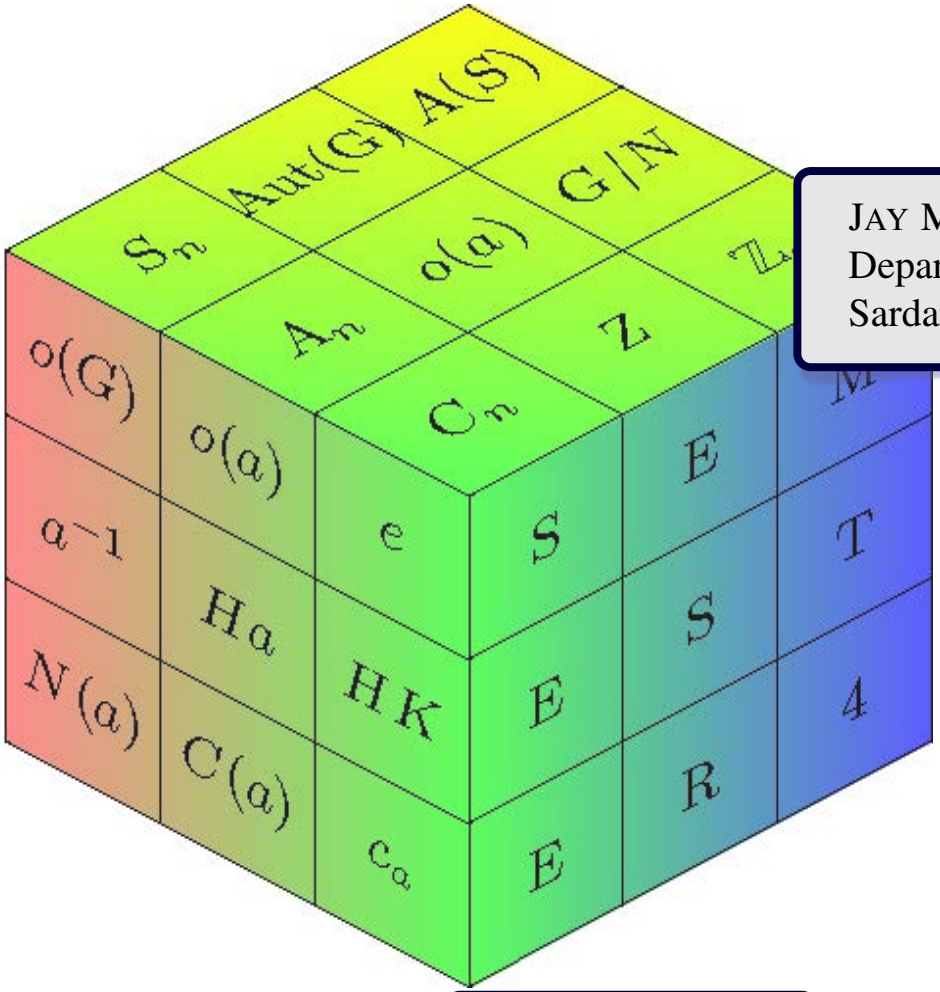
Lecture notes (Video Lectures Edition)
on

ADVANCED GROUP THEORY

PS03EMTH54



JAY MEHTA
Department of Mathematics,
Sardar Patel University.

SEMESTER - III
2023-24

$A(S)$ $HK < G$ S_n $1 + kp$ $n_1 \geqslant \cdots \geqslant n_k$

Preface and Acknowledgments

This note started when we (myself and Dr. D. J. Karia) first offered the course on Group Theory in 2017-18. In the subsequent years to follow, hopefully the note will take a good shape. This lecture note should not replace a human involvement of teaching but should serve purposes like:

- Saving of time of writing on the board by a teacher and copying by students in their notebooks. This will give, in turn, more time for discussion of concepts in the class.
- Saving students from the possibility of errors while taking down the notes and then spreading the errors unintentionally while passing on the notes taken by the students.

  At the same time, there might be errors in the typed notes too. We encourage students to read carefully and report the typos or errors in the notes, if any.
- A uniformity in approach in different classes.

This is a "*Video Lectures Edition*" an improvised/revised version of the covid-19 edition of lecture note. Due to the COVID-19 pandemic, hints or sketch of proof of some of the exercises were discussed in the online Google Meet or Microsoft Teams classes or in the YouTube videos. Since this is a special "*Video Lectures Edition*" of the lecture note, it contains QR-codes with links to YouTube Videos, and Video Clips of Google Meets which were provided to the students to facilitate online learning and to make it more convenient during the covid-19 pandemic.

This has many advantages. For example,

- it removes the hesitation experienced in the class to ask the teacher to repeat a concept once again,
- not losing link of the subject due to missed classes which happens in offline case,
- learn at one's convenience,
- revision of certain topics or concepts later on,
- not missing any lecture or topic due to lack/poor internet connection, etc.

JAY MEHTA

Contents

Syllabus

PS03EMTH54: Advanced Group Theory

Unit I: Definition of a group, some examples of groups, some preliminary lemmas, subgroups, Lagrange's theorem, Euler's theorem, Fermat's theorem, counting principle, the condition for HK to be a subgroup, order of HK, normal subgroups, and quotient groups, characterizations of normal subgroups, homomorphism, isomorphism, first isomorphism theorem, simple group, Cauchy's theorem for abelian groups, relation of two homomorphic groups.

Unit II: Automorphism, inner automorphism, Cayley's theorem and its applications, permutation groups, permutation as a product of disjoint cycles and transpositions, even and odd permutations, alternating group, another counting principle, conjugate classes, class equation and its applications, Cauchy's theorem (general case), number of conjugate classes in permutation group.

Unit III: Sylow's theorem, first proof, definition of p-Sylow subgroup, second proof of Sylow's theorem, double cosets and its order, existence of p-Sylow subgroup in subgroups, second part of Sylow's theorem, number of p-Sylow subgroups in a group, third part of Sylow's theorem, examples based on Sylow's theorems.

Unit IV: Direct products, external direct product and internal direct product, properties of internal direct product, finite abelian groups as direct product of cyclic groups, invariants of an abelian group of order power of prime p, the subgroup $G(s)$ of an abelian group G, for an integer s for a prime p, uniqueness of invariants, number of non-isomorphic abelian groups of a given order.

Reference Books

1. Herstein, I. N., Topics in Algebra, (Second Edition), Wiley Eastern Ltd., New Delhi, 1975.

2. Fraleigh J. B., A First Course in Abstract Algebra (Third Edition), Narosa, 1983.

3. Gallian, J.A., Contemporary Abstract Algebra (Fourth Edition), Narosa, 2008.

CHAPTER 1

Groups: Quick Revision

In this unit, we shall study the following.

Definition of a group, some examples of groups, some preliminary lemmas, subgroups, two equivalence relations $a \equiv b \mod H$ if $ab^{-1} \in H$ and $a \sim b \mod H$ if $a^{-1}b \in H$, Legrange's theorem. Euler's theorem, Fermat's theorem, counting principle, the condition for HK to be a subgroup and determination of $o(HK)$, normal subgroups, and quotient groups, characterizations of normal subgroups, homomorphism, isomorphism, first isomorphism theorem, simple group, Cauchy's theorem for abelian groups.

The intension of this unit is to have a quick look at the basic group theory that you have already studied. Consequently, we shall include a number of results, you have studied, as an exercise.

Significance and Motivation

Groups are a part of the underlying structure of many algebraic structure and notions like vector spaces, rings, fields, algebras, etc. Groups describe symmetry and so they are of great importance. The theory of groups has many applications in Elliptic curves, Cryptography, Elliptic curve cryptography, etc. It also has applications in other branches of sciences like Physical Sciences, Chemical Sciences, Computer Sciences, etc. Groups were studied since ancient times, even before the formal definition of such a structure was given.

Suppose we want to solve a simple algebraic equation $x+5=2$. We should look for an appropriate set in which we can find the solution. Certainly the set of positive integers $\mathbb{N}$ is not a probable candidate here. Let us look for the solution in the set of integers $\mathbb{Z}$. We solve this equation in the following steps.

- Adding the inverse of 5 (which is -5) on both the sides, we get

$$(x+5)+(-5)=2+(-5).$$

So one of the desired property we want our chosen set to have is the existence of inverse.

- Since we are looking for the value of x, we use associativity on the left hand side to get

$$x+(5+(-5))=2+(-5).$$

So another desired property our chosen set should possess is the associative property.

- Now we want the resultant of the operation addition to actually belong to the set. In left hand side we get 0 and in the right hand side we get -3. Both these number do not belong to $\mathbb{N}$ and so $\mathbb{N}$ is not a good choice of set which satisfy something what is called closure. So we get

$$x+0=-3.$$

Thus, we also should look for a set which is closed under the operation which we are applying. Here in our case the operation is addition.

- Finally, we want to the left hand side to be x, i.e., 0 is preferred to be the ideal element which has no effect on its operation with x. In other words, 0 should be the identity element for our set (which here we have chosen to be $\mathbb{Z}$). We have

$$x=-3.$$

Thus, our chosen set must have the property existence of identity.

This is just an example. To generalize such a concept, it is evident that a nonempty set which satisfies the above mentioned properties for a chosen operation is desirable. This leads us to the definition of Group.

1.1 Group: Definition and Examples

We start with the definition of a group.

Definition 1.1.1

Let G be nonempty set with an operation on it, denoted by $\cdot$ and satisfying the following properties: the following.

1. $a\cdot b\in G$ for all $a,b\in G$.
2. $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for all $a,b,c\in G$.
3. There is an element $e\in G$ such that $e\cdot a=a\cdot e=a$ for all $a\in G$.
4. For each $a\in G$, there is an element $a^{-1}\in G$ such that $a\cdot a^{-1}=a^{-1}\cdot a=e$.

Then G is called a *group*.

Remark 1.1.2. In the Definition 1.1.1, 1 is called the closure property. We also say that the operation $\cdot$ is a binary operation or the set G is closed under the operation $\cdot$, 2 is called associativity of operation $\cdot$, 3 is known as the *existence of identity in G*, and 4 is known as the *existence of inverse of each element in G*. e in (3) is called an[1] identity of G and a^{-1} in 4 is called an inverse of a.

[1]We use 'an' because we have yet not proved that identity and inverses are unique.

For the sake of convenience, we shall denote the binary operation $\cdot$ between two elements $a,b \in G$ as simply ab instead of $a \cdot b$. Though we shall call it "product ab", we keep in mind that it is not the multiplication in usual sense. It can be any specified operation on the set G.

Definition 1.1.3

A group G is said to be *abelian* (or *commutative*) if for every $a,b \in G$, $ab = ba$. A group which is not abelian is called *non-abelian*.

The number of elements in a group G is called *order of* G and is denote by $o(G)$. If it is finite, then we say that G is a finite group.

1.1.1 Some examples

Example 1.1.4. Now we list, without proof, some of the groups known to you.

1. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ are abelian groups under addition.
2. For $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$, the set of all integers divisible by n, is an abelian group under addition.
3. $\mathbb{C} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$, $(0,\infty)$ and $\{-1,1\}$ are abelian groups under multiplication.
4. For natural numbers m,n, the set of all $m \times n$ matrices with addition is an abelian group.
5. The set of all $n \times n$ invertible matrices over $\mathbb{R}$ is a group with multiplication.
6. The set of all $n \times n$ invertible real matrices whose determinant is 1 is a group with multiplication.

Example 1.1.5. Let $n \in \mathbb{N}$. Define $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, where $\overline{k}$ denotes the equivalence class $[k]$ for the relation $\equiv \mod n$. For $\overline{k}, \overline{m} \in \mathbb{Z}_n$, define

$$\overline{k} + \overline{m} = \overline{k+m} = \overline{t},$$

where $0 \leq t < n$ and $t = k + m \mod n$. Then $\mathbb{Z}_n$ is an abelian group under $+$.

Solution. **Claim 1:** $+$ is a binary operation on $\mathbb{Z}_n$. That is, $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ is a function.

Clearly, for every $(\overline{k}, \overline{m}) \in \mathbb{Z}_n \times \mathbb{Z}_n$, we get $\overline{k+m} \in \mathbb{Z}_n$. However, we need to prove its uniqueness. Let $j,k,l,m \in \mathbb{Z}$. If $j \equiv k \mod n$ and $l \equiv m \mod n$, then

$$\begin{aligned} & j - k = t_1 n \\ & l - m = t_2 n \\ \Rightarrow\ & j + l - (k+m) = (t_1 - t_2)n \\ \Rightarrow\ & j + l \equiv k + m \mod n. \end{aligned} \tag{1.1}$$

That is,

$$\overline{j} + \overline{l} = \overline{j+l} = \overline{k+m} = \overline{k} + \overline{m}. \tag{1.2}$$

Hence, $+$ is a binary operation on $\mathbb{Z}_n$.

Claim 2: $+$ is associative.

Let $\overline{j},\overline{k},\overline{m} \in \mathbb{Z}_n$. Then

$$\begin{aligned}(\overline{j}+\overline{k})+\overline{m} &= \overline{j+k}+\overline{m} = \overline{(j+k)+m} \\ &= \overline{j+(k+m)} = \overline{j}+\overline{k+m} = \overline{j}+(\overline{k}+\overline{m}). \end{aligned} \tag{1.3}$$

Thus $+$ is an associative operation on $\mathbb{Z}_n$.

Claim 3: $\overline{0}$ is the identity of $\mathbb{Z}_n$.

For every $\overline{k} \in \mathbb{Z}_n$,

$$\overline{k}+\overline{0} = \overline{k+0} = \overline{k} = \overline{0+k} = \overline{0}+\overline{k}. \tag{1.4}$$

Claim 4: Every $\overline{k} \in \mathbb{Z}_n$ has an inverse in $\mathbb{Z}_n$.

Let $\overline{k} \in \mathbb{Z}_n$. Then

$$\overline{k}+\overline{n-k} = \overline{k+n-k} = \overline{0} = \overline{n-k+k} = \overline{n-k}+\overline{k}. \tag{1.5}$$

Finally, for any $\overline{k},\overline{m} \in \mathbb{Z}_n$, we have

$$\overline{k}+\overline{m} = \overline{k+m} = \overline{m+k} = \overline{m}+\overline{k}. \tag{1.6}$$

Thus $(\mathbb{Z}_n,+)$ is an abelian group. □

Definition 1.1.6

For a nonempty set S, $A(S)$ denotes the set of all one-one onto functions from S to S.

Example 1.1.7. Let S be a set. Then $A(S)$ is a group with composition as operation.

Solution. **Step I:** To show that $A(S)$ is closed under composition.

Let $f,g \in A(S)$. Hence $f : S \to S$ and $g : S \to S$ are one-one, onto functions. Let $x,y \in S$ with $x \neq y$. Then

$$\begin{aligned} & (g\circ f)(x) = (g\circ f)(y) \\ \Rightarrow\ & g(f(x)) = g(f(y)) \\ \Rightarrow\ & f(x) = f(y) && (\because g \text{ is one-one.}) \\ \Rightarrow\ & x = y && (\because f \text{ is one-one.}) \end{aligned}$$

Hence, $g\circ f$ is one-one. Now let $z \in S$. Since g is onto,

$$\exists\, y \in S \text{ such that } g(y) = z. \tag{1.8}$$

Since $y \in S$ and f is onto,

$$\exists\, x \in S \text{ such that } f(x) = y. \tag{1.9}$$

By (1.8) and (1.9), there exists $x \in S$ such that $g \circ f(x) = z$. Hence $g \circ f \in A(S)$. Thus $A(S)$ is closed under composition.

Step II: To show that composition is associative.

Let $f, g, h \in A(S)$. For $x \in S$,

$$\begin{aligned} (h \circ g) \circ f(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h(g \circ f(x)) \\ &= h \circ (g \circ f)(x) \\ \therefore \quad (h \circ g) \circ f &= h \circ (g \circ f). \end{aligned}$$

Thus composition is associative.

Step III: To show that $A(S)$ has identity.

Define $\iota : S \to S$ by $\iota(x) = x$, $(x \in S)$. Then for $f \in A(S)$ and $x \in S$, $f \circ \iota(x) = f(\iota(x)) = f(x) = \iota(f(x)) = \iota \circ f(x)$. Hence $f \circ \iota = \iota \circ f = f$. Thus ι is the identity of $A(S)$.

Step IV: To show that to every $f \in A(S)$, there is a $g \in A(S)$ such that $f \circ g = g \circ f = \iota$.

Let $x \in S$. Since f is onto, there exists $y \in S$ such that $f(y) = x$. Since f is one-one, this y is unique. Define $g(x) = y$. Then

$$(g \circ f)(y) = g(f(y)) = g(x) = y = \iota(y)$$

and

$$(f \circ g)(x) = f(g(x)) = f(y) = x = \iota(x)$$

Therefore $g = f^{-1}$. Now it remains to show that $g \in A(S)$, i.e., g is bijective.

- For $x, y \in S$,

  $$g(x) = g(y) \Rightarrow f(g(x)) = f(g(y)) \Rightarrow (f \circ g)(x) = (f \circ g)(y) \Rightarrow \iota(x) = \iota(y) \Rightarrow x = y.$$

  Hence, g is one-one.

- Let $y \in S$. Then $y = \iota(y) = (g \circ f)(y) = g(f(y))$. Take $f(y) = x \in S$. Then $g(x) = y$. Hence, g is onto.

Hence $f^{-1} = g \in A(S)$. Thus $A(S)$ is a group with composition. □

Note that if S is a finite set with n elements, then the group $A(S)$, denoted by S_n, has cardinality $n!$ (see Exercise 1.10). Also the group $A(S)$ is nonabelian if and only if S has more than 2 elements (see Exercise 1.9).

Definition 1.1.8

Consider a finite set $S = \{x_1, x_2, \ldots, x_n\}$ and let $\theta \in A(S)$. Suppose

$$\theta(x_1) = x_{i_1}, \quad \theta(x_2) = x_{i_2}, \quad \ldots, \quad \theta(x_n) = x_{i_n};$$

that is, $\theta(x_k) = x_{i_k}$ for $k = 1, 2, 3, \ldots, n$. Such a θ is called *a permutation* and is written as

$$\theta = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \theta(x_1) & \theta(x_2) & \ldots & \theta(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix} \tag{1.10}$$

Usually, we take $S = \{1, 2, \ldots, n\}$ and write

$$\theta = \begin{pmatrix} 1 & 2 & \ldots & n \\ \theta(1) & \theta(2) & \ldots & \theta(n) \end{pmatrix} \tag{1.11}$$

Also, the set $A(S)$, in this case, is denoted by S_n. At times, we shall also write $k\theta$ for $\theta(k)$, $(1 \leq k \leq n)$, that is,

$$\theta = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1\theta & 2\theta & \ldots & n\theta \end{pmatrix} \tag{1.12}$$

Definition 1.1.9

Let $n \in \mathbb{N}$ and $\theta, \sigma \in S_n$. Then we define their product as

$$\theta\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(\theta(1)) & \sigma(\theta(2)) & \ldots & \sigma(\theta(n)) \end{pmatrix} \tag{1.13}$$

i.e.,

$$\theta\sigma = \sigma \circ \theta \tag{1.14}$$

Example 1.1.10. Let $n = 4$, $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ Then

$$\theta\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \tag{1.15}$$

and

$$\sigma\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \tag{1.16}$$

In the following example, we construct S_3.

Example 1.1.11 (A standard Example)**.** We set

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}. \tag{1.17}$$

Then $\varphi^2 = e = \psi^3$. Also,

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

$$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \psi^2\varphi = (\varphi\psi)^{-1}$$
$$\psi\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \varphi\psi^2 = (\psi\varphi)^{-1}$$

Thus $S_3 = \left\{ \begin{matrix} \varphi^2 \\ || \\ e \\ || \\ \psi^3 \end{matrix}, \varphi, \psi, \psi^2, \begin{matrix} (\varphi\psi)^{-1} \\ || \\ \varphi\psi \\ || \\ \psi^2\varphi \end{matrix}, \begin{matrix} (\psi\varphi)^{-1} \\ || \\ \psi\varphi \\ || \\ \varphi\psi^2 \end{matrix} \right\}$ is a group.
Throughout this note, without defining φ and ψ again, we shall refer to these elements.

Example 1.1.12. Let $n \in \mathbb{N}$ be fixed and $G = \{a^0, a, a^2, \cdots, a^{n-1}\}$, a set of symbols. Define $a^i a^j = a^{i+j}$ if $i+j < n$ and $a^i a^j = a^{i+j-n}$ if $i+j \geq n$. Then clearly G is a group. The group is denoted by C_n and called the *cyclic group of order n*.

Example 1.1.13. Let $S = \mathbb{Z}$ and $G = \{\sigma \in A(S) : \sigma(n) = n \text{ for all but finitely many } n \in \mathbb{Z}\}$. Then (show that) G is a group. (**Exercise**)

1.1.2 Some Preliminary Lemmas

We recall some results in this subsection. The proofs are left to the students as they have already done it in the undergrad.

Lemma 1.1.14

Let G be a group. Then

1. The identity element of G is unique.
2. Every $a \in G$ has a unique inverse in G.
3. For every $a \in G$, $(a^{-1})^{-1} = a$.
4. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Lemma 1.1.15

Given $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G. In particular, the following cancellation laws hold in G. For $a, u, w \in G$,

$$au = aw \Rightarrow u = w \quad \text{and} \quad ua = wa \Rightarrow u = w$$

hold in G.

1.2 Subgroups

Definition 1.2.1

Let G be a group and H be a nonempty subset of G. If H is also a group under the operation of G, then H is called a *subgroup* of G.

Example 1.2.2. Let G be any group. Clearly, $\{e\}$ and G are subgroups of G. They are called the *trivial subgroups* of G or the *improper subgroups* of G.

Example 1.2.3. Consider the group G of integers under addition, i.e., the group $(\mathbb{Z},+)$. Let H be the subset containing all the multiples of 5. That is, $H = 5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\}$. Then H is a subgroup of G.

Solution. We show that H is a subgroup of G.

- **Closure.** Let $x, y \in H = 5\mathbb{Z}$. Then $x = 5k_1$ and $y = 5k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then
$$x + y = 5k_1 + 5k_2 = 5(k_1 + k_2) \in 5\mathbb{Z}.$$
- **Associativity.** Let $x, y, z \in H$. Then $x, y, z \in G$. Then
$$x + (y + z) = (x + y) + z.$$
- **Identity.** Clearly the identity of G is the identity of H. Here 0 is the identity of H as $x + 0 = x = 0 + x$ for all $x \in H$.
- **Inverse.** Let $x \in H$. Then $x = 5k$ for some k and so $-x = -5k \in H$ and $x + (-x) = 0$. Thus, every element of H has an inverse.

□

Hence, $H = 5\mathbb{Z}$ is a subgroup of $G = \mathbb{Z}$ under addition. There is nothing special about 5 here. We can in general consider the subgroup $n\mathbb{Z}$ for any $n \in \mathbb{Z}$. What can be said about $n\mathbb{Z} \cap m\mathbb{Z}$? First try $4\mathbb{Z} \cap 6\mathbb{Z}$ and then generalize your observation.

Is "being subgroup of" an equivalence relation? Which properties of an equivalence relation are satisfied? Also, do we need to check all the properties of group for H to be a subgroup of G? Observe that the associativity in H is inherited from that of G. Also there is no need to check for identity element in H as it is assured from the existence of inverse of every element in H. Consequently we have the following results which we recall without proof as they are easy and you might have already studied them in your undergraduate course.

Lemma 1.2.4

Let G be a group and H be a nonempty subset of G. Then the following are equivalent.

1. H is a subgroup of G.
2. H is closed under the operation of G, i.e., $ab \in H$ for every $a, b \in H$, and every element of H has an inverse in H, i.e., $a^{-1} \in H$ for every $a \in H$.

3. $a,b \in H \Rightarrow ab^{-1} \in H$.

4. $a,b \in H \Rightarrow a^{-1}b \in H$.

Proof. Exercise. □

Lemma 1.2.5

Let H be a nonempty finite subset of a group G. Then H is a subgroup of G if it is closed under the operation of G.

Proof. Assignment/Seminar exercise. □

Example 1.2.6. Let G be a group of real numbers under addition, and let H be the set of all integers. Then H is a subgroup of G.

Example 1.2.7. Let G be the group of nonzero real numbers under multiplication, and let H be the set of positive rational numbers. Then H is a subgroup of G.

Example 1.2.8. Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad-bc\neq 0$ under multiplication. Let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid ad \neq 0 \right\}.$$

Then H is a subgroup of G.

Example 1.2.9. Let H be the group of 1.2.8, and let $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$. Then K is a subgroup of H.

Example 1.2.10. Let S be any set, $A(S)$ be the group of one-one mappings of S onto itself, under composition. For $x_0 \in S$, let $H(x_0) = \{\phi \in A(S) \mid \phi(x_0) = x_0\}$. Then $H(x_0)$ is a subgroup of $A(S)$. If $x_0, x_1 \in S$, $x_0 \neq x_1$, then what is $H(x_0) \cap H(x_1)$? Is it a subgroup of $A(S)$? Is it a subgroup of $H(x_0)$ or $H(x_1)$?

Example 1.2.11. Let G be a group, $a \in G$. Let $(a) = \{a^i \mid i = 0, \pm 1, \pm 2, \ldots\}$. Then **verify that** (a) is a subgroup of G. It is called the *cyclic subgroup generated by a*.

The group in the above example is sometimes denoted by $\langle a \rangle$ also. Above example yields us a way of producing subgroups of G. For any suitable choice of a, if $G = (a)$, then G is said to a *cyclic group*. Cyclic groups are very important in the theory of abelian groups. Note that a cyclic group is abelian but the converse is not true.

Example 1.2.12. Let G be a group and W be a subset of G. Let (W) be the set of all elements of G representable as a product of elements of W raised to positive, zero, or negative exponents. Then (W) is the *subgroup of G generated by W* and is the smallest subgroup of G containing W. Moreover, (W) is the intersection of all the subgroups of G which contains W. Note that such an intersection is never vacuous because G itself is a subgroup of G containing W.

Example 1.2.13. Let G be the group of nonzero complex numbers $a+ib$ (i.e., $a,b \in \mathbb{R}$, $a^2+b^2 \neq 0$) under multiplication. Let $H = \{a+ib \in G \mid a^2+b^2 = 1\}$. Then **verify that** H is a subgroup of G.

1.2.1 Right and left cosets of a subgroup

Definition 1.2.14

Let G be a group and H be a subgroup of G. For $a,b \in G$, we say that *a is congruent to b* mod H and write as $a \equiv b \mod H$, if $ab^{-1} \in H$. We say that *a is equivalent to b* mod H and write as $a \sim b \mod H$, if $a^{-1}b \in H$.

Lemma 1.2.15

Let H be a subgroup of a group G. For $a,b \in G$ show the following:

1. The relation $a \equiv b \mod H$ is an equivalence relation.
2. The relation $a \sim b \mod H$ is an equivalence relation.

Proof. Exercise. □

Let $G = \mathbb{Z}$ be the group under addition and $H = H_n = n\mathbb{Z}$, the subgroup of G of all the multiples of n. Since G is additive group, the relation $a \equiv b \mod H$, i.e., $ab^{-1} \in H$ is given by $a+(-b) = a-b \in H_n$. Thus, $a-b$ is a multiple of n or $n \mid a-b$. This is the usual number theoretic definition of congruence of two integers a and b. Thus, the relation defined above for an arbitrary modulo an arbitrary subgroup is a natural generalization of the congruence relation in number theory which is a familiar notion.

Definition 1.2.16

If H is a subgroup of G, $a \in G$, then $Ha = \{ha \mid h \in H\}$ and $aH = \{ah \mid h \in H\}$. The set Ha is called the *right coset of H in G* and the set aH is called the *left coset of H in G*.

Examples 1.2.17.

1. Consider group $G = S_3$ and its subgroup $H = \{e, \varphi\}$Then one can see that there are three distinct right cosets $H, H\psi, H\psi^2$ of H in G and three distinct left cosets $eH = H, \psi H, \psi^2 H$ of H in G. Also, since G is non-abelian, the right cosets and left cosets are not same except for H, for example, $H\psi \neq \psi H$.

2. Consider the group $G = \mathbb{Z}$ with addition and $H = 3\mathbb{Z}$. One can see that it also has three distinct right and left cosets. Since G is abelian, the right coset of $H+a$ is same the left coset $a+H$.

3. Consider $G = S_3$ and $H = \{e, \psi, \psi^2\}$. Find out the right cosets of H in G. **How many such distinct right cosets of H in G do we get? Observe the relationship between the order of H, order of G, and the number of distinct right cosets of H in G.**

Lemma 1.2.18

Let G be a group and H be a subgroup of G. For all $a \in G$, the equivalence class of a with respect to the relations $\equiv$ and $\sim$ are right and left cosets of H in G with respect to a. That

is,

$$Ha = \{x \in G \mid a \equiv x \mod H\}$$
$$aH = \{x \in G \mid a \sim x \mod H\}$$

Proof. Let $a \in G$.

- Let $x \in Ha$. Then $x = ha$ for some $h \in H$. We want to show that $x \in [a]$, where $[a] = \{x \in G \mid a \equiv x \mod H\}$ is the equivalence class of a. To show that $x \in [a]$ we have to show that $ax^{-1} \in H$. Now,

$$\begin{aligned} ax^{-1} &= a(ha)^{-1} && (\because x = ha) \\ &= a(a^{-1}h^{-1}) && (\because (ab)^{-1} = b^{-1}a^{-1}) \\ &= (aa^{-1})h^{-1} && (\text{associativity of } G) \\ &= eh^{-1} = h^{-1} \in H && (\because H \text{ is a subgroup and } h \in H). \end{aligned}$$

  Therefore $\boxed{Ha \subset [a]}$. To show $[a] \subset Ha$, consider $x \in [a]$.

$$\begin{aligned} x \in [a] &\Rightarrow a \equiv x \mod H && (\text{by defn. of equivalence class}) \\ &\Rightarrow ax^{-1} \in H && (\text{by defn. of congruence relation}) \\ &\Rightarrow ax^{-1} = h \text{ for some } h \in H \\ &\Rightarrow a = hx && (\text{multiply } x \text{ from right on both sides}) \\ &\Rightarrow h^{-1}a = x && (\text{multiply } h^{-1} \text{ from left on both sides}) \\ &\Rightarrow x = h^{-1}a \in Ha && (\because H \text{ is a subgroup and } h \in H). \end{aligned}$$

  Therefore $\boxed{[a] \subset Ha}$. Hence,

$$Ha = [a] = \{x \in G \mid a \equiv x \mod H\},$$

  i.e., the equivalence class of a (with respect to the relation $\equiv$) is the right coset of H in G (with respect to a).

- Let $\overline{a} = \{x \in G \mid a \sim x \mod H\}$ denote the equivalence class of a with respect to the relation $\sim$. Same as above, **show that** $aH = \overline{a}$.

□

We know that given two equivalence classes, either they are same or disjoint. Since left and right cosets are equivalence classes, we have the following corollary.

Corollary 1.2.19

Let H be a subgroup of G. Then

1. Two right cosets of H in G are either identical or disjoint.
2. Two left cosets of H in G are either identical or disjoint.

Lemma 1.2.20

Let G be a group and H be a subgroup of G. There is a one-to-one correspondence between any

1. two right cosets of H in G,
2. two left cosets of H in G, and
3. a left and a right coset of H in G.

Hint. For $a, b \in G$, prove that the following are one-one correspondences:

1. $ha \in Ha \leftrightarrow hb \in Hb$;
2. $ah \in aH \leftrightarrow bh \in bH$ and
3. $ah \in aH \leftrightarrow hb \in Hb$. □

Remark 1.2.21.

Above lemma is very significant when H is a finite subgroup, for then it says that any two right cosets (or left cosets) of H in G or a left and a right coset of H in G have the same number of elements. Note that $H = eH = He$, i.e., H itself is a right coset (or a left coset). So any right coset (or any left coset) of H in G has the same number of elements as that of H which is $o(H)$.

When the group G itself is finite, using the Lemma 1.2.18 and Lemma 1.2.20, and what we discussed above, we have the following well-known theorem called the Lagrange's theorem which states that order of a subgroup of a finite group divides the order of the group. We leave the proof as an exercise as you might have already seen it in the undergrad syllabus.

Theorem 1.2.22: Lagrange's Theorem

Let G be a finite group and H be a subgroup of G. Then order of H, that is $o(H)$, is a divisor of $o(G)$, that is $o(H) \mid o(G)$.

Proof. Assignment/Seminar exercise. □

Definition 1.2.23

Let H be a subgroup of a group G. The *index of H in G* is defined to be the number of distinct right cosets of H in G; and it is denoted by $i_G(H)$. If G is a finite group, then from the proof of Lagrange's theorem it is clear that

$$i_G(H) = \frac{o(G)}{o(H)} \tag{1.18}$$

What if we define index of a subgroup in the group as the number of distinct left cosets instead of right cosets? Is it possible? Does a subgroup H have the same number of right and left cosets in G? Justify (see Exercise 1.22).

Before we proceed to see some immediate consequences of the Lagrange's theorem, we make the following important remark regarding the same.

Remark 1.2.24. Note that the converse of Lagrange's theorem is **not true**. That is, a group G need not have a subgroup of order m if m is a divisor of $o(G)$. For example, there is a group of order 12 which does not have a subgroup of order 6 thought $6 \mid 12$. This group of order 12 can be found as a subgroup of the group S_4, the permutation group on 4 symbols. We shall study more about permutations in the next Unit.

The converse of Lagrange's theorem, however, is **true** for (finite) **abelian groups**.

Definition 1.2.25

Let G be a group and $a \in G$. We define the *order of a* to be the smallest $n \in \mathbb{N}$, if it exists, such that $a^n = e$ and in this case, we write $o(a) = n$. If such an n exists, then we say that a is of finite order. If such an n does not exist, then we say that a is of infinite order.

Corollary 1.2.26

If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.

Proof. Consider the cyclic subgroup H generated by a, i.e., $H = (a)$. Then H consists of elements of the form $e, a, a^2, \ldots$. Since G is a finite group, $H = (a)$ is also finite. We shall show that H has $o(a)$ elements.

Claim. $o(H) = o(a)$.

Clearly $a^{o(a)} = e$. So the group H has at most $o(a)$ distinct elements. If $o(H) < o(a)$, then $a^i = a^j$ for some integers $0 \leq i < j < o(a)$. Then $a^{j-i} = e$, where $0 < j - i < o(a)$ which is contradiction by the definition of $o(a)$. Hence, $o(H) = o(a)$. By Lagrange's theorem, $o(H) \mid o(G)$, i.e., $o(a) \mid o(G)$. □

Corollary 1.2.27

Let G be a finite group and $a \in G$. Then $a^{o(G)} = e$.

Proof. By above corollary, $o(a) \mid o(G)$. Therefore $o(G) = mo(a)$ for some integer m. Then

$$a^{o(G)} = a^{mo(a)} = \left(a^{o(a)}\right)^m = e^m = e.$$

□

Definition 1.2.28

Let $n \in \mathbb{N}$. The *Euler's totient function* also called *Euler's phi function* is defined as $\phi : \mathbb{N} \to \mathbb{N}$ as $\phi(1) = 1$ and $\phi(n) =$ number of positive integers less than n and relatively prime to n, for $n > 1$.

Prove that for a given integer $n > 1$, the set

$$G = \{k \in \mathbb{N} : k < n,\ \gcd(k,n) = 1\}$$

is a group under multiplication modulo n (see Exercise 1.23).

Clearly $o(G) = \phi(n)$. Consequently, we have the following particular case of Corollary 1.2.27.

Corollary 1.2.29: Euler

Let $n > 1$ be an integer and $a \in \mathbb{N}$ such that $\gcd(a,n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n. \tag{1.19}$$

We consider the following case when n is replaced by a positive prime integer p.

Corollary 1.2.30: Fermat

Let $a \in \mathbb{N}$ and $p \in \mathbb{N}$ be a prime. Then

$$a^p \equiv a \mod p. \tag{1.20}$$

Proof. **Case I:** $\gcd(a,p) = 1$.

Note that $\phi(p) = p - 1$. Hence by Corollary 1.2.29 (Euler's result),

$$a^{p-1} \equiv 1 \mod p$$
$$\therefore \quad a^p \equiv p \mod p.$$

Case II: $\gcd(a,p) \neq 1$.

In this case, the $\gcd(a,p) = p$. Consequently, $p \mid a$. Then $a \equiv 0 \mod p$ and so we also have $a^p \equiv 0 \mod p$. Hence,

$$a^p \equiv a \mod p.$$

This completes the proof. □

Corollary 1.2.31

If G is a finite group with $o(G) = p$, a prime integer, then G is cyclic.

Proof. Proof in seminar/assignment. □

1.3 A Counting Principle

Let H and K be two subgroups of a group G. In general HK is not a subgroup of G (see Exercise 1.24). However the following Lemma characterizes when HK is a subgroup of G.

Lemma 1.3.1

Let H, K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.

Proof. First assume that $HK = KH$. We shall prove that HK is a subgroup of G. Suppose $HK = KH$.

Claim 1: HK is closed under the product of G.

Let ,$x, y \in HK$. Then $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned}
xy &= (h_1k_1)(h_2k_2) \\
&= h_1(k_1h_2)k_2 && (\because \text{associativity}) \\
&= h_1(h_3k_3)k_2 && (\because k_1h_2 \in KH = HK, \text{ so } k_1h_2 = h_3k_3, \text{ for some } h_3 \in H,\ k_3 \in K) \\
&= (h_1h_3)(k_3k_2) && (\because \text{associativity}) \\
&\in HK && (\because h_1, h_3 \in H,\ k_2, k_3 \in K,\ H \ \&\ K \text{ are subgroups}).
\end{aligned}$$

Hence, HK is closed under the operation of G.

Claim 2: Every element of HK has an inverse in HK

Let $x = hk \in HK$, for some $h \in H$ and $k \in K$. Then $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$
$\therefore (x)^{-1} \in HK$.
Hence HK is a subgroup of G.
Conversely, assume that HK is a subgroup of G. Then we shall prove that $HK = KH$.
First we show that $KH \subset HK$. Let $x = kh \in KH$, where $h \in H, k \in K$. Then

$$\begin{aligned}
&\therefore h^{-1} \in H, k^{-1} \in K && (\because H \text{ and } K \text{ are subgroups}) \\
&\therefore h^{-1}k^{-1} \in HK \\
&\therefore (h^{-1}k^{-1})^{-1} \in HK && (\because HK \text{ is a subgroup}) \\
&\therefore kh \in HK && (\because kh = (h^{-1}k^{-1})^{-1}) \\
&\therefore KH \subset HK
\end{aligned}$$

Now we show that $HK \subset KH$. Let $x = hk \in HK$, where $h \in H, k \in K$.

$$\begin{aligned}
&\therefore x^{-1} \in HK && (\because HK \text{ is a subgroup}) \\
&\therefore (hk)^{-1} \in HK
\end{aligned}$$

$$\therefore (hk)^{-1} = h_1k_1 \qquad \text{(for some } h_1 \in H, k_1 \in K)$$
$$\therefore x = hk = k_1^{-1}h_1^{-1} \in KH \quad \text{(taking inverse on both sides)}$$
$$\therefore HK \subset KH$$

This completes the proof. □

Note that when G is commutative, $HK = KH$ automatically. Hence we have the following.

Corollary 1.3.2

Let H, K be two subgroups of an abelian group. Then HK is a subgroup of G.

Now we obtain a formula for counting the number of elements of HK.

Lemma 1.3.3

If H and K are finite subgroups of G of order $o(H)$ and $o(K)$ respectively, then

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}. \tag{1.21}$$

Proof. Let $H \cap K = \{e = r_1, r_2, \ldots, r_m\}$. Then $o(H \cap K) = m$.

Let us first list all elements of HK in the form

$$hk \ : \quad h \in H,\ k \in K \tag{1.22}$$

with all possible repetitions. So, there are $o(H)o(K)$ entries in (1.22). We show that each element of HK appears exactly m $(= o(H \cap K))$ times in this list.

Let $x \in HK$. Then there are $h \in H$ and $k \in K$ such that $x = hk$.

For $i = 1, 2, \ldots, m$, let

$$h_i = hr_i \text{ and } k_i = r_i^{-1}k.$$

Then $x = hk$ can be written in the form "an element of H times an element of K" in m distinct ways as shown below.

$$x = h_1k_1 = h_2k_2 = h_3k_3 = \cdots = h_mk_m \tag{1.23}$$

Now suppose hk can also be written as $h'k'$ with $h' \in H$ and $k' \in K$.

Claim 1: $h'k'$ is already listed in (1.23), that is, $h' = hr_i,\ k' = r_i^{-1}k$ for some i.

$$hk = h'k'$$
$$\Rightarrow (h')^{-1}h = k'k^{-1} \in H \cap K$$
$$\Rightarrow ((h')^{-1}h)^{-1} = (k'k^{-1})^{-1} \in H \cap K$$
$$\Rightarrow h^{-1}h' = k(k')^{-1} \in H \cap K$$
$$\Rightarrow h^{-1}h' = k(k')^{-1} = r_i \qquad \text{for some } r_i \in H \cap K$$

$$\Rightarrow r_i^{-1} = k'k^{-1}.$$

Consequently, $h' = (hh^{-1})h' = h(h^{-1}h') = hr_i$ and $k' = k'(k^{-1}k) = (k'k^{-1})k = r_i^{-1}k$.

Thus the repetition $h'k'$ is one of the forms listed in (1.23). Hence to count the exact number of elements of HK, we have to divide $o(H)o(K)$ by $m = o(H \cap K)$. This proves (1.21). □

Corollary 1.3.4

Let H, K be two subgroups of a finite group G. If

$$o(H) > \sqrt{o(G)} \quad \text{and} \quad o(K) > \sqrt{o(G)},$$

then $H \cap K \neq \{e\}$.

Proof. Since $HK \subset G$, $o(HK) \leq o(G)$. Let $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$. Suppose, if possible, $o(H \cap K) = 1$. Putting this value in (1.21)

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)} = o(G), \tag{1.24}$$

a contradiction to the fact that $o(HK) \leq o(G)$. Thus $o(H \cap K) \neq 1$. Thus $H \cap K \neq \{e\}$. □

As and application of the above corollary, we prove the following.

Proposition 1.3.5

Let $p, q \in \mathbb{N}$ be two prime numbers with $p > q$ and let G be a group of order $o(G) = pq$. Then G has at most one subgroup of order p.

Proof. Let H, K be two subgroups of G with $o(H) = o(K) = p$. We show that $H = K$. Now

$$\begin{aligned} & pq < p^2 && (\because q < p) \\ \Rightarrow\ & \sqrt{pq} < p \\ \Rightarrow\ & \sqrt{o(G)} < o(H) = o(K). \end{aligned}$$

Then by above corollary, $H \cap K \neq (e)$ and so $o(H \cap K) \neq 1$. Now, $H \cap K$ is a subgroup of H and K both. So, $o(H \cap K) \mid o(H)$ and $o(H \cap K) \mid o(K)$. That is, $o(H \cap K) \mid p$. Since $o(H \cap K) \neq 1$, it follows that $o(H \cap K) = p$.

Thus $H \cap K$ is a subset of H having p elements. Also H has p elements. Therefore, $H \cap K = H$ and similarly $H \cap K = K$. Hence, $H = K$. □

1.4 Normal Subgroups and Quotient Groups

Let G be a group, H be a subgroup of G and $a \in H$. Then the left and right cosets of H in G are

$$aH = \{ah \mid h \in H\} \quad \text{and} \quad Ha = \{ha \mid h \in H\}$$

respectively. Now if G is abelian, then clearly $aH = Ha$, i.e., a left coset of H in G is same as the right coset of H in G. When is this not true? Consider the following example in a non-abelian set-up.

Let $G = S_3$ and $H = (\varphi) = \{e, \varphi\}$. Then the following are the distinct right and left cosets of H in S_3.

Right cosets	**Left cosets**
$H\varphi = He = H = \{e, \varphi\}$	$\varphi H = eH = H = \{e, \varphi\}$
$H\varphi\psi = H\psi = \{\psi, \varphi\psi\}$	$\psi\varphi H = \psi H = \{\psi, \psi\varphi\}$
$H\psi\varphi = H\psi^2 = \{\psi^2, \varphi\psi^2 = \psi\varphi\}$	$\varphi\psi H = \psi^2 H = \{\psi^2, \psi^2\varphi = \varphi\psi\}$

Thus, there are three distinct right (or left) cosets of H in G and hence index of H in G is 3. Observe that $H\psi \neq \psi H$. Also the coset $H\psi$ is not a left coset. What is interesting is a subgroup for which every left coset is also a right coset, of course, this is trivial in case of abelian groups. Now, consider the following example.

Let $G = S_3$ and $N = (\psi) = \{e, \psi, \psi^2\}$. Then the following are the distinct right and left cosets of N in S_3.

Right cosets	**Left cosets**
$N\psi^2 = N\psi = Ne = N = \{e, \psi, \psi^2\}$	$\psi^2 N = \psi N = eN = N = \{e, \psi, \psi^2\}$
$N\psi\varphi = N\varphi\psi = N\varphi = \{\varphi, \psi\varphi, \psi^2\varphi\}$	$\psi\varphi N = \varphi\psi N = \varphi N = \{\varphi, \varphi\psi, \varphi\psi^2\}$
$\overset{\shortparallel}{\varphi\psi}$	$\overset{\shortparallel}{\psi\varphi}$

Note that there are two distinct cosets of N in G and hence index of N in G is 2. Not only that, but every left coset of N in G is also a right coset of N in G. Such subgroups are of special importance and called *normal subgroups* of the group G. We define here in a different way and then eventually we shall show that a subgroup N of G is normal if and only if every right coset of N in G is also a left coset of N in G.

Definition 1.4.1

Let G be a group and N be a subgroup of G. We say that N is a *normal subgroup of* G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$. Symbolically, this is written as $N \lhd G$.

Examples 1.4.2.

1. For any group G, the subgroups G and (e) are normal subgroups of G called the *improper normal subgroups* of G.
2. Any subgroup of an abelian group G is a normal subgroup of G.
3. The subgroup $N = (\psi)$ is a normal subgroup of S_3 (verify). Also check whether the subgroup $H = (\varphi)$ is a normal subgroup of S_3 or not. What are other normal subgroups of S_3?

Remark 1.4.3. For any $g \in G$, we have

$$gNg^{-1} = \{gng^{-1} \mid n \in N\}.$$

Hence, (from the definition of normal subgroup) equivalently we say that N is a normal subgroup of G if $gNg^{-1} \subset N$ for every $g \in G$. In fact, the reverse inclusion is also true and we have the following lemma.

Lemma 1.4.4

N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.

Proof. Assume that $gNg^{-1} = N$ for every $g \in G$. Then $gNg^{-1} \subset N$ for every $g \in G$ and hence N is normal in G.

Conversely, assume that N is normal in G. Then by definition for every $g \in G$, we have

$$gNg^{-1} \subset N.$$

If $g \in G$, then $g^{-1} \in G$ and so we can also write

$$g^{-1}Ng \subset N.$$

Hence for every $g \in G$,

$$\begin{aligned} g(g^{-1}Ng)g^{-1} &\subset g(N)g^{-1} \\ \Rightarrow N &\subset gNg^{-1}. \end{aligned}$$

Therefore, $gNg^{-1} = N$ for every $g \in G$. □

If $gNg^{-1} = N$ for every $g \in G$, then $gN = Ng$ for every $g \in G$. This means that every left coset of N in G is also a right coset of N in G. This leads us to the following lemma.

Lemma 1.4.5

The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

Proof. If N is normal in G, then by above lemma, $gNg^{-1} = N$ for every $g \in G$. Hence, $(gNg^{-1})g = Ng$, and equivalently $gN = Ng$ for every $g \in G$. Thus, the left coset gN is the right coset Ng.

Conversely, suppose that every left coset of N in G is a right coset of N in G. For any $g \in G$, consider the left coset gN of N in G. Suppose it is the right coset Na of N in G for some $a \in G$. That is, suppose

$$gN = Na.$$

Now, $g = g \cdot e \in gN$. Hence, $g \in Na$. But we have $g = e \cdot g \in Ng$. We know that any two right cosets of N in G are either identical or disjoint. Since $g \in Ng \cap Na$, we conclude that $Na = Ng$. Hence, $gN = Ng$ or $gNg^{-1} = N$ for every $g \in G$. Hence, N is a normal subgroup of G. □

Remark 1.4.6. We know that $HK = \{hk \mid h \in H,\ k \in K\}$. What if we take $K = H$. Then we have

$$HH = \{h_1h_2 \mid h_1, h_2 \in H\} \subset H \qquad (\because H \text{ is closed}).$$

On the other hand, $H = He \subset HH$. Hence, $HH = H$.

Now, suppose N is a normal subgroup of G and $a,b \in G$. Consider the right cosets Na and Nb. Since N is normal in G, by the above lemma, $aN = Na$. Therefore, we can multiply two right cosets to get a right coset as follows.

$$(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab.$$

Thus, product of two right cosets Na and Nb is again a right coset and precisely it is Nab, i.e., the right coset of N in G with respect to the product ab in G. Consequently, we have the following significant results.

Lemma 1.4.7

A subgroup N of G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Proof. Suppose N is normal in G and $a,b \in G$. Then

$$(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab.$$

Thus, the product of two right cosets of N in G is again a right coset of N in G.

Converse part of this is left as an **exercise** (see Exercise 1.25) □

Notation. Let G/N (read as "G quotient N") denote the collection of right cosets of N in G. (That is the elements of G/N are subsets of G and we define product in G/N as the product of right cosets defined above).

Then the number of elements in G/N is precisely $i_G(N)$, the index of N in G. We have the following theorem.

Theorem 1.4.8

If G is a group and N is a normal subgroup of G, then G/N is also a group.

Definition 1.4.9

Let N be a normal subgroup of a group G. The group G/N is called *the quotient group* or *the factor group* of G by N.

Proof of Theorem 1.4.8. For the *quotient product* of the right cosets defined above, we have

- Let $X,Y \in G/N$. Then $X = Na$ and $Y = Nb$ for some $a,b \in G$. Then

$$XY = (Na)(Nb) = Nab \in G/N.$$

- Let $X,Y,Z \in G/N$. Then $X = Na$, $Y = Nb$ and $Z = Nc$ for some $a,b,c \in G$. Now, since G is associative, we have

$$(XY)Z = (NaNb)Nc = (Nab)Nc = N(ab)c = Na(bc) = Na(Nbc) = Na(NbNc) = X(YZ).$$

- Consider the element $N = Ne \in G/N$. If $X \in G/N$, then $X = Na$ for some $a \in G$. Now,

$$XN = NaNe = Nae = Na = X.$$

  Similarly, $NX = X$. Consequently, $N = Ne$ is an identity element for G/N.

- Suppose $X = Na \in G/N$ with $a \in G$. Then $Na^{-1} \in G/N$, and

$$NaNa^{-1} = Naa^{-1} = Ne = N.$$

  Similarly, $Na^{-1}Na = Ne = N$. Hence, Na^{-1} is the inverse of Na in G/N.

Hence, if N is a normal subgroup of G, then G/N is a group with the quotient product of right cosets. □

What about the converse of the above theorem? If G/N is a group with the above defined operation, is it true that N must be a normal subgroup of G?

In addition, if G is a finite group, then we have the following lemma about the order of G/N.

Lemma 1.4.10

If G is a finite group and N is a normal subgroup of G, then

$$o(G/N) = o(G)/o(N). \tag{1.25}$$

Proof. Since the elements of G/N are the right cosets of N in G, the order of G/N is precisely

$$i_G(N) = \frac{o(G)}{o(N)}.$$

□

1.5 Homomorphisms

Definition 1.5.1

Let $G, \bar{G}$ be two groups. A mapping $\phi : G \to \bar{G}$ is said to be a *homomorphism from G to* $\bar{G}$ if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Below we give some examples of homomorphisms between different groups. In each of these examples, as an exercise, check the following things.

- whether ϕ is one-one
- whether ϕ is onto
- $\phi(e)$, where e is the identity of G
- $\phi(x)$ and $\phi(x^{-1})$ for $x \in G$

Example 1.5.2. For any group G and any group $\bar{G}$, the mapping $\phi : G \to \bar{G}$ by $\phi(x) = e$ for all $x \in G$ is a homomorphism called the *trivial homomorphism*.

For any group G, the map $\phi(x) = x$ for all $x \in G$ is also a homomorphism.

Example 1.5.3. Let $G = \mathbb{Z}$ with addition and let $\bar{G} = G$. Then the map $\phi : G \to \bar{G}$ defined by $\phi(x) = 2x$ is a homomorphism.

Example 1.5.4. Let $G = \mathbb{R}$ with addition and $\bar{G} = \mathbb{R} \setminus \{0\}$ with multiplication. Define $\phi : G \to \bar{G}$ by $\phi(a) = 2^a$. Then ϕ is a homomorphism as

$$\phi(ab) = 2^{a+b} = 2^a 2^b = \phi(a)\phi(b).$$

Since 2^a is always positive, note that, the image of ϕ is not all of $\bar{G}$, i.e., ϕ is not onto. ϕ is a mapping of G into $\bar{G}$.

Example 1.5.5. Let $G = S_3 = \{ \underset{\varphi^0\psi^0}{e}, \underset{\varphi}{\varphi^1\psi^0}, \underset{\varphi^0\psi^1}{\psi}, \underset{\psi^2}{\varphi^0\psi^2}, \underset{\varphi^1\psi^1}{\varphi\psi}, \underset{\psi\varphi}{\varphi^1\psi^2} \}$ and $\bar{G} = \{e, \varphi\}$. Define the mapping $f : G \to \bar{G}$ by $f(\varphi^i\psi^j) = \varphi^i$. That is

$$f : \begin{cases} e \mapsto & e \\ \varphi \mapsto & \varphi \\ \psi \mapsto & e \\ \psi^2 \mapsto & e \\ \varphi\psi \mapsto & \varphi \\ \psi\varphi \mapsto & \varphi \end{cases}$$

Verify that f is a homomorphism of G onto $\bar{G}$. One may also take $\bar{G} = S_3$. In that case, the homomorphism would not be onto.

Example 1.5.6. Let $G = \mathbb{R} \setminus \{0\}$ under multiplication and $\bar{G} = \{1, -1\}$ be the group under multiplication. Define $\phi : G \to \bar{G}$ by $\phi(x) = \begin{cases} 1 & \text{if } x \text{ is positive} \\ -1 & \text{if } x \text{ is negative.} \end{cases}$.

Then ϕ is a homomorphism.

Example 1.5.7. Let $G = \mathbb{Z}$ under addition and let $\bar{G}_n$ be the group of integers under addition modulo n. Define $\phi : G \to \bar{G}_n$ by $\phi(x) =$ remainder of x on division by n. Verify that ϕ is a homomorphism.

Example 1.5.8. Let G be the group positive real numbers with the operation multiplication and let $\bar{G} = \mathbb{R}$ with addition. Then $\phi : G \to \bar{G}$ by $\phi(x) = \log_{10} x$ is a homomorphism because

$$\phi(xy) = \log_{10}(xy) = \log_{10}(x) + \log_{10}(y) = \phi(x)\phi(y).$$

Example 1.5.9. Let $G = GL_2(\mathbb{R})$ be the group under matrix multiplication and let $\bar{G} = \mathbb{R} \setminus \{0\}$ under multiplication. Define $\phi : G \to \bar{G}$ by $\phi(A) = \det(A)$ for $A \in GL_2(\mathbb{R})$. Then verify that ϕ is a homomorphism of G onto $\bar{G}$.

The following observation can be made from the examples we have seen above.

Lemma 1.5.10

If ϕ is a homomorphism of G into $\bar{G}$, then

1. $\phi(e) = \bar{e}$, the unit element of $\bar{G}$.
2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

Proof. 1. Since ϕ is a homomorphism and $ee = e$,

$$\phi(e)\phi(e) = \phi(ee) = \phi(e).$$

By cancellation law in $\bar{G}$, $\phi(e) = \bar{e}$.

2. Since ϕ is a homomorphism,

$$\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e) = \bar{e}.$$

By the definition of inverse in $\bar{G}$, $\phi(x^{-1}) = \phi(x)^{-1}$.

□

Definition 1.5.11

Let G and $\bar{G}$ be two groups and $\phi : G \to \bar{G}$ be a homomorphism. Then the *kernel of* ϕ is denoted by K_ϕ or $\ker\phi$ and is defined by

$$\ker\phi = \{x \in G \mid \phi(x) = \bar{e}, \text{ where } \bar{e} \text{ is the identity of } \bar{G}\}.$$

Lemma 1.5.12

Let G and $\bar{G}$ be two groups. If ϕ is a homomorphism of G into $\bar{G}$ with kernel K, then K is a normal subgroup of G.

Proof. First we show that $K = \ker\phi$ is a subgroup of G.

Let $x, y \in \ker\phi$. Then $\phi(x) = \bar{e}$ and $\phi(y) = \bar{e}$. Since ϕ is a homomorphism,

$$\phi(xy) = \phi(x)\phi(y) = \bar{e}\bar{e} = \bar{e}.$$

Also for $x \in \ker\phi$, $\phi(x^{-1}) = \phi(x)^{-1} = \bar{e}^{-1} = \bar{e}$. That is $x^{-1} \in \ker\phi$. Hence, $\ker\phi$ is a subgroup of G.

Now we show that $K = \ker\phi$ is a normal subgroup of G.

For any $g \in G$ and $k \in \ker\phi$,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\bar{e}\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = \bar{e}.$$

Thus, $gkg^{-1} \in \ker\phi$ and hence $K = \ker\phi$ is a normal subgroup of G. □

Now, we give another example of a canonical homomorphism from a group to its quotient group by a normal subgroup in the form of the following lemma the proof of which is already seen earlier.

Lemma 1.5.13

Let G be a group and N be a normal subgroup of G. Define $\phi : G \to G/N$ by $\phi(x) = Nx$, $(x \in G)$. Then φ is an onto homomorphism with $\ker \varphi = N$.

Proof. First we show that ϕ is onto. Let $X \in G/N$. Then $X = Ny$ for some $y \in G$ and $\phi(y) = Ny = X$. Hence, ϕ is onto.

Now we show that ϕ is a homomorphism. If $x, y \in G$, then

$$\phi(xy) = Nxy = NxNy = \phi(x)\phi(y).$$

Finally,

$$\begin{aligned} \ker\phi &= \{x \in G \mid \phi(x) = N\} && (N \text{ is identity of } G/N) \\ &= \{x \in G \mid Nx = N\} \\ &= \{x \in G \mid x \in N\} = N. \end{aligned}$$

□

Now let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Let $\bar{g} \in \bar{G}$. What are all the inverse images of $\bar{g}$ in G? If $\bar{g} = \bar{e}$, then it is clear from the definition of kernel that inverse images of $\bar{e}$ is the kernel K. If we know one $x \in G$ which in inverse image of some $\bar{g} \in \bar{G}$, then we can find all the other inverse images by the following lemma.

Lemma 1.5.14

If ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is given by Kx, where x is any particular inverse image of $\bar{g}$ in G.

Proof. Let $\bar{g} \in \bar{G}$. Let $x \in G$ be any particular inverse image of $\bar{g}$, i.e. $\phi(x) = \bar{g}$. First we show that elements of Kx are the inverse images of $\bar{g}$ under ϕ.

Let $y \in Kx$, where K is $\ker\phi$. Then $y = kx$ for some $k \in K$ and

$$\phi(y) = \phi(kx) = \phi(k)\phi(x) = \bar{e}\bar{g} = \bar{g}.$$

Thus, y is also an inverse image of $\bar{g}$ under ϕ.

Now we show that any inverse image of $\bar{g}$ under ϕ is in Kx. Let z be any arbitrary inverse image of $\bar{g}$ under ϕ, i.e. $\phi(z) = \bar{g}$. Since $\phi(x) = \bar{g}$, we have

$$\begin{aligned} & \phi(z) = \phi(x) \\ \Rightarrow\ & \phi(z)\phi(x)^{-1} = \bar{e} \\ \Rightarrow\ & \phi(z)\phi(x^{-1}) = \bar{e} && (\because \phi(x)^{-1} = \phi(x^{-1})) \\ \Rightarrow\ & \phi(zx^{-1}) = \bar{e} && (\because \phi \text{ is homomorphism}) \\ \Rightarrow\ & zx^{-1} \in K = \ker\phi \\ \Rightarrow\ & z \in Kx. \end{aligned}$$

□

Definition 1.5.15

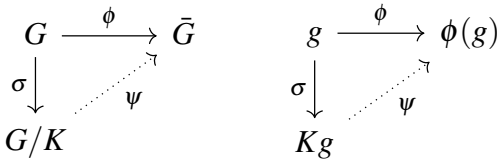
A homomorphism ϕ from G into $\bar{G}$ is said to be an *isomorphism* if ϕ is one-one.

Let $G, \bar{G}$ be two groups. We say that G *is isomorphic to* $\bar{G}$ if there exists an isomorphism from G onto $\bar{G}$. In this case, we write $G \approx \bar{G}$.

Theorem 1.5.16: First Isomorphism Theorem

Let $G, \bar{G}$ be two groups and $\varphi : G \to \bar{G}$ be an onto homomorphism with kernel K. Then $G/K \approx \bar{G}$.

Proof. The proof is left as exercise. The hint is shown below.



Define $\psi : G/K \to \bar{G}$ by $\psi(Kg) = \phi(g)$. Show that the map ψ is well-defined, bijective and a homomorphism, using the fact that ϕ is an onto homomorphism. □

1.5.1 Application: Cauchy's Theorem for Abelian Groups

Theorem 1.5.17: Cauchy's Theorem for Abelian Groups

Let G be a finite abelian group and $p \in \mathbb{N}$ be a prime such that $p \mid o(G)$. Then there is an element $a \neq e \in G$, such that $a^p = e$.

Proof. We prove this result by induction on $o(G)$.

Step I: $o(G) = 1$.

Suppose $o(G) = 1$. Then the result is vacuously true.[2]

Step II: Induction hypothesis: Suppose that the result is true for all abelian groups having order $< o(G)$.

Case I: G has no subgroup other than G and $\{e\}$.

In this case, $o(G)$ must be prime and that prime must be p. Thus G is cyclic and so there is $a \in G$ such that $o(a) = o(G) = p$.

Case II: G has a subgroup N other than G and $\{e\}$ and $p \mid o(N)$.

[2]Give me a prime p such that $p \mid 1$ and I will give you a such that $o(a) = p$.

By induction hypothesis, there is $a \in N$ such that $o(a) = p$. So, we are done.

Case III: G has a subgroup N other than G and $\{e\}$ and $p \nmid o(N)$.

Since G is commutative, N is normal. So, G/N is a group and $o(G/N) = o(G)/o(N) < o(G)$. Since G/N is commutative, by induction hypothesis, there is $X = Nb \in G/N$ such that $X \neq Ne$ and $X^p = Ne = N$. That is $\boxed{o(X) = p}$. Since $X \neq N$, $b \notin N$. Also since $X^p = N$, $(Nb)^p = Nb^p = N$ and so $b^p \in N$.

Then by a corollary of Lagrange's theorem, $(b^p)^{o(N)} = e$. That is $(b^{o(N)})^p = e$. Let $c = b^{o(N)}$. Then $c^p = e$. It remains to show that $c \neq e$.

$$\begin{aligned} c = e &\Rightarrow b^{o(N)} = e \\ &\Rightarrow Nb^{o(N)} = Ne = N \\ &\Rightarrow (Nb)^{o(N)} = N \\ &\Rightarrow X^{o(N)} = N \end{aligned}$$

But $(Nb)^p = N$, i.e., $o(X) = p$. So we have $p \mid o(N)$ which a contradiction to our assumption that $p \nmid o(N)$. Thus $c \neq e$. Hence $o(c) = p$. This completes the proof. □

1.6 Relation of two homomorphic groups

We will prove a result about the relation of two groups which are homomorphic. For this, consider the following lemma.

Lemma 1.6.1

Let ϕ be a homomorphism of G onto $\overline{G}$ with kernel K. For a subgroup $\overline{H}$ of $\overline{G}$, let $H = \{x \in G \mid \phi(x) \in \overline{H}\}$. Then H is a subgroup of G and $K \subset H$. If $\overline{H}$ is normal in G, then H is normal in G. Moreover, this association sets up a one-one mapping from the set of all subgroups of $\overline{G}$ onto the set of all subgroups of G containing K.

Proof. Left as a seminar/assignment exercise. Refer the reference book by I. N. Herstein. □

Theorem 1.6.2

Let ϕ be a homomorphism of G onto $\overline{G}$ with kernel K, and let $\overline{N}$ be a normal subgroup of $\overline{G}$, $N = \{x \in G \mid \phi(x) \in \overline{N}\}$. Then $G/N \approx \overline{G}/\overline{N}$. Equivalently, $G/N \approx (G/K)(N/K)$.

Proof. Left as a seminar/assignment exercise. Refer the reference book by I. N. Herstein. □

Exercises

These seminar topics will cover some of the exercises that you have already studied in your undergraduate course.

Exercise 1.1

Let $(G,*)$ be a group. Define $\times$ on G by $g \times h = h * g$, $(g,h \in G)$. Show that $(G,\times)$ is a group.

Exercise 1.2

Let $G = \{x \in \mathbb{C} : x^{27} = 1\}$. Show that G is a group under multiplication.

Exercise 1.3

Let G,H be two groups. For$(g_1,h_1),(g_2,h_2) \in G \times H$, define

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2). \tag{1.7}$$

Show that with this operations, $G \times H$ is a group.

Exercise 1.4

Show that the set of all 2×2 matrices form a group under matrix addition.

Exercise 1.5

Show that the set $GL(2,\mathbb{C})$ of all 2×2 matrices with nonzero determinant is a group under matrix multiplication.

Exercise 1.6

Let $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a,b \in \mathbb{R},\ a^2+b^2 \neq 0 \right\}$. Show that G is a group. Prove the same symbolically by writing $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = aI + bJ$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Exercise 1.7

Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}_p,\ ad-bc \neq 0 \right\}$. Show that G is a group.

Exercise 1.8

Let S be a set with one or two elements. Find the number of elements of $A(S)$.

Exercise 1.9

Show that for a set S, $A(S)$ is commutative, if and only if $|S| < 3$, here $|S|$ denotes the cardinality, that is, number of elements in S.

Exercise 1.10

Show that S_n has exactly $n!$ elements.

Exercise 1.11

Show that S_n is a group.

Exercise 1.12

Show that a group has a unique identity element.

Exercise 1.13

Show that to every element of a group, there is a unique inverse.

Exercise 1.14

State what do we mean by the cancellation laws in a group and prove them.

Exercise 1.15

Show that the set of all 2×2 matrices with determinant 1 is a subgroup of $GL(2,\mathbb{C})$.

Exercise 1.16

Does the set of all 2×2 matrices with determinant 1 or -1 form a subgroup of $GL(2,\mathbb{C})$? Prove your claim.

Exercise 1.17

Does the set of all 2×2 matrices with determinant -1 form a subgroup of $GL(2,\mathbb{C})$? Prove your claim.

Exercise 1.18

Let S be a set and $x_1 \in S$. Define $H(x_1) = \{f \in A(S) : x_1 = f(x_1)\}$. Show that $H(x_1)$ is a subgroup of $A(S)$.

Exercise 1.19

Let G be a group and $W \subset G$, define

$$\langle W \rangle = \{a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} : a_i \in W, n_i \in \mathbb{Z} \text{ for } 1 \leq i \leq k, k \in \mathbb{N}\}.$$

Show that $\langle W \rangle$ is a subgroup of G.

Exercise 1.20

Find all the right cosets of the subgroup $7\mathbb{Z} = \{7n : n \in \mathbb{Z}\}$ of $\mathbb{Z}$.

Exercise 1.21

Find all the right and left cosets of the subgroup $H = \langle \varphi \rangle$ of S_3 in S_3.

Exercise 1.22

Let G be a group and H be its subgroup. Show that the number of right cosets of H in G is same as the number of left cosets of H in G.

Exercise 1.23

Let $n > 1$ be an integer. Let $G = \{k \in \mathbb{N} : k < n,\ \gcd(k,n) = 1\}$. Show that G is a group under multiplication modulo n.

Exercise 1.24

Consider the subgroups $H = \{e, \phi\}$, $K = \{e, \phi\psi\}$ of S_3. Verify that $HK \neq KH$ and that none of them is a subgroup of S_3. Is HK or KH a subgroup of S_3? Justify.

Exercise 1.25

Let G be a group and N be a subgroup of G. If product of two right cosets of N in G is also a right coset of N in G, then show that N is normal in G.

Exercise 1.26

Show that "being isomorphic to" or "group isomorphism" is an equivalence relation.

Exercise 1.27

Let G be a finite group. If G has no proper subgroup, then show that G is a cyclic group of prime order.

Exercise 1.28

Let G be a group and $a \in G$ with $o(a) = n$. If $a^m = e$, then show that $n \mid m$.

CHAPTER 2

Conjugate Classes & Class Equation

In this unit, we shall study the following.

Automorphism, inner automorphism, Cayley's theorem and its applications, permutation groups, permutation as a product of disjoint cycles and transpositions, even and odd permutations, alternating group, another counting principle, conjugate classes, class equation and its applications, Cauchy's theorem (general case), number of conjugate classes in S_n.

2.1 Automorphisms

Definition 2.1.1

Let G be a group. An isomorphism from G onto G is called *an automorphism*. The set of all automorphisms of a group G will be denoted by $\mathrm{Aut}(G)$ or $\mathscr{A}(G)$.

Lemma 2.1.2

Let G be a group. Then the set $\mathscr{A}(G)$ is a group.

Proof. Let us note that $\mathscr{A}(G) \subset A(G)$. So, we need to prove that $\mathscr{A}(G)$ is nonempty and closed under composition and inversion. Since the identity map $I : G \to G$, defined by $I(g) = g$, $(g \in G)$, is an onto isomorphism, $\mathscr{A}(G) \neq \emptyset$. Also (since $A(G)$ is a group), we know that the composition of two one-one and onto functions is again one-one and onto. So now we prove that composition of two homomorphisms is a homomorphism. Let $S, T \in \mathscr{A}(G)$. Then for any $x, y \in G$,

$$\begin{aligned} (ST)(xy) &= S(T(xy)) && \text{(composition of functions)} \\ &= S(T(x)T(y)) && (\because T \text{ is a homomorphism}) \end{aligned}$$

$$\begin{aligned} &= S(T(x))S(T(y)) && (\because S \text{ is a homomorphism}) \\ &= (ST)(x)(ST)(y) && (\text{composition of functions}). \end{aligned}$$

Thus, ST is a homomorphism and hence $\mathscr{A}(G)$ is closed under composition.

Now we prove that for every $T \in \mathscr{A}(G)$, $T^{-1} \in \mathscr{A}(G)$. Let $T \in \mathscr{A}(G)$. So, $T \in A(G)$ and this implies $T^{-1} \in A(G)$. Also,

$$\begin{aligned} xy &= I(x)I(y) \\ xy &= TT^{-1}(x)TT^{-1}(y) \\ &= T(T^{-1}(x)T^{-1}(y)) \end{aligned}$$

So $T^{-1}(xy) = (T^{-1}(x)T^{-1}(y))$. Thus, every element of $\mathscr{A}(G)$ has an inverse in $\mathscr{A}(G)$. Hence $\mathscr{A}(G)$ is a subgroup of $A(G)$. □

Example 2.1.3. Let G be a group. Let $T : G \to G$ be defined by $T(x) = x^{-1}$. Then

1. $T \in A(G)$.
2. $T \neq I$ (i.e. T is non-trivial automorphism) if and only if there is $x_0 \in G$ such that $x_0 \neq x_0^{-1}$.
3. $T \in \mathscr{A}(G)$ if and only if G is abelian.

Solution. (1) Clearly, $T(x) = T(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow x \neq y$. Thus T is one-one. Also for any $x \in G$, $x^{-1} \in G$ and $T(x^{-1}) = (x^{-1})^{-1} = x$. So, T is onto.

(2)

$$\begin{aligned} x = x^{-1} \text{ for all } x \in G &\Leftrightarrow T(x) = x \text{ for all } x \in G \\ &\Leftrightarrow T = I. \end{aligned}$$

(3) Note that T is one-one and onto. Now,

$$\begin{aligned} T \text{ is a homomorphism } &\Leftrightarrow T(xy) = T(x)T(y) \text{ for all } x, y \in G \\ &\Leftrightarrow (xy)^{-1} = x^{-1}y^{-1} \text{ for all } x, y \in G \\ &\Leftrightarrow (xy) = (x^{-1}y^{-1})^{-1} \text{ for all } x, y \in G \\ &\Leftrightarrow G \text{ is abelian.} \end{aligned}$$

□

Lemma 2.1.4

Let G be a group and $g \in G$. Define $T_g : G \to G$ by $T_g(x) = gxg^{-1}$, $(x \in G)$. Then $T_g \in \mathscr{A}(G)$.

Proof. For $x, y \in G$,

$$\begin{aligned} T_g(xy) &= gxyg^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= T_g(x)T_g(y). \end{aligned}$$

Thus T_g is a homomorphism. Also, for $y \in G$, taking $x = g^{-1}yg$, we see that $T_g(x) = gxg^{-1} = gg^{-1}ygg^{-1} = y$. So, T_g is onto. Finally, for $x, y \in G$,

$$T_g(x) = T_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y.$$

This completes the proof. □

Definition 2.1.5

Let G be a group and $g \in G$. Then the automorphism $T_g : G \to G$ defined by $T_g(x) = gxg^{-1}$, $(x \in G)$, is called an *inner automorphism corresponding to* g. The set of all inner automorphisms is denoted by $\mathscr{I}(G)$.

Remark 2.1.6. Note that here we deviate from the definition of the inner automorphism given by [Herstein I. N., p. 68]. His definition is also valid but he operates a function on an element from right and we from left. So, we have to change.

If G is a non-abelian group, then $ab \neq ba$ for some $a, b \in G$. Therefore $a \neq bab^{-1}$. Then $T_b(a) = bab^{-1} \neq a = I(a)$. Thus $T_b \neq I$, i.e. T_b is a non-trivial automorphism.

Lemma 2.1.7

Let G be a group and $\mathscr{I}(G) = \{T_g \in \mathscr{A}(G) \mid g \in G\}$. Show that $\mathscr{I}(G)$ is a group.

Proof. Exercise. □

Lemma 2.1.8

Let G be a group. $\mathscr{I}(G) \approx G/Z$, where $\mathscr{I}(G)$ is the group of inner automorphisms of G, and Z is the center of G.

Proof. Define $\psi : G \to \mathscr{I}(G)$ by $\psi(g) = T_g$.

From Lemma 2.1.7, it follows that ψ is a homomorphism.

Now

$$\begin{aligned} g \in \ker(\psi) &\Leftrightarrow T_g = I \\ &\Leftrightarrow T_g(x) = x \qquad \forall\, x \in G \\ &\Leftrightarrow gxg^{-1} = x \qquad \forall\, x \in G \\ &\Leftrightarrow gx = xg \qquad \forall\, x \in G \\ &\Leftrightarrow g \in Z \end{aligned}$$

Thus, $\ker(\psi) = Z$, the centre of G.

Finally, for any $T_g \in \mathscr{I}(G)$, $\psi(g) = T_g$. Thus, the image of ψ is $\mathscr{I}(G)$, i.e. ψ is onto. So, by the first isomorphism theorem, $G/\ker(\psi) \approx \psi(G)$ that is $\mathscr{I}(G) \approx G/Z$. □

Lemma 2.1.9

Let G be a group and $\varphi \in \mathscr{A}(G)$. If $a \in G$ with $o(a) > 0$, then $o(\varphi(a)) = o(a)$.

Proof. Suppose $o(a) = n$ for some $n \in \mathbb{N}$. Then $\varphi(a)^n = \varphi(a^n) = \varphi(e) = e$. Also for any $1 \leq k < n$, if $\varphi(a)^k = e$, then $\varphi(a^k) = e$ and so $a^k = e$ ($\because \phi$ is one-one). This is a contradiction since $o(a) = n$. So, $\phi(a)^k \neq e$ for any $1 \leq k < n$ and hence $o(\varphi(a)) = n$. □

Next we compute the automorphisms of cyclic groups.

Example 2.1.10. Consider a finite cyclic group of order r, $G = (a)$, $a^r = e$ and also $o(a) = r$. Let $T \in \mathscr{A}(G)$. Observe that if $T(a)$ is known then $T(g)$ is known for all $g \in G$. This is because if $g \in G$, then $g = a^i$ for some i and $T(a^i) = T(a)^i$. Thus, we need to consider only the possibilities of $T(a)$ in G.

Since $T(a) \in G$ and G is cyclic, assume that $T(a) = a^t$ for some t. Since T is automorphism, by the above lemma, $T(a)$ must have the same order as that of a, i.e., order of $T(a)$ also must be r.

Claim. $\gcd(t,r) = 1$.

Suppose $d = \gcd(t,r)$. Then $(Ta)^{r/d} = (a^t)^{r/d} = (a^r)^{t/d} = e^{t/d} = e$. Hence $o(Ta)$ is a divisor of r/d. But $o(Ta) = r$. Therefore $d = 1$.

Denote the map $T \in \mathscr{A}(G)$ given by $T(a) = a^i$ by T_i. Now consider $U_r = \{t \in \mathbb{N} : 1 \leq t < r, (t,r) = 1\}$, the group of all integers relatively prime to r under multiplication modulo r. One easily sees that $T_i T_j = T_{ij}$.Thus, the mapping $i \mapsto T_j$ is an isomorphism of U_r onto $\mathscr{A}(G)$ and hence $U_r \approx \mathscr{A}(G)$.

Example 2.1.11. Determine automorphism of an infinite cyclic group (**Exercise**).

2.2 Cayley's Theorem

Throughout this section, G will denote a group.

Definition 2.2.1

Let G be a group and $g \in G$. We define $\tau_g : G \to G$ by $\tau_g(x) = gx$, $(x \in G)$.

Theorem 2.2.2: Cayley

Every group is isomorphic to a subgroup of $A(S)$ for some set S.

Proof. We set $S = G$.

Claim 1: $\{\tau_g : g \in G\}$ is a nonempty subset of $A(G)$.

Let $g \in G$. For $a, b \in G$,

$$\tau_g(a) = \tau_g(b) \Rightarrow ga = gb \Rightarrow a = b \quad \text{(by the left cancellation law).}$$

Hence τ_g is one-one. Also for any $y \in G$, let $x = g^{-1}y$. Then

$$\tau_g(x) = g(g^{-1}y) = y.$$

Hence τ_g onto. Thus $\{\tau_g : g \in G\} \subset A(G)$. Since $\tau_e \in \{\tau_g : g \in G\}$, it is nonempty.

Define $\psi : G \to A(G)$ by $\psi(g) = \tau_g$, $(g \in G)$, so that $\psi(G) = \{\tau_g : g \in G\}$.

Claim 2: ψ is a homomorphism.

For $g, h \in G$,

$$\begin{aligned} & \tau_{gh}(x) = (gh)x = g(hx) = \tau_g(hx) = \tau_g\tau_h(x) \\ \therefore\ & \tau_{gh} = \tau_g\tau_h \\ \therefore\ & \psi(gh) = \psi(g)\psi(h). \end{aligned} \tag{2.1}$$

Claim 3: ψ is an isomorphism (i.e. ψ is one-one).

Suppose $\psi(g) = \psi(h)$ for some $g, h \in G$.

$$\begin{aligned} & \psi(g) = \psi(h) \\ \Rightarrow\ & \tau_g = \tau_h \\ \Rightarrow\ & \tau_g(x) = \tau_h(x) && (\forall\, x \in G) \\ \Rightarrow\ & gx = hx && (\forall\, x \in G) \\ \Rightarrow\ & g = h && (\text{taking } x = e). \end{aligned}$$

Thus ψ is an isomorphism. □

Lemma 2.2.3

Let G be a group and H be a subgroup of G. Consider the set of all left cosets of H in G

$$S = \{xH : x \in G\}. \tag{2.2}$$

For $g \in G$, define $t_g : S \to S$ by

$$t_g(xH) = gxH, \quad (xH \in S), \tag{2.3}$$

and $\theta : G \to A(S)$ by

$$\theta(g) = t_g, \quad (g \in G). \tag{2.4}$$

Then θ is a homomorphism and $\ker(\theta)$ is the largest normal subgroup of G contained in H.

Proof. We divide the proof in several steps.

Claim 1: $t_g \in A(S)$ for every $g \in G$.

For a fixed $g \in G$, clearly $t_g(x) = gxH \in A(S)$. Thus t_g is a mapping from S to S. Also, for $xH, yH \in S$,

$$\begin{aligned} & t_g(xH) = t_g(yH) \\ \Rightarrow\ & gxH = gyH \\ \Rightarrow\ & xH = yH. \end{aligned}$$

Thus t_g is one-one.

Also for $yH \in S$, define $x = g^{-1}y$. Then $t_g(xH) = gxH = gg^{-1}yH = yH$. So, t_g is onto.

Claim 2: θ is a homomorphism.

Note that for $g, k \in G$ and $xH \in S$,

$$\begin{aligned} & t_{gk}(xH) = (gk)xH = g(kx)H = t_g(kxH) = t_g t_k(xH) \\ \Rightarrow\ & t_{gk} = t_g t_k \\ \Rightarrow\ & \theta(gk) = \theta(g)\theta(k) && \text{for all } g, k \in G. \end{aligned}$$

Thus θ is a homomorphism.

Claim 3: $\ker(\theta) \subset H$.

Let $\iota : S \to S$ denote the map $\iota(xH) = xH$, $(xH \in S)$.

$$\begin{aligned} h \in \ker(\theta) \Rightarrow & \theta(h) = \iota \\ \Rightarrow\ & t_h = \iota \\ \Rightarrow\ & t_h(xH) = \iota(xH) = xH && \text{for every } xH \in S \\ \Rightarrow\ & hxH = xH && \text{for every } xH \in S \\ \Rightarrow\ & heH = eH \\ \Rightarrow\ & hH = eH \\ \Rightarrow\ & h \in H \end{aligned}$$

Claim 4: $\ker(\theta)$ a normal subgroup of G.

Indeed, kernel of every homomorphism is a normal subgroup. So, the claim follows.[1]

Claim 5: If N is a subgroup of H such that N is a normal subgroup of G, then $N \subset \ker(\theta)$.

Let $n \in N$. Then for all $x \in G$,

$$\begin{aligned} & x^{-1}nx \in N \subset H && \text{(because } N \text{ is normal in } G \text{ and } n \in N) \\ \Rightarrow\ & x^{-1}nxH = eH = H \\ \Rightarrow\ & nxH = xH \end{aligned}$$

[1] Here we used this result. Let $\phi : G \to \bar{G}$ be a homomorphism, then $\ker(\phi)$ is a normal subgroup of G.

$$
\begin{aligned}
&\Rightarrow t_n(xH) = xH \qquad \text{for every } xH \in S \\
&\Rightarrow t_n = \iota \\
&\Rightarrow \theta(n) = \iota \\
&\Rightarrow h \in \ker(\theta) \\
&\Rightarrow N \subset \ker(\theta).
\end{aligned}
$$

This completes the proof. □

Taking $H = (e)$ in the above lemma, we get Cayley's theorem. As a consequence of the above theorem, we have the following result which is useful in proving that subgroups of certain order in the group G will contain a normal subgroup of G and as a result G cannot be a simple group. We have not yet defined simple group and we will define it in the next Unit, where we apply such results.

Corollary 2.2.4

Let H be a subgroup of a finite group G. If $o(G) \nmid i_G H!$, then H must have a subgroup $N \neq \{e\}$ such that N is normal in G, that is H must contain a nontrivial normal subgroup of G.

Proof. Let $S = \{xH : x \in G\}$ and $\theta : G \to A(S)$ be the mapping as in Lemma 2.2.3. By the above lemma, we know that θ is a homomorphism and $\ker\theta$ is a normal subgroup of G contained in H. Now, we prove that $\ker\theta$ is non-trivial. Suppose, if possible, that θ is an isomorphism. So, $o(G) = o(\theta(G))$. Now

$$
\begin{aligned}
&o(\theta(G)) \mid o(A(S)) \\
&\Rightarrow o(G) \mid o(A(S)) \quad (\text{because } o(G) = o(\theta(G))) \\
&\Rightarrow o(G) \mid i_G H!, \quad \text{a contradiction} \\
&\Rightarrow \theta \text{ is not an isomorphism} \\
&\Rightarrow \ker(\theta) \neq \{e\}
\end{aligned}
$$

Thus, $\ker(\theta)$ is nontrivial normal subgroup of G contained in H. □

2.2.1 Applications

The above corollary is an important result which can be used to prove, in certain cases, that a group has a proper normal subgroup. We will see this in again in Unit-3 but below we consider a couple of examples based on the above result.

Example 2.2.5. Let G be a group of order 36. Suppose G has a subgroup H of order 9 (we will prove later in Unit-3 that it will always have a subgroup of order 9). Then $i(H) = \frac{o(G)}{o(H)} = 4$. Then $i(H)! = 4! = 24 < 36 = o(G)$. Thus, $o(G) \nmid i(H)!$. Then by the above corollary, H has a subgroup $N \neq (e)$ which is normal in G. Since N is a subgroup of H, $o(N) \mid o(H)$. So $o(N) = 3$ or 9. If $o(N) = 9$, then $N = H$, i.e., H itself (is subgroup of H which) is normal in G.

Example 2.2.6. Let G be a group of orer 99 and suppose that H is a subgroup of G or order 11 (such a subgroup always exists by Cauchy's theorem, i.e., the cyclic subgroup generated by an element of order 11 in G). Then $i(H) = 9$ and $99 \nmid 9!$. Thus, $o(G) \nmid i(H)!$ and hence by the above corollary, H has a subgroup $N \neq (e)$ which is normal in G. Since N is a subgroup of H, $o(N) \mid o(H)$ and so $o(N) = 11$ which implies. $N = H$. That is, H is a normal subgroup of G.

2.3 Permutation groups

We recall the following from an earlier section for ready reference.

Definition 2.3.1

Consider a finite set $S = \{x_1, x_2, \ldots x_n\}$ and let $\sigma \in A(S)$. Suppose

$$\sigma(x_1) = x_{i_1}, \quad \sigma(x_2) = x_{i_2}, \quad \ldots, \quad \sigma(x_n) = x_{i_n};$$

that is, $\sigma(x_k) = x_{i_k}$ for $k = 1, 2, 3, \ldots, n$. Such a σ is called *a permutation* and is written as

$$\sigma = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix} \tag{2.5}$$

Usually, we take $S = \{1, 2, \ldots, n\}$ and write

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \tag{2.6}$$

Also, the set $A(S)$, in this case, is denoted by S_n. At times, we shall also write $k\sigma$ for $\sigma(k)$, $(1 \leq k \leq n)$, that is,

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1\sigma & 2\sigma & \ldots & n\sigma \end{pmatrix} \tag{2.7}$$

Definition 2.3.2

Let $n \in \mathbb{N}$ and $\sigma, \psi \in S_n$. Then we define their product as

$$\sigma\psi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \psi(\sigma(1)) & \psi(\sigma(2)) & \ldots & \psi(\sigma(n)) \end{pmatrix} \tag{2.8}$$

i.e.,

$$\sigma\psi = \psi \circ \sigma \tag{2.9}$$

Definition 2.3.3

Let S be any set and $\theta \in A(S)$. For $a, b \in S$, we write $a \equiv_\theta b$ if $b = a\theta^i$ for some $i \in \mathbb{Z}$, that is, $b = \theta^i(a)$.

Lemma 2.3.4

Given $\theta \in A(S)$, the relation $\equiv_\theta$ is an equivalence relation.

Proof.
- **Reflexivity.** Let $a,b,c \in S$. Clearly, $a \equiv_\theta a$ because $a = a\theta^0$. Thus $\equiv_\theta$ is reflexive.
- **Symmetry.**

$$\begin{aligned} & a \equiv_\theta b \\ \Rightarrow\ & \exists\, i \in \mathbb{Z} \text{ such that } b = a\theta^i \\ \Rightarrow\ & b\theta^{-i} = a \\ \Rightarrow\ & b \equiv_\theta a. \end{aligned}$$

  Thus $\equiv_\theta$ is symmetric.
- **Transitivity.**

$$\begin{aligned} & a \equiv_\theta b,\ b \equiv_\theta c \\ \Rightarrow\ & \exists\, i,j \in \mathbb{Z} \text{ such that } b = a\theta^i, c = b\theta^j \\ \Rightarrow\ & a\theta^{i+j} = a\theta^i\theta^j = b\theta^j = c \\ \Rightarrow\ & a \equiv_\theta c. \end{aligned}$$

  Hence $\equiv_\theta$ is transitive.

□

Definition 2.3.5

Let $\theta \in A(S)$, and $s \in S$. The equivalence class of s with respect to the relation $\equiv_\theta$ is called the *orbit of "s" under* θ. Thus the orbit of s under θ is the set

$$\{\ldots, \theta^{-2}(s), \theta^{-1}(s), \theta^0(s), \theta^1(s), \theta^2(s), \ldots\} \subset S.$$

Lemma 2.3.6

Let S be a finite set, $\theta \in A(S)$ and $s \in S$. Then there exists smallest positive integer $l = l(s)$, depending upon s, such that $s\theta^l = s$. Also, in this case, $s, s\theta, s\theta^2, \ldots, s\theta^{l-1}$ are all distinct elements of S.

Proof. Exercise. □

Definition 2.3.7

Let S be a finite set and $\theta \in A(S)$. Then the orbit of s under θ consists of elements $s, \theta(s), \ldots, \theta^{l-1}(s)$, where l is the smallest positive integer such that $\theta^l(s) = s$.

By a *cycle of* θ we mean the *ordered set*

$$(s, s\theta, s\theta^2, \ldots, s\theta^{l-1}) \tag{2.10}$$

for some $s \in S$ and l.

If we know all the cycles of θ then we can find θ since we would know the image of all the elements of S under θ. Since each cycle is an ordered set (tuple) of elements of an equivalence class (orbit), the cycles of θ are disjoint. We can also define cycle as a permutation as follows.

Definition 2.3.8

Let S be a finite set. By a *cycle* in $A(S)$, we mean an ordered subset

$$(i_1, i_2, i_3, \ldots, i_r), \tag{2.11}$$

where $i_1, i_2, i_3, \ldots, i_r$ are distinct elements of S and $r \in \mathbb{N}$. We also identify this cycle in (2.11) with the permutation $\theta \in A(S)$ which maps

$$i_1 \text{ to } i_2,\ i_2 \text{ to } i_3,\ \ldots\ i_{r-1} \text{ to } i_r,\ i_r \text{ to } i_1 \text{ and } a \text{ to } a \text{ if } a \neq i_k \text{ for any } k = 1, 2, \ldots, r.$$

We shall refer to this permutation as the cycle $(i_1, i_2, i_3, \ldots, i_r)$. We say that *the order of this cycle* is r or this is an r-cycle. We also say that the *length of this cycle* is r.

The following example will make the concept of cycles and their product clear.

Example 2.3.9. 1. In S_5, $(1,4,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

2. In S_4, $(1,4,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$.

3. In S_6,

$$(1,4,2)(3,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix}.$$

4. In S_5,

$$(1,4,3,2)(3,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}.$$

In the following example, an r-cycle is expressed in different ways.

Example 2.3.10. Let us write an r-cycle $(i_1, i_2, i_3, \ldots, i_r)$ as cycles in different ways.

Solution.

$$\begin{aligned} (i_1, i_2, i_3, \ldots, i_r) &= (i_2, i_3, \ldots, i_r, i_1) \\ &= (i_3, i_4 \ldots, i_r, i_1, i_2) \end{aligned}$$

$$\begin{aligned} &\dots \\ &= (i_k, i_{k+1}, \dots, i_r, i_1, i_2, \dots, i_{k-1}) \\ &\dots \\ &= (i_r, i_1, i_2, \dots, i_{r-1}) \end{aligned} \tag{2.12}$$

We consider all of these to be the same except writing a cycle differently. □

Definition 2.3.11

Let S be a finite set. The cycles $(i_1, i_2, i_3, \dots, i_r)$ and $(j_1, j_2, j_3, \dots, j_t)$ in $A(S)$ are said to be *disjoint cycles*, if $i_k \neq j_p$ for any $1 \leq k \leq r$ and $1 \leq p \leq t$.

Example 2.3.12.

1. $(1,3,2)$ and $(3,4,5)$ are not disjoint because 3 appears in both the cycles.
2. $(1,3,2)$ and $(6,4,5,7)$ are disjoint as they do not have any element in common.
3. $(1,5)$ and $(3,4,5)$ are not disjoint because 5 appears in both the cycles.

Example 2.3.13. We obtain the orbits and cycles of each $i \in \{1,2,3,\dots,7\}$ under the permutation $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 6 & 5 & 7 & 2 \end{pmatrix}$

Solution.

$$\begin{aligned} 1\theta = 3, 1\theta^2 = 3\theta = 1 \\ \therefore orb(1) = \{1,3\}, l(1) = 2 \end{aligned}$$

orbit of 3 = orbit of 1 and $l(3) = l(1) = 2$

$$\begin{aligned} 2\theta = 4, 2\theta^2 = 4\theta = 6, 2\theta^3 = 6\theta = 7, 2\theta^4 = 7\theta = 2 \\ \therefore orb(2) = \{2,4,6,7\}, l(2) = 4 \end{aligned}$$

orbit of 4 = orbit of 6 = orbit of 7 = orbit of 2 and $l(4) = l(6) = l(7) = l(2) = 4$. Finally,

$$\begin{aligned} 5\theta = 5 \\ \therefore orb(5) = \{5\}, l(5) = 1. \end{aligned}$$

Consequently,

$$(1,3), (2,4,6,7), (5)$$

are the cycles of θ. One easily verifies that $(1,3)(2,4,6,7)(5)$. □

Proposition 2.3.14

Every permutation is the product of its cycles.

Proof. Let θ be a permutation. Then its cyclers are of the form $(s, s\theta, \ldots, s\theta^{l-1})$. Since such a cycle is the equivalence class of s, the cycles of θ are disjoint. Let ψ be the product of all the cycles of θ. We shall show that $\psi = \theta$.

Let $s' \in S$. Since the cycles of θ are disjoint, s' is exactly in one cycle of θ. Hence, the image of s' under θ is same as the image of s' under the product, ψ, of all distinct cycles of θ. Therefore $\theta(s') = \psi(s')$, i.e., θ and ψ have the same effect on every elments of S. Hence $\psi = \theta$ which means that every permutation θ can be written as the product of its (disjoint) cycles.

□

Remark 2.3.15. Every permutation is the product of its cycles. Since disjoint cycles commute and a cycle of length 1 is identity permutation, this product is unique upto

1. changing the order in which cycles appear,
2. an equivalent way of writing any cycle and
3. omission of any 1-cycle.

Definition 2.3.16

A cycle of length 2 is called a *transposition*.

Example 2.3.17. Now that we know how to multiply the cycles, the following, which expresses some cycles as a product of transpositions, is apparent.[2]

1. $(1,3,2,5,6) = (1,3)(1,2)(1,5)(1,6) = (6,1)(6,3)(6,2)(6,5)$
2. $(1,2,3) = (1,2)(1,3) = (2,3)(2,1) = (1,3)(3,2)$

Motivated from the above, we have the following theorem.

Theorem 2.3.18

Every cycle can be written as a product of transpositions.

Proof. Exercise. □

Corollary 2.3.19

Every permutation can be written as a product of 2-cycles (i.e. transpositions).

Proof. Combining the above two results (Proposition and Theorem), the corollary follows. □

The 2-cycles are important and have many applications. We define a type of permutation based on these 2-cycles.

[2] Verify!

Definition 2.3.20

A permutation is said to be *even* if it can be written as a product of even number of transposition. A permutation which is not even is called an *odd* permutation.

Is it possible that in one representation a permutation is written as the product of even number of transposition and in another representation the same permutation is written as the product of odd number of transposition? If so, then is that permutation considered even or odd? We shall show that this cannot happen. For this we introduce a polynomial in multiple variables.

In what follows, p_n denotes the polynomial [3]

$$\begin{aligned} p_n(x_1,x_2,\ldots,x_n) &= (x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)(x_2-x_3)(x_2-x_4)\cdots(x_2-x_n) \\ &\qquad \cdots(x_{n-2}-x_{n-1})(x_{n-2}-x_n)(x_{n-1}-x_n) \\ &= \prod_{\substack{i=1 \\ i<j}}^{n}(x_i-x_j). \end{aligned}$$

in n variables $x_1,x_2,\ldots,x_n$.

Definition 2.3.21

Let $\theta \in S_n$. Define

$$\theta p_n(x_1,x_2,x_3,\ldots,x_n) = p_n(x_{\theta(1)},x_{\theta(2)},x_{\theta(3)},\ldots,x_{\theta(n)})$$

i.e.,

$$\theta \prod_{\substack{i=1 \\ i<j}}^{n}(x_i-x_j) = \prod_{\substack{i=1 \\ i<j}}^{n}(x_{\theta(i)}-x_{\theta(j)})$$

The effect of any permutation on the plynomial p_n is just in the sign of p_n. We record this result as the following lemma without proof. The proof was given by Dr. D. J. Karia in our old lecture note. Interested students can read the proof from that note.

Lemma 2.3.22

Let $\theta \in S_n$. Then $\theta p_n = \pm p_n$.

What is interesting and concerns us is the effect of a transposition on the polynomial p_n for which we have the following lemma.

Lemma 2.3.23

[3] Write p_1, p_2, p_3, p_4

If φ is a transposition in S_n, then $\varphi p_n = -p_n$.

Proof. Exercise. □

Corollary 2.3.24

If a permutation θ can be written as a product of even number of transpositions, then in every representation of θ, as a product of transpositions, the number of transposition will be even.

Proof. Let $\theta \in S_n$ can be written as a product of even number of transpositions. Say,

$$\theta = \varphi_1 \varphi_2 \cdots \varphi_{2k}$$

Thus $\theta p_n = \varphi_1 \varphi_2 \cdots \varphi_{2k} p_n = p_n$. If $\theta = \psi_1 \psi_2 \ldots \psi_r$, where each ψ_i is a transposition, then $p_n = \theta p_n = \psi_1 \psi_2 \ldots \psi_r p_n$. So, $\psi_1 \psi_2 \ldots \psi_r$ does not change sign of p_n. But each ψ_i changes the sign of p_n. So, $\psi_1 \psi_2 \ldots \psi_r$ must change the sign of p_n even number of times. So, r is even. □

Let A_n be the subset of S_n consisting of all the even permutations. Is it a subgroup of S_n? Is it normal? What is its order?

Lemma 2.3.25

Let W be the group $\{1, -1\}$ under multiplication. Define $\psi : S_n \to W$ by

$$\psi(\theta) = \begin{cases} 1, & \text{if } \theta \text{ is even} \\ -1, & \text{if } \theta \text{ is odd.} \end{cases}$$

Then ψ is a homomorphism. Also $\ker(\psi) = A_n$.

Proof. Assignment Exercise. □

Corollary 2.3.26

1. A_n is a normal subgroup of S_n
2. $o(A_n) = \dfrac{o(S_n)}{2} = \frac{n!}{2}$.

Proof. 1. Since kernel of a homomorphism is a normal subgroup of the domain group, A_n is a normal subgroup of S_n.

2. Since ψ is a homomorphism of S_n onto $W = \{-1, 1\}$ with kernel A_n, by first isomorphism theorem,
$$S_n/A_n \approx W.$$
Therefore, $o(S_n/A_n) = o(W)$ and so $\frac{o(S_n)}{o(A_n)} = 2$. Hence, $o(A_n) = \frac{n!}{2}$.

□

Definition 2.3.27

Let $n \in \mathbb{N}$. We define the *alternating group A_n to be the subgroup of S_n of order $\frac{n!}{2}$* of all the even permuations. That is,
$$A_n = \{\theta \in S_n : \theta \text{ is even}\} \tag{2.13}$$

From our discussion above, we have the following lemma.

Lemma 2.3.28

S_n has a normal subgroup of index 2, the alternating group A_n, consisting of all even permutations.

2.4 Another Counting Principle

Definition 2.4.1

Let G be a group and $a, b \in G$. We say that *b is conjugate of a* if there exists $c \in G$ such that $b = c^{-1}ac$. In this case, we write $a \sim b$.

Lemma 2.4.2

Conjugacy is an equivalence relation on group G.

Proof. Clearly, $a = a^{-1}aa$ proves that $a \sim a$. Next,
$$\begin{aligned} a \sim b &\Rightarrow b = x^{-1}ax && \text{for some } x \in G \\ &\Rightarrow xbx^{-1} = a \\ &\Rightarrow (y)^{-1}by = a, && \text{where } y = x^{-1} \\ &\Rightarrow b \sim a. \end{aligned}$$

Finally,
$$a \sim b, b \sim c \Rightarrow b = x^{-1}ax, c = y^{-1}by \qquad \text{for some } x, y \in G \tag{2.14}$$

$$\Rightarrow c = y^{-1}x^{-1}axy = (xy)^{-1}a(xy) \tag{2.15}$$
$$\Rightarrow a \sim c. \tag{2.16}$$

This completes the proof. □

Notation: The equivalence class of a under the relation of "being conjugate of" is called the *conjugate class of a* and is denoted by $C(a)$. That is,

$$C(a) = \{x \in G : a \sim x\} = \{y^{-1}ay : y \in G\}. \tag{2.17}$$

Also, c_a will denote the number of elements in $C(a)$.

Summing up what we discussed, we conclude that for a finite group G,

$$o(G) = \sum c_a, \tag{2.18}$$

where the summation is taken over one a from each conjugate class. We shall need this observation in the class equation that we are heading to obtain.

Definition 2.4.3

Let G be a group and $a \in G$. Then the *normalizer of a* in G is the set

$$N(a) = \{x \in G : xa = ax\}$$

Thus, $N(a)$ consists of precisely those elements in G which commute with a.

Lemma 2.4.4

Let G be a group and $a \in G$. Then $N(a)$ is a subgroup of G.

Proof.

- Let $x, y \in N(a)$. Then $xa = ax$ and $ya = ay$. Now,

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

  Thus, xy commutes with a and so $xy \in N(a)$.

- Let $x \in N(a)$. Then $xa = ax$. Therefore $x^{-1}(xa) = x^{-1}ax$, i.e., $a = x^{-1}ax$. So, $ax^{-1} = x^{-1}axx^{-1}$ or $ax^{-1} = x^{-1}a$. That is, x^{-1} commutes with a. Hence, $x^{-1} \in N(a)$.

Hence, $N(a)$ is a subgroup of G. □

Theorem 2.4.5

Let G be a finite group and $a \in G$. Then

$$c_a = i_G N(a) = o(G)/o(N(a)). \tag{2.19}$$

Proof. Consider the set $G/N(a) = \{N(a)x : x \in G\}$ of all right cosets of $N(a)$ in G. Define $\varphi : G/N(a) \to C(a)$ by $\varphi(N(a)x) = x^{-1}ax$. Note that for $N(a)x, N(a)y \in G/N(a)$,

$$\begin{aligned} N(a)x = N(a)y \; N(a)e = N(a) = N(a)yx^{-1} \qquad (2.20)\\ \Leftrightarrow yx^{-1} \in N(a)\\ \Leftrightarrow yx^{-1}a = ayx^{-1}\\ \Leftrightarrow x^{-1}ax = y^{-1}ay \qquad (2.21)\end{aligned}$$

$N(a)x = N(a)y \Rightarrow x^{-1}ax = y^{-1}ay$ in (2.21) means that φ is well defined and $x^{-1}ax = y^{-1}ay \Rightarrow N(a)x = N(a)y$ means that φ is well defined.

Clearly, for any $x^{-1}ax \in C(a) \in G$, we see that $\varphi(N(a)x) = x^{-1}ax$. Hence φ is onto also. Thus the number of distinct elements in $C(a)$ is the same as the distinct right cosets of $N(a)$ in G. So, $c_a = o(C(a)) = o(G)/N(a) = i_G N(a)$. This completes the proof. □

Corollary 2.4.6

For a finite group G,

$$o(G) = \sum \frac{o(G)}{o(N(a))}, \qquad (2.22)$$

where the sum is taken over one element a in each conjugate class.

Proof. Note that "being conjugate of" is an equivalence relation and $C(a)$ are precisely the equivalence classes of this relation. So, $\{C(a) : a \in G\}$ is a partition of G. Thus,

$$o(G) = \sum c_a = \sum \frac{o(G)}{o(N(a))},$$

where the sum is taken over one element a in each conjugate class. □

The equation (2.22) is called the ***class equation of*** G.

Example 2.4.7. Compute $N(a)$ and $C(a)$ for all $a \in S_3$.

Solution. Recall that

$$S_3 = \{e, \varphi, \psi, \psi^2, \varphi\psi, \varphi\psi^2\},$$

with the relations

$$\varphi^2 = \psi^2 = e, \varphi\psi = \psi^{-1}\varphi$$

Also recall that $\varphi = (1,2)$ and $\psi = (1,2,3)$.

N(e), C(e)

$$e \in Z \Rightarrow N(e) = G, \text{ and } C(e) = e. \qquad (2.23)$$

$N(\varphi)$, $C(\varphi)$

$$e\varphi = \varphi = \varphi e \; \Rightarrow e \in N(\varphi)$$

$$\begin{aligned}
\text{Clearly } \varphi \text{ commutes with } \varphi &\Rightarrow e \in N(\varphi)\\
\varphi\psi = \psi^2\varphi \neq \psi\varphi &\Rightarrow \psi \notin N(\varphi)\\
\varphi\psi^2 = \psi\varphi \neq \psi^2\varphi &\Rightarrow \psi^2 \notin N(\varphi)\\
\varphi(\varphi\psi) = \psi \neq (\varphi\psi)\varphi = \psi^2 &\Rightarrow \varphi\psi \notin N(\varphi)\\
\varphi(\psi\varphi) = \psi^2 \neq (\psi\varphi)\varphi = \psi &\Rightarrow \psi\varphi \notin N(\varphi)
\end{aligned}$$

Thus, $N(\varphi) = \{e, \varphi\}$ and $o(N(\varphi)) = 2$. Therefore, by the above theorem, we must have

$$o(C(\varphi)) = o(S_3)/o(N(\varphi)) = \frac{6}{2} = 3.$$

Now, we shall find $C(\varphi)$. By definition $C(\varphi) = \{x^{-1}\varphi x \mid x \in S_3\}$.

$$\begin{aligned}
e^{-1}\varphi e &= \varphi\\
\varphi^{-1}\varphi\varphi &= \varphi\\
\psi^{-1}\varphi\psi &= \varphi\psi^2\\
(\psi^2)^{-1}\varphi\psi^2 &= \varphi\psi^4 = \varphi\psi\\
(\varphi\psi)^{-1}\varphi(\varphi\psi) &= \psi^{-1}\varphi^{-1}\psi = \psi^{-1}\varphi\psi = \varphi\psi^2\\
(\varphi\psi^2)^{-1}\varphi(\varphi\psi^2) &= (\psi^2)^{-1}\varphi\psi^2 = \psi\psi\varphi = \varphi\psi
\end{aligned}$$

Collecting all the above we get,

$$C(\varphi) = \{\varphi, \varphi\psi, \varphi\psi^2\}.$$

$\boxed{N(\psi),\ C(\psi)}$

Verify that $N(\psi) = \{e, \psi, \psi^2\}$ and $C(\psi) = \{\psi, \psi^2\}$.

Compute all other $N(a)$ and $C(a)$ for all other $a \in S_3$. Note that some of the above relations and expressions will be helpful.

□

2.4.1 Applications

In this subsection we study couple of applications of Theorem 2.4.5. First consider the following lemma.

Lemma 2.4.8

$a \in Z$ if and only if $N(a) = G$. If G is finite, then $a \in Z$ if and only if $o(N(a)) = o(G)$.

Proof. If $a \in Z$, then $xa = ax$ for all $x \in G$. That is, all $x \in G$ commutes with a and hence $N(a) = G$.

Conversely, suppose $N(a) = G$. That is, $xa = ax$ for all $x \in G$. In other words, a commutes with every $x \in G$. Hence, $a \in Z$.

In particular, if G is a finite group, then

$$a \in Z \Leftrightarrow N(a) = G \Leftrightarrow o(N(a)) = o(G).$$

□

Remark 2.4.9. In the above lemma, we saw that $a \in Z \Leftrightarrow N(a) = G$. Thus, if G is a finite group, for such an a, $\frac{o(G)}{o(N(a))} = 1$. Hence, taking elements of Z, outside the sum in the class equation of G, we have

$$o(G) = o(Z) + \sum \frac{o(G)}{o(N(a))}, \tag{2.24}$$

where the sum is taken over one element a in each conjugate class such that $o(N(a)) < o(G)$ or $o(N(a)) \neq o(G)$.

Application 1

Theorem 2.4.10

Let p be a prime number and G be a group of order p^n for some $n \in \mathbb{N}$. Then $Z(G) \neq \{e\}$.

Proof. Recall the Class Equation (2.24),

$$o(G) = o(Z) + \sum \frac{o(G)}{o(N(a))}, \tag{2.25}$$

where the sum is taken over one element a in each conjugate class such that $o(N(a)) < o(G)$. For $N(a)$ appearing in the sum on the right hand side,

$$\begin{aligned}
o(N(a)) < o(G) &\Rightarrow o(N(a)) = p^{k_a} \text{ for some } k_a < n \\
&\Rightarrow \frac{o(G)}{o(N(a))} = p^{n-k_a} \\
&\Rightarrow p \mid \frac{o(G)}{o(N(a))} \text{ whenever } o(N(a)) < o(G) \\
&\Rightarrow p \mid \sum \frac{o(G)}{o(N(a))} \\
&\Rightarrow p \mid \left(o(G) - \sum \frac{o(G)}{o(N(a))} \right) \\
&\Rightarrow p \mid o(Z)
\end{aligned}$$

Since $o(Z) > 0$, $o(Z)$ is at least p. Thus $Z \neq \{e\}$. □

Corollary 2.4.11

If $o(G) = p^2$ for some prime number p, then G is abelian.

Proof. We need to prove that $G = Z(G)$. So, we need to prove that $o(Z(G)) = o(G)$. By the above theorem, $Z(G) \neq \{e\}$. So, $o(Z(G)) = p$ or $o(Z(G)) = p^2$.

Suppose, if possible, that $Z(G) \neq G$. Thus $o(Z(G)) = p$. So, we get $a \in G \setminus Z(G)$. Now,

$$\begin{aligned} b \in Z(G) &\Rightarrow bc = cb && \text{for all } c \in G \\ &\Rightarrow ba = ab \\ &\Rightarrow b \in N(a) \\ &\Rightarrow Z(G) \subset N(a). \end{aligned}$$

But $a \in N(a)$ and $a \notin Z(G)$

$$\begin{aligned} &\Rightarrow o(Z(G)) < o(N(a)) \leq p^2 \\ &\Rightarrow p < o(N(a)) \leq p^2 \\ &\Rightarrow o(N(a)) = p^2 && (\text{because } o(N(a)) \mid o(G)) \\ &\Rightarrow N(a) = G \\ &\Rightarrow a \in Z(G), \end{aligned}$$

a contradiction. Thus $Z(G) = G$. □

Remark 2.4.12. All groups of order $4, 9, 25, 49, 121$ are commutative.

Application 2

As an application of the counting principle, we prove the general case of Cauchy's theorem.

Theorem 2.4.13: Cauchy's Theorem

Let G be a finite group and $p \in \mathbb{N}$ be a prime such that $p \mid o(G)$. Then G has an element of order p.

Proof. We prove this result by induction on $o(G)$.

Step I: $o(G) = 1$.

In this case, the result is vacuously true.[4]

Step II: Induction hypothesis: The result is true for all finite groups having order $< o(G)$.

If there is a proper subgroup W of G such that $p \mid o(W)$, then by induction hypothesis there exists an element of order p in W and so in G. Thus, we may assume that G does not have any proper subgroup W such that $p \mid o(W)$.

Recall the class equation of G:

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

[4]Give me a prime p such that $p \mid 1$ and I will give you a such that $o(a) = p$.

Since $p \mid o(G)$, $p \nmid o(N(a))$, we have

$$p \mid \frac{o(G)}{o(N(a))},$$

and so

$$p \mid \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}.$$

Since $p \mid o(G)$, the class equation gives,

$$p \mid \left(o(G) - \sum \frac{o(G)}{o(N(a))} \right) \Rightarrow p \mid o(Z(G))$$

Thus $Z(G)$ is a subgroup of G whose order is divisible by p. Since we have assumed that p does not divide order of any proper subgroup of G, we conclude that $Z(G)$ is not proper. But $Z(G) \neq (e)$ as $p \mid o(Z(G))$. So $G = Z(G)$, and hence, G is abelian. So, by the Cauchy's theorem for abelian groups, there is an element $a \in G$ such that $o(a) = p$. This completes the proof. □

2.4.2 Conjugate Classes in S_n

Now we turn to computation of conjugate classes of S_n.

Definition 2.4.14

Let $n \in \mathbb{N}$. We say that $n_1, n_2, n_3, \ldots, n_r$ is a *partition* of n if

1. $0 < n_1 \leq n_2 \leq n_3 \leq \cdots \leq n_r$ and
2. $n = n_1 + n_2 + n_3 + \cdots + n_r$.

we say that two partitions $n_1, n_2, n_3, \ldots, n_r$ and $n'_1, n'_2, n'_3, \ldots, n'_s$ are the same if $s = r$ and $n_i = n'_i$ for all $i = 1, 2, \ldots, r$. We denote the number of distinct partitions of n by $p(n)$.

Example 2.4.15.

$n = 1$.

$1 = 1$ is the only way to write 1. So, there is only one partition of 1. Hence $p(1) = 1$.

$n = 2$.

$$\begin{aligned} 2 &= 2 \\ &= 1 + 1 \end{aligned}$$

are the only two ways to write 2. So, 2 has two partitions. Hence $p(2) = 2$

$n = 3$.

$$\begin{aligned} 3 &= 3 \\ &= 1+2 \\ &= 1+1+1 \end{aligned}$$

are the only three ways to write 3. Hence $p(3) = 3$.

$n = 4$.

$$\begin{aligned} 4 &= 4 \\ &= 1+3 \\ &= 1+1+2 \\ &= 1+1+1+1 \\ &= 2+2 \end{aligned}$$

are the only five ways to write 4. Hence $p(4) = 5$.

$n = 5$.

$$\begin{aligned} 5 &= 5 \\ &= 1+4 \\ &= 1+1+3 \\ &= 1+1+1+2 \\ &= 1+1+1+1+1 \\ &= 2+2 \\ &= 1+2+2 \\ &= 2+3 \end{aligned}$$

are the only seven ways to write 5. Hence $p(5) = 7$.

Now let us recall from Proposition 2.3.14 that every permutation can be written as a product of disjoint cycles. This representation, partitions n. Let us understand it by means of an example.

Example 2.4.16. Suppose we are given a permutation $\theta \in S_{10}$ and after writing it as a product of disjoint cycles, we get

$$\theta = (1,3,4)(2,5,6)(7,9). \tag{2.26}$$

It seems that the 8 and 10 do not appear in the above representation of θ as a product of disjoint cycles. So, we rewrite the product by including 1-cycles also. Not only this, but we also arrange the cycles in ascending order according to their lengths. So, we get,

$$\theta = (10)(8)(7,9)(1,3,4)(2,5,6). \tag{2.27}$$

Now in this representation, each number from 1 to 10 occurs exactly once. Clearly, the sum of the lengths of the cycles equals to 10. Thus θ gives us a partition

$$10 = 1+1+2+3+3. \tag{2.28}$$

It is apparent that each permutation will give unique partition as it can be written uniquely as a product of disjoint cycles. We shall call this partition a cycle decomposition.

Example 2.4.17. Two different permutations may give rise to the same partition. To see this observer that the permutations

$$\sigma = (7)(9)(1,2)(3,4,5)(6,8,10)$$
$$\theta = (1,3,4)(2,5,6)(7,9).$$

are not equal but they give rise to the same partition of 10 which is $10 = 1+1+2+3+3$. Also, note that $\theta = (7)(9)(11)(1,2)(3,4,5)(6,8,10)$ can be considered as an element of S_{11} and the corresponding partition will be $11 = 1+1+1+2+3+3$.

Definition 2.4.18

Let $\sigma \in S_n$. We say that

$$1 \leq n_1 < n_2 < \cdots < n_k \leq n \tag{2.29}$$

is the *cycle decomposition* of σ if there are disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_k \in S_n$ with $\ell(\sigma_i) = n_i$ for $1 \leq i \leq k$ satisfying the following.

1. $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ and
2. $n = n_1 + n_2 + \cdots + n_k$.

Our next goal is to prove that two permutations in S_n give the same partition of n (i.e., they have the same cycle decomposition) if and only if they are conjugate to each other.

Lemma 2.4.19

Let $\sigma, \theta \in S_n$.

$$i\sigma = j, i\theta = s, j\theta = t \Rightarrow s\theta^{-1}\sigma\theta = t. \tag{2.30}$$

Proof. $s\theta^{-1}\sigma\theta = i\sigma\theta = j\theta = t$. □

Thus, if σ maps i to j, then $\theta^{-1}\sigma\theta$ maps $\theta(i)$ to $\theta(j)$.

Remark 2.4.20. If $(i_1, i_2, \ldots, i_k)$ is a cycle of σ, if and only if $(i_1\theta, i_2\theta, \ldots i_k\theta)$ is a cycle of $\theta^{-1}\sigma\theta$

Corollary 2.4.21

Let $\sigma \in S_n$. Then every conjugate of σ has the same cycle decomposition.

Example 2.4.22. For $\sigma = (4,5)(1,2,3),(2,4,1)(3,5,6,7) \in S_7$, compute $\theta^{-1}\sigma\theta$.

Solution. By the Remark 2.4.20

$$\theta^{-1}\sigma\theta = (4\theta,5\theta)(1\theta,2\theta,3\theta) = (1,6)(2,4,5).$$

□

Corollary 2.4.23

Let σ, ψ have the same cycle decomposition. Then they are conjugate.

Proof. Let $1 \leq n_1 \leq n_2 < n_3 < \cdots < n_k$ be the cycle decomposition of σ and ψ, so that

$$\sigma = (i_1, i_2, \ldots, i_{n_1})(i_{n_1+1}, i_{n_1+2}, \ldots, i_{n_1+n_2}) \cdots (i_{n_1+n_2+\cdots+n_{k-1}}, \ldots, i_n) \tag{2.31}$$

and

$$\psi = (j_1, j_2, \ldots, j_{n_1})(j_{n_1+1}, j_{n_1+2}, \ldots, j_{n_1+n_2}) \cdots (j_{n_1+n_2+\cdots+n_{k-1}}, \ldots, j_n) \tag{2.32}$$

Define $i_t\theta = j_t$, $t = 1,2,\ldots,n$. Then from Lemma 2.4.19, it is clear that

$$\theta^{-1}\sigma\theta = \psi \tag{2.33}$$

□

So, we have proved the following theorem in the above Lemma and Corollaries.

Theorem 2.4.24

Two permutations in S_n have the same cycle decomposition if and only if they are conjugate of each other.

Proof. Combine Lemma 2.4.19, Corollary 2.4.21 and Corollary 2.4.23. □

Lemma 2.4.25

The number of conjugate classes in S_n is $p(n)$, the number of distinct partitions of n.

Proof. We have seen that a permutation gives unique cycle decomposition, which is nothing but a partition of n. Also, two conjugate permutations give rise to the same cycle decomposition. Conversely, given a partition $1 \leq n_1 \leq n_2 < n_3 < \cdots < n_k$ of n, define

$$\sigma = (1,2,\ldots,n_1)(n_1+1, n_1+2, \ldots, n_1+n_2) \cdots (n_1+n_2+\cdots+n_{k-1}, \ldots, n). \tag{2.34}$$

Then the cycle decomposition of σ is $1 \leq n_1 \leq n_2 \leq n_3 \leq \cdots \leq n_k$. Thus number of conjugate classes of S_n is the same as the number of partitions of n. □

2.4.3 Applications

Example 2.4.26. Find the elements that commute with $(1,2)$ in S_n.

Solution. Since disjoint cycles commute, permutations leaving 1 and 2 both fixed certainly commute with $(1,2)$. There are $(n-2)!$ such permutations in S_n (which fixes both 1 and 2). Also, $(1,2)$ commutes with with itself. Thus, $(1,2)\theta$ commutes with $(1,2)$, where θ is a permutation among the $(n-2)!$ permutations. This way we get $2(n-2)!$ such permutations. Now, we shall show that these are the only ones which commute with $a=(1,2)$.

We know that $c_a = \frac{o(G)}{o(N(a))}$. Therefore, the number of permutations which commute with $a=(1,2)$ in S_n is

$$o(N(a)) = \frac{o(S_n)}{c_a} = \frac{n!}{\text{no. of conjugates of } (1,2)}.$$

Since two conjugates have the same cycle decomposition, a conjugate of $(1,2)$ is of the form (a,b) where a has n possibilities and b has $n-1$ possibilities. But since $(a,b)=(b,a)$, the number of conjugates of $(1,2)$ is $\frac{n(n-1)}{2}$. Therefore, $o(N(a)) = \frac{n!}{n(n-1)/2} = 2(n-2)!$.

Thus, the above listed permutations are the only ones in S_n which commute with $(1,2)$. That is, if $\sigma \in S_n$ commutes with $(1,2)$, then $\sigma = (1,2)^i\tau$, where $i=0$ or 1 and τ is a permutation fixing both 1 and 2. □

Example 2.4.27. Show that the n-cycle $(1,2,\ldots,n) \in S_n$ commutes only with its powers.

Solution. Let $\theta = (1,2,\ldots,n)$. Then $\theta^n = e$ and clearly θ commutes with its powers. This gives n elements which commute with θ. Now, we show that no other element commutes with θ by determining the order of its normalizer, i.e., $o(N(\theta))$.

Since the conjugates have the same cycle decomposition, any conjugate of θ is an n-cycle. There are $(n-1)!$ such elements in S_n. Therefore,

$$o(N(\theta)) = \frac{o(S_n)}{c_\theta} = \frac{n!}{(n-1)!} = n.$$

Hence, an n-cycle in S_n commutes only with its powers. That is, there are exactly n-elements in S_n which commute with $\theta = (1,2,\ldots,n)$. □

Exercises

Exercise 2.1

Show that two disjoint cycles in S_n commute. Is the converse true? Justify. Show that a cycle of length 1 is the identity permutation.

Exercise 2.2

Let A_n denote the set of all even permutations in S_n. Show that A_n is a normal subgroup of S_n.

Exercise 2.3

Let H be a subgroup of a group G and $a \in G$. Show that aHa^{-1} is a subgroup of G and

$$o(aHa^{-1}) = o(H).$$

Exercise 2.4

For $a, b \in \mathbb{R}$, define $\tau_{ab} : \mathbb{R} \to \mathbb{R}$ by $\tau_{ab}(x) = ax + b$, $(x \in \mathbb{R})$. Show that

$$G = \{\tau_{ab} : a, b \in \mathbb{R}, a \neq 0\}.$$

is a subgroup of $A(\mathbb{R})$.

Exercise 2.5

A group of order 21 has exactly _____ elements of order 7.

1. 3
2. 4
3. 6
4. 7

Exercise 2.6

For $g \in G$, define $\lambda_g : G \to G$ by $\lambda_g(x) = xg$, $(x \in G)$. Show that

1. $\lambda_g \in A(G)$ and
2. $\lambda_{gh} = \lambda_h \lambda_g$.

Exercise 2.7

Let λ_g be defined as in (2.6) above and τ_g be defined as in Definition 2.2.1. Show that $\lambda_g \tau_h = \tau_h \lambda_g$ for $g, h \in G$.

Exercise 2.8

Let H be a subgroup of a group G. Show that $\bigcap_{g \in G} gHg^{-1}$ is a normal subgroup of G.

Exercise 2.9

Find the smallest possible group containing a, b satisfying

1. $a^2 = b^3 = e$ and
2. $ab = b^{-1}a$

Exercise 2.10

Find all the normal subgroups of S_3.

Exercise 2.11

Find the centre of S_3.

Exercise 2.12

Write the following permutations as product of disjoint cycles.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 6 & 2 & 3 & 7 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
4. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Exercise 2.13

Write each cycle of permutations in (2.12) as a product of transpositions in more than one ways.

Exercise 2.14

Find all transpositions in S_4 commuting with $(2,3)$. Find all three cycles in S_4 commuting with $(2,3)$.

Exercise 2.15

Find $(1,2,3)^{-1}$ in S_5.

Exercise 2.16

Let $\theta = (i_1, i_2, \ldots, i_k)$ be a cycle in S_n, $(k \leq n)$. What is the order of θ? Justify.

Exercise 2.17

What is the order of the permutation $\theta = (i_1, i_2, i_3)(i_3, i_4)$, where i_1, i_2, i_3, i_4 are distinct.

Exercise 2.18

Let $\theta_1, \theta_2, \ldots, \theta_k$ be disjoint cycles, each with order $m_1, m_2, \ldots, m_k$ respectively. Show that the order of $\theta_1\theta_2\ldots\theta_k = \text{lcm}(m_1, m_2, \ldots, m_k)$.

Exercise 2.19

Prove or disprove: two distinct cycles θ and σ in S_n have the same orbits.

Exercise 2.20

For $n \in \mathbb{N}$ and $\psi, \theta \in S_n$, define $\phi \sim \theta$ if $\phi\theta^{-1}$ is an even permutation.

1. Show that $\sim$ is an equivalence relation.
2. Find equivalence classes of this relation.
3. Show that $[e]$ is a subgroup.

Exercise 2.21

Define $\psi : S_n \to \{-1, 1\}$ by

$$\psi(\theta) = \begin{cases} 1, & \text{if } \theta \text{ is even} \\ -1, & \text{if } \theta \text{ is odd.} \end{cases}$$

Exercise 2.22

Prove or disprove: For every integer n, a group of order n^2 is abelian.

Exercise 2.23

Prove or disprove: For every prime number p, a group of order p^3 is abelian.

Exercise 2.24

List all the partitions of 6 to obtain $p(6) = 11$.

Exercise 2.25

Find the order of the normalizer of a transposition in S_n. Also find the order of a conjugate class of a transposition in S_n and hence deduce the order of its normalizer.

Exercise 2.26

Find $C(\sigma)$ and $N(\sigma)$ for an n-cycle $\sigma \in S_n$.

Exercise 2.27

Find the number of r-cycles in S_n.

Exercise 2.28

Compute all conjugates of $(1,2)(3,4)$ in S_n. Also find all $\sigma \in S_n$ commuting with $(1,2)(3,4)$.

Exercise 2.29

Find two permutations in A_5 which are conjugate in S_5 but not in A_5.

Exercise 2.30

Compute the conjugate classes in A_5.

Exercise 2.31

Compute all automorphisms of an infinite cyclic group.

Exercise 2.32

Find all automorphisms of S_3. Is $\mathscr{A}(S_3) = \mathscr{I}(S_3)$?

Exercise 2.33

Show that for any automorphism T of a group G, $T(Z) \subset Z$.

Exercise 2.34

For a fixed $n \in \mathbb{Z}$, show that the automorphism $x \in \mathbb{Z} \mapsto nx \in \mathbb{Z}$ is not an inner automorphism.

CHAPTER 3

Sylow's Theorem

In this unit, we shall study the following.

Sylow's theorems and applications, and simple groups.

3.1 Sylow's Theorem

Recall that by Lagrange's theorem we have, for finite groups, order of a subgroup divides order of a group. However, the converse of Lagrange's theorem is not true (Exercise 3.1), i.e. if G is a group of order n and m is a positive integer such that $m \mid n$, then G need not have any subgroup of order m. Sylow's theorem relates to answering the converse of Lagrange's theorem partially.

In this section we shall study Sylow's theorem and its applications. Sylow's theorem is one of the important and basic result in the theory of finite groups. There are three results due to Sylow, collectively called Sylow's theorem, known as first part of Sylow's theorem, second part of Sylow's theorem and third part of Sylow's theorem. They are also known as First Sylow theorem, Second Sylow theorem and Third Sylow theorem.

The First Sylow theorem, i.e. the first part of the Sylow's theorem has many different proofs, three proofs among which are presented in our text [**?**]. The first proof is based on number-theoretic and combinatorial arguments. The second proof is based on the class equation and the topics that we have already covered so far in the course. The third proof is based on the idea of showing that Sylow's theorem hold for a larger group than the one we are considering and the method involves of showing existence of a p-Sylow subgroup (see Definition 3.1.3) of S_{p^k} by constructing it inductively. Some of the concepts used in the third proof, which are essential tools for proving other two parts of Sylow's theorem, are already covered in this chapter.

3.1.1 First proof of Sylow's theorem

Let us recall that $\binom{n}{r} = \frac{n!}{k!(n-k)!}$. Now we turn to computation of conjugate classes of S_n.

Lemma 3.1.1

Let p be a prime and $n, m, r, \alpha \in \mathbb{N}$ such that $n = p^\alpha m, p^r \mid m$ but $p^{r+1} \nmid m$. Then $p^r \mid \binom{p^\alpha m}{p^\alpha}$ but $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$.

Proof. We have,

$$\begin{aligned}
\binom{p^\alpha m}{p^\alpha} &= \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} \\
&= \frac{[p^\alpha m(p^\alpha m-1)\cdots(p^\alpha m - p^\alpha + 1)][(p^\alpha m - p^\alpha)!]}{p^\alpha!(p^\alpha m - p^\alpha)!} \\
&= \frac{p^\alpha m(p^\alpha m-1)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha!} \\
&= \frac{p^\alpha m(p^\alpha m-1)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha-1)\cdots(p^\alpha - p^\alpha + 1)} \\
&= \frac{m(p^\alpha m-1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{(p^\alpha-1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)} \qquad (3.1)
\end{aligned}$$

Let us note that in the above expression, for $k \geq \alpha$, $p^k \nmid p^\alpha - i$. On the other hand,

$$\begin{aligned}
p^k \mid (p^\alpha - i) &\Leftrightarrow p^\alpha - i = ap^k && \text{for some } a \\
&\Leftrightarrow -i = ap^k - p^\alpha && \text{for some } a \\
&\Leftrightarrow p^\alpha m - i = p^\alpha m + ap^k - p^\alpha && \text{for some } a \\
&\Leftrightarrow p^\alpha m - i = p^\alpha(m-1) + ap^k && \text{for some } a \\
&\Leftrightarrow p^\alpha m - i = p^k(p^{\alpha-k}(m-1) + a) && \text{for some } a
\end{aligned}$$

Thus the all powers of p dividing $p^\alpha - i$ for some i in the numerator in (3.1) will be cancelled out. But the power of p dividing m will not be cancelled. This completes the proof. □

Theorem 3.1.2: Sylow's Theorem

Let p be a prime number and $p^\alpha \mid o(G)$. Then G has a group of order p^α.

Proof. Since $p^\alpha \mid o(G)$, there is $m \in \mathbb{N}$ such that $o(G) = p^\alpha m$. Assume that

$$p^r \mid m \text{ but } p^{r+1} \nmid m. \qquad (3.2)$$

Thus, $p^{\alpha+r} \mid o(G)$. Let $\mathscr{M}$ denote the set of all subsets of G having exactly p^α elements. Note that there are $\binom{p^\alpha m}{p^\alpha}$ elements in $\mathscr{M}$. Also by above lemma, $p^r \mid \binom{p^\alpha m}{p^\alpha}$ but $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$. That is p^{r+1} does not divide the number of elements in $\mathscr{M}$.

Claim 1: Equivalence relation on $\mathscr{M}$

For $M_1, M_2 \in \mathscr{M}$, define $M_1 \sim M_2$ if $M_1 = M_2 g$ for some $g \in G$. We show that $\sim$ is an equivalence relation on $\mathscr{M}$. Indeed $M = Me$ for all $M \in \mathscr{M}$. Thus $\sim$ is reflexive. Also, $M = Ng \Leftrightarrow N = Mg^{-1}$. Thus $\sim$ is symmetric. Finally $M = Ng, N = Hk \Rightarrow M = Hkg$ gives the transitivity of $\sim$. So, $\sim$ is an equivalence relation.

Claim 2: For some equivalence class $[M]$ of $\sim$, p^{r+1} does not divide the number of elements in $[M]$.

Suppose for each class $[M]$ for this equivalence relation, p^{r+1} divides $[M]$. So, p^{r+1} divides the number of elements in $\mathscr{M}$, a contradiction to the above lemma, as $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and p^{r+1} does not divide m. Thus there is some equivalence class $[M]$ such that p^{r+1} does not divide number of elements in $[M]$. Let

$$[M] = \{M_1, M_2, \ldots, M_n\}. \tag{3.3}$$

Clearly (by the definition of the above equivalence relation),

$$g \in G,\ M_i \in [M] \Rightarrow M_i g \in [M].$$

Define

$$H = \{g \in G : M_1 g = M_1\}. \tag{3.4}$$

Claim 3: H is a subgroup of G.

Let $g, h \in H$. Then $M_1 g = M_1 = M_1 h$

$$M_1 g h^{-1} = (M_1 g)h^{-1} = (M_1)h^{-1} = (M_1 h)h^{-1} = M_1$$

Thus $gh^{-1} \in H$. So, H is a subgroup of G.

Claim 4: The map $\psi : [M] \to \{Hg : g \in G\}$, defined by $\psi(M_1 g) = Hg$, $(M_1 g \in [M])$, is a bijection.

First of all note that

$$\begin{aligned} M_1 g_1 = M_1 g_2 &\Leftrightarrow M_1 g_1 g_2^{-1} \\ &\Leftrightarrow g_1 g_2^{-1} \in H \\ &\Leftrightarrow g_1 \in H g_2 \\ &\Leftrightarrow H g_1 = H g_2 \\ &\Leftrightarrow \psi(M_1 g_1) = \psi(M_1 g_2) \end{aligned}$$

The $\Rightarrow$ part of this gives the well-definedness of ψ and $\Leftarrow$ part gives the injectivity of ψ.

Now, we show that ψ is onto. Clearly for Hg, we choose $M_1 g$ and $\psi(M_1 g) = Hg$. Thus ψ is onto and hence it is bijective.

Thus $n = i_G(H) = o(G)/o(H)$. So, $no(H) = o(G) = p^\alpha m$. Recall that $p^{\alpha+r} \mid o(G)$. So, $p^{\alpha+r} \mid no(H)$. But $p^{r+1} \nmid n$ and so, $p^\alpha \mid o(H)$. So, $p^\alpha \leq o(H)$.

On the other hand, for any $m \in M_1$, $mH \subset M_1$. So $o(H) = o(mH) \leq o(M_1) = p^\alpha$. This proves that $o(H) = p^\alpha$. □

Definition 3.1.3: p-Sylow subgroup

Let G be a finite group and p be a prime such that $p^m | o(G)$ but $p^{m+1} \nmid o(G)$ for some integer $m \geq 1$. Then a subgroup of G order p^m is called a *p-Sylow subgroup* of G.

Actually the following Corollary 3.1.4 is known as the Sylow's Theorem or First Sylow theorem and it ensures the existence of p-Sylow subgroup.

Corollary 3.1.4

If $p^m | o(G)$, $p^{m+1} \nmid o(G)$, then G has a subgroup of order p^m.

Second proof of Sylow's theorem

Now, we present the second proof of (first) Sylow's theorem which is based on an application of class equation and the tools that we covered in the course so far. In the second proof, we prove the version stated in the above corollary first and then as a consequence we have the result stated in Theorem 3.1.2.

Theorem 3.1.5: First Sylow Theorem

Let G be a finite group and p be a prime such that $p^m | o(G)$ but $p^{m+1} \nmid o(G)$ for some integer $m \geq 1$. Then G has a subgroup of order p^m.

In other words, if G is a finite group and p is a prime dividing $o(G)$, then G has a p-Sylow subgroup.

Proof. We prove the result by induction on the order of the group G.

Let $o(G) = 1$. Then the result is vacuously true.
Let us consider another base case where $o(G) = 2$. Then the only prime dividing the order of the group G is 2. In this case G has a subgroup of order 2 which is itself. Hence, the theorem holds in this case too.

Now, assume that the result holds for all groups with order less than $o(G)$. Then we have to show that the result also holds for the group G.

Let p be a prime such that $p^m | o(G)$ but $p^{m+1} \nmid o(G)$ for some $m \geq 1$. Then we have the following two cases.

Case I: G has a proper subgroup H such that $p^m | o(H)$.

Since H is a proper subgroup of G, $o(H) < o(G)$. Also, $p^m | o(H)$ and $p^{m+1} \nmid o(H)$ as $p^{m+1} \nmid o(G)$. Then by induction hypothesis, H has a subgroup K of order p^m. Now, since K is a subgroup of H and H is a subgroup of G, K is a subgroup of G. Thus, K is the required p-Sylow subgroup of G.

Case II: $p^m \nmid o(H)$ for any proper subgroup H of G.

Recall the class equation (2.24) of G,

$$o(G) = z + \sum \frac{o(G)}{o(N(a))}, \tag{2.24}$$

where $z = o(Z)$ and the sum is taken over one element a in each conjugate class such that $o(N(a)) < o(G)$. Also recall that for $a \notin Z$, we have $N(a) \neq G$. Therefore $N(a)$ is a proper subgroup of G, i.e. $o(N(a)) < o(G)$. So by our assumption in this case $p^m | o(G)$ but $p^m \nmid o(N(a))$. Therefore we must have

$$p \Big| \frac{o(G)}{o(N(a))}.$$

Thus, $p \Big| \dfrac{o(G)}{o(N(a))}$ for every $a \in G$ such that $a \notin Z$, i.e. $o(N(a)) < o(G)$. Therefore,

$$p \Big| \sum_{a \notin Z} \frac{o(G)}{o(N(a))}.$$

This implies $p \Big| \left(o(G) - \sum \dfrac{o(G)}{o(N(a))} \right)$. Hence by the class equation of G, $p|z$. Then by Cauchy's theorem, Z has an element b $(\neq e)$ of order p. Let $B = \langle b \rangle$ be the subgroup generated by b. Then $o(B) = p$. Since $B \subset Z$, every element of B commutes with all the elements of G. Hence, B must be normal. Therefore we can form the quotient group $G' = G/B$. Now,

$$o(G') = \frac{o(G)}{o(B)} = \frac{o(G)}{p} < o(G).$$

Since $p^m | o(G)$ but $p^{m+1} \nmid o(G)$, it is clear that $p^{m-1} | o(G')$ but $p^m \nmid o(G')$. Thus, by induction hypothesis, G' has a subgroup P' of order p^{m-1}. Let

$$P = \{x \in G \mid xB \in P'\}.$$

Then P is a subgroup of G. Moreover, $P' \approx P/B$ (Exercise 3.2). Thus,

$$p^{m-1} = o(P') = \frac{o(P)}{o(B)} = \frac{o(P)}{p}.$$

Hence, $o(P) = p^m$. Therefore, P is the required p-Sylow subgroup of G and this completes the proof of the theorem, by induction. □

The second proof of the Sylow's theorem can be adapted to obtain the following result.

Theorem 3.1.6

Let p be a prime number and $p^\alpha \mid o(G)$. Then G has a group of order p^α.

Proof. Modify the (second) proof in the above theorem accordingly.
Hint: In induction, use $p^\alpha | o(G)$ instead of $p^m | o(G)$ but $p^{m+1} \nmid o(G)$. □

Third proof of Sylow's theorem

The third proof of the Sylow's theorem is framed in following steps:

1. First we prove that if G is a subgroup of a finite group M and M has a p-Sylow subgroup, then G has a p-Sylow subgroup.
2. Next we show that for a prime p, all the symmetric groups S_{p^r} have p-Sylow subgroups.
3. Since by Cayley's theorem, we know that every group G is isomorphic to a subgroup of S_n for some n, we take $M = S_{p^k}$ for sufficiently large k in step (1) and then use step (2) to prove the existence of p-Sylow subgroup of G.

Lemma 3.1.7

Let H be a subgroup of a group G and $x \in G$. Then

1. $x^{-1}Hx$ and xHx^{-1} are subgroups of G.
2. $\psi : H \to x^{-1}Hx$ defined by $\psi(h) = x^{-1}hx$, $(h \in H)$ is an onto isomorphism.
3. $\varphi : H \to xHx^{-1}$ defined by $\varphi(h) = xhx^{-1}$, $(h \in H)$ is an onto isomorphism.

Proof. Proof in seminar. □

In order to execute the first step of the proof, we begin with the following notion of double cosets and some preliminaries.

Definition 3.1.8

Let G be a group, A, B be subgroups of G. For $x, y \in G$, define $x \sim y$ if $y = axb$ for some $a \in A$ and $b \in B$.

Lemma 3.1.9

The relation $\sim$ defined above is an equivalence relation on G. The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$.

Proof. First we show that the relation $\sim$ defined above is an equivalence relation.

Step I: $\sim$ is reflexive, i.e. $x \sim x$ for all $x \in G$.

Since A and B are subgroups of G, $e \in A$ and $e \in B$. Therefore, for all $x \in G$, we write $x = exe$ whence $x \sim x$ and the relation $\sim$ is reflexive.

Step II: $\sim$ is symmetric, i.e. if $x \sim y$ then $y \sim x$ for all $x, y \in G$.

Let $x \sim y$. Then $y = axb$ for some $a \in A$ and $b \in B$. Therefore we can write $x = a^{-1}yb^{-1}$. Since A and B are subgroups of G and $a \in A$, and $b \in B$, we have $a^{-1} \in A$ and $b^{-1} \in B$ such that $x = a^{-1}yb^{-1}$. Hence, $y \sim x$ and therefore $\sim$ is symmetric.

Step III: $\sim$ is transitive, i.e. if $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in G$.

Since $x \sim y$, $y = a_1xb_1$ for some $a_1 \in A$ and $b_1 \in B$. Similarly, $y \sim z$ gives $z = a_2yb_2$ for some $a_2 \in A$ and $b_2 \in B$. Then

$$z = a_2yb_2 = a_2(a_1xb_1)b_2 = (a_2a_1)x(b_1b_2).$$

Since A and B are subgroups of G, $a_2a_1 \in A$ and $b_1b_2 \in B$. Therefore $x \sim z$ and hence the relation $\sim$ is transitive.

Thus, $\sim$ is an equivalence relation. The equivalence class of any $x \in G$ under $\sim$ is given by

$$\begin{aligned}[x] &= \{y \in G \mid x \sim y\} \\ &= \{y \in G \mid y = axb, \text{ for some } a \in A, b \in B\} \\ &= \{axb \mid a \in A, b \in B\} = AxB.\end{aligned}$$

Thus, the equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$. □

Definition 3.1.10

The set AxB, i.e. the equivalence class of $x \in G$ under the relation $\sim$, is called a *double coset* of A, B in G.

If A and B are finite subgroups of G, then we determine the number of elements in the double coset AxB of $x \in G$. We have the following lemma.

Lemma 3.1.11

If A, B are finite subgroups of a group G, then

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

Proof. First we show that $o(AxB) = o(AxBx^{-1})$. For this, we define a map $T : AxB \to AxBx^{-1}$ by $T(axb) = axbx^{-1}$ and show that it is one-one and onto.

Claim 1: T is one-one.

Let $a_1xb_1, a_2xb_2 \in AxB$. Then

$$T(a_1xb_1) = T(a_2xb_2) \Rightarrow a_1xb_1x^{-1} = a_2xb_2x^{-1} \Rightarrow a_1xb_1 = a_2xb_2.$$

Therefore T is one-one

Claim 2: T is onto.

Let $y \in AxBx^{-1}$. Then $y = axbx^{-1}$ for some $a \in A$ and $b \in B$. Then we have $axb \in AxB$ and $T(axb) = axbx^{-1} = y$. Hence, T is onto.

Thus, we have proved that T is bijective. Consequently, we have $o(AxB) = o(AxBx^{-1})$.

Now, clearly xBx^{-1} is a subgroup of G and $o(xBx^{-1}) = o(B)$. Therefore by Lemma 1.3.3, we have

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

□

Now, we come to the first step, i.e. we prove that if a larger group M has a p-Sylow subgroup, then its subgroup G also has a p-Sylow subgroup. More precisely, we have the following lemma:

Lemma 3.1.12

Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose that M has a p-Sylow subgroup Q, then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.

Proof. Let $p^m \mid o(M)$ but $p^{m+1} \nmid o(M)$ and Q be the p-Sylow subgroup of M, i.e. Q is the subgroup of M of order p^m. Let $o(G) = p^n t$ such that $p \nmid t$. Then we have to show that G has a p-Sylow subgroup, i.e. G has a subgroup of order p^n.

Now, consider the decomposition of the group M into double cosets given by G and Q, i.e.

$$M = \bigcup GxQ.$$

Then by previous lemma, we have

$$o(GxQ) = \frac{o(G)o(Q)}{o(G \cap xQx^{-1})} = \frac{p^n t p^m}{o(G \cap xQx^{-1})}.$$

Since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, its order is p^{m_x} for some positive integer $m_x \leq n$.

Claim: $m_x = n$ for some $x \in M$.
Suppose if possible, $m_x < n$ for all $x \in M$, then $n - m_x \geq 1$ for all $x \in M$ and hence

$$o(GxQ) = \frac{p^n t p^m}{p^{m_x}} = t p^{m+n-m_x}.$$

Thus, $p^{m+1}|o(GxQ)$. Now, since M is disjoint union of (distinct) double cosets, i.e. $M = \bigcup GxQ$, we have

$$o(M) = \sum o(GxQ),$$

where the sum is runs over one element from each double coset. Also,

$$p^{m+1}|o(GxQ) \Rightarrow p^{m+1}\Big|\sum o(GxQ) \Rightarrow p^{m+1}|o(M)$$

which is a contradiction to our assumption that $p^{m+1} \nmid o(M)$. Thus, $m_x = n$ for some $x \in M$. Hence

$$o(G \cap xQx^{-1}) = p^n.$$

Thus, $P = G \cap xQx^{-1}$ is the subgroup of G of order p^n, i.e. P is the p-Sylow subgroup of G. □

Now, we investigate how large a p-Sylow subgroup of S_{p^r} should be. For this, it is necessary to determine what power of p divides $(p^r)!$. In this regard, we introduce the following notation.

Notation:
For a fixed prime p, let $n(k)$ denote the highest power of a prime p which divides $(p^k)!$, i.e.

$$p^{n(k)}|(p^k)! \text{ but } p^{n(k)+1} \nmid (p^k)!.$$

The following lemma determines $n(k)$.

Lemma 3.1.13

$n(k) = 1 + p + \cdots + p^{k-1}$.

Proof. Omitted □

We shall need the following lemma.

Lemma 3.1.14

Let $n, m \in \mathbb{N}$ and $m < n$. Define

$$A = \{\tau \in S_n : i\tau = i \text{ for all } i > m\}. \tag{3.5}$$

Then $A \approx S_m$.

Proof. Define $\psi : S_m \to A$ by

$$\psi(\theta) = \begin{pmatrix} 1 & 2 & \dots & m & m+1 & \dots & n \\ 1\theta & 2\theta & \dots & m\theta & m+1 & \dots & n \end{pmatrix} \tag{3.6}$$

Then it is easy to verify that ψ is an onto isomorphism. Thus $A \approx S_m$. □

The final preparation to give the third proof of Sylow's theorem is the following particular case of Sylow's theorem.

Lemma 3.1.15

Let $p \in \mathbb{N}$ be prime and $k \in \mathbb{N}$. Then S_{p^k} has a p-Sylow subgroup.

Proof. Omitted. □

Finally, we combine all these results to give the third proof of the Sylow's theorem below:

Third proof of Sylow's Theorem. Let G be a finite group and $p^m | o(G)$ but $p^{m+1} \nmid p(G)$. By Cayley's theorem, G can be isomorphically embedded in the symmetric group S_n for some n. Choose k large such that $n < p^k$. Then S_n can be isomorphically embedded into S_{p^k}. Hence, G can be isomorphically embedded in S_{p^k}.

By Lemma 3.1.15, S_{p^k} has a p-Sylow subgroup. Hence, by Lemma 3.1.12, G must have a p-Sylow subgroup. This completes the third proof of the Sylow's theorem. □

The third proof yields more than what we intended to prove. The tools developed during the course of the third proof, enables us to prove the other two parts of the Sylow's theorem which we present in the next section.

3.2 Other Parts of Sylow's Theorem

In this section, we determine the number of p-Sylow subgroups for a finite group G. Precisely, we prove the second and the third part of Sylow's theorem also known as Second Sylow theorem and Third Sylow theorem.

We begin by proving the second part of Sylow's theorem which states that any two p-Sylow subgroups are conjugate of each other.

Theorem 3.2.1: Second Sylow theorem

If G is a finite group, p a prime such that $p^n | o(G)$ but $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.

Proof. Let A, B be two p-Sylow subgroups of G, i.e. $o(A) = p^n = o(B)$. We want to show that A and B are conjugate, i.e. $A = gBg^{-1}$ for some $g \in G$.

Now, decompose G into double cosets of A and B, i.e. write G as a disjoint union of double cosets as follows:

$$G = \bigcup AxB.$$

Then

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

If $A \neq xBx^{-1}$ for every $x \in G$, then since $(A \cap xBx^{-1})$ is a proper subgroup of A, we have $o(A \cap xBx^{-1}) = p^m$, where $m < n$. Thus,

$$o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{n+(n-m)}.$$

Thus, $p^{n+1}|o(AxB)$ for every $x \in G$ and since $o(G) = \sum o(AxB)$, we get $p^{n+1}|o(G)$ which is a contradiction as $p^{n+1} \nmid o(G)$. Hence, $A = xBx^{-1}$ for some $x \in G$. Thus, any two p-Sylow subgroups are conjugate. □

As a consequence of the second Sylow theorem, we can say that for any prime p a unique p-Sylow subgroup is normal.

Corollary 3.2.2

A unique p-Sylow subgroup is normal.

Proof. Let G be a finite group and P be a p-Sylow subgroup of G. Then for every $x \in G$, xPx^{-1} is also a subgroup of G and $o(xPx^{-1}) = o(P)$. Thus, xPx^{-1} is also a p-Sylow subgroup of G, for all $x \in G$. Since G has unique p-Sylow subgroup P, we must have

$$P = xPx^{-1}, \forall\, x \in G.$$

Hence, P is normal. □

Since p-Sylow subgroups are conjugate, we can now determine the number of p-Sylow subgroups of a finite group G. This number is given by the following lemma, the proof of which is similar to the proof of Theorem 2.4.5.

Lemma 3.2.3

The number of p-Sylow subgroups in G is equal to $\dfrac{o(G)}{o(N(P))}$, where P is any p-Sylow subgroup of G. In particular, this number is a divisor of $o(G)$.

Proof. Let $\mathscr{P}$ be the collection of all p-Sylow subgroups of G and $P \in \mathscr{P}$ be any p-Sylow subgroup of G. Since any two p-Sylow subgroups are conjugate to each other, every element of $\mathscr{P}$ can be written of the form xPx^{-1} for some $x \in G$.

Let $N(P)$ denote the normalizer of P. Define $\phi : \mathscr{P} \to G/N(P)$ by

$$\phi(xPx^{-1}) = N(P)x.$$

To prove this result, we show that ϕ is well-defined, one-one and onto.

For any two p-Sylow subgroups $xPx^{-1}, yPy^{-1} \in \mathscr{P}$, for some x and y in G, we have

$$\begin{aligned} xPx^{-1} = yPy^{-1} &\Leftrightarrow Px^{-1}y = x^{-1}yP \\ &\Leftrightarrow x^{-1}y \in N(P) \\ &\Leftrightarrow N(P)x = N(P)y \end{aligned}$$

$xPx^{-1} = yPy^{-1} \Rightarrow N(P)x = N(P)y$ shows that ϕ is well-defined and $N(P)x = N(P)y \Rightarrow xPx^{-1} = yPy^{-1}$ shows that ϕ is one-one.

To show that ϕ is onto, let $N(P)x \in G/N(P)$. Then since $o(xPx^{-1}) = o(P)$, xPx^{-1} is a p-Sylow subgroup, i.e. $xPx^{-1} \in \mathscr{P}$ and $\phi(xPx^{-1}) = N(P)x$. Thus, ϕ is onto. □

Theorem 3.2.4: Third Sylow theorem

Let p be a prime. The number of p-Sylow subgroups of G is of the form $1+kp$.

Proof. Let P be a p-Sylow subgroup of G with $o(P) = p^n$. So, we have $p^{n+1} \nmid o(G)$.

Decompose G into double cosets of P and P, i.e. $G = \bigcup PxP$. Also,

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}.$$

If $P \cap xPx^{-1} \neq P$, then $P \cap xPx^{-1}$ is a proper subgroup of P and hence $o(P \cap xPx^{-1}) \leq p^{n-1}$. Therefore, $p^{n+1} | o(PxP)$.

Now, $P \cap xPx^{-1} \neq P \Rightarrow xP \neq Px \Rightarrow x \notin N(P)$. Then the above statement can be rewritten as, if $x \notin N(P)$ then $p^{n+1} | o(PxP)$. However, if $x \in N(P)$, i.e. $Px = xP$, then $PxP = P^2x = Px$ and so $o(PxP) = o(Px) = o(P) = p^n$. Therefore,

$$o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP),$$

where each sum runs over one element from each double coset.

Observe that if $x \in N(P)$ then $PxP = Px$ and so the first sum in the above expression is $\sum_{x \in N(P)} o(Px)$ over distinct cosets of P in $N(P)$. Thus, the first sum is $o(Px) \cdot \frac{o(N(P))}{o(P)} = o(N(P))$.

Now, the second sum is over $x \notin N(P)$ and so as remarked earlier $p^{n+1} | o(PxP)$ for each term in the second sum. Therefore

$$p^{n+1} \Big| \sum_{x \notin N(P)} o(PxP).$$

Then we can write the second sum as

$$\sum_{x \notin N(P)} o(PxP) = p^{n+1}u \qquad \text{(for some } u\text{)}.$$

Therefore, $o(G) = o(N(P)) + p^{n+1}u$ and so

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}. \tag{3.7}$$

Now, $N(P)$ being a subgroup of G, $o(N(P)) | o(G)$. But $p^{n+1} \nmid o(G)$ and so $p^{n+1} \nmid o(N(P))$. Hence, $p \Big| \frac{p^{n+1}u}{o(N(P))}$. Then, the above equation can be written as

$$\frac{o(G)}{o(N(P))} = 1 + kp.$$

By above lemma, we know that the number of p-Sylow subgroups of G is $\frac{o(G)}{o(N(P))}$. Thus, the number of p-Sylow subgroups of G is for the form $1+kp$ for some non-negative integer k. □

Sylow's theorem, particularly second and third part, has many applications to finite groups. For instance, in certain cases we can determine, just from the order of the group, whether the given group is abelian or not, whether it is simple or not. So before we begin with the concluding section of this chapter on the applications of the Sylow theorem, we define *simple group* and *solvable group* in the following section.

3.3 Applications of Sylow's theorem

Definition 3.3.1

A group G is said to be *simple* if it does not have any proper normal subgroup.

To demonstrate application of second and third Sylow theorems, we present two examples below. In the first example we show that the group of given order is abelian and in the second example we show that the group of given order cannot be simple.

Example 3.3.2. Show that the group of order $20499 = 11^2 \times 13^2$ is abelian.

Solution. Let G be a group of order $11^2 \times 13^2$. We determine the number of 11-Sylow subgroups and 13-Sylow subgroups in G. By Theorem 3.2.4, we know that, the number of 11-Sylow subgroups in G is of the form $1+11k$. Also by Lemma 3.2.3, this number divides $o(G)$. Thus,

$$1+11k \mid 11^2 \cdot 13^2.$$

Note that $(1+11k, 11^2) = 1$ and therefore $1+11k \mid 13^3$. Thus, k must be 0. Hence, the number of 11-Sylow subgroup in G is $1+11k = 1$ $(\because k = 0)$. Thus G has unique 11-Sylow subgroup, say A, i.e. $o(A) = 11^2$. Then by Corollary 3.2.2, A is normal.

Similarly, the number of 13-Sylow subgroup $1+13k \mid 11^2 \cdot 13^2$. But $(1+13k, 13^2) = 1$ and hence $1+13k \mid 11^2$. Thus, k must be 0. Hence G has a unique 13-Sylow subgroup, say B. Then $o(B) = 13^2$ and again by Corollary 3.2.2, B is normal.

We know that any group of order p^2, where p is prime, is abelian. Hence, A and B are abelian. Now, we determine the $o(AB)$. For this, first we show that $A \cap B = \{e\}$. Let $x \in A \cap B$, then $o(x) \mid o(A)$ and $o(x) \mid o(B)$. Hence, $o(x) \mid (o(A), o(B)) = (11^2, 13^2) = 1$ and so $x = e$. Therefore,

$$o(AB) = \frac{o(A)o(B)}{o(A \cap B)} = 11^2 \times 13^2 = o(G).$$

Thus $G = AB$, where A and B are abelian. Finally, to show that G is abelian, it suffices to show that elements of A and B commute.

Let $a \in A$ and $b \in B$. Since A is normal, $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A$. Similarly, since B is normal, $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B$. Thus,

$$ba^{-1}b^{-1} \in A \cap B = \{e\}.$$

Thus, $ba^{-1}b^{-1} = e \Rightarrow ab = ba$ and hence A and B commutes. Thus, any group of order $11^2 \cdot 13^2$ is abelian. □

Example 3.3.3. Show that a group of order 72 cannot be simple.

Solution. Let G be a group with $o(G) = 72 = 2^3 3^2$. We determine the number of 3-Sylow subgroups of G. Let this number be $n_3 = 1 + 3k$. We know that $n_3 \mid o(G) = 72$. But $(1 + 3k, 3^2) = 1$ and therefore, $1 + 3k \mid 2^3$. Then either $k = 0$ or $k = 1$. If $k = 0$, then $n_3 = 1$, i.e. G has a unique 3-Sylow subgroup and hence it is normal. Then G cannot be simple.

However, if $k = 1$ then $n_3 = 4$, i.e. the number 3-Sylow subgroups in G is 4. Let N be the normalizer of the 3-Sylow subgroup. Then by Lemma 3.2.3, the number of 3-Sylow subgroups in G is equal to index of the normalizer of a 3-Sylow subgroup. Thus, $i_G(N) = 4$.

Now, $72 \nmid 4!$, i.e. $o(G) \nmid i_G(N)!$. Hence by Corollary 2.2.4, N must contain a non-trivial normal subgroup of G. Thus, G cannot be simple. □

Exercises

Exercise 3.1

Show that the converse of Lagrange's theorem does not hold.

Exercise 3.2

Let G be a group and H be a normal subgroup of G. Let $G' = G/H$ and K' be a subgroup of G'. Let $K = \{x \in G \mid xH \in K'\}$. Then prove the following:

1. K is a subgroup of G.
2. $K' \approx K/H$.
3. $K = \bigcup_{xH \in K'} xH$.

Exercise 3.3

In Lemma 3.1.15, verify the following:

1. Property (2) of σ defined in the lemma.
2. $\sigma T \sigma^{-1} = T$.
3. P (defined in lemma) is a subgroup of S_{p^k}.

Exercise 3.4

If $o(G) = pq$ for distinct primes p and q, $p < q$ such that $p \nmid (q-1)$ then G is cyclic.

Exercise 3.5

Find the number and discuss the nature of all possible p-Sylow subgroups in a group of order 225.

Exercise 3.6

Find the possible number of 11-Sylow subgroups, 7-Sylow subgroups and 5-Sylow subgroups in a group of ofer $5^2 \cdot 7 \cdot 11$.

Exercise 3.7

Show that in a group G of order 30, a 3-Sylow subgroup or a 5-Sylow subgroup of G must be normal.

Exercise 3.8

Show that a group of order 108 cannot be simple.

Exercise 3.9

Show that any group of order 1986, 42 or 200 cannot be simple.

Exercise 3.10

If G is S_3 and $A = ((1,2))$ in G, find all the double cosets AxA of A in G.

Exercise 3.11

Discuss the number and nature of the 3-Sylow subgroups and 5-Sylow subgroups of a group of order $3^2 \cdot 5^2$.

Exercise 3.12

If G is a group of order 231, prove that the 11-Sylow subgroup is in the center of G.

Exercise 3.13

If G is of order p^2q, p,q primes, prove that G has a non-trivial normal subgroup, i.e., G cannot be simple.

CHAPTER 4

Fundamental Theorem of Finite Abelian Groups

In this unit, we shall study the following.

Direct products and Fundamental theorem of finite abelian groups.

4.1 Direct Products

In this section we shall define the notions of *external direct product* and *internal direct product* of groups. Eventually we will show that both of them are isomorphic and henceforth we shall address it only as *direct product* of groups without using the word internal or external.

Before we can give the formal definitions of direct products, we state the following exercises solving which will bring us in the position to state these definitions.

Exercises 4.1.1. 1. Let A and B be any two groups. Show that their Cartesian product

$$G = A \times B = \{(a,b) \mid a \in A, b \in B\}$$

is a group under the operation (componentwise multiplication) given by

$$(a_1,b_1)(a_2,b_2) := (a_1a_2, b_1b_2), \qquad \forall\ (a_1,b_1),(a_2,b_2) \in G.$$

We call the group $G = A \times B$ as the *external direct product* of groups A and B.

2. Let $\bar{A} = \{(a,f) \in G \mid a \in A\} \subset G = A \times B$, where f is the unit element of B. Show that $\bar{A}$ is a subgroup of G. Similarly, $\bar{B} = \{(e,b) \in G \mid b \in B\}$, where e is the unit element of A is a subgroup of G.

3. Show that $\bar{A}$ is isomorphic to A.
Hint: Show that $\phi : A \to \bar{A}$ defined by $\phi(a) = (a,f)$ is an isomorphism of A onto $\bar{A}$. Similarly, $\bar{B}$ is isomorphic to B.

4. Show that $\bar{A}$ is normal in G. Similarly, $\bar{B}$ is normal in G.

5. Show that $G = \bar{A}\bar{B}$, i.e. every $g \in G$ can be written as $g = \bar{a}\bar{b}$ with $\bar{a} \in \bar{A}$ and $\bar{b} \in \bar{B}$. Also show that such expression of $g = \bar{a}\bar{b}$ is unique.

   In this case, we call the group $G = \bar{A}\bar{B}$ the *internal direct product* of normal subgroups $\bar{A}$ and $\bar{B}$.

Now we are in a position to define *external direct product* and *internal direct product* of groups. The definitions are same as in the above exercises but instead of two groups, we define for n groups where $n > 1$.

Definition 4.1.2: External Direct Product

Let $G_1, G_2, \ldots, G_n$ be any n groups. Let

$$G = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$$

be the Cartesian product of $G_1, G_2, \ldots, G_n$, i.e. set of all ordered n-tuples. Then G is a group with componentwise multiplication defined by

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

We call this group G the *external direct product* of groups $G_1, G_2, \ldots, G_n$.

Remark 4.1.3.

1. The product in the ith component in the above product is carried out in the group G_i.

2. The unit element in the group G defined above as the external direct product is given by $(e_1, e_2, \ldots, e_n)$, where e_i is the unit element in the group G_i. The inverse of the element $(g_1, g_2, \ldots, g_n)$ in G is given by $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$, i.e.

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}).$$

3. In $G = G_1 \times G_2 \times \cdots \times G_n$ let $\bar{G}_i = \{(e_1, e_2, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n) \mid g_i \in G_i\}$. Then $\bar{G}_i$ is a normal subgroup of G. Then $\bar{G}_i$ is a normal subgroup of G and is isomorphic to G_i. Also $G = \bar{G}_1 \bar{G}_2 \cdots \bar{G}_n$ and every $g \in G$ can be uniquely written as $g = \bar{g}_1 \bar{g}_2 \cdots \bar{g}_n$, where $\bar{g}_i \in \bar{G}_i$, $i = 1, 2, \ldots, n$. (Verify!)

   Here, we have realized G as an internal direct product of normal subgroups $\bar{G}_1, \bar{G}_2, \ldots, \bar{G}_n$. More precisely, we have the following definition.

Definition 4.1.4: Internal Direct Product

Let G be a group and $N_1, N_2, \ldots, N_n$ be normal subgroups of G such that

1. $G = N_1 N_2 \cdots N_n$.
2. Every $g \in G$ can be uniquely written as $g = m_1 m_2 \cdots m_n$, $m_i \in N_i$.

Then we say that G is the *internal direct product* of $N_1, N_2, \ldots, N_n$.

Example 4.1.5. Let $G = K_4 = \{e,a,b,c\}$ be the Klein-4 group, i.e. $a^2 = b^2 = c^2 = e$ and $ab = c = ba$, $ac = b = ca$, $bc = a = cb$. Let $H_1 = \{e,a\}$ and $H_2 = \{e,b\}$ be two subgroups of G of order 2. We show that $G = K_4$ is the internal direct product of H_1 and H_2

Since G is abelian, $H_1H_2 = H_2H_1$ and hence H_1H_2 is a subgroup of G. Also G being abelian implies that H_1 and H_2 are normal in G. Note that $H_1 \cap H_2 = \{e\}$. Therefore

$$o(H_1H_2) = \frac{o(H_1)o(H_2)}{o(H_1 \cap H_2)} = \frac{2 \cdot 2}{1} = 4 = o(G).$$

Thus, $G = H_1H_2$. Observe that every element $g \in G$ can be uniquely written as $g = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$ as follows:

$$e = e \cdot e, \qquad a = a \cdot e, \qquad b = e \cdot b, \qquad c = a \cdot b.$$

Hence $G = K_4$ is internal direct product of its normal subgroups H_1 and H_2 defined above.

Example 4.1.6. Let G be a finite abelian group of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_i > 0$. Then by Sylow's theorem G has p_1-Sylow subgroup P_1, p_2-Sylow subgroup P_2, ..., p_k-Sylow subgroup P_k. Since G is abelian, each of these Sylow subgroups are normal. Then show that G is the internal direct product of $P_1, P_2, \ldots, P_k$ (see Exercise 4.1).

Before we prove that external direct product and internal direct product are isomorphic, we have the following lemma.

Lemma 4.1.7

Suppose G is the internal direct product of $N_1, N_2, \ldots, N_n$. Then $N_i \cap N_j = \{e\}$ for $i \neq j$. Also if $a \in N_i$, $b \in N_j$ then $ab = ba$.

Proof. Let $x \in N_i \cap N_j$. Then $x \in N_i$ and so x can be written as

$$x = e_1 \cdots e_{i-1} x e_{i+1} \cdots e_j \cdots e_n,$$

where $e_t = e$. Also $x \in N_j$. Thus, viewing x as an element of N_j, we can write

$$x = e_1 \cdots e_i \cdots e_{j-1} x e_{j+1} \cdots e_n,$$

where $e_t = e$. Since G is internal direct product of $N_1, N_2, \ldots, N_n$, every element $x \in G$ has a unique representation of the form $m_1m_2 \cdots m_n$, where $m_i \in N_i$. Since x has above two decompositions they must coincide. So the entry in N_i in each of the above decompositions of x must be equal, for all i. Comparing the ith or the jth entry in the above two decompositions of x, we get $x = e_i = e_j = e$. Thus, $N_i \cap N_j = \{e\}$ for $i \neq j$.

Now, suppose that $a \in N_i$ and $b \in N_j$ for $i \neq j$. Then $aba^{-1} \in N_j$ since N_j is normal ad so $aba^{-1}b^{-1} \in N_j$. Also, $a^{-1} \in N_i$ and since N_i is normal, $ba^{-1}b^{-1} \in N_i$. Thus, $aba^{-1}b^{-1} \in N_i$. Therefore $aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$. Thus, $aba^{-1}b^{-1} = e$ which implies that $ab = ba$. □

Remark 4.1.8. The converse of the above lemma is not true. That is if $K_1, K_2, \ldots, K_n$ are normal subgroups of G such that $G = K_1K_2 \cdots K_n$ and $K_i \cap K_j = \{e\}$ for $i \neq j$ then it *need not be true* that G is the internal direct product of $K_1, K_2, \ldots, K_n$ (see Exercise 4.2). An example is already provided. Find another example yourself.

A more stronger condition is needed for it to be true (see Exercise 4.3). Prove this equivalent condition for internal direct product.

Next, we prove that external direct product is isomorphic to internal direct product. Henceforth, we shall use the phrase only direct product of groups and avoid the prefix external or internal. We have the following theorem.

Theorem 4.1.9

Let G be a group and suppose that G is the internal direct product of $N_1, N_2 \ldots, N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G is isomorphic to T.

Proof. Define the map $\psi : T \to G$ by

$$\psi((b_1, b_2, \ldots, b_n)) = b_1 b_2 \cdots b_n,$$

where $b_i \in N_i$ for $i = 1, 2, \ldots, n$. We show that ψ is an isomorphism of T onto G.

First we show that ψ is a homomorphism. Let $X = (a_1, a_2, \ldots, a_n), Y = (b_1, b_2, \ldots, b_n) \in T$. Then

$$\begin{aligned} \psi(XY) &= \psi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) \\ &= \psi((a_1 b_1, a_2 b_2, \ldots, a_n b_n)) \\ &= a_1 b_1 a_2 b_2 \cdots a_n b_n. \end{aligned}$$

Since G is the internal direct product of $N_1, \ldots, N_n$, by above lemma, $a_i b_j = b_j a_i$ for $i \neq j$. Thus,

$$\begin{aligned} a_1 b_1 a_2 b_2 \cdots a_n b_n &= a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n \\ &= \psi((a_1, a_2, \ldots, a_n))\psi((b_1, b_2, \ldots, b_n)) \\ &= \psi(X)\psi(Y). \end{aligned}$$

Therefore $\psi(XY) = \psi(X)\psi(Y)$ and hence ψ is a homomorphism.

Now, we show that ψ is one-one. Let $X, Y \in T$ such that

$$\begin{aligned} &\psi(X) = \psi(Y) \\ \Rightarrow\ &\psi((a_1, a_2, \ldots, a_n)) = \psi((b_1, b_2, \ldots, b_n)) \\ \Rightarrow\ &a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n, \end{aligned}$$

where $a_i, b_i \in N_i$ for $i = 1, 2, \ldots, n$. Since G is the internal direct product of $N_1, \ldots, N_n$ every element in G has a unique representation as product of elements from $N_1, N_2, \ldots, N_n$. Therefore, $a_i = b_i$ for all $i = 1, 2, \ldots, n$ and hence $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$, i.e. $X = Y$ which proves that ψ is one-one.

Finally, we show that ψ is onto. Let $x \in G$. Since G is the internal direct product of $N_1, N_2, \ldots, N_n$, $x = a_1 a_2 \cdots a_n$, where $a_i \in N_i$ for $1 \leq i \leq n$. But then $(a_1, a_2, \ldots, a_n) \in T$ and $\psi((a_1, a_2, \ldots, a_n)) = a_1 a_2 \cdots a_n = x$. Thus, ψ is onto.
Hence ψ is isomorphism of T onto G, i.e. $T \approx G$. □

4.2 Finite Abelian Groups

In this section we prove one of the main result of this chapter and in the theory of finite abelian groups. The result states that every finite abelian group is the direct product of cyclic groups. Before we prove this result, we see the couple of exercises given below, which will be used in the proof of the theorem.

Example 4.2.1. Let G and G' be two groups and $\phi : G \to G'$ be a homomorphism. Then for all $g \in G$, $o(\phi(g)) \mid o(g)$.

Solution. For $g \in G$, let $o(g) = m$ and $o(\phi(g)) = n$. Then we have to show that $n \mid m$. Now,

$$\begin{aligned}(\phi(g))^m &= \underbrace{\phi(g)\phi(g)\cdots\phi(g)}_{m \text{ times}} \\ &= \phi(g^m) && (\because \phi \text{ is a homomorphism}) \\ &= \phi(e) = e' && (\because o(g) = m).\end{aligned}$$

Thus, $(\phi(g))^m = e'$, where e' is identity of group G'. But $o(\phi(g)) = n$. Therefore $n \mid m$. □

Example 4.2.2. Let G be a group and A_1 be a subgroup of G. Then the map $\pi : G \to G/A_1$ defined by $\pi(b) = \bar{b} = bA_1$, $b \in G$, is a homomorphism.

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

$$\pi(a)\pi(b) = \bar{a}\bar{b} = (aA_1)(bA_1) = abA_1 = \overline{ab} = \pi(ab).$$

Thus π is a homomorphism. □

Theorem 4.2.3

Every finite abelian group is the direct product of cyclic groups.

Proof. We know, by Exercise (4.1), that every finite abelian group is the direct product of its Sylow subgroups. If we show that every Sylow subgroup is the direct product of cyclic subgroups then get the desired result by combining two results. Since every Sylow subgroup has order which is a prime power, it suffices to show that every abelian group G with $o(G) = p^n$, for prime p and for some $n \in \mathbb{N}$, can written as the direct product of cyclic subgroups.

Let $a_1 \in G$ be an element of maximal (highest possible) order, say p^{n_1}. Let $A_1 = (a_1)$. Then $o(A_1) = o(a_1) = p^{n_1}$. Let $b_2 \in G$ be such that its image (under the map $\pi : G \to G/A_1$), $\bar{b}_2 = b_2A_1$ in G/A_1 has maximal order p^{n_2}, i.e. $o(\bar{b}_2) = p^{n_2}$. Then (by above two exercises) we have $o(\bar{b}_2) \mid o(b_2)$ and since a_1 has maximal order in G,

$$p^{n_2} = o(\bar{b}_2) \leq o(b_2) \leq o(a_1) = p^{n_1}.$$

This gives $\boxed{n_1 \geq n_2}$. In order to write G has direct product of cyclic groups, we need $A_1 \cap (b_2) = \{e\}$. If this is true then we proceed further. However, this may not be the case, i.e.

$A_1 \cap (b_2) \neq \{e\}$. By our choice of b_2, it is clear that (Verify!) ${b_2}^{p^{n_2}}$ is the first power of b_2 to belong to A_1, i.e. ${b_2}^{p^{n_2}} \in A_1 \cap (b_2)$. Then we have $\boxed{{b_2}^{p^{n_2}} = {a_1}^i}$ for some i. Therefore

$$ {a_1}^{ip^{n_1-n_2}} = \left({a_1}^i\right)^{p^{n_1-n_2}} = \left({b_2}^{p^{n_2}}\right)^{p^{n_1-n_2}} = {b_2}^{p^{n_1}} = e. $$

Since $o(a_1) = p^{n_1}$, we have $p^{n_1} \mid ip^{n_1-n_2}$. Now,

$$ \begin{aligned} p^{n_1} \mid ip^{n_1-n_2} &\Rightarrow p^{n_2}p^{n_1} \mid ip^{n_1} && (\because a \mid b \Rightarrow ac \mid bc) \\ &\Rightarrow p^{n_2} \mid i && (\because ac \mid bc \Rightarrow a \mid b) \\ &\Rightarrow i = jp^{n_2} \text{ for some } j. \end{aligned} $$

Substituting this value of i above, we get

$$ {b_2}^{p^{n_2}} = {a_1}^i = {a_1}^{jp^{n_2}} \tag{4.1} $$

Take $\boxed{a_2 = {a_1}^{-j}b_2}$. Then a_2 is an required element such that $A_1 \cap (a_2) = \{e\}$. First observe that, by equation (4.1)

$$ {a_2}^{p^{n_2}} = {a_1}^{-j}{b_2}^{p^{n_2}} = {a_1}^{-jp^{n_2}}{b_2}^{p^{n_2}} = e. \tag{4.2} $$

Claim 1: Let $A_2 = (a_2)$. Then $A_1 \cap A_2 = \{e\}$.

Suppose ${a_2}^t \in A_1$ for some t. Then

$$ \begin{aligned} {a_2}^t \in A_1 &\Rightarrow \left({a_1}^{-j}b_2\right)^t \in A_1 \\ &\Rightarrow {a_1}^{-jt}{b_2}^t \in A_1 \\ &\Rightarrow {b_2}^t \in A_1 && (\because {a_1}^{-jt} \in A_1) \\ &\Rightarrow (b_2A_1)^t = {b_2}^tA_1 = A_1 && (\text{where } A_1 \text{ is the identity in } G/A_1) \\ &\Rightarrow (\bar{b}_2)^t = A_1 && (\because \bar{b}_2 = b_2A_1) \\ &\Rightarrow p^{n_2} \mid t && (\because o(\bar{b}_2) = p^{n_2}) \\ &\Rightarrow t = sp^{n_2} \text{ for some } s. \end{aligned} $$

Therefore by equation (4.2), we have

$$ {a_2}^t = {a_2}^{sp^{n_2}} = \left({a_2}^{p^{n_2}}\right)^s = e^s = e. $$

This proves that $A_1 \cap A_2 = \{e\}$.

Similarly, let $b_3 \in G$ be such that its image $\bar{b}_3 \in G/(A_1A_2)$ has maximal order, say $o(\bar{b}_3) = p^{n_3}$. Then as before, we have $n_1 \geq n_2 \geq n_3$. Now, $(A_1A_2) \cap (b_3) = \{e\}$ may not be the case. Then carrying out the same procedure as above, we obtain $a_3 \in G$ such that $o(a_3) = p^{n_3}$ and $A_3 \cap (A_1A_2) = \{e\}$, where $A_3 = (a_3)$.

Continuing this way, we obtain cyclic subgroups $A_1 = (a_1)$, $A_2 = (a_2), \ldots, A_k = (a_k)$ of order $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$ respectively with $n_1 \geq n_2 \geq \cdots \geq n_k$ such that $G = A_1A_2\cdots A_k$ and $A_i \cap (A_1A_2\cdots A_{i-1}) = \{e\}$ for each i. Hence, (by Exercise 4.3) G is the direct product of cyclic subgroups $A_1, A_2, \ldots, A_k$. □

Definition 4.2.4: Invariants

Let G is an abelian group of order p^n, where p is a prime. Suppose $G = A_1 \times A_2 \times \cdots \times A_k$, where each $A_i = (a_i)$ is a cyclic group of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k$. Then the integers $n_1, n_2, \ldots, n_k$ are called the *invariants* of the group G.

Remarks 4.2.5.

1. If $G = A_1 \times A_2 \times \cdots \times A_k$, where A_i are cyclic subgroups of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Then

$$\begin{aligned} & o(G) = o(A_1)o(A_2)\cdots o(A_k) \\ \Rightarrow \quad & p^n = p^{n_1}p^{n_2}\cdots p^{n_k} = p^{n_1+n_2+\cdots+n_k} \\ \Rightarrow \quad & n = n_1 + n_2 + \cdots + n_k. \end{aligned}$$

   Thus, $n_1, n_2, \ldots, n_k$ gives a partition of n. We shall conclude this section and the unit showing that the number of non-isomorphic abelian groups of order p^n are equal to the number of partitions of n, i.e. $p(n)$.

2. Next we show that that invariants of a group G are unique. However the choice of the cyclic subgroups $A_1, A_2, \ldots, A_k$ and their generators $a_1, a_2, \ldots, a_k$ respectively, need not be unique. Consider the following example demonstrating this.

Example 4.2.6. Let $G = K_4 = \{e, a, b, c\}$ be the Klein-4 group, i.e. $a^2 = b^2 = c^2 = e$ and $ab = c = ba$, $ac = b = ca$, $bc = a = cb$. Let $H_1 = (a) = \{e, a\}$, $H_2 = (b) = \{e, b\}$ and $H_3 = (c) = \{e, c\}$ be subgroups of G of order 2.

As seen in Example 4.1.5, $G = K_4$ can be written as the direct product of H_1 and H_2. Similarly, G can also be written as the direct product of subgroups H_2 and H_3 or also as the direct product of H_1 and H_3. Thus, decomposition of G into cyclic subgroups need not be unique. However, (we will prove that) their orders (i.e. the invariants of G) are unique.

Definition 4.2.7

Let G be an abelian group and s be an integer. Then $G(s) = \{x \in G \mid x^s = e\}$.

Note that $G(s)$ is the set of all elements of G whose order divide the integer s. Since G is abelian, it is clear that $G(s)$ is a subgroup of G.

Lemma 4.2.8

If G and G' are isomorphic abelian groups, then for every integer s, $G(s)$ and $G'(s)$ are isomorphic.

Proof. Let ϕ be an isomorphism of G onto G'. To show that $G(s)$ and $G'(s)$ are isomorphic, we show that ϕ maps $G(s)$ isomorphically onto $G'(s)$. We first show that $\phi(G(s)) = G'(s)$.

For this we first show that $\phi(G(s)) \subset G'(s)$. Let $y \in \phi(G(s))$. Then

$$\begin{aligned} y \in \phi(G(s)) &\Rightarrow \phi(x) = y && (\text{for some } x \in G(s)) \\ &\Rightarrow x^s = e && (\because x \in G(s)) \\ &\Rightarrow \phi(x^s) = \phi(e) = e' && (\text{where } e' \text{ is identity of } G') \\ &\Rightarrow y^s = (\phi(x))^s = e' && (\because \phi \text{is homomorphism}) \\ &\Rightarrow y \in G'(s). \end{aligned}$$

Next we show that $G'(s) \subset \phi(G(s))$. Let $u' \in G'(s) \subset G$. Then by definition of $G'(s)$, $(u')^s = e'$. Since ϕ is onto, for $u' \in G$ there exists $y \in G$ such that $\phi(y) = u'$. Now,

$$\begin{aligned} (u')^s = e' &\Rightarrow (\phi(y))^s = e' && (\because \phi(y) = u') \\ &\Rightarrow \phi(y^s) = e' = \phi(e) && (\because \phi \text{ is homomorphism}) \\ &\Rightarrow y^s = e && (\because \phi \text{ is one-one}) \\ &\Rightarrow y \in G(s) \\ &\Rightarrow u' = \phi(y) \in \phi(G(s)). \end{aligned}$$

□

Lemma 4.2.9

Let G be an abelian group of order p^n, where p is prime. Suppose that $G = A_1 \times A_2 \times \cdots \times A_k$, where each $A_i = (a_i)$ is cyclic of order p^{n_i}, and $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. If m is an integer such that $n_t > m \geq n_{t+1}$ then

$$G(p^m) = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k,$$

where B_i is cyclic group of order p^m, generated by ${a_i}^{p^{n_i - m}}$, for $i \leq t$. Also, the order of $G(p^m)$ is p^u, where

$$u = mt + \sum_{i=t+1}^{k} n_i.$$

Proof. First we show that the direct product of $B_1, \ldots, B_t, A_{t+1}, \ldots, A_k$ is contained in $G(p^m)$.

For this we begin by showing that $A_{t+1}, \ldots, A_k$ are all in $G(p^m)$. Since $m \geq n_{t+1} \geq \cdots \geq n_k > 0$, if $j \geq t+1$ then

$${a_j}^{p^m} = \left({a_j}^{p^{n_j}}\right)^{p^{m-n_j}} = (e)^{p^{m-n_j}} = e \qquad (\because o(a_j) = p^{n_j}).$$

Thus, $a_j \in G(p^m)$ and hence $A_j \subset G(p^m)$ for all $j \geq t+1$.

Next we show that $B_1, \ldots, B_t$ are all in $G(p^m)$. If $i \leq t$ then $n_i > m$. Therefore

$$\left({a_i}^{p^{n_i - m}}\right)^{p^m} = {a_i}^{p^{n_i}} = e.$$

Thus, for each i, the generator ${a_i}^{p^{n_i-m}}$ of subgroup B_i is in $G(p^m)$ and hence $B_i \subset G(p^m)$.

Since B_i are subgroups of A_i and the product $A_1 \times A_2 \times \cdots \times A_k$ is direct product, the product $B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$ is also direct product. Also since $B_1, \ldots, B_t, A_{t+1}, \ldots, A_k$ are all in $G(p^m)$, their direct product is also in $G(p^m)$, i.e.

$$B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k \subset G(p^m).$$

For the reverse inclusion, let $x \in G(p^m)$. Then $x^{p^m} = e$. Also note that $x \in G(p^m) \subset G = A_1 \times \cdots \times A_k$. Then x can be written in the following form:

$$x = {a_1}^{\lambda_1} {a_2}^{\lambda_2} \cdots {a_k}^{\lambda_k},$$

where $a_i \in A_i$. Since $x^{p^m} = e$, we have $e = x^{p^m} = {a_1}^{\lambda_1 p^m} {a_2}^{\lambda_2 p^m} \cdots {a_k}^{\lambda_k p^m}$. Since the product of subgroups $A_1, \ldots, A_k$ is direct, $e \in G$ can be uniquely written as $e = e_1 e_2 \cdots e_k$, where $e_i = e \in A_i$. Therefore, we must have

$$ {a_1}^{\lambda_1 p^m} = e, \ldots, {a_k}^{\lambda_k p^m} = e.$$

Since $o(a_i) = p^{n_i}$, we have $p^{n_i} \mid p^m$ for all $i = 1, 2, \ldots, k$. Since $m \geq n_{t+1} \geq \cdots \geq n_k$, for $i \geq t+1$, $p^{n_i} \mid p^m$ and hence above is true for any choice of λ_i for $i \geq t+1$. However for $i \leq t$, $n_i > m$ and hence

$$p^{n_i} \mid \lambda_i p^m \Rightarrow p^{n_i - m} \mid \lambda_i \Rightarrow \lambda_i = v_i p^{n_i - m} \qquad \text{for some } v_i.$$

Substituting all these values of λ_i in the above expression of x, we get

$$x = {a_1}^{v_1 p^{n_1 - m}} \cdots {a_t}^{v_t p^{n_t - m}} {a_{t+1}}^{\lambda_{t+1}} \cdots {a_k}^{\lambda_k} \Rightarrow x \in B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k.$$

This implies $G(p^m) \subset B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$ and hence

$$G(p^m) = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k.$$

Since each B_i is of order p^m and $o(A_i) = p^{n_i}$, we have

$$o(G) = o(B_1) \cdots o(B_t) o(A_{t+1}) \cdots o(A_k) = \underbrace{p^m p^m \cdots p^m}_{t \text{ times}} p^{n_{t+1}} \cdots p^{n_k}.$$

Thus, if $o(G(p^m)) = p^u$, then $u = mt + \sum_{i=t+1}^{k} n_i$. □

Corollary 4.2.10

If G is as in Lemma 4.2.9, then $o(G(p)) = p^k$.

Proof. Applying the above lemma to the case $m = 1$, we get $u = k$. Hence, $o(G(p)) = p^k$. □

Now we conclude the section and the chapter by proving couple of results. We begin by showing the uniqueness of invariants of an abelian group of order p^n. The following is the result.

Theorem 4.2.11

Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.

In other words, if G and G' are abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$, where each A_i is a cyclic group of order p^{n_i}, $n_1 \geq \cdots \geq n_k > 0$, and $G' = B'_1 \times \cdots \times B'_s$, where each B'_i is a cyclic group of order p^{h_i}, $h_1 \geq \cdots \geq h_s > 0$, then G and G' are isomorphic if and only if $k = s$ and for each i, $n_i = h_i$.

Proof. First we show that if G and G' have the same invariants then they are isomorphic. If G and G' have the same invariants then we have

$$G = A_1 \times \cdots \times A_k,$$

where each $A_i = (a_i)$ is a cyclic group of order p^{n_i}, and

$$G' = B'_1 \times \cdots \times B'_k,$$

where each $B_i = (b'_i)$ is a cyclic group of order p^{n_i}. Define $\phi : G \to G'$ by

$$\phi({a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k}) = (b'_1)^{\alpha_1} \cdots (b'_k)^{\alpha_k}.$$

Then we show that ϕ is an isomorphism of G onto G'. First we show that ϕ is homomorphism. Let $g = {a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k}$, $h = {a_1}^{\beta_1} \cdots {a_k}^{\beta_k} \in G$. Then

$$\begin{aligned}
\phi(gh) &= \phi\left(({a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k})({a_1}^{\beta_1} \cdots {a_k}^{\beta_k})\right) \\
&= \phi\left({a_1}^{\alpha_1+\beta_1} \cdots {a_k}^{\alpha_k+\beta_k}\right) && (\because G \text{ is direct product, by Lemma 4.1.7}) \\
&= (b'_1)^{\alpha_1+\beta_1} \cdots (b'_k)^{\alpha_k+\beta_k} && (\text{by definition of } \phi) \\
&= \left((b'_1)^{\alpha_1} \cdots (b'_k)^{\alpha_k}\right)\left((b'_1)^{\beta_1} \cdots (b'_k)^{\beta_k}\right) && (\because G' \text{ is direct product, by Lemma 4.1.7}) \\
&= \phi(g)\phi(h).
\end{aligned}$$

To show that ϕ is one-one, let $\phi(g) = \phi(h)$, i.e. $(b'_1)^{\alpha_1} \cdots (b'_k)^{\alpha_k} = (b'_1)^{\beta_1} \cdots (b'_k)^{\beta_1}$. Since G' is direct product of subgroups B'_i, by uniqueness of representation of every element of G', we must have $\alpha_i = \beta_i$ for all $i = 1, 2, \ldots, k$ and hence ${a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k} = {a_1}^{\beta_1} \cdots {a_k}^{\beta_k} \Rightarrow g = h$.

Clearly, ϕ is onto because if $g' = (b'_1)^{\alpha_1} \cdots (b'_k)^{\alpha_k} \in G'$ for some $\alpha_1, \alpha_2, \ldots, \alpha_k$, then $g = {a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k} \in G$ and $\phi(g) = g'$.

Conversely suppose $G = A_1 \times \cdots \times A_k$, $G' = B'_1 \times \cdots \times B'_s$, $A_i = (a_i)$, $B'_i = (b'_i)$ be cyclic groups of orders p^{n_i} and p^{h_i} respectively, where $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. Assume that G and G' are isomorphic, then we have to show that $k = s$ and $n_i = h_i$ for all i.

Since G and G' are isomorphic, $G(p^m)$ and $G'(p^m)$ are isomorphic for any integer $m \geq 0$ and in particular, they have the same order. Considering $m = 1$ by above Corollary, we have

$$o(G(p)) = o(G'(p)) \Rightarrow p^k = p^s \Rightarrow k = s.$$

Hence, we conclude that the number of invariants for G and G' is the same. Finally we show that, in fact, they all coincide.

Let t be the first integer such that $n_t \neq h_t$ .Without loss of generality assume that $n_t > h_t$. Let $m = h_t$, and $H = \{x^{p^m} \mid x \in G\}$ and $H' = \{(x')^{p^m} \mid x' \in G'\}$ be subgroups of G and G' respectively. Since G and G' are isomorphic, H and H' are isomorphic (see Exercise 4.5). Since $n_t > m = h_t$, assume that $n_r > m \geq n_{r+1}$ for some $r \geq t$. Since G is direct product of A_i's, we get

$$H = C_1 \times \cdots \times C_t \times \cdots \times C_r,$$

where $C_r = \left(a_i{}^{p^m}\right)$ is cyclic of order $p^{n_i - m}$. Thus, the invariants of H are $n_1 - m, n_2 - m, \ldots, n_r - m$ and the number of invariants is $r \geq t$. Similarly since $h_{t-1} > m \geq h_t$ and since G' is direct product of B_i''s, we get

$$H' = D_1' \times \cdots \times D_{t-1}',$$

where $D_i' = \left((b_i')^{p^m}\right)$ is cyclic of order $p^{h_i - m}$. Thus, the invariants of H' are $h_1 - m$, $h_2 - m, \ldots, h_{t-1} - m$ and the number of invariants is $t - 1$.

But as H and H' are isomorphic, they must have the same number of invariants. Thus $r \geq t$ is not possible and hence $n_t \neq h_t$ is not possible. This implies there does not exists i such that $n_i \neq h_i$, i.e. $n_i = h_i$ for all i. □

As an immediate consequence of the above theorem, we have

Theorem 4.2.12

The number of non-isomorphic abelian groups of order p^n, where p is prime, equals $p(n)$, i.e. the number of partitions of n.

Proof. From the definition of invariants, it is clear (as remarked earlier) that a given set of invariants gives a partition of n.

On the other hand, let $n_1 \geq \cdots \geq n_k > 0$, $n = n_1 + \cdots + n_k$ be a partition of n. Then let A_i be the cyclic group of order p^{n_i} and $G = A_1 \times \cdots \times A_k$. Then G is an abelian group of order p^n with invariants $n_1, \ldots, n_k$. Thus, a partition of n gives a group G of order p^n having the same invariants as in the partition.

Finally by above theorem we know that two different partitions of n (i.e. two different set of invariants) give rise to non-isomorphic groups of order p^n. Hence, the number of non-isomorphic abelian groups of order p^n is equal to the number of partitions of n. □

Remarks 4.2.13.

1. Notice that the number of non-isomorphic abelian groups of order p^n depends only on the exponent n and **not** the prime p. For instance, the number of non-isomorphic abelian groups of order 2^4, 3^4 or 5^4 is same, i.e. $p(4) = 5$ (as $4 = 4, 3+1, 2+2, 2+1+1, 1+1+1+1$).

   However, this is not the case with 4^4 as 4 is not a prime. But $4^4 = (2^2)^4 = 2^8$. Thus, the number of non-isomorphic abelian groups of order 4^4 is $p(8) = 22$.

2. Since every finite abelian group is a direct product of its Sylow subgroups, we can say that two finite abelian groups are isomorphic if and only if their corresponding Sylow subgroups are isomorphic. Finally, we have the following Corollary.

Corollary 4.2.14

The number of non-isomorphic abelian groups of order $n = {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$, where p_i are distinct primes and each $\alpha_i > 0$, is $p(n) = p(\alpha_1)p(\alpha_2)\cdots p(\alpha_r)$.

Exercises

Exercise 4.1

Show that G is isomorphic to the direct product of its Sylow subgroups.

Exercise 4.2

Give an example of a group G and normal subgroups $N_1, \ldots, N_n$ such that $G = N_1 \cdots N_n$ and $N_i \cap N_j = \{e\}$ for $i \neq j$ but G is *not* the internal direct product of $N_1, \ldots, N_n$.

Exercise 4.3

Prove that G is the internal direct product of the normal subgroups $N_1, \ldots, N_n$ if and only if

1. $G = N_1 \cdots N_n$.
2. $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n) = \{e\}$ for $i = 1, 2, \ldots, n$.

Exercise 4.4

If G is an abelian group of order p^n, p a prime and $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, are the invariants of G, then show that the maximal order of any element in G is p^{n_1}.

Exercise 4.5

Let G and G' be two abelian groups of order p^n and s be a positive integer. Let $H = \{x^s \mid x \in G\}$ and $H' = \{(x')^s \mid x' \in G'\}$ be subgroups of G and G' respectively. If G and G' are isomorphic then show that H and H' are isomorphic.

Exercise 4.6

Prove that if a finite abelian group has subgroups of order m and n respectively, then it has a subgroup of order equal to least common multiple of m and n. [**Hint:** Use Theorem 4.2.3].

Exercise 4.7

Describe all the finite abelian groups of order

1. 2^6.
2. 11^6.
3. 7^5.
4. $2^4 \cdot 3^4$.

Exercise 4.8

Show how to obtain all abelian groups of order $2^3 \cdot 3^4 \cdot 5$.

Exercise 4.9

Let G is an abelian group of order p^n with invariants $n_1 \geq \cdots \geq n_k > 0$ and $H \neq \{e\}$ is a subgroup of G. Show that if $h_1 \geq \cdots \geq h_s > 0$ are invariants of H, then $k \geq s$ and $h_i \leq n_i$ for each $i = 1, 2, \ldots, s$.

Index

N

O

P

R

S

T