\forall i = 1, 2, \ldots, n$.

When a group is an internal direct product of its subgroups, it satisfies the following theorem.

Theorem 1 : Let a group G be the internal direct product of its subgroups H and K. Then
a) each x E G can be uniquely expressed as x = hk, where h ∈ H, k ∈ K; and
b) hk = kh ∀ h ∈ H, k ∈ K.

Proof : a) We know that G = HK. Therefore, if x E G, then x = hk, for some h ∈ H, k ∈ K. Now suppose x = h_1k_1 also, where h_1 E H and k_1 E K. Then hk = h_1k_1.
∴ $h_1^{-1}h = k_1k^{-1}$. Now $h_1^{-1}h \in H$.
Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1}h$ E K. ∴ h_1^{-1} h ∈ H ∩ K = {e}.
∴ $h_1^{-1}h$ = e, which implies that h = h_1.
Similarly, k_1 k^{-1} = e, so that k_1 = k.
Thus, the representation of x as the product of an element of H and an element of K is unique.
b) The best way to show that two elements x and y commute is to show that their commutator $x^{-1}y^{-1}$ xy is identity. So, let h ∈ H and k E K and consider $h^{-1}k^{-1}hk$. Since K ◁ G, $h^{-1}k^{-1}h \in K$.
∴ $h^{-1}k^{-1}hk$ E K.
By similar reasoning, $h^{-1}k^{-1}hk \in H$. ∴ $h^{-1}k^{-1}hk \in H \cap K = \{e\}$.
∴ $h^{-1}k^{-1}hk$ = e, that is, hk = kh.

Try the following exercise now.

E 6) Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that G = H X K.

Now let us look at the relationship between internal direct products and quotient groups.

Theorem 2 : Let H and K be normal subgroups of a group G such that G = H X K. Then G/H ≃ K and G/K ≃ H.

Proof: We will use Theorem 8 of Unit 6 to prove this result.
Now G = HK and H ∩ K = {e}. Therefore,
G/H = HK/H ≃ K/H ∩ K = K/{e} ≃ K.
We can similarly prove that G/K ≃ H.

We now give a result which immediately follows from Theorem 2 and which will be used in Sec. 8.4.

Theorem 3 : Let G be a finite group and H and K be its subgroups such that G = H × K. Then o(G) = o(H) o(K).

We leave the proof to you (see the following exercise).

E 7) Use Theorem 2 to prove Theorem 3.

And now let us discuss some basic results about the structure of any finite group.

8.3 SYLOW THEOREMS

In Unit 4 we proved Lagrange's theorem, which says that the order of a subgroup of a finite group divides the order of the group. We also said that if G is a finite cyclic group and' m | o(G), then G has a subgroup of order m. But if G is not cyclic, this statement need not be true, as you have seen in the previous unit. In this context, in 1845 the mathematician Cauchy proved the following useful result:

Theorem 4 : If a prime p divides the order of a finite group G, then G contains an element of order p.

The direct product of finite cyclic groups is cyclic iff their orders are relatively prime.

E 4) Prove that $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$, where $Z(G)$ denotes the centre of G (see Theorem 2 of Unit 3).

E 5) Let A and B be cyclic groups of order m and n, respectively, where (m, n) = 1. Prove that $A \times B$ is cyclic of order mn.
(Hint : Define $f : Z \to Z_m \times Z_n : f(r) = (r + mZ, r + nZ)$. Then apply the Fundamental Theorem of Homomorphism to show that $Z_m \times Z_n \simeq Z_{mn}$.

So, far we have seen the construction of $G_1 \times G_2$ from two groups G_1 and G_2. Now we will see under what conditions we can express a group as a direct product of its subgroups.

8.2.2 Internal Direct Product

Let us begin by recalling from Unit 5 that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. We are interested in the case when HK is the whole of G. We have the following definition.

Definition : Let H and K be normal subgroups of a group G. We call G the internal direct product of H and K if
$G = HK$ and $H \cap K = \{e\}$.
We write this fact as $G = H \times K$.

For example, let us consider the familiar Klein 4-group
$K_4 = \{e, a, b, ab\}$, where $a^2 = e$, $b^2 = e$ and $ab = ba$.
Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Then $H \cap K = \{e\}$. Also, $K_4 = HK$.
$\therefore K_4 = H \times K$.

Note that $H \simeq Z_2$ and $K \simeq Z_2$ $\therefore$ $K_4 \simeq Z_2 \times Z_2$.

For another example, consider Z_{10}. It is the internal direct product of its subgroups $H = \{\bar{0}, \bar{5}\}$ and $K = \{0, 2, 4, 6, 8\}$. This is because

i) $Z_{10} = H + K$, since any element of Z_{10} is the sum of an element of H and an element of K, and

ii) $H \cap K = \{\bar{0}\}$.

Now, can an external direct product also be an internal direct product? Well, go back to E 3. What does it say? It says that the external product of $G_1 \times G_2$ is the internal product $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

We would like to make a remark here.
Remark 2 : Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is isomorphic to the external direct product of H and K. Therefore, when we talk of an internal direct product of subgroups we can drop the word internal, and just say 'direct product of subgroups'.

Let us now extend the definition of the internal direct product of two subgroups to that of several subgroups.
Definition : A group G is the internal direct product of its normal subgroups $H_1, H_2, \ldots, H_n$ if

i) $G = H_1 H_2 \ldots H_n$, and
ii) $H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = \{e\}$ $\forall$ i = 1, ... , n.

For example, look at the group G generated by {a, b, c), where $a^2 = e = b^2 = c^2$ and ab = ba, ac = ca, bc = cb. This is the internal direct product of $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$. That is $G \simeq Z_2 \times Z_2 \times Z_2$.

Now, can every group be written as an internal direct product of two or more of its proper normal subgroups? Consider Z. Suppose $Z = H \times K$, where H, K are subgroups of Z. From Example 4 of Unit 3 you know that $H = \langle m \rangle$ and $K = \langle n \rangle$ for some m, $n \in Z$. Then $mn \in H \cap K$. But if $H \times K$ is a direct product, $H \cap K = \{0\}$. So, we reach a contradiction. Therefore, Z can't be written as an internal direct product of two subgroups.,

By the same reasoning we can say that Z can't be expressed as $H_1 \times H_2 \times \ldots \times H_n$, where $H_i \leq Z$ $\forall$ i = 1, 2, ... , n.

When a group is an internal direct product of its subgroups, it satisfies the following theorem.

Theorem 1 : Let a group G be the internal direct product of its subgroups H and K. Then

a) each x E G can be uniquely expressed as $x = hk$, where $h \in H$, $k \in K$; and

b) $hk = kh \ \forall\ h$ E H, $k \in$ K.

Proof : a) We know that $G = HK$. Therefore, if $x \in G$, then $x = hk$, for some $h \in H$, k E K. Now suppose $x = h_1k_1$ also, where $h_1 \in H$ and k_1 E K. Then $hk = h_1k_1$.
$\therefore h_1^{-1}h = k_1k^{-1}$. Now $h_1^{-1}h$ E H.
Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1}h \in K$. $\therefore h_1^{-1}h \in H \cap K = \{e\}$.
$\therefore h_1^{-1}h = e$, which implies that $h = h_1$.
Similarly, $k_1 k^{-1} = e$, so that $k_1 = k$.
Thus, the representation of x as the product of an element of H and an element of K is unique.
b) The best way to show that two elements x and y commute is to show that their commutator $x^{-1}y^{-1}xy$ is identity. So, let $h \in H$ and $k \in K$ and consider $h^{-1}k^{-1}hk$. Since $K \trianglelefteq G$, $h^{-1}k^{-1}h$ E K.
$\therefore h^{-1}k^{-1}hk$ E K.
By similar reasoning, $h^{-1}k^{-1}hk \in H$. $\therefore h^{-1}k^{-1}hk \in H \cap K = \{e\}$.
$\therefore h^{-1}k^{-1}hk = e$, that is, $hk = kh$.

Try the following exercise now.

E 6) Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that $G = H \times K$.

Now let us look at the relationship between internal direct products and quotient groups.

Theorem **2** : Let H and K be normal subgroups of a group G such that $G = H \times K$. Then $G/H \simeq K$ and $G/K \simeq H$.

Proof: We will use Theorem 8 of Unit 6 to prove this result.
Now $G = HK$ and $H \cap K = \{e\}$. Therefore,
$G/H = HK/H \simeq K/H \cap K = K/\{e\} \simeq K$.
We can similarly prove that $G/K \simeq H$.

We now give a result which immediately follows from Theorem 2 and which will be used in Sec. 8.4.

Theorem **3** : Let G be a finite group and H and K be its subgroups such that $G = H \times K$. Then $o(G) = o(H)\, o(K)$.

We leave the proof to you (see the following exercise).

E 7) Use Theorem 2 to prove Theorem 3.

And now let us discuss some basic results about the structure of any finite group.

8.3 SYLOW THEOREMS

In Unit 4 we proved Lagrange's theorem, which says that the order of a subgroup of a finite group divides the order of the group. We also said that if G is a **finite cyclic** group and $m \mid o(G)$, then G has a subgroup of order m. But if G is not cyclic, this statement need not be true, as you have seen in the previous unit. In this context, in 1845 the mathematician Cauchy proved the following useful result:

Theorem 4 : If a prime p divides the order of a finite group G, then G contains an element of order p.

The proof of this result involves a knowledge of group theory that is beyond the scope of this course. Therefore, we omit it. An immediate consequence of this result is the following.

Theorem 5 : If a prime p divides the order of a finite group G, then G contains a subgroup of order p.

Proof: Just take the cyclic subgroup generated by an element of order p. This element exists because of Theorem 4.

So, by Theorem 5 we know that any group of order 30 will have a subgroup of order 2, a subgroup of order 3 and a subgroup of order 5. In 1872 Ludwig Sylow, a Norwegian mathematician, proved a remarkable extension of Cauchy's result. This result, called the first Sylow theorem, has turned out to be the basis of finite group theory. Using this result we can say, for example, that any group of order 100 has subgroups of order 2, 4, 5 and 25. Let us see what this powerful theorem is.

Theorem 6 (First Sylow Theorem) : Let G be a finite group such that $o(G) = p^n m$, where p is a prime, $n \geq 1$ and $(p, m) = 1$. Then G contains a subgroup of order $p^k \; \forall \; k = 1, \ldots, n$.

We shall not prove this result or the next two Sylow theorems either. But, after stating all these results we shall show how useful they are.

The next theorem involves the concepts of conjugacy and Sylow p-subgroups which we now define.

Definition : Two subgroups H and K of a group G are conjugate in G if $\exists\, g \in G$ such that $K = g^{-1}Hg$, and then K is called a conjugate of H in G.

Can you do the following exercise now?

E 8) Show that $H \trianglelefteq G$ iff the only conjugate of H in G is H itself.

Now we define Sylow p-subgroups.

Definition : Let G be a finite group and p be a prime such that $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$, for some $n \geq 1$. Then a subgroup of G of order p^n is called a Sylow p-subgroup of G.

So, if $o(G) = p^n m$, $(p, m) = 1$, then a subgroup of G of order p^n is a Sylow p-subgroup. Theorem 6 says that this subgroup always exists. But, a group may have more than one Sylow p-subgroup. The next result tells us how two Sylow p-subgroups of a group are related.

Theorem 7 (Second Sylow Theorem) : Let G be a group such that $o(G) = p^n m$, $(p, m) = 1$, p a prime. Then any two Sylow p-subgroups of G are conjugate in G.

And now let us see how many Sylow p-subgroups a group can have.

Theorem 8 (Third Sylow Theorem) : Let G be a group of order $p^n m$, where $(p, m) = 1$ and p is a prime. Then n_p, the number of distinct Sylow p-subgroups of G, is given by $n_p = 1 + kp$ for some $k \geq 0$. And further, $n_p \mid o(G)$.

We would like to make a remark about the actual use of Theorem 8.

Remark 3 : Theorem 8 says that $n_p \equiv 1 \pmod p$ (see Sec. 2.5.1). Also, $(n_p, p^n) = 1$. Also, since $n_p \mid o(G)$, using Theorem 9 of Unit 1 we find that $n_p \mid m$. This fact helps us to cut down the possibilities for n_p, as you will see in the following examples.

Example 1 : Show that any group of order 15 is cyclic.

Solution : Let G be a group of order $15 = 3 \times 5$. Theorem 6 says that G has a Sylow 3-subgroup. Theorem 8 says that the number of such subgroups must divide 15 and must be congruent to $1 \pmod 3$. In fact, by Remark 3 the number of such subgroups must divide 5 and must be congruent to $1 \pmod 3$. Thus, the only possibility is 1. Therefore, G has a unique Sylow 3-subgroup, say H. Hence, by Theorem 7 and E 8 we know that $H \trianglelefteq G$. Since H is of prime order, it is cyclic.

Similarly, we know that G has a subgroup of order 5. The totalnumber of such subgroups is 1, 6 or 11 and must divide 3. Thus, the only possibility is I. So G has a unique subgroup of order 5, say K. Then $K \triangleleft G$ and K is cyclic.

Now, let us look at $H \cap K$. Let $x \in H \cap K$. Then $x \in H$ and $x \in K$.
$\therefore o(x) \mid o(H)$ and $o(x) \mid o(K)$ (by E 8 of Unit 4), i.e., $o(x) \mid 3$ and $o(x) \mid 5$.
$\therefore o(x) = 1$. $\therefore x = e$. That is, $H \cap K = \{e\}$. Also,

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = 15 = o(G).$$

$\therefore G = HK$.
So, $G = H \times K \simeq \mathbf{Z}_3 \times \mathbf{Z}_5 \simeq \mathbf{Z}_{15}$, by E 5.

Example 2 : Show that a group G of order 30 either has a normal subgroup of order 5 or a normal subgroup of order 3, i.e. G is not simple. A group G is called simple if its only normal subgroups are $\{e\}$ and G itself.

Solution : Since $30 = 2 \times 3 \times 5$, G has a Sylow 2-subgroup, a Sylow 3-subgroup and a Sylow 5-subgroup. The number of Sylow 5-subgroups is of the form $1 + 5k$ and divides 6 (by Remark 3). Therefore, it can be 1 or 6. If it is 1, then the Sylow 5-subgroup is normal in G.

On the other hand, suppose the number of Sylow 5-subgroups is 6. Each of these subgroups are distinct cyclic groups of order 5, the only common element being e. Thus, together they contain $24 + 1 = 25$ elements of the group. So, we are left with 5 elements of the group which are of order 2 or 3. Now, the number of Sylow 3-subgroups can be 1 or 10. We can't have 10 Sylow 3-subgroups, because we only have at most 5 elements of the group which are of order 3. So, if the group has 6 Sylow 5-subgroups, then it has only 1 Sylow 3-subgroup. This will be normal in G.

Try the following exercises now.

E 9) Show that every group of order 20 has a proper normal non-trivial subgroup.

E 10) Determine all the Sylow p-subgroups of $\mathbf{Z}_{24}$, where p varies over all the primes dividing 24.

E 11) Show that a group G of order 255 ($= 3 \times 5 \times 17$) has either 1 or 51 Sylow 5-subgroups. How many Sylow 3-subgroups can it have?

Now let us use the powerful Sylow theorems to classify groups of order 1 to 10. In the process we will show you the algebraic structure of several types of finite groups.

8.4 GROUPS OF ORDER 1 TO 10

In this section we will apply the results of the previous section to study some finite groups. In particular, we will list all the groups of order 1 to 10, upto isomorphism.

We start with proving a very useful result.
Theorem 9 : Let G be a group such that $o(G) = pq$, where p, q are primes such that $p > q$ and $q \nmid p - 1$. Then G is cyclic.

Proof : Let P be a Sylow p-subgroup and Q be a Sylow q-subgroup of G. Then $o(P) = p$ and $o(Q) = q$. Now, any group of prime order is cyclic, so $P = \langle x \rangle$ and $Q = \langle y \rangle$ for some $x, y \in G$. By the third Sylow theorem, the number n_p of subgroups of order p can be $1, 1 + p, 1 + 2p, \ldots$, and it must divide q. But $p > q$. Therefore, the only possibility for n_p is 1. Thus, there exists only one Sylow p-subgroup, i.e., P. Further, by Sylow's second theorem $P \triangleleft G$.
Again, the number of distinct Sylow q-subgroups of G is $n_q = 1 + kq$ for some k, and $n_q \mid p$. Since p is a prime, its only factors are 1 and p. $\therefore n_q = 1$ or $n_q = p$. Now if $1 + kq = p$, then $q \mid p - 1$. But we started by assuming that $q \nmid p - 1$. So we reach a contradiction. Thus, $n_q = 1$ is the only possibility. Thus, the Sylow q-subgroup Q is normal in G.

Now we want to show that $G = P \times Q$. For this, let us consider $P \cap Q$. The order of any element of $P \cap Q$ must divide p as well as q, and hence it must divide $(p, q) = 1$.
$\therefore P \cap Q = \{e\}$. $\therefore o(PQ) = o(P)\,o(Q) = pq = o(G)$. $\therefore G = PQ$.
So we find that $G = P \times Q \simeq Z_p \times Z_q \simeq Z_{pq}$, by E 5.
Therefore, G is cyclic of order pq.

Using Theorem 9, we can immediately say that any group of order 15 is cyclic (Example 1). Similarly, if $o(G) = 35$, then G is cyclic.

Now if $q \mid p - 1$, then does $o(G) = pq$ imply that G is cyclic? Well, consider S_3. You know that $o(S_3) = 6 = 2.3$, but S_3 is not cyclic. In fact, we have the following result.

Theorem 10 : Let G be a group such that $o(G) = 2p$, where p is an odd prime, Then either G is cyclic or G is isomorphic to the dihedral group D_{2p} of order 2p.
(Recall that $D_{2p} = \langle x, y \mid x^p = e = y^2 \text{ and } yx = x^{-1}y \rangle$.)

Proof : As in the proof of Theorem 9, there exists a subgroup $P = \langle x \rangle$ of order p with $P \trianglelefteq G$ and a subgroup $Q = \langle y \rangle$ of order 2, since $p > 2$. Since $(2, p) = 1$,
$P \cap Q = \{e\}$. $\therefore o(PQ) = o(G)$.
$\therefore G = PQ$.
Now, two cases arise, namely, when $Q \trianglelefteq G$ and when $Q \not\trianglelefteq G$.

If $Q \trianglelefteq G$, then $G = P \times Q$. And then $G = \langle xy \rangle$.

If Q is not normal in G, then G must be non-abelian.
(Remember that every subgroup of an abelian group is normal.)
$\therefore xy \neq yx$. $\therefore y^{-1}xy \neq x$.
Now, since $P = \langle x \rangle \trianglelefteq G$, $y^{-1}xy \in P$. $\therefore y^{-1}xy = x^r$, for some
$r = 2, \ldots, p - 1$.
Therefore, $y^{-2}xy^2 = y^{-1}(y^{-1}xy)y = y^{-1}x^r y = (y^{-1}xy)^r = (x^r)^r = x^{r^2}$.
$\Rightarrow x = x^{r^2}$, since $o(y) = 2$.
$\Rightarrow x^{r^2-1} = e$.
But $o(x) = p$. Therefore, by Theorem 4 of Unit 4, $p \mid r^2 - 1$, i.e., $p \mid (r - 1)(r + 1)$
$\Rightarrow p \mid (r - 1)$ or $p \mid (r + 1)$. But $2 \leq r \leq p - 1$. $\therefore p = r + 1$,
i.e., $r = p - 1$. So we see that
$y^{-1}xy = x^r = x^{p-1} = x^{-1}$
So, $G = PQ = \langle \{x, y \mid x^p = e, y^2 = e, y^{-1}xy = x^{-1}\} \rangle$, which is exactly the same algebraic structure as that of D_{2p}.
$\therefore G \simeq D_{2p} = \{e, x, x^2, \ldots, x^{p-1}, y, xy, x^2y, \ldots, x^{p-1}y\}$

You can see the utility of Theorem 10 in the following example.

Example 3 : What are the possible algebraic structures of a group of order 6?

Solution : Let G be a group of order 6. Then, by Theorem 10, $G \simeq Z_6$ or $G \simeq D_6$. Of course, in E 7 of Unit 5, you must have already noted that $S_3 \simeq D_6$. So, if G is not cyclic, then $G \simeq S_3$. You may like to try the following exercise now.

E 12) Show that if G is a group of order 10, then $G \simeq Z_{10}$ or $G \simeq D_{10}$.

Now, from Theorem 6 of Unit 4, we know that if $o(G)$ is a prime, then G is cyclic. Thus, groups of orders 2, 3, 5 and 7 are cyclic. This fact, together with Example 3 and E 12, allows us to classify all groups whose orders are 1, 2, 3, 5, 6, 7 or 10. What about the structure of groups of order $4 = 2^2$ and $9 = 3^2$? Such groups are covered by the following result.

Theorem 11 : If G is a group of order p^2, p a prime, then G is abelian.

We will not prove this result, since its proof is beyond the scope of this course. But, using this theorem, we can easily classify groups of order p^2.

Theorem 12 : Let G be a group such that $o(G) = p^2$, where p is a prime. Then either G is cyclic or $G \simeq Z_p \times Z_p$, a direct product of two cyclic groups of order p.

Proof : Suppose G has an element a of order p^2. Then $G = \langle a \rangle$.

On the other hand, suppose G has no element of order p^2. Then, for any $x \in G$, $o(x) = 1$ or $o(x) = p$ (using Lagrange's Theorem).

Let $x \in G$, $x \neq e$ and $H = \langle x \rangle$. Since $x \neq e$, $o(H) \neq 1$

$\therefore o(H) = p$.

Therefore, $\exists\ y \in G$ such that $y \notin H$. Then, by the same reasoning, $K = \langle y \rangle$ is of order p. Both H and K are normal in G, since G is abelian (by Theorem 11).

We want to show that $G = H \times K$. For this, consider $H \cap K$. Now $H \cap K \leq H$.

$\therefore o(H \cap K) \mid o(H) = p$. $\therefore o(H \cap K) = 1$ or $o(H \cap K) = p$.

If $o(H \cap K) = p$, then $H \cap K = H$, and by similar reasoning, $H \cap K = K$. But then, $H = K$. $\therefore y \in H$, a contradiction.

$\therefore o(H \cap K) = 1$, i.e., $H \cap K = \{e\}$.

So, $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$ and $o(HK) = p^2 = o(G)$.

$\therefore G = H \times K \simeq Z_p \times Z_p$.

Now, try the following exercise.

E 13) What are the possible algebraic structures of groups of order 4 and 9?

So far we have shown the algebraic structure of all groups of order 1 to 10, except groups of order 8. Now we will list (without proof) the classification of groups of order 8.
If G is an abelian group of order 8, then

i) $G \simeq Z_8$, the cyclic group or order 8, or
ii) $G \simeq Z_4 \times Z_2$, or
iii) $G \simeq Z_2 \times Z_2 \times Z_2$.

If G is a non-abelian group of order 8, then

i) $G \simeq Q_8$, the quaternion group discussed in Example 4 of Unit 4, or
ii) $G \simeq D_8$, the dihedral group discussed in Example 4 of Unit 5.

So, we have seen what the atgebraic structureof any group of order 1, 2, ... , 10 must be. We have said that this classification is upto isomorphism. So, for example, any group of order 10 is isomorphic to Z_{10} or D_{10}. It need not be equal to either of them.

Let us now summarise what we have done in this unit.

8.5 SUMMARY

In this unit We have discussed the following points.

1. The definition and examples of external direct products of groups.
2. The definition and examples of internal direct products of normal subgroups.
3. If $(m, n) = 1$, then $Z_m \times Z_n \simeq Z_{mn}$.
4. $o(H \times K) = o(H)\, o(K)$.
5. The statement and application of Sylow's theorems, which state that:
   Let G be a finite group of order $p^n m$, where p is a prime and $p \nmid m$. Then
   i) G contains a subgroup of order $p^k\ \forall\ k = 1, \ldots, n$;
   ii) any two Sylow p-subgroups are conjugate in G;
   iii) the number of distinct Sylow p-subgroups of G is congruent to 1 (mod p) and divides $o(G)$ (in fact, it divides m).
6. Let $o(G) = pq$, p a prime, $p > q$, $q \nmid p - 1$. Then G is cyclic.

7. Let $o(G) = p^2$, p a prime. Then
   i) G is abelian.
   ii) G is cyclic or $G \simeq \mathbf{Z}_p \times \mathbf{Z}_p$.
8. The classification of groups of order 1 to 10, which we give in the following table.

o(G)	Algebraic structure
1	{e}
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$ or S_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$ or $\mathbf{Z}_4 \times \mathbf{Z}_2$ or $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ (if G is abelian) Q_8 or D_8 (if G is non-abelian)
9	$\mathbf{Z}_9$ or $\mathbf{Z}_3 \times \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$ or D_{10}

8.6 SOLUTIONS/ANSWERS

E 1) $*$ is associative : Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.
Use the fact that $*_1$ and $*_2$ are associative to prove that
$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3))$.
The identity element of G is (e_1, e_2), where e_1 and e_2 are the identities in G_1 and G_2, respectivelv.
The inverse of $(x, y) \in G$ is (x^{-1}, y^{-1}).

E 2) Define $f : G_1 \times G_2 \longrightarrow G_2 \times G_1 : f(a, b) = (b, a)$.
Then f is 1-1, surjective and a homomorphism. That is, f is an isomorphism.
$\therefore G_1 \times G_2 \simeq G_2 \times G_1$.

E 3) We need to show that any element of $G_1 \times G_2$ is of the form hk, where $h \in H$ and $k \in K$.
Now, any element of $G_1 \times G_2$ is $(x, y) = (x, e_2)(e_1, y)$ and $(x, e_2) \in H$, $(e1, y) \in K$.
$\therefore G_1 \times G_2 = HK$.
Now, let us look at $H \cap K$. Let $(x, y) \in H \cap K$.
Since $(x, y) \in H$, $y = e_2$. Since $(x, y) \in K$, $x = e_1$.
$\therefore (x, y) = (e1, e_2)$. $\therefore H \cap K = \{(e1, e_2)\}$.

E 4) Now, $(x, y) \in Z(G_1 \times Gz)$.
$\iff (x, y)(a, b) = (a, b)(x, y) \; \forall (a, b) \in G_1 \times G_2$
$\iff (xa, yb) = (ax, by) \; \forall a \in G_1, b \in G_2$
$\iff xa = ax \; \forall a \in G_1$ and $yb = by \; \forall b \in G_2$
$\iff x \in Z(G_1)$ and $y \in Z(G_2)$
$\iff (x, y) \in Z(G_1) \times Z(G_2)$
$\therefore Z(G_1 \times Gz) = Z(G_1) \times Z(G_2)$

E 5) Let $A = \langle x \rangle$ and $B = \langle y \rangle$, where $o(x) = m$, $o(y) = n$.
Then $A \simeq Z$, and $B \simeq \mathbf{Z}_n$.
If we prove that $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$, then we will have-proved that $A \times B \simeq \mathbf{Z}_{mn}$, that is, A X B is cyclic of order mn.
So, let us prove that if $(m, n) = 1$, then $\mathbf{Z}_{mn} \simeq \mathbf{Z}_m \times \mathbf{Z}_n$.
Define $f : \mathbf{Z} \longrightarrow \mathbf{Z}_m \times \mathbf{Z}_n : f(r) = (r + m\mathbf{Z}, r + n\mathbf{Z})$.
(Remember that $\mathbf{Z}_s = \mathbf{Z}/s\mathbf{Z}$, for any $s \in N$.)
Now, f is a homomorphism because
$f(r + s) = ((r + s) + m\mathbf{Z}, (r + s) + n\mathbf{Z})$
$= (r + m\mathbf{Z}, r + n\mathbf{Z}) + (s + m\mathbf{Z}, s + n\mathbf{Z})$.
$= f(r) + f(s)$.
$\text{Ker } f = \{r \in \mathbf{Z} \mid r \in m\mathbf{Z} \cap n\mathbf{Z}\}$
$= \{r \in \mathbf{Z} \mid r \in mn\mathbf{Z}\}$
$= mn\mathbf{Z}$.

Finally, we will show that f is surjective. Now, take any element $(u + mZ, v + nZ) \in Z_m \times Z_n$. Since $(m, n) = 1$, 3 s, t E Z such that $ms + nt = 1$ (see Sec. 1.6). Using this equation we see that $f(u(1 - ms) + v(1 - nt)) = (u + mZ, v + nZ)$.
Thus, f is surjective.
Now, we apply the Fundamental Theorem of Homomorphism and find that $Z/\text{Ker } f \simeq \text{Im } f$, that is, $Z/mnZ \simeq Z_m \times Z_n$, that is, $Z_{mn} \simeq Z_m \times Z_n$.
$\therefore$ A $\times$ B is cyclic of order mn.

E 6) We know that each $x \in G$ can be expressed as hk, where $h \in H$ and $k \in K$.
$\therefore$ $G = HK$.
We need to show that $H \cap K = \{e\}$. Let $x \in H \cap K$.
Then $x \in H$ and $x \in K$. $\therefore$ xe E HK and $ex \in HK$.
So, x has two representations, xe and ex, as a product of an element of H and an element of K. But we have assumed that each element must have only one such representation. So the two representations xe and ex must coincide, that is, $x = e$. $\therefore$ $H \cap K = \{e\}$.
$\therefore$ $G = H \times K$.

E 7) $G = H \times K \Rightarrow G/H \simeq K \Rightarrow o(G/H) = o(K) \Rightarrow o(G)/o(H) = o(K)$.
$\Rightarrow o(G) = o(H)\, o(K)$.

E 8) $H \trianglelefteq G \iff g^{-1}Hg = H \; \forall g \in G \iff$ the only conjugate of H in G is H.

E 9) Let G be a group of order 20. Since $20 = 2^2 \times 5$, G has a Sylow 5-subgroup. The number of such subgroups is congruent to 1(mod 5) and divides 4. Thus, the number is 1. Therefore, the Sylow 5-subgroup of G is normal in G, and is the required subgroup.

E 10) $o(Z_{24}) = 24 = 2^3 \times 3$.
$\therefore$ Z_{24} has a Sylow 2-subgroup and a Sylow 3-subgroup. The number of Sylow 2-subgroups is 1 or 3 and the number of Sylow 3-subgroups is 1 or 4. Now, if Z_{24} has only 1 Sylow 2-subgroup, this accounts for 8 elements of the group. So, we are left with 16 elements of order 3. But this is not possible because we can only have at most 4 distinct Sylow 3-subgroups (i.e., 8 elements of order 3). So, we reach a contradiction.
$\therefore$ Z_{24} must have 3 Sylow 2-subgroups. And then it will have only 1 Sylow 3-subgroup. These are all the Sylow p-subgroups of Z_{24}.

E 11) $255 = 3 \times 5 \times 17 = 5 \times 51$.
The number of Sylow 5-subgroups is congruent to 1(mod 5) and must divide 51. Thus, it is 1 or 51.
Since $255 = 3 \times 85$, the number of Sylow 3-subgroups that G can have is congruent to 1(mod 3) and must divide 85. Thus, it is 1 or 85.

E 12) We can apply Theorem 10 here.

E 13) Applying Theorem i2, we see that
i) $o(G) = 4 \Rightarrow G \simeq Z_4$ or $G \simeq 2\,2 \times Z_2$.
ii) $o(G) = 9 \Rightarrow G \simeq Z_9$ Or $G \simeq Z_3 \times Z_3$.

VIDEO PROGRAMME NOTES (MTE-06)

Groups of Symmetries

(To be viewed **after** studying Block 2)

Content Coordinator: Dr. **Parvin Sinclair**
School of Sciences
IGNOU

Producer: Sunil Das
Communication Division
IGNOU

A symmetry of an object is a movement that brings the object into superposition with itself. In this programme we look at the symmetries of various two-and three-dimensional geometrical objects. We use them as examples to concretise certain concepts of group theory that you have studied in the first two blocks of this course.

During the programme you will see that the set of all symmetries of an object forms a group, which is the group of symmetries (or the **symmetry** group) of the object. It turns out that this group is a permutation group.

An object can have rotational as well as reflection symmetries. In the programme you will see that the set of rotational symmetries is a subgroup of the group of symmetries of the object. In particular, you will see that

i) the group of rotational symmetries of a regular n-sided polygon is the dihedral group
$D_{2n} = \langle \{x,y \mid x^2 = e,\ y^n = e,\ xy = y^{-1}x\} \rangle$,
where e is the identity of the group.

ii) the group of rotational symmetries of a regular tetrahedron is A_4 and the group of all its symmetries is S_4.

iii) the group of rotational symmetries of a cube is S_4.

iv) the group of rotational symmetries of a regular octahedron is S_4, since a cube and regular octahedron are the duals of each other.

During the programme we have given you the following activities to do after viewing the programme.

1) Check that the composition of symmetries of an object is an associative operation.

2) Obtain the group of symmetries of a snow crystal.
(Hint: As we have said in the programme, this is the same as the group of symmetries of a regular hexagon. You need to check that this group is D_{12}. Note that a 5-cycle can't be a symmetry of a hexagon, because any symmetry that moves 5 vertices must move all 6 vertices.)

3) Find the group of rotational symmetries of a methane molecule.
(Hint: The molecule's structure is tetrahedral, with the hydrogen atoms at the vertices and the carbon atom inside the tetrahedron, at an equal distance from each of the vertices.)

4) Find all the **24** rotational symmetries of a cube.
(In the programme we have shown you that these symmetries are elements of S_4, S_6 or S_8, depending on whether we are observing the permutations of its diagonals, its faces or its vertices.)