Study Material on Group Theory - II

Department of Mathematics, P. R. Thakur Govt. College
MTMACOR12T: (Semester - 5)

University Syllabus

Unit 1: Automorphism, inner automorphism, automorphism groups. Automorphism groups of finite and infinite cyclic groups, applications of factor groups to automorphism groups, Characteristic subgroups, Commutator subgroup and its properties.

Unit 2 : Properties of external direct products, the group of units modulo n as an external direct product, internal direct products, Fundamental Theorem of finite abelian groups.

Unit 3 : Group actions, stabilizers and kernels, permutation representation associated with a given group action. Applications of group actions. Generalized Cayley's theorem. Index theorem.

Unit 4 : Groups acting on themselves by conjugation, class equation and consequences, conjugacy in S_n, p-groups, Sylow's theorems and consequences, Cauchy's theorem, Simplicity of A_n for $n \geq 5$, non-simplicity tests.

0 Review of the previous study

In this section we recall some definitions state some results without proof from what we have already studied.

Definition. 0.1 Let $(G, \cdot)$ and $(G', *)$ be two groups, a function $\phi : G \to G'$ is called a *group homomorphism* if for all $a, b \in G$, $\phi(a \cdot b) = \phi(a) * \phi(b)$.

If $\phi : G \to G'$ is an injective group homorphism then it is called a *monomorphism*. If ϕ is bijective it is called an *isomorphism* and in this case the groups G and G' are called *isomorphic*.

When we are not so formal and do not mention the group operations we simply write it as $\phi(ab) = \phi(a)\phi(b)$. However we always remember the fact that in left hand side ab means $a \cdot b$, i.e., the operation in group $(G, \cdot)$ and in right hand side

$\phi(a)\phi(b)$ means $\phi(a) * \phi(b)$, i.e., the operation in the group $(G', *)$. Henceforth by a homomorphism we shall mean a group homomorphism.

THEOREM. 0.2 *Let $\phi : G \to G'$ be a homomorphism. Then*

1. *If e, e' are the identity elements of G and G' respectively then $\phi(e) = e'$.*
2. *For any $a \in G$, $\phi(a^{-1}) = (\phi(a))^{-1}$.*
3. *If H is a subgroup of G then $H' = \phi(H) = \{\phi(h) : h \in H\}$ is a subgroup of G'.*
4. *If K' is a subgroup of G' then $K = \phi^{-1}(K') = \{h \in G : \phi(h) \in K'\}$ is a subgroup of G.*

DEFINITION. 0.3 A subgroup H of a group G is called a *normal subgroup* if for all $g \in G$ for all $h \in H$, $ghg^{-1} \in H$. In symbol it is written as $gHg^{-1} \subset H$ for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

When G is an abelian group then every subgroup of G is a normal subgroup.

DEFINITION. 0.4 Let G be a group and H be a subgroup of G. For any $a \in G$ the set $aH = \{ah : h \in H\}$ is called a *left coset* of H. Similarly the set $Ha = \{ha : h \in H\}$ is a *right coset* of H.

THEOREM. 0.5 *If H is a normal subgroup of G then for any $a \in G$, $aH = Ha$, i.e., the left coset and the right coset of a normal group are the same.*

In view of the above theorem we shall not distinguish between the left cosets and right cosets of a normal subgroup and say only cosets.

THEOREM. 0.6 *If H is a normal subgroup of a group G then the set of all cosets of H, denoted by G/H, form a group under the operation $(aH)(bH) = abH$ for all $aH, bH \in G/H$. This group is called the* factor group *or* quotient group.

THEOREM. 0.7 *If G, G' are groups and $\phi : G \to G'$ is a homomorphism then the kernel of ϕ defined by $\ker \phi = \{x \in G : \phi(x) = e'\}$, where e' is the identity element of G', is a normal subgroup of G.*

THEOREM. 0.8 *If $\phi : G \to G'$ is a homomorphism of groups then $G/\ker \phi$ is a group and is isomorphic to $\phi(G)$.*

In the above theorem if ϕ is onto G' then $G/\ker \phi$ is isomorphic to G'. If $\ker \phi = H$, for $a \in G$, $aH \mapsto \phi(a)$ is the isomorphism of G/H onto G'.

0.1 Exercise

1. For $n \in \mathbb{N}$ show that $(\mathbb{Z}_n, +)$ is a commutative group, where the addition is modulo n.

2. Write down the composition table of $(\mathbb{Z}_2, +)$.

3. Show that S_n, the set of all permutations on the set $\{1, 2, \ldots, n\}$ is a group with respect to composition of functions. Is it commutative? support your answer.

4. Verify which of the following functions are homomorphisms and find the kernels of each homomorphism:

   (a) $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$, where $\phi(n) =$ the remainder when n is divided by 2.

   (b) $\phi : \mathbb{Z}_9 \to \mathbb{Z}_2$, where $\phi(n) =$ the remainder when n is divided by 2.

   (c) $\phi : S_3 \to \mathbb{Z}_2$ defined by $\phi(\sigma) = 0$ if σ is an even permutation, and $\phi(\sigma) = 1$ if σ is an odd permutation.

   (d) $\phi : M_n \to \mathbb{R}$ defined by $\phi(A) = |A|$, where M_n denotes the additive group of all $n \times n$ real matrices and for $A \in M_n$, $|A|$ denotes the determinant of A.

5. Let H be a normal subgroup of a group G, a relation ρ_H on G is defined by $a\rho_H b$ iff $a^{-1}b \in H$. Show that ρ_H is an equivalence relation on G and identify the equivalence classes.

6. Let $p > 1$ be an integer, define $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$ by $\phi_p(n) =$ remainder when n is divided by p. Verify that ϕ_p is a homomorphism, find the kernel $\ker \phi_p$ and find the quotient group $\mathbb{Z}/\ker \phi_p$.

1 Automorphism

1.1 Definition and elementary properties

Definition. 1.1 An isomorphism from a group G onto itself is called an automorphism on G. The set of all automorphisms on a group G is denoted by $\mathrm{Aut}(G)$.

Let G be a group and S_G denote the set of all bijections from G to G, If G is finite then S_G is nothing but the permutation group of the set G. Thus $\mathrm{Aut}(G)$ is a subset of S_G. We know that S_G is a group under composition of mappings. Also composition of two homomorphisms is also a homomorphism and inverse of an isomorphism is an isomorphism, it follows that $\mathrm{Aut}(G)$ is a group under composition of mappings. Hence the following result follows immediately.

Theorem. 1.2 $\mathrm{Aut}(G)$, *the set of all automorphisms of a group G is a group under composition of mappings and is a subgroup of S_G.*

Definition. 1.3 The group $\mathrm{Aut}(G)$ is called the *automorphism group* of G, where G is a group.

Theorem. 1.4 *Let G be a group. For each $g \in G$ define $i_g : G \to G$ by*

$$i_g(x) = gxg^{-1} \text{ for all } x \in G.$$

Then i_g is an automorphism.

Proof. First, to show that i_g is a homomorphism choose $x_1, x_2 \in G$. Then $i_g(x_1x_2) = g(x_1x_2)g^{-1} = g(x_1ex_2)g^{-1} = (gx_1)(g^{-1}g)(x_2g^{-1}) = (gx_1g^{-1})(gx_2g^{-1}) = i_g(x_1)ig(x_2)$. Hence i_g is a homomorphism.

To show that i_g is one-one, take $x_1, x_2 \in G$ such that $i_g(x_1) = i_g(x_2)$. Then $gx_1g^{-1} = gx_2g^{-1}$, by cancellation law we have $x_1 = x_2$.

Finally, for $y \in G$ take $x = g^{-1}yg$. Then $i_g(x) = gxg^{-1} = g(g^{-1}yg)g^{-1} = (gg^{-1})y(gg^{-1}) = y$. This i_g is onto. Hence $i_g : G \to G$ is an isomorphism, i.e., i_g is an automorphism on G. ■

Definition. 1.5 Let G be a group, for $g \in G$ the automorphism i_g is called an *inner automorphism*. The set of all inner automorphisms of G is denoted by $\mathrm{Inn}(G)$.

THEOREM. 1.6 *For a group G,* $\text{Inn}(G)$ *is a subgroup of* $\text{Aut}(G)$*.*

PROOF. Take $i_g, i_h \in \text{Inn}(G)$ where $g, h \in G$. Then for $x \in G$, $i_g \circ i_h(x) = i_g(i_h(x)) = i_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = i_{gh}(x)$. Since this is true for all $x \in G$ it follows that $i_g \circ i_h = i_{gh}$ and since $i_{gh} \in \text{Inn}(G)$ it follows that $i_g \circ i_h \in \text{Inn}(G)$. Thus $\text{Inn}(G)$ is closed under composition of mappings.

Also for $i_g \in \text{Inn}(G)$ and for $x \in G$, $i_g(x) = y \Rightarrow gxg^{-1} = y \Rightarrow x = g^{-1}yg \Rightarrow x = i_{g^{-1}}(y)$. Hence $i_g^{-1} = i_{g^{-1}}$ and hence $i_g^{-1} \in \text{Inn}(G)$.

Thus $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$. ■

We have already studied centralizer and center of a group in our previous classes. However we recall the definition and a few elementary properties without proof.

DEFINITION. 1.7 Let G be a group and A be a non-empty subset of G. Then the set $\{g \in G : gag^{-1} = a \ \forall a \in A\}$ is called the *centralizer* of the set A and is denoted by $C_G(A)$. When $A = \{a\}$ is a singleton set, instead of $C_G(\{a\})$, we write its centralizer as $C_G(a)$, or simply by $C(a)$ when no confusion about G may arise.

It can be noted that for $a \in A$ and $g \in G$, $gag^{-1} = a$ is true if and only if $ga = ag$. Thus the centralizer of a set A is actually those elements of G which commute with every member of A.

THEOREM. 1.8 *The centralizer of a subset of a group is a subgroup of that group.*

DEFINITION. 1.9 The *center* of a group G is the set of all those members of G which commute with every member of G and is denoted by $Z(G)$. Thus $Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$.

It can be observed that $Z(G)$ is nothing but the centralizer of the whole group G, i.e., $Z(G) = C_G(G)$. Since centralizer of a subset of G is a subgroup of G as a particular case we can conclude immediately that $Z(G)$ is a subgroup of G. More precisely, one can prove that

THEOREM. 1.10 *For a group G, $Z(G)$ is a normal subgroup of G.*

THEOREM. 1.11 *Let G be a group, the function $\phi : G \to \text{Aut}(G)$, defined by $\phi(g) = i_g$ for all $g \in G$, is a homomorphism. The image $Im(\phi) = \text{Inn}(G)$ and the kernel is $\ker \phi = Z(G)$, the center of G.*

PROOF. For $g, h \in G$, $\phi(gh) = i_{gh} = i_g \circ i_h$ (already verified) $= \phi(g) \circ \phi(h)$. Hence ϕ is a homomorphism of G into $\text{Aut}(G)$. Since for $g \in G$, $\phi(g) = i_g$, is an inner automorphism, $\phi(G) \subset \text{Inn}(G)$. To show that $Im(\phi) = \text{Inn}(G)$ take $i_g \in \text{Inn}(G)$, since $\phi(g) = i_g$ it follows that ϕ is onto $\text{Inn}(G)$. Thus $Im(\phi) = \text{Inn}(G)$.

For the last part, let $g \in \ker \phi$. Then $\phi(g) = i$, the identity mapping of G which is the identity element of $\text{Aut}(G)$. Then

$$\begin{aligned} & i_g(x) = i(x) \quad \text{for all } x \in G \\ \Rightarrow\ & gxg^{-1} = x \quad \text{for all } x \in G \\ \Rightarrow\ & gx = xg \quad \text{for all } x \in G \\ \Rightarrow\ & g \in Z(G). \end{aligned}$$

Thus $\ker \phi \subset Z(G)$. On the other hand

$$\begin{aligned} g \in Z(G) \ \Rightarrow\ & gx = xg \quad \text{for all } x \in G \\ \Rightarrow\ & gxg^{-1} = x \quad \text{for all } x \in G \\ \Rightarrow\ & i_g(x) = x \quad \text{for all } x \in G \\ \Rightarrow\ & i_g = i \ \Rightarrow\ \phi(g) = i, \end{aligned}$$

i.e., $g \in \ker \phi$. Thus $Z(G) \subset \ker \phi$. Hence $\ker \phi = Z(G)$. ■

THEOREM. 1.12 *For a group G, $G/Z(G) \simeq \text{Inn}(G)$.*

PROOF. This result follows from the previous theorem and the First Isomorphism Theorem. ■

We know there is only one (up to isomorphism) infinite cyclic group $(\mathbb{Z}, +)$ and the only non-zero homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are of the type $a \mapsto na$ where $n \in \mathbb{Z}$. The map $a \mapsto na$ is onto if and only if $n = 1$, i.e., the identity map. Hence the only automorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is the identity map, in other words we have $\text{Aut}(\mathbb{Z}) = \{i\}$, where i denotes the identity map.

We now try to find $\text{Aut}(G)$ where G is a finite cyclic group. Recall that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ is the additive group of integers modulo n whose elements are $(0), (1), (2), \ldots, (n-1)$. Note that $\mathbb{Z}_n$ is also a commutative ring, known as residue class ring modulo n. An element (k) of $\mathbb{Z}_n$ is called an unit if there exists $(l) \in \mathbb{Z}_n$ such that $(k)(l) = (1)$, i.e., if (k) has a multiplicative inverse in $\mathbb{Z}_n$. Note that the element (k) is a unit if and only if $\gcd(k, n) = 1$ and hence the number of units of $\mathbb{Z}_n$ is $\phi(n)$. The set of all the units of $\mathbb{Z}_n$ is denoted by U_n. U_n forms an abelian group under multiplication (modulo n) and is denoted by $(\mathbb{Z}/n\mathbb{Z})^{\times}$. However we shall write it as $(U_n, \cdot)$.

THEOREM. 1.13 *If G is a cyclic group of order n then its automorphism group* $\mathrm{Aut}(G)$ *is isomorphic to* $(U_n, \cdot)$.

PROOF. Let x be a generator of G, i.e., $G = \langle x \rangle$. Since $|G| = n$ we have $|x| = n$ and $G = \{1, x, x^2, \ldots, x^{n-1}\}$. If $f \in \mathrm{Aut}(G)$ then there exists $k \in \{0, 1, \ldots, n-1\}$ such that $f(x) = x^k$. Note that this k uniquely determines f and hence we can write $f = f_k$. Now f_k being an automorphism and x being a generator of G we have $f_k(x) = x^k$ is also a generator of G, and hence x and x^k have the same order n. This is true if and only if $\gcd(n, k) = 1$, i.e., if and only if $(k) \in U_n$.

Define a map $\Psi : \mathrm{Aut}(G) \to U_n$ as follows: $\Psi(f_k) = (k)$ for all $f_k \in \mathrm{Aut}(G)$. First note that Ψ is onto, since for each $(k) \in U_n$, $\Psi(f_k) = (k)$. To prove that Ψ is a homomorphism, take $f_k, f_l \in \mathrm{Aut}(G)$. Then $(f_k \circ f_l)(x) = f_k(f_l(x)) = f_k(x^l) = (x^l)^k = x^{kl} = x^m = f_m(x)$, where $kl \equiv m \ (mod\ n)$. Hence $\Psi(f_k \circ f_l) = (m) = (kl) = (k)(l) = \Psi(f_k)\Psi(f_l)$. Finally, to check that Ψ is injective take $f_k, f_l \in \mathrm{Aut}(G)$. Then $\Psi(f_k) = \Psi(f_l) \iff (k) = (l)$. Hence $\Psi : \mathrm{Aut}(G) \to (U_n, \cdot)$ is an isomorphism. ■

1.2 Characteristic subgroups and Commutator Subgroups

A subgroup N of a group G is a normal subgroup if $gNg^{-1} \subset N$ for all $g \in G$. As the inequality $gNg^{-1} \subset N$ for all $g \in G$ implies the reverse inequality $N \subset gNg^{-1} = N$ for all $g \in G$, it follows that N is a normal subgroup if and only if $gNg^{-1} = N$ for all $g \in G$. Considering the inner automorphism i_g for $g \in G$ we can see that a subgroup N of G is a normal subgroup if and only if $i_g(N) \subset N$ for all $g \in G$, where $i_g(N) = \{i_g(x) : x \in N\}$. Now replacing inner automorphism with any automorphism we get a class of subgroups stronger than normal subgroups.

DEFINITION. 1.14 A subgroup H of a group G is called a *Characteristic subgroup of G* or *Characteristic in G* if $\phi(H) \subset H$ for every automorphism ϕ on G. If H is a Characteristic subgroup of G it is denoted by H *char* G.

THEOREM. 1.15 *A Characteristic subgroup is always a normal subgroup.*

PROOF. This immediate follows as i_g is an automorphism for all $g \in G$. ■

Recall that $N \lhd G$ means N is a normal subgroup of G. The following example shows that if $N' \lhd N$ and $N \lhd G$ then it does not follows that $N' \lhd G$, i.e., transitivity of normality does not hold.

EXAMPLE. 1.16 Let $G = D_4$ the dihedral group of all the symmetric transformations of a square generated by the rotation r by $90°$ about its centre and flip s about the vertical line through the center. The elements of D_4 are $1, r, r^2, r^3, s, rs, r^2s, r^3s$. Let $N = \{1, s, r^2, r^2s\}$ and $N' = \{1, s\}$. Note that $N' < N < G$. Also, since $\frac{|G|}{|N|} = 2$ and $\frac{|N|}{N'|} = 2$ it follows that $N' \lhd N$ and $N \lhd G$. But N' is not a normal subgroup of G, since for $r \in G, s \in N'$, $rsr^{-1} \notin N'$.

The transitivity of characteristic subgroups hold.

THEOREM. 1.17 *If G is a group, H, K are subgroups of G such that K char H and H char G. Then K char G.*

PROOF. Let $\phi \in \text{Aut}(G)$. Then, since H *char* G, we have $\phi(H) = H$ and hence $\phi|_H$, the restriction of ϕ on H, is an automorphism of H. Since K *char* H, $\phi|_H(K) = K$. But $\phi|_H(K) = \phi(K)$ and hence $\phi(K) = K$. Since ϕ has been chosen arbitrarily in $\text{Aut}(G)$ it follows that K *char* G. ■

THEOREM. 1.18 *For a group G the center $Z(G)$ of G is Characteristic in G.*

PROOF. Note that $Z(G) = \{x \in G : xg = gx\ \forall g \in G\}$. Let $\phi \in \text{Aut}(G)$, then we have to show that $\phi(Z(G)) \subset Z(G)$. Let us choose $x \in Z(G)$. For $g \in G$ since ϕ is an automorphism on G there exists $h \in G$ such that $g = \phi(h)$. Then

$$\begin{aligned} \phi(x)g &= \phi(x)\phi(h) = \phi(xh) \\ &= \phi(hx) \text{ (since } x \in Z(G)) \\ &= \phi(h)\phi(x) = g\phi(x). \end{aligned}$$

This shows that $\phi(x) \in Z(G)$. Since x has been chosen arbitrarily in $Z(G)$ it follows that $\phi(Z(G)) \subset Z(G)$. ϕ has been chosen arbitrarily in $\text{Aut}(G)$, hence $\phi(Z(G)) \subset Z(G))$ for all $\phi \in \text{Aut}(G)$. Thus $Z(G)$ *char* G. ■

The following corollary has already been stated without proof (Theorem 1.10).

COROLLARY. 1.19 *$Z(G)$ is a normal subgroup of G.*

DEFINITION. 1.20 Let G be a group. For $x, y \in G$ the element $x^{-1}y^{-1}xy$ is called *commutator* of the elements x and y and is denoted by $[x, y]$. An element $z \in G$ is called a *commutator* of G if there exists $x, y \in G$ such that $z = [x, y]$. The group generated by the set of all the commutators of G is called the *commutator subgroup* of G.

It immediately follows that for $x, y \in G$, (i) $[x, y]^{-1} = [y, x]$ and (ii) if $f : G \to H$ is a homomorphism then $f([x, y]) = [f(x), f(y)]$.

THEOREM. 1.21 *A group is G abelian if and only if its commutator group is $\{e\}$, the trivial subgroup.*

PROOF. This immediately follows since $[x,y] = e$ for all $x, y \in G$ if and only if $x^{-1}y^{-1}xy = e$ for all $x, y \in G$ if and only if $xy = yx$ for all $x, y \in G$. ■

THEOREM. 1.22 *If $\phi \in \text{Aut}(G)$ then for $x, y \in G$, $\phi([x,y]) = [\phi(x), \phi(y)]$.*

PROOF. Since ϕ is a homomorphism,

$$\begin{aligned}\phi([x,y]) &= \phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y) \\ &= (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y) = [\phi(x), \phi(y)].\end{aligned}$$

THEOREM. 1.23 *The commutator subgroup of G is a characteristic subgroup of G*

PROOF. Let H be the commutator subgroup of G. Choose $\phi \in \text{Aut}(G)$, to show that $\phi(H) \subset H$. Since H is generated by all the commutators of G it is sufficient to show that for any commutator $x^{-1}y^{-1}xy$ of G $\phi(x^{-1}y^{-1}xy)$ is also a commutator. Since

$$\phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y)$$

it follows that $\phi(x^{-1}y^{-1}xy)$ is the commutator of $\phi(x)$ and $\phi(y)$ and hence H is a characteristic subgroup of G. ■

THEOREM. 1.24 *For a group G if H is the commutator subgroup of G then the quotient group G/H is abelian.*

PROOF. Since H *char* G, H is a normal subgroup of G and hence the group G/H is defined. Let us take two left cosets xH, yH in G/H. Then

$$\begin{aligned}xHyH &= xyH = xy(y^{-1}x^{-1}yx)H \quad (\text{since } y^{-1}x^{-1}yx \in H) \\ &= (xyy^{-1}x^{-1})yxH = yxH = yHxH.\end{aligned}$$

Hence G/H is abelian. ■

THEOREM. 1.25 *Let $\phi : G \to G'$ be a homomorphism where the group G' is abelian. Then the commutator subgroup of G is contained in* $\ker\phi$.

PROOF. Since the commutator subgroup H is generated by all the commutators of G it is sufficient to show that all the commutators of G belong to $\ker\phi$. Let us take a commutator $x^{-1}y^{-1}xy$, where $x, y \in G$. Then $\phi(x), \phi(y) \in G'$. Since G' is abelian we have

$$\begin{aligned} & \phi(x)\phi(y) = \phi(y)\phi(x) \\ \Rightarrow\ & \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) = e', \quad \text{where } e' \text{ is the identity element of } g' \\ \Rightarrow\ & \phi(x^{-1}y^{-1}xy) = e' \\ \Rightarrow\ & x^{-1}y^{-1}xy \in \ker\phi. \end{aligned}$$

Hence $H \subset \ker\phi$. ■

THEOREM. 1.26 *If N is a normal subgroup of a group G then G/N is abelian if and only if the commutator subgroup of G is a normal subgroup of N.*

PROOF. Let H denote the commutator subgroup of G. Assume that G/N is abelian. Let $\phi : G \to G/N$ be the natural homomorphism of G onto G/N. Since G/N is abelian, $H \subset \ker\phi$. But $\ker\phi = N$ and hence H is a subgroup of N. Since H is a characteristic subgroup it is a normal subgroup of N.

Conversely, assume that H is a normal subgroup of N, to show that G/N is abelian. Take $xN, yN \in G/N$. Then

$$\begin{aligned} xNyN &= xyN = xy(y^{-1}x^{-1}yx)N \quad (\text{since } y^{-1}x^{-1}yx \in H \subset N) \\ &= (xyy^{-1}x^{-1})yxN = yxN = yNxN. \end{aligned}$$

Thus G/N is an abelian group. ■

1.3 Exercises

1. Let G be an infinite cyclic group. Prove that the group of automorphism of G is isomorphic to the additive group $\mathbb{Z}_2$ of integers modulo 2.

2. Find (i) Aut($\mathbb{Z}_{15}$) (ii) Aut($\mathbb{Z}_{13}$) (iii) Aut($\mathbb{Z}_{16}$) and (iv) Aut($\mathbb{Z}_{30}$).

3. Write down the composition table of D_4 and find $Z(D_4)$ and the commutator subgroup of D_4.

4. Write down the composition table of S_3 and find $Z(S_3)$ and the commutator subgroup of S_3.

5. Let H be a subgroup of a group G. Prove that $H \subset G'$ if and only if H is a normal subgroup of G and the factor group G/H is Abelian, where G' denotes the commutator subgroup of G.

2 Direct product of groups

2.1 External Direct Product

DEFINITION. 2.1 Let $G_1, G_2, \ldots, G_n$ be n groups. A binary operation $\cdot$ can be introduced on the product set $G_1 \times G_2 \times \cdots \times G_n$ by the following rule: for $(g_1, g_2, \ldots, g_n), (g_1', g_2', \ldots, g_n') \in G_1 \times G_2 \times \cdots \times G_n$,

$$(g_1, g_2, \ldots, g_n) \cdot (g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n'),$$

where for $1 \leq i \leq n$, $g_i g_i'$ is the composition in the respective group G_i.

With respect to this binary operation the product set $G_1 \times G_2 \times \cdots \times G_n$ becomes a group, called the *external direct product* of the groups $G_1, G_2, \ldots, G_n$ and is denoted by $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

It immediately follows that if e_i is the identity element of the group G_i, $1 \leq i \leq n$, then $(e_1, e_2, \ldots, e_n)$ is the identity element of the group $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

EXAMPLE. 2.2 1. Let $G_1 = \mathbb{Z}_2$ and $G_2 = \mathbb{Z}_3$, the residue classes of $\mathbb{Z}$ modulo 2 and 3 respectively. Then $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$. The composition table is as follows:

$\cdot$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Note that the composition for the first component is addition modulo 2 whereas the composition for the second component is addition modulo 3.

2. Recall that for $n \in \mathbb{N}$ the group of units of $\mathbb{Z}_n$ is the set $U_n = \{[k] \in \mathbb{Z}_n : 1 \leq k \leq n, \gcd(k,n) = 1\}$ where is composition is multiplication modulo n. For example as $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$, $U_8 = \{1,3,5,7\}$. Similarly $U_6 = \{1,5\}$. Then

$$U_6 \oplus U_8 = \{(1,1), (1,3), (1,5), (1,7), (5,1), (5,3), (5,5), (5,7)\}$$

The composition for the first component is multiplication modulo 6 and for the second component is multiplication modulo 8. For example $(5,3) \cdot (5,7) =$

$(25, 21) = (1, 5)$. Similarly $(1, 7) \cdot (5, 7) = (5, 49) = (5, 1)$. The composition table is given as follows:

$\cdot$	$(1,1)$	$(1,3)$	$(1,5)$	$(1,7)$	$(5,1)$	$(5,3)$	$(5,5)$	$(5,7)$
$(1,1)$	$(1,1)$	$(1,3)$	$(1,5)$	$(1,7)$	$(5,1)$	$(5,3)$	$(5,5)$	$(5,7)$
$(1,3)$	$(1,3)$	$(1,1)$	$(1,7)$	$(1,5)$	$(5,3)$	$(5,1)$	$(5,7)$	$(5,5)$
$(1,5)$	$(1,5)$	$(1,7)$	$(1,1)$	$(1,3)$	$(5,5)$	$(5,7)$	$(5,1)$	$(5,3)$
$(1,7)$	$(1,7)$	$(1,5)$	$(1,3)$	$(1,1)$	$(5,7)$	$(5,5)$	$(5,3)$	$(5,1)$
$(5,1)$	$(5,1)$	$(5,3)$	$(5,5)$	$(5,7)$	$(1,1)$	$(1,3)$	$(1,5)$	$(1,7)$
$(5,3)$	$(5,3)$	$(5,1)$	$(5,7)$	$(5,5)$	$(1,3)$	$(1,1)$	$(1,7)$	$(1,5)$
$(5,5)$	$(5,5)$	$(5,7)$	$(5,1)$	$(5,3)$	$(1,5)$	$(1,7)$	$(1,1)$	$(1,3)$
$(5,7)$	$(5,7)$	$(5,5)$	$(5,3)$	$(5,1)$	$(1,7)$	$(1,5)$	$(1,3)$	$(1,1)$

3. In a similar manner $U_8 \oplus U_{12} = \{(1,1), (1,5), (1,7), (1,11), (3,1), (3,5), (3,7), (3,11), (5,1), (5,5), (5,7), (5,11), (7,1), (7,5), (7,7), (7,11)\}$. The composition for the first component is multiplication modulo 8 and for the second component is multiplication modulo 12. For example $(3,5) \cdot (5,7) = (15,35) = (7,11)$. Similarly, $(3,7) \cdot (7,11) = (21,77) = (5,5)$.

4. We know $\mathbb{R}$ is an additive group. The group $\mathbb{R} \oplus \mathbb{R}$ is the Cartesian product $\mathbb{R}^2$ with addition is defined as $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $(0,0)$ being the identity element. Similarly taking n copies of $\mathbb{R}$ we get the additive group $\mathbb{R}^n$, where addition is component wise.

THEOREM. 2.3 *For n finite groups $G_1, G_2, \ldots, G_n$ and for any $(a_1, a_2, \ldots, a_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$, the order $o(a_1, a_2, \ldots, a_n) = \operatorname{lcm}(o(a_1), o(a_2), \ldots, o(a_n))$.*

PROOF. Let $o(a_i) = k_i, 1 \leq i \leq n$, $m = \operatorname{lcm}(k_1, k_2, \ldots, k_n)$ and $k = o(a_1, a_2, \ldots, a_n)$. Then m is a multiple of each k_i. Now $(a_1, a_2, \ldots, a_n)^m = (a_1^m, a_2^m, \ldots, a_n^m) = (e_1, e_2, \ldots, e_n)$, where e_i is the identity element of G_i. So m is a multiple of k, i.e., k divides m.

On the other hand, $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$ shows that $a_i^k = e_i$ for $i = 1, 2, \ldots, n$, hence k must be a multiple of k_i for each $i = 1, 2, \ldots, n$. Thus m divides k. Hence $k = m$, i.e., $o(a_1, a_2, \ldots, a_n) = \operatorname{lcm}(o(a_1), o(a_2), \ldots, o(a_n))$. ∎

It can be observed that the group $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is a group of order 6, The group $\mathbb{Z}_6$ is also a group of order 6 which is cyclic. The group $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is generated by $(1,1)$, for $2(1,1) = (2,2) = (0,2), 3(1,1) = (3,3) = (1,0), 4(1,1) = (4,4) = (0,1), 5(1,1) = (5,5) = (1,2)$ and $6(1,1) = (6,6) = (0,0)$. Thus $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is also a cyclic group of order 6. Since cyclic groups of same order are isomorphic, $\mathbb{Z}_6$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ are isomorphic.

The group $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ is a group of order 4. Note that order of each element of this group is 2 and hence it can not be a cyclic group.

The following theorem answers the question when the external product of two cyclic groups is also a cyclic group.

THEOREM. 2.4 *If G and H are finite cyclic groups then $G \oplus H$ is cyclic if and only if $o(G)$ and $o(H)$ are prime to each other.*

PROOF. Let G, H be cyclic groups with $o(G) = m, o(H) = n$. Then $o(G \oplus H) = mn$.

Assume that $\gcd(m,n) = 1$, $G = \langle a \rangle$ and $H = \langle b \rangle$. Then $o(a) = m$ and $o(b) = n$ and hence $o(a,b) = \text{lcm}(o(a), o(b)) = \text{lcm}(m,n) = mn$. This shows that (a,b) is a generator of $G \oplus H$ and hence $G \oplus H$ is a cyclic group.

Conversely, assume that $G \oplus H$ is a cyclic group. Let (a,b) be a generator of $G \oplus H$. Note that $a^m = e_1$ and $b^n = e_2$, where e_1, e_2 are the identity elements of G and H respectively. If $d = \gcd(m,n)$ then d divides both m and n. Now $(a,b)^{mn/d} = (a^{mn/d}, b^{mn/d}) = ((a^m)^{n/d}, (b^n)^{m/d}) = (e_1^{n/d}, e_2^{m/d}) = (e_1, e_2)$. This shows that $o(a,b) \leq \frac{mn}{d}$, but (a,b) being a generator of $G \oplus H$ we must have $o(a,b) = mn$. Thus $d = 1$, i.e., m, n are prime to each other. ■

COROLLARY. 2.5 *For $m, n \in \mathbb{N}$, $\mathbb{Z}_m \oplus \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ if and only if m and n are prime to each other.*

This result immediately follows from the fact that $\mathbb{Z}_m$, $\mathbb{Z}_n$ and $\mathbb{Z}_{mn}$ are cyclic groups of order m, n and mn respectively. The next result is extension of the above theorem to n number of cyclic groups.

COROLLARY. 2.6 *If $G_1, G_2, \ldots, G_n$ are finite cyclic groups of order $k_1, k_2, \ldots, k_n$ respectively, then the external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is cyclic if and only if $\gcd(k_i, k_j) = 1$ for $k_i \neq k_j$, $1 \leq i, j \leq n$.*

When applying this result to the groups $\mathbb{Z}_m$, $m \in \mathbb{N}$ we have,

COROLLARY. 2.7 *For $k_1, k_2, \ldots, k_n \in \mathbb{N}$, $\mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n} \approx \mathbb{Z}_{k_1 k_2 \ldots k_n}$ if and only if $\gcd(k_i, k_j) = 1$ for $k_i \neq k_j$, $1 \leq i, j \leq n$.*

2.2 Group of units of $\mathbb{Z}_n$

Recall that an element x in a ring R with unity is called an *unit* if it has the multiplicative inverse, i.e., if there exists $y \in R$ such that $xy = yx = 1$, where 1 is the unity element of R. The set of all the units of the ring $\mathbb{Z}_n$, where $n \in \mathbb{N}$, is denoted by U_n. Evidently U_n is a group under multiplication modulo n, called the group of units modulo n.

DEFINITION. 2.8 For $n \in \mathbb{N}$ if k is a divisor of n then $U_k(n)$ is defined by

$$U_k(n) \quad = \quad \{x \in U_n : x \equiv 1(\text{mod } k)\}.$$

For example, note that $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Then $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.

THEOREM. 2.9 *If k in a divisor of n then $U_k(N)$ is a subgroup of U_n.*

PROOF. If $x, y \in U_k(n)$ then $x \equiv 1(\text{mod } k)$ and $y \equiv 1(\text{mod } k)$ and hence $xy \equiv 1(\text{mod } k)$ showing that $xy \in U_k(n)$. Also if $x \equiv 1(\text{mod } k)$ then $k|(x-1)$. If y is the inverse of x in U_n then $xy \equiv 1(\text{mod } n)$, i.e., $n|(xy-1)$. Since $k|n$ we have $k|(xy-1)$ and hence $k|(xy-1)-(x-1)$, i.e., $k|x(y-1)$. Since $k \not| x$, we have $k|y-1$, i.e., $y \equiv 1(\text{mod } \ k)$. Hence $y \in U_k(n)$. Thus $U_k(n)$ is a subgroup of U_n. ■

THEOREM. 2.10 *Let p, q are relatively prime numbers. Then $U_{pq} \approx U_p \oplus U_q$. Moreover, $U_p \approx U_q(pq)$ and $U_q \approx U_p(pq)$.*

PROOF. Define a mapping $\phi : U_{pq} \to U_p \oplus U_q$ by $\phi(x) = (x \text{ mod } p, x \text{ mod } q)$ for all $x \in U_{pq}$. Then for $x, y \in U_{pq}$, $\phi(x)\phi(y) = (x \text{ mod } p, x \text{ mod } q)(y \text{ mod } p, y \text{ mod } q) = (xy \text{ mod } p, xy \text{ mod } q) = \phi(xy)$. Thus ϕ is a homomorphism.

Take $x, y \in U_{pq}$ such that $\phi(x) = \phi(y)$. Then x mod $p = y$ mod p and x mod $q = y$ mod q. Hence $p|(x-y)$ and $q|(x-y)$ which implies that $pq|(x-y)$, i.e., $x \equiv y(\text{mod } pq)$, i.e., $x = y$ in U_{pq}. Thus ϕ is injective.

Finally, if $(i, j) \in U_p \oplus U_q$ then $\gcd(i, p) = 1 = \gcd(j, q)$. Since $\gcd(p, q) = 1$, $\gcd(i, pq) = 1$ and $\gcd(j, pq) = 1$ and hence $\gcd(ij, pq) = 1$. Thus $ij \in U_{pq}$. Taking $x = ij$, $\phi(x) = (x \text{ mod } p, x \text{ mod } q) = (i, j)$. Thus ϕ is onto. ■

2.3 Internal Direct Product

DEFINITION. 2.11 Let H, K be normal subgroups of a group G. Then G is said to be the *internal direct product* of H and K if every element g of G can be expressed uniquely as $g = hk$ where $h \in H$ and $k \in K$.

The number of ways in which an element $g \in G$ can be expressed as $g = hk$, where $h \in H$ and $k \in K$, is the number of elements in $H \cap K$. Thus the expression $g = hk$ is unique if and only if $H \cap K = \{e\}$, e being the identity element of G.

DEFINITION. 2.12 Let $N_1, N_2, \ldots, N_n$ be normal subgroups of a group G. Then G is said to be the *internal direct product* of the subgroups $N_1, N_2, \ldots, N_n$ if every element g of G can be expressed uniquely as $g = g_1 g_2 \ldots g_n$ where $g_i \in N_i$, $1 \leq i \leq n$.

THEOREM. 2.13 *If G is the internal direct product of n normal subgroups $N_1, N_2, \ldots, N_k$ Then for $i \neq j$, $1 \leq i, j \leq k$, $N_i \cap N_j = \{e\}$.*

PROOF. $G = N_1 N_2 \cdots N_k$, any element $x \in G$ is uniquely represented as $x = n_1 n_2 \ldots n_k$ where $n_i \in N_i$, $1 \leq i \leq k$. If $a \in N_i \cap N_j$ then $a \in G$ can be represented as $a = ee \ldots eae \ldots e$ where $a \in N_i$ appears in i-th place. The element $a \in G$ can also be represented as $a = ee \ldots eae \ldots e$ where $a \in N_j$ appears in j-th place. Hence the representation is unique only if $a = e$. Thus $N_i \cap N_j = \{e\}$. ■

It has already been shown that for groups $G_1, G_2, \ldots, G_n$, the subgroup $\bar{G}_i = \{e_1, e_2, \ldots, e_{i-1}, g, e_{i+1}, \ldots, e_n : g \in G_i\}$ of $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is an isomorphic copy of G_i for $1 \leq i \leq n$. Also each $\bar{G}_i$ is a normal subgroup. Thus we have the following result.

THEOREM. 2.14 *If $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is the external direct product then G is the internal direct product of the normal subgroups $\bar{G}_1, \bar{G}_2, \ldots, \bar{G}_n$.*

PROOF. An arbitrary element of G is $g = (g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$, $1 \leq i \leq n$. Then for $1 \leq i \leq n$, $\bar{g}_i = (e_1, e_2, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n) \in \bar{G}_i$ and $g = \bar{g}_1 \bar{g}_2 \cdots \bar{g}_n$. Since this representation is unique, the result follows. ■

3 Group Action

DEFINITION. 3.1 Let G be a group, X be a set. A function from $G \times X$ to X, $(g, x) \mapsto g \cdot x$, is called a *group action* if the following conditions hold:

1. $e \cdot x = x$ for all $x \in X$, where e is the identity element of G,
2. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$ for all $x \in X$.

In such a case we say G is acting on X and X is called a G-set.

EXAMPLE. 3.2

1. Every group acts on its underlying set, If $(G, *)$ is a group then for $g, x \in G$, $g \cdot x = g * x$ is a group action.

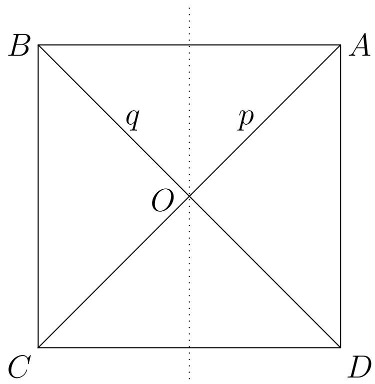
2. Let X be any set, S_X denote the permutation group of X and G be any subgroup of S_X. Then for $\sigma \in G$ and $x \in X$, define $\sigma \cdot x = \sigma(x)$, then $(\sigma, x) \mapsto \sigma \cdot x$ is a group action.

3. In particular, in the above example, if $X = \{1, 2, 3\}$ and $G = \{i, \sigma, \rho\}$ where i is the identity mapping, $\sigma = (1\ 2\ 3)$ and $\rho = (1\ 3\ 2)$, the three-cycles. Then the group action can be stated in the following tabular form:

	1	2	3
i	1	2	3
σ	2	3	1
ρ	3	1	2

4. Consider the group D_4, the dihedral group of a square. Let X be the set $\{A, B, C, D, p, q\}$, where A, B, C, D are the four vertices of the square and p, q are respectively the diagonal AB and CD. for $g \in D_4$ the action of g on an element x in X is the effect of g on X. This is a group action. Note that $D_4 = \{i, r, r^2, r^3, s, rs, r^2s, r^3s\}$, where r denotes the rotation about the center by an angle $90°$ in counterclockwise direction and s denotes the flip about the vertical line through the center.

	A	B	C	D	p	q
i	A	B	C	D	p	q
r	B	C	D	A	q	p
r^2	C	D	A	B	p	q
r^3	D	A	B	C	q	p
s	B	A	D	C	q	p
rs	C	B	A	D	p	q
r^2s	D	C	B	A	q	p
r^3s	A	D	C	B	p	q



5. Group action on itself by conjugation: Let G be a group, then it acts on its underlying set G by conjugation as follows: for $g \in G$ and $x \in G$, $g \cdot x = gxg^{-1}$. Obviously for $e \in G$ and $x \in G$, $e \cdot x = exe^{-1} = x$ and got $g, h \in G$ and $x \in G$, $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = h(gxg^{-1})h^{-1} = hgx(hg)^{-1} = (hg) \cdot x$.

If X is a G-set then every element of G induces a permutation on the set X.

THEOREM. 3.3 *Let X be a G-set. Then for all $g \in G$ the mapping $\pi_g : X \to X$, defined by $\pi_g(x) = g \cdot x$ for all $x \in X$, is a permutation on X.*

PROOF. For $g \in G$, to show that π_g is injective, take $x_1, x_2 \in X$ such that $\pi_g(x_1) = \pi_g(x_2)$. Then $g \cdot x_1 = g \cdot x_2$. Since $g^{-1} \in G$, it follows that $g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2)$. By property of group action, $(g^{-1}g) \cdot x_1 = (g^{-1}g) \cdot x_2$, i.e., $e \cdot x_1 = e \cdot x_2$ which gives $x_1 = x_2$. Hence π_g is one-one.

For $y \in X$ take $x = \pi_{g^{-1}}(y) = g^{-1} \cdot y$. Then $\pi_g(x) = g \cdot x = g \cdot (g^{-1} \cdot y) = (gg^{-1}) \cdot y = e \cdot y = y$. Hence π_g is surjective. Thus π_g is a bijective map, i.e., a permutation. ■

THEOREM. 3.4 *Let X be a G-set. Then the mapping $\phi : G \to S_X$, defined by $\phi(g) = \pi_g$ for all $g \in G$, is a homomorphism.*

PROOF. For $g_1, g_2 \in G, x \in X$,

$$\begin{aligned}\phi(g_1g_2)(x) &= \pi_{g_1g_2}(x) = (g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot (\pi_{g_2}(x)) \\ &= \pi_{g_1}(\pi_{g_2}(x)) = (\pi_{g_1} \circ \pi_{g_2})(x) = (\phi(g_1) \circ \phi(g_2))(x).\end{aligned}$$

Hence for all $g_1, g_2 \in G$ and for all $x \in X$, $\phi(g_1g_2)(x) = (\phi(g_1) \circ \phi(g_2))(x)$ which shows that $\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$. This shows that $\phi : G \to S_X$ is a homomorphism. ■

DEFINITION. 3.5 Let X be a G-set. The mapping $\phi : G \to S_X$ defined by $g \mapsto \pi_g$ for all $g \in G$ is called the *permutation representation* of the group action.

DEFINITION. 3.6 Let a group G act on a set X. Then the set

$$\{g \in G : g \cdot x = x \text{ for all } x \in X\}$$

is called the *kernel* of the group action and is denoted by G_0.

It can be observed that if ϕ is the permutation representation of a group action then the kernel of the group G_0 action is the kernel of the homomorphism ϕ.

DEFINITION. 3.7 Let a group G act on a set X. For $x \in X$ the *stabilizer* of x is the set $\{g \in G : g \cdot x = x\}$, i.e., the set of the members of G those fix the element x. The stabilizer of x is denoted by G_x.

A point $x \in X$ is called a *fixed point* of the action if $g \cdot x = x$ for all $g \in G$.

Hence $x \in X$ is a fixed point if and only if $G_x = G$.

THEOREM. 3.8 *For a G-set X and for $x \in X$ the stabilizer G_x is a subgroup of G.*

PROOF. Since $e \cdot x = x$, $e \in G_x$, thus $G_x \neq \emptyset$. If $g, h \in G_x$ then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ hence $gh \in G_x$. Also $g \cdot x = x \Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x \Rightarrow (g^{-1}g) \cdot x = g^{-1} \cdot x \Rightarrow x = g^{-1} \cdot x$ showing that $g^{-1} \in G_x$. Hence G_x is a subgroup of G. ■

COROLLARY. 3.9 *Kernel of a group action is a normal subgroup.*

PROOF. If G acts on X then kernel $G_0 = \cap\{G_x : x \in X\}$ which is the intersection of a family of subgroups of G, hence is a subgroup of G. Also for $g \in G, h \in G_0$ and $x \in X$, $(ghg^{-1}) \cdot x = g \cdot (h \cdot (g^{-1} \cdot x)) = g \cdot (g^{-1} \cdot x)$ (since $h \in G_0$) $= (gg^{-1}) \cdot x = x$ which shows that $ghg^{-1} \in G_0$. Thus G_0 is a normal subgroup.

Alternatively, we can say that $G_0 = \ker \phi$, where $\phi : G \to S_X$ is the permutation representation of the group action, which is a homomorphism. Hence $G_0 = \ker \phi$ is a normal subgroup. ■

THEOREM. 3.10 *If a group G acts on X, then for any $x \in X$ and any $g \in G$, $G_{g \cdot x} = gG_xg^{-1}$.*

PROOF. For $h \in G$,

$$\begin{aligned} h \in G_{g\cdot x} &\iff h \cdot (g \cdot x) = g \cdot x \iff (hg) \cdot x = g \cdot x \\ &\iff g^{-1} \cdot ((hg) \cdot x) = g^{-1}(g \cdot x) \\ &\iff (g^{-1}hg) \cdot x = (g^{-1}g) \cdot x \ = \ x \\ &\iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}. \end{aligned}$$

Hence the result. ■

EXAMPLE. 3.11 Let $G = D_4$, $X = \{A, B, C, D, p, q, O\}$, A, B, C, D are four vertices, O is the centre and p, q are the diagonals of the square. The action of G on X is the effect of the members of G on the members of X. It can be observed that the kernel of this action is $\{i\}$. We can also find the stabilizers from the table, for example, $G_A = G_C = \{i, r^3s\}$, $G_p = \{i, r^2, rs, r^3s\}$, $G_O = G$ etc.

DEFINITION. 3.12 A group action is called a *faithful* if its kernel consists of only the identity element.

It follows immediately that a group action is faithful if and only if different elements of G act differently on the elements of X, i.e., for $g, h \in G$ there exists $x \in X$ such that $g \cdot x \neq h \cdot x$. Equivalently, the action is faithful if and only the permutation representation $\phi : G \to S_X$ is injective.

PROPOSITION. 3.13 *Let X be a G-set. The relation $\sim$ on X, defined by for all $x, y \in X$, $x \sim y$ if and only if there exists $g \in G$ such that $g \cdot x = y$, is an equivalence relation on X.*

PROOF. Since $e \cdot x = x$, where e is the identity element of G, we have $x \sim x$. Thus $\sim$ is reflexive. Also for $x, y \in X$, $x \sim y \Rightarrow \exists g \in G$ such that $g \cdot x = y$ $\Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y \Rightarrow (g^{-1}g) \cdot x = g^{-1} \cdot y \Rightarrow e \cdot x = g^{-1} \cdot y \Rightarrow x = g^{-1} \cdot y \Rightarrow y \sim x$. Thus $\sim$ is symmetric. Finally, for $x, y, z \in X$ let $x \sim y$ and $y \sim z$. Then there exist $g_1, g_2 \in G$ such that $y = g_1 \cdot x$ and $z = g_2 \cdot y$. Hence $z = g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x$ showing that $x \sim z$. Thus $\sim$ is transitive. Hence $\sim$ is an equivalence relation. ■

DEFINITION. 3.14 Let X be a G-set. The equivalence classes related to the action of G on X are called the *orbits* of the action. The orbit containing the element x is denoted by $\mathcal{O}(x)$.

The orbits on X form a partition of X. For a fixed point $x \in X$, $\mathcal{O}(x) = \{x\}$.

THEOREM. 3.15 (ORBIT-STABILIZER THEOREM) *Let a finite group G act on a set X. Then for $x \in X$, $|\mathcal{O}(x)| = [G : G_x]$, i.e., the number of elements in the orbit of x is the index of the stabilizer of x in G.*

PROOF. Note that if $y \in \mathcal{O}(x)$ then there exists $g \in G$ such that $y = g \cdot x$. Define a mapping $f : \mathcal{O}(x) \to G/G_x$ by $f(y) = gG_x$ for all $y = gx \in \mathcal{O}(x)$. (Here we do not require G_x to be a normal subgroup of G, we are considering just the set of left cosets of G_x in G.) If $y, z \in \mathcal{O}(x)$ then there exist $g, h \in G$ such that $y = g \cdot x, z = h \cdot x$. Then,

$$\begin{aligned} f(y) = f(z) &\Rightarrow gG_x = hG_x \Rightarrow h^{-1}g \in G_x \Rightarrow (h^{-1}g) \cdot x = x \\ &\Rightarrow h \cdot (h^{-1} \cdot (g \cdot x)) = h \cdot x \Rightarrow g \cdot x = h \cdot x \Rightarrow y = z. \end{aligned}$$

Thus f is injective. Also for $gG_x \in G/G_x$, if $y = g \cdot x$ then $f(y) = gG_x$. Thus f is surjective. Hence f is a bijection.

Thus $|\mathcal{O}(x)| = |G/G_x|$. Since $[G : G_x] = |G/G_x| = \frac{|G|}{|G_x|}$, the result follows. ■

COROLLARY. 3.16 *Let a finite group act on a finite set X. If the disjoint orbits are represented by the elements $x_1, x_2, \ldots, x_k$ then*

$$|X| = \sum_{i=1}^{k} |\mathcal{O}(x_i)| = \sum_{i=1}^{k} [G : G_{x_i}].$$

PROOF. First part follows from the fact that $X = \bigcup_{i=1}^{k} \mathcal{O}(x_i)$ and for $i \neq j, 1 \leq i < j \leq k$, $\mathcal{O}(x_i) \cap \mathcal{O}(x_j) = \emptyset$. The Second part follows from $|\mathcal{O}(x_i)| = [G : G_{x_i}] = \frac{|G|}{|G_{x_i}|}$.

DEFINITION. 3.17 An action of a group G on a set X is called *transitive* if there is only one orbit. That is, for any two elements $x, y \in X$, there is a $g \in G$ such that $g \cdot x = y$. A subgroup of S_X is called transitive if it acts transitively on X.

EXAMPLE. 3.18 Let $X = \{1, 2, 3\}$ and $G = S_3$. Then G acts on X as the effect of the members of S_3 on the elements of X. If $G = \{i, \sigma, \rho, f, g, h\}$ where i is the identity mapping, $\sigma = (1\ 2\ 3), \rho = (1\ 3\ 2)$, the three cycles and $f = (1\ 2), g = (3\ 1), h = (2\ 3)$, the transpositions. The action can be viewed in the following table:

	1	2	3
i	1	2	3
σ	2	3	1
ρ	3	1	2
f	2	1	3
g	3	2	1
h	1	3	2

Here it can be observed that $\mathcal{O}(1) = \mathcal{O}(2) = \mathcal{O}(3) = X$, hence the action is transitive. It can also be observed that the subgroup $A_3 = \{i, \sigma, \rho\}$ acts transitively on X and hence S_3 and A_3 are transitive subgroups of S_3. The subgroup $H = \{i, f\}$ is not transitive since $\mathcal{O}(1) = \{1, 2\} = \mathcal{O}(2)$ and $\mathcal{O}(3) = \{3\}$. Similarly the subgroups $\{i, g\}$ and $\{i, h\}$ are not transitive subgroups.

4 Sylow's Theorem

4.1 Group action by conjugacy

DEFINITION. 4.1 Let G be a group. Two elements $x, y \in G$ are called *conjugate* if there exists an element $g \in G$ such that $y = gxg^{-1}$.

The relation of being conjugate is an equivalence relation on G, the equivalence classes are called the *conjugacy classes*. Thus for $x \in G$ the conjugate class of x is $Cl(x) = \{y \in G : \exists g \in G \text{ s.t. } y = gxg^{-1}\} = \{gxg^{-1} : g \in G\}$.

We recall the following definition.

DEFINITION. 4.2 The conjugacy defines a group action on itself as follows: for $g \in G$ and $x \in G$ define $g \cdot x = gxg^{-1}$. We call it as *group acts on itself by conjugation.*

It follows immediately from definition that

1. For $x \in G$ the orbit of x is $\mathcal{O}(x) = Cl(x)$, the conjugacy class of x.

2. When $x \in Z(G)$, the center of G, then $gx = xg$ for all $g \in G$. Hence the orbit of x is given by $\mathcal{O}(x) = \{y \in G : \exists g \in G \text{ s.t. } y = gxg^{-1}\}$. But as $gxg^{-1} = x$ we have $\mathcal{O}(x) = Cl(x) = \{x\}$.

3. For any $x \in G$ the stabilizer of x with respect to this particular group action is $G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x)$, the centralizer of x.

THEOREM. 4.3 (THE CLASS EQUATION) *Suppose that a finite group G acts on itself by conjugation. If $x_1, x_2, \ldots, x_n$ be the representatives of the distinct non-trivial orbits, then*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G|/|G_{x_i}|$$

PROOF. Note that as the orbits form a partition on G,

$$G = \bigcup \{\mathcal{O}(x) : x \in \text{distinct orbits}\}.$$

Since for $x \in Z(G)$, $\mathcal{O}(x) = \{x\}$ it follows that

$$G = Z(G) \cup \{\mathcal{O}(x) : x \in \{x_1, x_2, \ldots, x_n\}\}.$$

Since distinct orbits are disjoint it follows that

$$|G| = |Z(G)| + \sum_{i=1}^{n} |\mathcal{O}(x_i)|.$$

By Orbit-Stabilizer Theorem we have $|\mathcal{O}(x_i)| = [G : G_{x_i}] = \frac{|G|}{|G_{x_i}|}$, hence

$$|G| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|G_x|}.$$

Hence the result. ■

THEOREM. 4.4 *If p is a prime number and G be a group of order p^k for some $k \geq 1$ then $Z(G)$ is non-trivial.*

PROOF. By class equation we have $|G| = |Z(G)| + \sum_{x \text{ in distinct orbits}} [G : G_x]$. Since for each $x \notin Z(G)$, G_x is a subgroup of G, $|G_x|$ divides $|G| = p^k$, we have $|G_x| = p^j$ for some $1 \leq j < k$. Hence p divides $[G : G_x]$ for each $x \in G \setminus Z(G)$. Also p divides $|G|$. Thus, p divides $|Z(G)|$. This shows that $Z(G)$ is non-trivial. ■

COROLLARY. 4.5 *If p is a prime number then any group of p^2 is abelian. Moreover G is either isomorphic to $\mathbb{Z}_{p^2}$ or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.*

PROOF. By class equation $Z(G)$ is nontrivial. Since $|Z(G)|$ divides $|G|$ and $|G| = p^2$ we have either $|Z(G)| = p^2$ or $|Z(G)| = p$.

If $Z(G) = p^2$ then $G = Z(G)$, hence G is abelian.

If $|Z(G)| = p$ choose $x \in G \setminus Z(G)$. Then G_x is a subgroup of G. Also $g \in Z(G) \Rightarrow gx = xg \Rightarrow gxg^{-1} = x \Rightarrow g \cdot x = x$, showing that $g \in G_x$. Hence $Z(G) \subsetneqq G_x$ as $x \in G_x \setminus Z(G)$. If $G_x = G$ then $g \cdot x = x$ for all $g \in G$, i.e., $gxg^{-1} = x$ for all $g \in G$ which implies that $x \in Z(G)$ — a contradiction. Hence G_x is a proper subgroup of G and $p = |Z(G)| < |G_x| < |G| = p^2$ — which is again a contradiction as p is a prime.

Hence we must have $|Z(G)| = p^2$, i.e., G is abelian.

For the second part, if G contains an element a of order p^2 then $G = \langle a \rangle$, i.e., a cyclic group of order p^2, hence is isomorphic to $\mathbb{Z}_{p^2}$.

Otherwise all non-identity elements of G are of order p. Choose $x \in G$ with $o(x) = p$. Then $\langle x \rangle$ is a subgroup of order p. Choose $y \in G - \langle x \rangle$, then $\langle y \rangle$ is also subgroup of order p. Also since $p = |\langle x \rangle| < |\langle x, y \rangle| \leq |G| = p^2$ we must have $|\langle x, y \rangle| = p^2$ and hence $G = \langle x, y \rangle$. Now, $\langle x \rangle, \langle y \rangle$ being cyclic groups of order p we have $\langle x \rangle \times \langle y \rangle$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Define a mapping $\phi : \langle x \rangle \times \langle y \rangle \to \langle x, y \rangle$ by $\phi(x^i, y^j) = x^i y^j$ for all $(x^i, y^j) \in \langle x \rangle \times \langle y \rangle$. It immediately follows that ϕ is an isomorphism and hence G is isomorphic tp $\mathbb{Z}_p \times \mathbb{Z}_p$. ■

4.2 Sylow's Theorem

Recall that for a group G and $x \in G$ the centralizer of x is $C_G(x) = \{y \in G : yxy^{-1} = x\}$. It has been proved that $C_G(x)$ is a subgroup of G. When a group G acts on itself by conjugacy then the conjugacy class of an element $a \in G$ is given by $Cl(x) = \{gxg^{-1} : g \in G\}$. It has also been proved that $Cl(x) = \mathcal{O}(x)$, orbit of x with respect to the group action by conjugacy. The following gives the size of a conjugacy class.

THEOREM. 4.6 *For a finite group G and $x \in G$, $|Cl(x)| = [G : C_G(x)]$.*

PROOF. By Orbit-Stabilizer Theorem, $|\mathcal{O}(x)| = [G : G_x]$. Since for the group action by conjugacy $\mathcal{O}(x) = Cl(x)$ and $G_x = C_G(x)$, the result follows. ■

It is known from the Lagrange's Theorem that if G is a group of order n and it has a subgroup of order m then m divides n. The converse need not be true always, for example the alternation group A_4 is of order 12 has no subgroup of order 6, though 6 divides 12. A sufficient condition is given here for which the converse of Lagrange's Theorem holds partially.

We recall a theorem for finite abelian group which will be used to prove the Sylow's Theorem.

THEOREM. 4.7 *If G is a finite abelian group and if p is a prime that divides the order of G then G has an element of order p.*

PROOF. The proof will be done by induction on the order of G. If $|G| = 2$ the result holds trivially. Let G be a group of order $n > 2$. If for a proper subgroup H of G, p divides $|H|$ then by induction hypothesis H has an element of order p — hence the result is proved. So we assume that for all proper subgroup H of G, p does not divide $|H|$.

For a proper subgroup H of G, $|G| = |G/H| \cdot |H|$. Since p divides $|G|$ and p does not divide $|H|$ we must have p divides $|G/H|$. Hence by induction hypothesis G/H has an element, say aH, of order p. Thus $(aH)^p = H$, or $a^p \in H$. If $|H| = m$ then $(a^p)^m = e$, i.e., $a^{mp} = e$ hence $(a^m)^p = e$, where e is the identity element of G. Taking $b = a^m$ we can say that b is an element of order p if $b \neq e$.

If possible suppose that $b = a^m = e$. Then $(aH)^m = a^m H = H$. Since p and m are prime to each other, there exist integers x, y such that $mx + py = 1$. Then

$$\begin{aligned} aH &= a^{mx+py}H = (aH)^{mx}(aH)^{py} \\ &= ((aH)^m)^x((aH)^p)^y = H^x H^y = H \end{aligned}$$

this is a contradiction since $|aH| = p$. Thus, we have $b \neq e$ and hence b is the required element of G with order p. ■

THEOREM. 4.8 (SYLOW'S FIRST THEOREM) *Let G be a finite group and p be a prime such that p^k divides $|G|$. Then G has a subgroup of order p^k.*

PROOF. The theorem will be proved by induction on $n = |G|$. If $n = 1$ the result holds trivially. So let us assume that $n > 1$ and the result holds for all groups of order less than n.

If G has a proper subgroup H such that p^k divides $|H|$ then by induction hypothesis H has a subgroup of order p^k and hence G has a subgroup of order p^k, i.e., the theorem is proved. So we assume that G has no proper subgroup whose order is divisible by p^k.

Since $|G|$ is divisible by p^k it follows that $|Z(G)|$ is divisible by p (Theorem 4.4). Since $Z(G)$ is an abelian group, $Z(G)$ has an element, say a, of order p. Then $N = \langle a \rangle$ is a group of order p. Also since $a \in Z(G)$ it follows that N is a normal subgroup of G. So we may consider the quotient group G/N, whose order is $\frac{|G|}{|N|}$ which is divisible by p^{k-1}.

By induction hypothesis G/N has a subgroup, say M, of order p^{k-1}. Let $\phi : G \to G/N$ be the natural homomorphism $g \mapsto gN$ for all $g \in G$. Consider the set $H = \{g \in G : \phi(g) \in M\} = \phi^{-1}(M)$. Then $g_1, g_2 \in H \Rightarrow g_1N, g_2N \in M \Rightarrow g_1g_2^{-1}N \in M \Rightarrow g_1g_2^{-1} \in H$. Thus H is a subgroup of G. Hence $M = H/N$. Since $|M| = p^{k-1} = \frac{|H|}{|N|}$ and $|N| = p$, we have $|H| = p^k$ — contradiction that G has no proper subgroup of order p^k.

Hence G must have a proper subgroup of order p^k. This completes the proof. ■

EXAMPLE. 4.9 Let G be a group of order 180. Since $180 = 2^2 3^2 5$, the above theorem says that G has subgroups of order $2, 4, 3, 9$ and 5. However this theorem can not say whether G has subgroups of order $6, 10, 12, 15, 18, 20, 30, 45, 60$ or 90 even though each of these number divides 180.

DEFINITION. 4.10 Let G be a finite group and p be a prime. A subgroup of order p is called a p-subgroup of G. If p^k divides $|G|$ and P^{k+1} does not divide $|G|$ then a subgroup of order p^k of G is called a *Sylow p-subgroup* of G (also called p-Sylow subgroup).

For a group of order 180 a subgroup of order 4 is a Sylow 2-subgroup, a subgroup of order 9 is Sylow 3-subgroup and a subgroup of order 5 is a Sylow 5-subgroup. However a subgroup of order 3 is a 3-subgroup of G, not a Sylow 3-subgroup.

DEFINITION. 4.11 Two subgroups H, K of a group G are said to be conjugate if there exists $g \in G$ such that $H = gKg^{-1}$.

LEMMA. 4.12 *Let H be a p-group, where p is a prime number, S is a finite set and H acts on S. Let $S_0 = \{s \in S : \mathcal{O}(s) = \{s\}\}$ be the collection of all those elements of S which are fixed by the group action. Then $|S| \equiv |S_0| (\text{mod } p)$.*

PROOF. Since the orbits form a partition on S, $|S| = \sum |\mathcal{O}(s)|$, where summation is taken over the representatives of all the distinct orbits. S_0 being the collection of elements of singleton orbits we have $|S| = |S_0| + \sum |\mathcal{O}(s)|$, where summation is taken over the representatives of non-trivial orbits. By orbit-Stabilizer theorem we have $|\mathcal{O}(s)| = |H|/|H_s|$, where H_s is the stabilizer of $s \in S$. Since $|H| = p^k$ for some $k \geq 1$ and H_s is a subgroup of H, we have $|H_s| = p^m$ for some $m < k$, hence $|\mathcal{O}(s)|$ is divisible by p. Thus $|S| \equiv |S_0| (\text{mod } p)$. ■

THEOREM. 4.13 (SYLOW'S SECOND THEOREM) *Let G be a finite group and p be a prime such that $p^k \mid |G|$ but $p^{k+1} \nmid |G|$. Then (i) Any p-subgroup of G is contained in some Sylow p-subgroup of G and (ii) any two Sylow p-subgroups are conjugate.*

PROOF. (i) Let H be a p-subgroup of G and P be a Sylow p-subgroup of G. Take $S = \{gP : g \in G\}$, the set of all left cosets of P. Let H act on S by left multiplication: $h \cdot gP = hgP$ for all $h \in H$, for all $gP \in S$. Let $S_0 \subset S$ denote the set of fixed points of the group action, i.e., $S_0 = \{gP \in S : h \cdot gP = gP \ \forall h \in H\}$. Then by the above lemma we have $|S_0| \equiv |S| (\text{mod } p)$. Since $|S| = \frac{|G|}{|P|}$ is not divisible by p we have $|S_0| \geq 1$. Let $gP \in S_0$. Then,

$$\begin{aligned} & hgP = gP \ \ \forall h \in H \ \ \Rightarrow \ \ g^{-1}hgP = P \ \ \forall h \in H \\ \Rightarrow \ \ & g^{-1}hg \in P \ \ \forall h \in H \ \ \Rightarrow \ \ g^{-1}Hg \subset P \ \ \Rightarrow \ \ H \subset gPg^{-1} \end{aligned}$$

Since conjugacy is an automorphism, gPg^{-1} is also a Sylow p-group and hence H is contained in a Sylow p-subgroup.

(ii) In particular if $H = P_1$ is another Sylow p-subgroup, then $P_1 \subset gPg^{-1}$, but $|P_1| = |gPg^{-1}|$, and hence $P_1 = gPg^{-1}$. Thus any two Sylow p-subgroups are conjugate. ■

THEOREM. 4.14 (SYLOW'S THIRD THEOREM) *Let p be a prime and G be a finite group of order $p^k m$ where $p \nmid m$. If P is a Sylow p-subgroup then (i) the number of Sylow p-subgroups is $n_p = [G : N_G(P)]$, where $N_G(P)$ is the normalizer of P, (ii) n_p divides $|G|/|P|$ and (iii) $n_p \equiv 1 (\text{mod } p)$.*

PROOF. (i) Let S denote the set of all Sylow p-subgroups of G. Let G act on S by conjugacy operation, $g \cdot P = gPg^{-1}$ for all $g \in G$ and for all $P \in S$. By Sylow's Second Theorem for any $P \in S$, $\mathcal{O}(P) = S$. By Orbit-Stabilizer Theorem $|\mathcal{O}(P)| = [G : G_P]$, where G_P is the stabilizer of P.

Since $G_P = \{g \in G : g \cdot P = P\} = \{g \in G : gPg^{-1} = P\} = N_G(P)$ it follows that $n_p = |S| = |\mathcal{O}(P)| = [G : N_G(P)]$. Hence (i) follows.

(ii) Note that P is a normal subgroup of $N_G(P)$ and $N_G(P)$ is a subgroup of G.

Also $[G : N_G(P)] = \frac{|G|}{|N_G(P)|}$ and $[N_G(P) : P] = \frac{|N_G(P)|}{|P|}$. Hence $\frac{|G|}{|P|} = [G : N_G(P)] \times [N_G(P) : P] = n_p \times [N_G(P) : P]$. This shows that n_p divides $\frac{|G|}{|P|}$.

(iii) Let P act on S by conjugacy and S_0 denote the set of elements of S fixed by group action, i.e., $S_0 = \{Q \in S : g \cdot Q = Q \ \forall g \in P\}$. Then for $g \in P$ and $Q \in S_0$, $gQg^{-1} = Q$ which implies that $g \in N_G(Q)$ and hence $P \subset N_G(Q)$. By Sylow's second Theorem P and Q are conjugate in G and hence in particular conjugate in $N_G(Q)$, also Q is normal in $N_G(Q)$, thus $P = Q$. This shows that $S_0 = \{P\}$. By Lemma $|S| \equiv |S_0| (\text{mod } p)$, i.e., $n_p \equiv 1 (\text{mod } p)$. This completes the proof. ■

COROLLARY. 4.15 *For a prime p a finite group G has a unique Sylow p-subgroup P if and only if P is normal.*

PROOF. Assume that P is the only Sylow p-subgroup of G. Then for any $g \in G$, gPg^{-1} is a Sylow p-subgroup and hence $gPg^{-1} = P$. Thus P is normal. Conversely, Assume that P is normal. If Q is a Sylow p-subgroup then there exists $g \in G$ such that $Q = gPg^{-1} = P$. Hence P is the only Sylow p-subgroup of G. ■.

COROLLARY. 4.16 *If p, q are primes, $p < q$ and $p \nmid q - 1$ then a group G of order pq is isomorphic to $\mathbb{Z}_{pq}$.*

PROOF. Let P be a Sylow p-subgroup and Q be a Sylow q-subgroup of G. Then $n_p \equiv 1 (\text{mod } p)$, i.e, $n_p = 1 + kp$ for some integer $k \geq 0$ and $n_p \mid q$. Similarly $n_q = 1 + lq$ for some integer $l \geq 0$ and $n_q \mid p$. Since $p < q$, $n_q = 1 + lq \mid p$ is possible only if $l = 0$, thus $n_q = 1$ and hence Q is a normal subgroup of G.

Since n_p divides the prime number q, either $n_p = 1$ or $n_p = q$. Since $p \nmid q - 1$ and $p \mid n_p - 1$, $n_p = q$ is false. Thus $n_p = 1$ and hence P is a normal subgroup of G.

P, Q being groups of prime orders p, q respectively, they are cyclic groups. Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Obviously $G = PQ$. Since $P \cap Q = \{e\}$, $G = P \times Q$.

Also since $P \approx \mathbb{Z}_p$ and $Q \approx \mathbb{Z}_q$ we have $P \times Q \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$. ■

EXAMPLE. 4.17

1. Let us consider a group G of order 40. Since $40 = 2^3 5$, a Sylow 2-subgroup is of order 8 and a Sylow 5-subgroup is of order 5.

   There are n_2 number of Sylow 2-subgroups, then $2 \mid n_2 - 1$ and $n_2 \mid \frac{40}{8} = 5$, i.e., $n_2 = 2k + 1 \mid 5$. Hence $n_2 = 1$ or 5 (for $k = 0$ and $k = 2$). If $n_2 = 1$, the Sylow 2-subgroup is normal, if $n_2 = 5$ none of the five Sylow 2-subgroups is normal.

The number of Sylow 5-subgroups is n_5, then $5 \mid n_5 - 1$ and $n_5 \mid \frac{40}{5} = 8$, i.e., $n_5 = 5k + 1 \mid 5$. Hence $n_5 = 1$ is the only solution ($k = 0$), the only Sylow 5-subgroup is normal.

2. How many Sylow p-subgroups of S_5 are there?

   $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$. It has Sylow 2-subgroups of order 8, Sylow 3-subgroups of order 3 and Sylow 5-subgroups of order 5.

   The number of Sylow 2-subgroups is n_2. So $2 \mid n_2 - 1$ and $n_2 \mid 120/8 = 15$, i.e., $n_2 = 2k + 1 \mid 15$. The solutions are $n_2 = 1, 3, 5$ or 15. Note that any four elements of $\{1, 2, 3, 4, 5\}$ can form four vertices of a square which generates D_4, the dihedral group of order 4. Since $|D_4| = 8$, D_4 is a Sylow 2-subgroup. The 4 vertices can be arranges in 24 ways, the vertices arranged in same 4-cycle structure give the same group. (for example, $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$). Also the vertices interchanges horizontally give the same group (for example $(1\ 2\ 3\ 4)$ and $(2\ 1\ 4\ 3)$ give same group). Hence 24 arrangements give 3 different groups of order 8. There are ${}^5C_4 = 5$ ways to choose 4 elements from $\{1, 2, 3, 4, 5\}$. Each choice give 3 different group of order 8. Hence $n_2 = 5 \times 3 = 15$.

   The number of Sylow 3-subgroups is n_3. So $n_3 = 3k + 1 \mid 120/3 = 40$, i.e., $n_3 = 1, 10$ or 40 (for $k = 0, 3, 13$).

   The number of Sylow 5-subgroups is n_5. So $n_5 = 5k + 1 \mid 120/5 = 24$, i.e., $n_5 = 1, 6$ are the possibility.

   Since a Sylow p-subgroup in A_5 is also a Sylow p-subgroup in S_5 and A_5 is simple (i.e., it has no proper normal subgroup), in both the cases above $n_3 = 1$ and $n_5 = 1$ are cancelled. Thus, $n_3 = 10$ or 40 and $n_5 = 6$.

   An element in S_5 has an order is 3 if and only if it is a 3-cycle. The number of distinct 3-cycles in S_5 is $\frac{5!}{3 \cdot 2!} = 20$. Each Sylow 2-subgroup contains 2 non-identity elements, and hence there can be $20/2 = 10$ such groups. Hence $n_3 = 10$.

3. The possibilities for the number of elements of order 5 in a group of order 100.

   $100 = 2^2 5^2$, so a group of order 100 can have Sylow 2-subgroups of order 4 and Sylow 5-subgroups of order 25.

   $n_5 = 5k + 1 \mid 4$, the only possibility is $k = 0$, i.e., $n_5 = 1$. Hence the group has only one Sylow 5-subgroup P which of order 25. So either $P \approx \mathbb{Z}_{25}$ or $P \approx \mathbb{Z}_5 \oplus \mathbb{Z}_5$. In former case the elements in $\mathbb{Z}_{25}$ of order 5 are $\bar{5}, \bar{10}, \bar{15}$ and $\bar{20}$, thus P has four elements of order 5. In the later case all the elements of

$\mathbb{Z}_5 \oplus \mathbb{Z}_5$ other than the identity element are of order 5. Hence in that case the number of elements of order 5 in P is 24.

4. A group of order 175 is Abelian.

   Let G be a Group of order 175. We have $175 = 3^2 \cdot 5^2$. so the order of Sylow 3-subgroup is 9. The number of Sylow 3-subgroups is $n_3 = 3k + 1 \mid 25$, hence $n_3 = 1$ is the only possibility. Also the order of Sylow 5-subgroup is 25. The number of Sylow 5-subgroup is $n_5 = 5k + 1 \mid 9$, hence $n_5 = 1$.

   Let H, K denote the Sylow 3-subgroup and Sylow 5-subgroup respectively. Then H, K are normal and $|H| = 3^2, |K| = 5^2$ which imply that both H, K are Abelian. Each non-identity element of H has order 3 or 9 and each nonidentity element of K has order 5 or 25. Hence $H \cap K = \{e\}$. This Shows that $G = HK$. Since H, K are Abelian, G is Abelian.

4.3 Conjugacy classes in S_n

PROPOSITION. 4.18 *For $n \geq 3$ the product of two transpositions in S_n is either a 3-cycle or a product of two 3-cycles.*

PROOF. Let τ_1, τ_2 be two transpositions in S_n, where $n \geq 3$. If $\tau_1 = \tau_2$ then since $\tau_1 = \tau_1^{-1}$ we have $\tau_1\tau_2 = i = (1\ 2\ 3)(1\ 3\ 2)$, a product of two 3-cycles.

Assume that $\tau_1 \neq \tau_2$. Then two cases may arise, (i) either τ_1 and τ_2 have a common element or (ii) they are disjoint. For the first case assume that $\tau_1 = (i_1\ i_2)$ and $\tau_2 = (i_2\ i_3)$, then $\tau_1\tau_2 = (i_1\ i_2\ i_3)$ — a 3-cycle. For the second case, let $\tau_1 = (i_1\ i_2)$ and $\tau_2 = (i_3\ i_4)$, then $\tau_1\tau_2 = (i_1\ i_2)(i_3\ i_4) = (i_1\ i_4\ i_3)(i_1\ i_2\ i_3)$ — a product of two 3-cycles. ■

PROPOSITION. 4.19 *For $n \geq 3$ every element of the alternating group A_n is a product of 3-cycles.*

PROOF. An element $\sigma \in A_n$ is a product of an even number of transpositions. Since product of every pair of transpositioins is either a 3-cycle or a product of two 3-cycles it follows that σ is a product of 3-cycles. ■

PROPOSITION. 4.20 *Let $\sigma, \tau \in S_n$. Then $\tau\sigma\tau^{-1}$ is obtained by replacing the symbol i in σ by $\tau(i)$.*

PROOF. For $i \in \{1, 2, \ldots, n\}$ let $\sigma(i) = j$, $\tau(i) = s$ and $\tau(j) = t$. Then $\tau\sigma\tau^{-1}(s) = \tau\sigma(\tau^{-1}(s)) = \tau\sigma(i) = \tau(j) = t$. Hence when σ moves i to j then $\tau\sigma\tau^{-1}$ moves s to

t, i.e., $\tau\sigma\tau^{-1}$ moves $\tau(i)$ to $\tau(j)$. Hence $\tau\sigma\tau^{-1}$ is obtained by replacing the symbol i in σ by $\tau(i)$. ∎

EXAMPLE. 4.21 Let in S_5, $\sigma = (1\ 5\ 3\ 2)$ and $\tau = (2\ 4)(1\ 5)$. Then $\tau(1) = 5, \tau(5) = 1, \tau(3) = 3$ and $\tau(2) = 4$. Thus $\tau\sigma\tau^{-1} = (\tau(1)\ \tau(5)\ \tau(3)\ \tau(2)) = (5\ 1\ 3\ 4) = (1\ 3\ 4\ 5)$. This can be viewed in tabular form also:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \tau\sigma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}.$$

EXAMPLE. 4.22 Let $\sigma = (2\ 3)(4\ 6\ 8)(1\ 5\ 7\ 9)$ and $\tau = (1\ 3)(7\ 9\ 8)(3\ 4\ 6)$. Then $\tau\sigma\tau^{-1} = (2\ 4)(6\ 1\ 7)(3\ 5\ 9\ 8)$.

PROPOSITION. 4.23 *Two k-cycles in S_n are conjugate.*

PROOF. Let $\sigma = (i_1\ i_2\ \ldots\ i_k)$ and $\rho = (j_1\ j_2\ \ldots\ j_k)$ be two k-cycles. Take $\tau \in S_n$ as follows: $\tau(i_1) = j_1, \tau(i_2) = j_2, \ldots, \tau(i_k) = j_k$. Then $\tau\sigma\tau^{-1} = \rho$, hence σ and ρ are conjugate. ∎

PROPOSITION. 4.24 *Two permutations in S_n are conjugate if and only if they have the same cycle structure.*

PROOF. If σ and ρ in S_n have the same cycle structure, then since the cycles of same length are conjugate and conjugacy is an automorphism it follows that σ and ρ are conjugate.

Conversely, if σ and ρ are conjugate then $\rho = \tau\sigma\tau^{-1}$ for some $\tau \in S_n$. But in this case ρ is obtained by replacing the entries of σ by their τ images and hence ρ and σ have the same cycle structure. ∎

DEFINITION. 4.25 For $n \in \mathbb{N}$, a *partition* of n is a non-decreasing sequence of integers $n_1, n_2, \ldots, n_k$ whose sum is n, i.e., $0 \le n_1 \le n_2 \le \cdots \le n_k$ such that $n_1 + n_2 + \cdots + n_k = n$.

THEOREM. 4.26 *The number of conjugacy classes in S_n is equal to the number of partitions of n.*

PROOF. Let $\sigma \in S_n$. Arrange the disjoint cycles of σ (including 1-cycles) in non-decreasing order so that the cycle lengths form a partition of n. Any member $\rho \in S_n$ conjugate to σ has the same cycle structure and hence defines the same partition of n. Thus a conjugate class defines a unique partition of n. On the other hand, given any partition of n a permutation can be constreucted having the cycle lengths of the partition members. Hence the number of conjugacy classes in S_n is equal to the number of partitions of n. ■

EXAMPLE. 4.27 1. Take $n = 4$. The partitions of 4 are, $4 = 1 + 1 + 1 + 1, 4 = 1 + 1 + 2, 4 = 1 + 3, 4 = 2 + 2, 4 = 4$. Hence S_4 has five conjugacy classes, i.e., $(1)(2)(3)(4) = i$, $(1)(2)(3\ 4) = (3\ 4)$, $(1)(2\ 3\ 4) = (2\ 3\ 4)$, $(1\ 2)(3\ 4)$ and $(1\ 2\ 3\ 4)$.

2. When $n = 5$, the partitions of 5 and a representative of each conjugate class are given in the following table. Here the 1-cycles are omitted.

Partition of n	Representative of the conjugate class
1+1+1+1+1	i
1+1+1+2	(1 2)
1+1+3	(1 2 3)
1+2+2	(1 2)(3 4)
1+4	(1 2 3 4)
2+3	(1 2)(3 4 5)
5	(1 2 3 4 5)

4.4 simplicity of A_n

In this section we shall prove that for $n \geq 5$ the group A_n contains no normal subgroup other than itself and the trivial group.

PROPOSITION. 4.28 *For $n \geq 5$ any two 3-cycles are conjugate in A_n.*

PROOF. Let σ, ρ be two 3-cycles in A_n. It is known that any two k-cycles in S_n are conjugate, hence, in particular, the 3-cycles σ, ρ are conjugate in S_3.

Without any loss of generality we may assume that $\sigma = (1\ 2\ 3)$, so there exists $\tau \in S_3$ such that $\rho = \tau\sigma\tau^{-1}$. If $\tau \in A_n$ then σ, ρ become conjugate in A_n. If $\tau \notin A_n$, i.e., τ is an odd permutation, take $\mu = \tau(4\ 5)$ so that $\mu \in A_n$. Then $\mu\sigma\mu^{-1} = \tau(4\ 5)(1\ 2\ 3)(4\ 5)^{-1}\tau^{-1} = \tau(4\ 5)(1\ 2\ 3)(4\ 5)\tau^{-1} = \tau(1\ 2\ 3)\tau^{-1} = \rho$. Thus σ and ρ are conjugate in A_n. ■

LEMMA. 4.29 *For $n \geq 3$, $Z(S_n) = \{i\}$.*

PROOF. Let $\sigma \in S_n$, $\sigma \neq i$. So there exists $k \in \{1, 2, \ldots, n\}$ such that $\sigma(k) = l \neq k$. Since $n \geq 3$ choose $m \in \{1, 2, \ldots, n\}$ such that $m \notin \{k, l\}$. Consider the transposition $\tau = (l\ m)$. Then $\tau\sigma\tau^{-1}(k) = \tau\sigma(k) = \tau(l) = m$ and $\sigma(k) = l$. Hence

$\tau\sigma\tau^{-1}(k) \neq \sigma(k)$, which shows that $\tau\sigma\tau^{-1} \neq \sigma$, i.e., $\tau\sigma \neq \sigma\tau$. Thus $\sigma \notin Z(S_n)$ and hence $Z(S_n) = \{i\}$. ■

THEOREM. 4.30 *For an integer $n \geq 5$ the only non-trivial proper normal subgroup of S_n is A_n.*

PROOF. For every $n \in \mathbb{N}$, A_n is a normal subgroup of S_n. To prove for $n \geq 5$, A_n is the only normal subgroup other than $\{i\}$ and S_n.

Let N be a normal subgroup of S_n, $N \neq \{i\}$ and $N \neq S_n$. Take $\sigma \in N$. Since $Z(S_n)$ is the trivial subgroup, and members of S_n are products of transpositions there exists a transposition τ such that $\sigma\tau \neq \tau\sigma$, i.e., $\sigma\tau\sigma^{-1} \neq \tau$. Let $\tau_1 = \sigma\tau\sigma^{-1}$, then τ and τ_1 are conjugate and hence τ_1 is a transposition.

Since $\tau = \tau^{-1}$ and $\sigma \in N$ it follows that $\tau\tau_1 = \tau\sigma\tau\sigma^{-1} = (\tau\sigma\tau^{-1})\sigma^{-1} \in N$. Hence N contains a product of two transpositions τ and τ_1.

If τ, τ_1 has a common symbol then $\tau\tau_1$ is a 3-cycle. If τ and τ_1 are disjoint, say $\tau = (1\ 2)$ and $\tau_1 = (3\ 4)$ then, since $n \geq 5$, taking $(1\ 5)$ we have $(1\ 5)\tau\tau_1(1\ 5)^{-1} \in N$, i.e., $(1\ 5)(1\ 2)(3\ 4)(1\ 5) \in N$, which shows that $(2\ 5)(3\ 4) \in N$. Hence $(1\ 2)(3\ 4)(2\ 5)(3\ 4) \in N$, i.e., $(1\ 2\ 5) \in N$. Hence in any case N contains a 3-cycle.

Note that all 3-cycles in S_n are conjugate and hence by normality of N all 3-cycles belong to N. Since for $n \geq 3$, A_n is precisely the product of 3-cycles we have $A_n \subset N$. But there does not any subgroup H such that $A_n \subsetneqq H \subsetneqq S_n$ and$N \neq S_n$, we must have $N = A_n$. Hence the result. ■

EXAMPLE. 4.31 The result is not true for $n = 4$. For example The set $N = \{i, (1\ 2)(3\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$ is a proper normal subgroup of S_4 which is different from A_4.

DEFINITION. 4.32 A group G is called a *simple group* if has no proper non-trivial subgroup.

We may recall that for a subset S of a group G the *normalizer* of S is the set $N_G(S) = \{g \in G : gSg^{-1} \subset S\}$. It can also be remembered that $N_G(S)$ is a subgroup of G and if S is a subgroup of G then $N_G(S)$ is the largest subgroup of G in which S is normal.

EXAMPLE. 4.33 The number of k-cycles in S_n is $(k-1)!\binom{n}{k} = \frac{n!}{k(n-k)!}$

The number of k elements subsets of $\{1, 2, \ldots, n\}$ is $\binom{n}{k}$. A k element set $\{i_1, i_2, \ldots, i_k\}$ can form $k!$ number of k-cycles. Any k-cycle $(i_1\ i_2\ \ldots\ i_k)$ has k number of representations, as $(i_1\ i_2\ \ldots\ i_k) = (i_2\ i_3\ \ldots\ i_k\ i_1) \ldots (1_k\ i_1\ \ldots\ i_{k-1})$. Hence the number of distinct k-cycles generated from the k-element set $\{i_1, i_2, \ldots, i_k\}$ is $\frac{k!}{k} = (k-1)!$. Thus the number of k-cycles is $(k-1)!\binom{n}{k} = \frac{n!}{k(n-k)!}$. ■

THEOREM. 4.34 *A_5 is a simple group of order 60.*

PROOF. If possible suppose that there are normal subgroups of A_5 other than A_5 and $\{i\}$. Let us take a normal subgroup N of A_5 with smallest order > 1. Consider the normalizer $T = \{\sigma \in S_5 : \sigma N \sigma^{-1} \subset N\}$ of N in S_5. Then T is a subgroup of S_5 and N is a normal subgroup of T. Since N is a normal subgroup of A_5, for $\sigma \in A_5$, $\sigma N \sigma^{-1} \subset N$ and hence $\sigma \in T$. Thus $A_5 \subset T$.

Now, $T \neq A_5 \Rightarrow T = S_5$ (since there is no subgroup between A_5 and S_5) $\Rightarrow N$ is normal in $S_5 \Rightarrow N = A_5$ — contradiction of our assumption. Hence we have $T = A_5$.

Consider the transposition $(1\ 2)$ and $M = (1\ 2)N(1\ 2)^{-1}$. Since $(1\ 2) \notin A_5 = T$, we have $N \neq M$. Also $(1\ 2)M(1\ 2)^{-1} = N$ and hence M is a normal subgroup of A_5. This implies that MN and $M \cap N$ are normal subgroups of A_n. Since N is of minimal order and $M \neq N$ we must have $M \cap N = \{i\}$. Also $|M| = |N|$.

Now, $(1\ 2)MN(1\ 2)^{-1} = (1\ 2)M(1\ 2)(1\ 2)^{-1}N(1\ 2)^{-1} = NM = MN$ (since M, N are normal and $M \cap N = \{i\}$), thus $(1\ 2)$ is in the normalizer of MN in S_5. SInce MN is normal in A_5 it follows that $MN = A_5$ (as shown in the case of T).

Thus $|A_5| = |MN| = |N|^2$ — which is a contradiction as $|A_5| = 60$ is not a square of any integer. Hence A_5 is a simple group. ■

THEOREM. 4.35 *A_6 is a simple group.*

PROOF. Since $|A_6| = \frac{6!}{2} = 360$, which is not a square of any integer, by the arguments similar to the one adopted in the proof for the case of A_5, one can conclude that A_6 is simple. ■

It can be noted that for $1 < m < n$, any $\sigma \in S_m$ can be treated as a member of S_n, from which we can conclude that S_n contains an isomorphic copy of S_m.

THEOREM. 4.36 *For $n \geq 6$, A_n is a simple group.*

PROOF. As in the case for $n = 5, 6$ the result has been proved. Assume that $n > 6$. Let $N \lhd A_n$, $N \neq A_n, N \neq \{i\}$. Choose $\sigma \in N$, $\sigma \neq i$. Since $Z(S_n) = \{i\}$ and A_n is generated by 3-cycles, there exists $\tau \in A_n$ such that $\sigma\tau \neq \tau\sigma$, i.e., $\tau\sigma\tau^{-1}\sigma^{-1} \neq \{i\}$. Now, $\tau\sigma\tau^{-1} \in N$ and $\sigma^{-1} \in N$ implies that $\tau\sigma\tau^{-1}\sigma^{-1} \in N$. Also $\sigma\tau^{-1}\sigma^{-1}$, being a conjugate to a 3-cycle, is a 3-cycle. Hence $\tau\sigma\tau^{-1}\sigma^{-1}$ is a product of two three cycles, non-idetity and belongs to N.

Since $n \geq 6$ the element $\tau\sigma\tau^{-1}\sigma^{-1}$ can contain at most six symbols and hence can be considered as an element of A_6. Aslo A_n contains an isomorphic copy of A_6. Thus $\tau\sigma\tau^{-1}\sigma^{-1}$ is a non-identity element of $N \cap A_6$ which is a normal subgroup of A_6. By simplicity of A_6 we have $N \cap A_6 = A_6$. Thus N contains a 3-cycle. Since all the three cycles are conjugate in A_n and N is normal subgroup of A_n it follows that all the three cycles in S_n are in N. A_n is generated by 3-cycles and hence $A_n \subset N$. Consequently $A_n = N$. ■