

$A(S)$

Lecture notes on
GROUP THEORY

PS04EMTH37

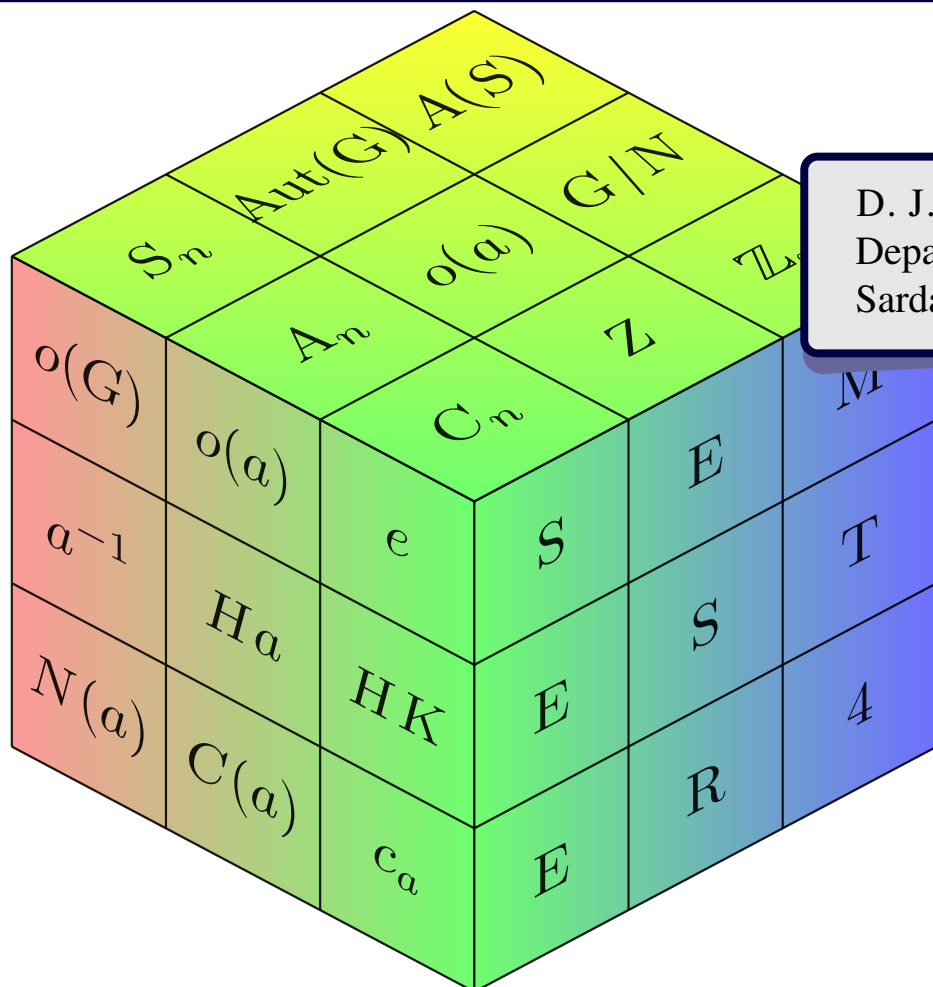
$HK = KH$

D. J. KARIA & JAY MEHTA
Department of Mathematics,
Sardar Patel University.

G

$1 + kp$

$A \times B$



SEMESTER - IV
2018-19

Preface and Acknowledgments

This note started when we offered 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.
- A uniformity in approach in different classes.

Acknowledgment

JAY MEHTA

Contents

	Syllabus	7
1	Groups: Quick Revision	9
1.1	Groups and Subgroups	9
1.2	A Counting Principle	18
	Exercises	24
2	Conjugate Classes & Class Equation	27
2.1	Automorphisms	27
2.2	Cayley's Theorem	31
2.3	Permutation groups	34
2.4	Another Counting Principle	43
	Exercises	54
3	Sylow's Theorem	59
3.1	Sylow's Theorem	59
3.1.1	First proof of Sylow's theorem	60
3.2	Other Parts of Sylow's Theorem	70
3.3	Simple group and Solvable group	72
3.4	Applications of Sylow's theorem	73
	Exercises	74
4	Fundamental Theorem of Finite Abelian Groups	77
4.1	Direct Products	77
4.2	Finite Abelian Groups	80
	Exercises	87
	Index	91

Syllabus

PS04EMTH37: Group Theory

- Unit I:** Definition of a group, some examples of groups, some preliminary lemmas, subgroups, two equivalence relations $a \equiv b \pmod{H}$ if $ab^{-1} \in H$ and $a \sim b \pmod{H}$ if $a^{-1}b \in H$, Lagrange'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.
- 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 S_n .
- Unit III:** Sylow's theorem, first proof, definition of p -Sylow subgroup, second proof of Sylow's theorem, existence of p -Sylow subgroup in S_{p^k} , 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 p^n for prime p , the subgroup $G(s)$ of an abelian group G , for an integer s , $o(G(p^m))$ for a prime p , uniqueness of invariants, number of non-isomorphic abelian groups of order $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where p_i are distinct primes and $\alpha_i > 0$.

Text Book

1. Herstein, I.N., Topics in Algebra, (Second Edition), John Wiley & Sons, Inc., New Delhi, 2006.

Chapter 2: § 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 (except Application 2 and its Corollary, Lemma 2.7.5 and Theorem 2.7.2), 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14.

Reference Books

1. Fraleigh, J.B., *A First Course in Abstract Algebra, (Tenth Printing)*, Narosa Publishing House, New Delhi, 2003.
2. Gallian, J.A., *Contemporary Abstract Algebra (Fourth Edition)*, Narosa, 2008.

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 $a \equiv b \pmod{H}$ if $ab^{-1} \in H$ and $a \sim b \pmod{H}$ if $a^{-1}b \in H$, Lagrange'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 intention 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.

1.1 Groups and Subgroups

We start with the definition of a group.

Definition 1.1.1

Let G be nonempty set with a binary operation $(a, b) \in G \times G \mapsto ab \in G$, satisfying the following. the following.

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

Then G is called a *group*. Further, if

4. $ab = ba$ for all $a, b \in G$,

then G is called an *abelian group* or *commutative group*.

Remark 1.1.2. 1. In the Definition 1.1, (1) is called associativity of operation, (2) is known as the *existence of identity in G* , and (3) is known as the *existence of inverse of*

each element in G . e in (2) is called an¹ identity of G and a^{-1} in (3) is called an inverse of a .

2. A group which is not abelian is called a non-abelian group.

Example 1.1.3. Let $n \in \mathbb{N}$. Define $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$, where \bar{k} denotes the equivalence class $[k]$ for the relation $\equiv \pmod{n}$. For $\bar{k}, \bar{m} \in \mathbb{Z}_n$, define

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

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

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

Clearly, for every $(\bar{k}, \bar{m}) \in \mathbb{Z}_n \times \mathbb{Z}_n$, 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 $j \equiv k \pmod{n}$ and $l \equiv m \pmod{n}$, then

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

That is,

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

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

Claim 2: $+$ is associative.

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

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

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

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

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

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

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

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

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

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

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

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

¹We use ‘an’ because we have yet not proved that identity and inverses are unique.

Definition 1.1.4

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

Example 1.1.5. 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 $f : S \rightarrow S$ and $g : S \rightarrow S$ are one-one, onto functions. Let $x, y \in S$ with $x \neq y$. Then

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

Now let $z \in S$. Since g is onto,

$$\exists y \in S \text{ such that } g(y) = z. \quad (1.7)$$

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

$$\exists x \in S \text{ such that } f(x) = y. \quad (1.8)$$

By (1.7) and (1.8), 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 $x \in S$,

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

Thus composition is associative.

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

Define $\iota : S \rightarrow S$ 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

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

Thus $A(S)$ is a group with composition. □

Definition 1.1.6

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

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

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

$$\theta = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \theta(x_1) & \theta(x_2) & \dots & \theta(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} \quad (1.9)$$

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

$$\theta = \begin{pmatrix} 1 & 2 & \dots & n \\ \theta(1) & \theta(2) & \dots & \theta(n) \end{pmatrix} \quad (1.10)$$

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,

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

Definition 1.1.7

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

$$\theta\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\theta(1)) & \sigma(\theta(2)) & \dots & \sigma(\theta(n)) \end{pmatrix} \quad (1.12)$$

i.e.,

$$\theta\sigma = \sigma \circ \theta \quad (1.13)$$

Example 1.1.8. 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

$$\theta\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad (1.14)$$

and

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

In the following example, we construct S_3 .

Example 1.1.9 (A standard Example). We set

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}. \quad (1.16)$$

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

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

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

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

Thus $S_3 = \{e, \varphi, \psi, \psi^2, \varphi\psi, \psi\varphi\}$ is a group. Throughout this note, without defining φ and ψ again, we shall refer to these elements.

Example 1.1.10. 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 1.1.11. Let $n \in \mathbb{N}$ be fixed and $G = \{a^0, a, a^2, \dots, a^{n-1}\}$, 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 1.1.12. Let $S = \mathbb{Z}$ and $G = \{\sigma \in A(S) : \sigma(n) = n \text{ for all but finitely many } n \in \mathbb{Z}\}$. Then clearly, G is a group.

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 1.1.13

Let G be a group.

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 $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
5. 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 $a, u, w \in G$,

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

Subgroups

Definition 1.1.14

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

We recall the following results without proof as you have already studied them.

Lemma 1.1.15

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 and every element of H has an inverse in H .
3. $a, b \in H \Rightarrow ab^{-1} \in H$.
4. $a, b \in H \Rightarrow a^{-1}b \in H$.

If further, H is finite, then each of the above is equivalent to

5. H is closed under operation of G .

Proof. Proof in seminar/assignment. □

Right and left cosets of a subgroup

Definition 1.1.16

Let H be a subgroup of a group G . For $a, b \in G$, define $a \equiv b \pmod{H}$, if $ab^{-1} \in H$. An equivalence class containing a is the set

$$Ha = \{ha : h \in H\}, \quad (1.17)$$

which is called a *right coset* of H in G . For $a, b \in G$, define also define $a \sim b \pmod{H}$, if $a^{-1}b \in H$. An equivalence class containing a for this relation is the set

$$aH = \{ah : h \in H\}, \quad (1.18)$$

which is called a *left coset* of H in G .

Lemma 1.1.17

Let H be a subgroup of a group G .

1. The relation $\equiv \pmod{H}$ defined above in Definition 1.1 is an equivalence relation with its equivalence classes of the form

$$Ha = \{x : a \equiv x \pmod{H}\}, \quad (\forall a \in G). \quad (1.19)$$

2. The relation $\sim \pmod{H}$ defined above in Definition 1.1 is an equivalence relation with its equivalence classes of the form

$$aH = \{x : a \sim x \pmod{H}\}, \quad (\forall a \in G). \quad (1.20)$$

Proof. Proof in seminar/assignment. □

We make the general definition for a later use

Definition 1.1.18

Let A, B be two nonempty subsets of a group G and $x \in G$. We define

$$AxB = \{ab : a \in A, b \in B\}.$$

When $x = e$, the above set turns out to be

$$AB = \{ab : a \in A, b \in B\}.$$

Corollary 1.1.19

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.

Proof. Proof in seminar/assignment. □

You have also studied the following.

Lemma 1.1.20

There is a one-to-one correspondence between any

1. two right cosets,
2. two left cosets and
3. a left and a right coset.

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. $ah \in aH \leftrightarrow hb \in Hb$. □

Recall that for a finite subset A of a group, $o(A)$ denotes the number of elements of A . Using Lemma 1.1, one easily obtains the following theorem, known as the Lagrange's theorem.

Theorem 1.1.21: 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 $o(H) \mid o(G)$.

Definition 1.1.22

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 $i_G(H)$.

Corollary 1.1.23

Let G be a finite group and H be its subgroup. Then

$$i_G(H) = \frac{o(G)}{o(H)} \tag{1.21}$$

Proof. Proof in seminar/assignment. □

Definition 1.1.24

Let G be a group and $a \in G$ and $n \in \mathbb{Z}$. Then we define

$$a^n = \begin{cases} \underbrace{a \cdot a \cdots a}_{n \text{ times}}, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ (a^{-1})^{-n}, & \text{if } n < 0. \end{cases} \tag{1.22}$$

Lemma 1.1.25

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

$$\langle a \rangle = (a) = \{a^n : n \in \mathbb{Z}\} \tag{1.23}$$

is an abelian subgroup of G .

Proof. Proof in seminar/assignment. □

Definition 1.1.26

Let G be a group and $a \in G$. The subgroup in (1.23) is called the *cyclic subgroup of G generated by a* . If G is a cyclic subgroup of G , then G is called a *cyclic group*.

Definition 1.1.27

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.

Remark 1.1.28. It is clear from the Lagrange's theorem and Lemma 1.1 that $o(a) \mid o(G)$, provided $o(G) < \infty$. As a result, we have the following Corollary.

Corollary 1.1.29

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

Proof. Proof in seminar/assignment. □

Definition 1.1.30

Let $n \in \mathbb{N}$. We define the *Euler's totient function* also called *Euler's phi function* $\phi : \mathbb{N} \rightarrow \mathbb{N}$ as $\phi(n) =$ number of positive integers less than n and relatively prime to n and $\phi(1) = 1$.

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 . Clearly $o(G) = \phi(n)$. Consequently, we have the following particular case of Corollary 1.1.

Corollary 1.1.31: Euler

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

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{1.24}$$

Proof. Proof in seminar/assignment. □

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

Corollary 1.1.32: Fermat

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

$$a^p \equiv a \pmod{p}. \quad (1.25)$$

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

Note that $\phi(p) = p - 1$. Hence by Corollary 1.1,

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ \therefore a^p &\equiv a \pmod{p}. \end{aligned}$$

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

In this case, the $\gcd(a, p) = p$. Consequently, $p \mid a$.

$$\begin{aligned} \therefore a^p &\equiv 0 \pmod{p} \\ \therefore a^p &\equiv a \pmod{p} \quad (\text{because } a \equiv 0 \pmod{p}) \end{aligned}$$

This completes the proof. □

Corollary 1.1.33

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

Proof. Proof in seminar/assignment. □

1.2 A Counting Principle

Let H, K be two subgroups of a group G . In general HK is not a subgroup of G (See Exercise 2.1). However the following Lemma characterizes when HK is a subgroup of G .

Lemma 1.2.1

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

Proof. Step I: If part

Suppose $HK = KH$.

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

Let $h_1 k_1, h_2 k_2 \in HK$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then
 $k_1 h_2 \in HK = KH \Rightarrow k_1 h_2 = h_3 k_3$ for some $h_3 \in H, k_3 \in K$.

$\therefore h_1 k_1 h_2 k_2 = h_1 h_3 k_3 k_2 \in HK$ because $h_1, h_3 \in H, k_1, k_3 \in K$ and H and K are subgroups.

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

Let $hk \in HK$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

$\therefore (hk)^{-1} \in HK$.

Thus HK is a subgroup of G .

Step II: Only if part

Suppose HK is a subgroup of G . Let $x = kh \in KH$, where $h \in H, k \in K$. Then

$\therefore h^{-1} \in H, k^{-1} \in K$ ($\because H$ and K are subgroups)

$\therefore h^{-1}k^{-1} \in HK$

$\therefore (h^{-1}k^{-1})^{-1} \in HK$ ($\because HK$ is a subgroup)

$\therefore kh \in HK$ ($\because kh = (h^{-1}k^{-1})^{-1}$)

$\therefore KH \subset HK$

Now let $x = hk \in HK$, where $h \in H, k \in K$.

$\therefore x^{-1} \in HK$ ($\because HK$ is a subgroup)

$\therefore k^{-1}h^{-1} \in HK$

$\therefore k^{-1}h^{-1} = h_1 k_1$ (for some $h_1 \in H, k_1 \in K$)

$\therefore hk = k_1^{-1}h_1^{-1} \in KH$ (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 1.2.2

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 1.2.3

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

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}. \quad (1.26)$$

Proof. Let $H \cap K = \{e = r_1, r_2, \dots, r_m\}$.

Let us first list all elements of HK in the form

$$hk : h \in H, k \in K \quad (1.27)$$

with all possible repetitions. So, there are $o(H)o(K)$ entries in (1.27). We show that each element of HK appears exactly m times in this list.

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

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

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

Then x can be written in the form “an element of H into an element of K ” in m distinct ways as shown in (1.28)

$$x = h_1k_1 = h_2k_2 = h_3k_3 = \dots = h_mk_m \quad (1.28)$$

Claim 1: All h_i in (1.28) are distinct.

If $h_i = h_j$, then $hr_i = hr_j$. So, by the cancellation law, $r_i = r_j$. So, $i = j$. Thus there are m distinct representations of hk in (1.28).

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

Claim 2: $h'k'$ is already listed in (1.28), that is, $h' = hr_i, k' = r_i^{-1}k$ for some i .

$$\begin{aligned} hk &= h'k' \\ \therefore h'^{-1}h &= k'k^{-1} \in H \cap K \\ \therefore (h'^{-1}h)^{-1} &= (k'k^{-1})^{-1} \in H \cap K \\ \therefore h^{-1}h' &= kk'^{-1} \in H \cap K \\ \therefore h^{-1}h' &= kk'^{-1} = r_i \quad \text{for some } r_i \in H \cap K \\ \therefore r_i^{-1} &= k'k^{-1}. \end{aligned}$$

Consequently, $h' = hh^{-1}h' = hr_i$ and $k' = k'k^{-1}k = r_i^{-1}k$. Thus the repetition $h'k'$ is one of the forms listed in (1.28). 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 (1.26). \square

Corollary 1.2.4

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. Let $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$. Suppose, if possible, $o(H \cap K) = 1$. Putting this value in (1.26)

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)} = o(G), \quad (1.29)$$

a contradiction. Thus $o(H \cap K) \neq 1$. Thus $H \cap K \neq \{e\}$. \square

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

Proposition 1.2.5

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 having order p .

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

$$\begin{aligned} o(H) &= o(K) = p = \sqrt{p^2} > \sqrt{pq} = \sqrt{o(G)} \\ \therefore H \cap K &\neq \{e\} \\ \therefore o(H \cap K) &> 1 \\ \text{But } o(H \cap K) &| o(H) \\ \therefore o(H \cap K) &= p \end{aligned}$$

Thus $H \cap K$ is a subset of H having p elements. Also H has p elements.

$$\begin{aligned} \therefore H \cap K &= H \\ \text{Similarly, } H \cap K &= K. \end{aligned}$$

This completes the proof. □

Definition 1.2.6

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 $x \in N$, $g x g^{-1} \in N$. Symbolically, this is written as $N \triangleleft G$.

We collect the characterization of a normal subgroup of a group familiar to you in the following theorem.

Theorem 1.2.7

Let G be a group and N be a subgroup of G . The following are equivalent.

1. N is normal in G .
2. $gNg^{-1} \subset N$ for every $g \in G$.
3. $gNg^{-1} = N$ for every $g \in G$.
4. Every left coset of N in G is also a right coset of N in G .
5. For every $a, b \in G$, $NaNb = Nab$.
6. For every $a, b \in G$, $aNbN = abN$.
7. The equivalence relations $\sim \pmod{N}$ and $\equiv \pmod{N}$ are the same equivalence relation.

Proof. Proof in seminar/assignment □

Definition 1.2.8

Let G be a group and N be a subgroup of G . We define

$$G/N = \{Na : a \in G\}.$$

Example 1.2.9. Let G be a group and N be a normal subgroup of G if and only if G/N is a group with the usual quotient multiplication.

Proof. Follows from Theorem 1.2(5). □

Definition 1.2.10

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 .

The following is clear from the Lagrange's theorem.

Proposition 1.2.11

Let N be a normal subgroup of a finite group G . Then

$$o(G/N) = o(G)/o(N). \tag{1.30}$$

Proof. Proof in seminar/assignment □

Definition 1.2.12

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

$$\ker(\psi) = K_\psi = \{x \in G : \psi(x) = \bar{e}\}$$

is called the *kernel of ψ* , where \bar{e} is the identity of \bar{G} . If further ψ is also one-one, then ψ is called an *isomorphism*.

Definition 1.2.13

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 $G \approx \bar{G}$.

We record the following without proof as you have already studied it in undergraduate.

Lemma 1.2.14

Let G, \bar{G} be groups with identities e, \bar{e} respectively and $\varphi : G \rightarrow \bar{G}$ be a homomorphism. Then

1. $\varphi(e) = \bar{e}$.
2. $\varphi(a^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.
3. $\ker(\varphi)$ is a normal subgroup of G .
4. φ is one-one if $\ker \varphi = \{e\}$.

Lemma 1.2.15

Let G be a group and N be a normal subgroup of G . Define $\sigma_N : G \rightarrow G/N$ by $\sigma(x) = Nx$, ($x \in G$). Then σ is an onto homomorphism with $\ker \sigma = N$.

Theorem 1.2.16: First Isomorphism Theorem

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

Application of Lagrange's theorem**Theorem 1.2.17: 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 $a \in G$, such that $o(a) = p$.

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 $p \mid o(N)$.

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 $p \nmid o(N)$.

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

Since G is commutative, N is normal. So, G/N is a group and by Proposition 1.2, $o(G/N) = o(G)/o(N) < o(G)$. Since G/N is commutative, by induction hypothesis, there is $X = Nb \in G/N$ such that $o(X) = p$, that is,

$$b \notin N \text{ and } b^p \in N. \quad (1.31)$$

Let $c = b^{o(N)}$.

Then $c^p = (b^p)^{o(N)} = e$, because $b^p \in N$.

In order to show that $o(c) = p$, we need to show that $c \neq e$.

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

Combining this with $(Nb)^p = N$ and $p \nmid o(N)$

$$\begin{aligned} &\Rightarrow Nb = N \\ &\Rightarrow b \in N, \end{aligned}$$

a contradiction. Thus $c \neq e$. Hence $o(c) = p$. This completes the proof. \square

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. Show that G is a group with the operation, $gh = h * g$, $(g, h \in G)$

Exercise 1.2

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 1.3

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

Exercise 1.4

Let $G = \{12^n 15^m : n, m \in \mathbb{Z}\}$ is a group. Find the relation between G and the group $H = \{3^n 5^m 2^k : n, m \in \mathbb{Z}\}$.

Exercise 1.5

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

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2). \quad (1.32)$$

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

Exercise 1.6

Show that a group has a unique identity element.

Exercise 1.7

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

Exercise 1.8

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

Exercise 1.9

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 1.10

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

Exercise 1.11

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 1.12

Show that S_n has exactly $n!$ elements.

Exercise 1.13

Show that S_n is a group.

Exercise 1.14

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

Exercise 1.15

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

Exercise 1.16

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

Exercise 1.17

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 1.18

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 1.19

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 1.20

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

Exercise 1.21

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 1.22

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 1.23

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

Exercise 1.24

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

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 $\text{Aut}(G)$ or $\mathcal{A}(G)$.

Lemma 2.1.2

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

Proof. Let us note that $\mathcal{A}(G) \subset A(G)$. So, we need to prove that $\mathcal{A}(G)$ is nonempty and closed under composition and inversion. Since the identity map $I : G \rightarrow G$, defined by $I(g) = g$, ($g \in G$), is an onto isomorphism, $\mathcal{A}(G) \neq \emptyset$. Also, composition of two homomorphisms is again a homomorphism. So, we need only to prove that for every $T \in \mathcal{A}(G)$, $T^{-1} \in \mathcal{A}(G)$. Let $T \in \mathcal{A}(G)$. So, $T \in A(G) \Rightarrow T^{-1} \in A(G)$. Also,

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

So,

$$T^{-1}(xy) = (T^{-1}(x)T^{-1}(y)).$$

This completes the proof. □

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

1. $T \in A(G)$.
2. $T \neq I$ if and only if there is $x_0 \in G$ such that $x_0 \neq x_0^{-1}$.
3. $T \in \mathcal{A}(G)$ if and only if G is abelian.

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

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

□

Lemma 2.1.4

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

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 $T_g : G \rightarrow G$ defined by $T_g(x) = gxg^{-1}$, ($x \in G$), is called an *inner automorphism*. The set of all inner automorphisms is denoted by $\mathcal{I}(G)$.

Remark 2.1.6. Note that here we deviate from the definition of the inner automorphism given by [?, 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.

Lemma 2.1.7

Let G be a group and $g, h \in G$, then

1. $T_{gh} = T_g T_h$
2. $T_{g^{-1}} = T_g^{-1}$.

Proof. For $x \in G$,

$$\begin{aligned} T_{gh}(x) &= (gh)xgh^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= T_g(hxh^{-1}) \\ &= T_g T_h(x) \end{aligned}$$

This proves (1).

Also, for $x \in G$,

$$T_g T_{g^{-1}}(x) = gg^{-1}xgg^{-1} = x = g^{-1}gxg^{-1}g = T_{g^{-1}} T_g(x) \quad (2.1)$$

This proves (1) and completes the proof. \square

Lemma 2.1.8

Let G be a group. Define $\psi : G \rightarrow \mathcal{I}(G)$ by $\psi(g) = T_g$. Then

1. ψ is a homomorphism.
2. $\ker(\psi) = Z$, the centre of G .
3. ψ is onto, so that $\mathcal{I}(G) \approx G/Z$.

Proof. (1) follows from Lemma 2.1(1). Now

$$\begin{aligned} g \in \ker(\psi) &\Rightarrow T_g = I \\ &\Leftrightarrow T_g(x) = x \forall x \in G \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow gxg^{-1} = x \forall x \in G \\ &\Leftrightarrow gx = xg \forall x \in G \\ &\Leftrightarrow g \in Z \end{aligned}$$

This proves (2). Finally, for any $T_g \in \mathcal{A}(G)$, $\psi(g) = T_g$. Thus ψ is onto. So, by the first isomorphism theorem, $\mathcal{I}(G) \approx G/\ker(\psi) \approx G/Z$. \square

Lemma 2.1.9

Let G be a group. Then $\mathcal{I}(G)$ is a normal subgroup of $\mathcal{A}(G)$.

Proof. Let $S \in \mathcal{A}(G)$ and $T_g \in \mathcal{I}(G)$. Then for any $x \in G$

$$S(T_g(S^{-1}(x))) = S(gS^{-1}(x)g^{-1}) = S(g)S(S^{-1}(x))S(g^{-1}) = S(g)xS(g)^{-1} = T_{S(g)}(x)$$

This completes the proof. \square

Definition 2.1.10

The element of $\mathcal{A}(G)/\mathcal{I}(G)$ are called the *outer automorphisms*.

Lemma 2.1.11

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

Proof. Suppose $o(a) = n > 0$. Then $\varphi(a)^n = \varphi(a^n) = e$. Also for any $1 \leq k < n$, $\varphi(a)^k = e \Rightarrow \varphi(a^k) = e \Rightarrow a^k = e$, a contradiction. So, $o(\varphi(a)) = n$. \square

Next we compute the automorphisms of cyclic groups.

Example 2.1.12. Let $G = \langle a \rangle$ be a cyclic group. For $t \in \mathbb{Z}$, define $T_t(a^i) = a^{ti}$, ($a^i \in G$). Then T_t is a homomorphism. Conversely, given a homomorphism, T , there is a unique $0 \leq t < o(G)$ such that $T = T_t$. (In this case, $T(a) = a^t$).

solution. Straight verification. \square

Example 2.1.13. Consider a finite cyclic group $G = \langle a \rangle$, $a^r = e$, of order r . Let $T_t \in \mathcal{A}(G)$. Assume that $d = (t, r) > 1$. Then $(a^t)^{n/d} = (a^{t/d}d)^{n/d} = (a^{t/d})^n = e$. Hence $o(a^t) = n/d < o(a)$, a contradiction. Thus $d = 1$. Conversely, suppose $d = (t, r) = 1$. Now suppose for some $1 \leq i < r$, $T_t(a^i) = e$. Then $a^{ti} = e$. Clearly, $ti \geq o(a) = r$. Hence $r \mid ti$. Since $(t, r) = 1$, $n \mid i$, a contradiction. Thus T_t is injective. Thus as the sets $\mathcal{A}(G) = \{T_t : 1 \leq t < r, (t, r) = 1\}$.

Now consider $U_r = \{t \in \mathbb{N} : 1 \leq t < r, (t, r) = 1\}$, the group of all integers relatively prime to r modulo r . One easily sees that $T_t T_s = T_q$, where $q = ts \pmod r$. Thus, $U_r \approx \mathcal{A}(G)$.

Example 2.1.14. Consider the infinite cyclic group $G = \langle a \rangle$, $a^r = e \Leftrightarrow r = 0$. For $t \in \mathbb{Z}$, assume that T is an automorphism. Then for some i , $T_t(a^i) = a$. Hence $a^{ti} = a \Rightarrow a^{ti-1} = e \Rightarrow ti - 1 = 0 \Rightarrow ti = 1$. This forces $t = \pm 1$. Conversely, $T_{\pm 1} \in \mathcal{A}(G)$. Thus $\mathcal{A}(G) = \{1, -1\} = C_2$, the cyclic group of order 2.

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

Claim 2: ψ is a homomorphism.

For $g, h \in G$,

$$\begin{aligned} \tau_{gh}(x) &= (gh)x = g(hx) = \tau_g(hx) = \tau_g \tau_h(x) \\ \therefore \tau_{gh} &= \tau_g \tau_h \\ \therefore \psi(gh) &= \tau_{gh} = \tau_g \tau_h = \psi(g)\psi(h). \end{aligned} \tag{2.2}$$

Claim 3: ψ is an isomorphism.

Note that $\iota : G \rightarrow G$ defined by $\iota(g) = g$, ($g \in G$), is the identity of $A(S)$. Let $g \in G$ ¹

$$\begin{aligned} \psi(g) &= \iota \\ \Rightarrow \tau_g &= \iota \\ \Rightarrow \tau_g(x) &= \iota(x) \quad \forall x \in G \\ \Rightarrow gx &= x \quad \forall x \in G \\ \Rightarrow g &= e \\ \Rightarrow \ker(\psi) &= \{e\}. \end{aligned}$$

Thus ψ is an isomorphism. □

¹Prove in different way that $\psi(g) = \psi(h) \Rightarrow g = h$.

Definition 2.2.3

Let S be a set and G be a group. A homomorphism from G to $A(S)$ is called an *action of G on S* .

Lemma 2.2.4

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

$$S = \{xH : x \in G\}. \quad (2.3)$$

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

$$t_g(xH) = gxH, \quad (xH \in S), \quad (2.4)$$

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

$$\theta(g) = t_g, \quad (g \in G). \quad (2.5)$$

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 $xH, yH \in S$,

$$\begin{aligned} t_g(xH) &= t_g(yH) \\ \Rightarrow gxH &= gyH \\ \Rightarrow (gy)^{-1}gx &\in H \\ \Rightarrow y^{-1}g^{-1}gx &\in H \\ \Rightarrow y^{-1}x &\in H \\ \Rightarrow xH &= yH. \end{aligned}$$

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 $xH \in S$,

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

Thus θ is a homomorphism.

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

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

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

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

Indeed, kernel of every homomorphism is a normal subgroup. So, the claim follows.²

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

Let $h \in N$ and $xH \in S$ with $x \in G$.

$$\begin{aligned} x^{-1}hx &\in N \subset H \quad (\text{because } N \text{ is normal in } G \text{ and } h \in N) \\ \Rightarrow hx &\sim x \pmod{H} \\ \Rightarrow hxH &= xH \\ \Rightarrow t_h(xH) &= xH \quad \text{for every } xH \in S \\ \Rightarrow t_h &= \iota \\ \Rightarrow h &\in \ker(\theta) \\ \Rightarrow N &\subset \ker(\theta). \end{aligned}$$

This completes the proof. □

Corollary 2.2.5

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 $i_G H = n$. Let $S = \{xH : x \in G\}$ and $\theta : G \rightarrow A(S)$ be the action of G on S as in Lemma 2.2. Suppose, if possible, that θ is an isomorphism. So, $o(G) = o(\theta(G))$. Now

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

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

²Here we used this result. Let $\phi : G \rightarrow \bar{G}$ be a homomorphism, then $\ker(\phi)$ 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 $S = \{x_1, x_2, \dots, x_n\}$ and let $\sigma \in A(S)$. Suppose

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

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

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} \quad (2.6)$$

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

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad (2.7)$$

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,

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ 1\sigma & 2\sigma & \dots & n\sigma \end{pmatrix} \quad (2.8)$$

Definition 2.3.2

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

$$\sigma\psi = \begin{pmatrix} 1 & 2 & \dots & n \\ \psi(\sigma(1)) & \psi(\sigma(2)) & \dots & \psi(\sigma(n)) \end{pmatrix} \quad (2.9)$$

i.e.,

$$\sigma\psi = \psi \circ \sigma \quad (2.10)$$

For the group S_3 of all permutations on three symbols $\{1, 2, 3\}$, we set

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \quad (2.11)$$

The following example lists all elements of S_3 in terms of φ and ψ .

Example 2.3.3.

$$S_3 = \{e = \varphi^2 = \psi^3, \varphi, \psi, \psi^2, \varphi\psi = \psi^2\varphi, \varphi\psi^2 = \psi\varphi\}$$

or

$$S_3 = \{e = \varphi^2 = \psi^3, \varphi, \psi, \psi^2, \varphi\psi, \varphi\psi^2\},$$

with

1. $\phi^2 = \psi^3 = e$,
2. $\phi\psi = \psi^{-1}\phi$.

Solution. We need to verify the products.

$$\begin{aligned}\phi\psi &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \\ \psi^2\phi &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \\ \phi\psi^2 &= (\phi\psi)\psi = (\psi^2\phi)\psi = \psi^2(\phi\psi) = \psi^2(\psi^2\phi) = \psi\phi.\end{aligned}$$

□

Definition 2.3.4

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

$$(i_1, i_2, i_3, \dots, i_r), \quad (2.12)$$

where $i_1, i_2, i_3, \dots, i_r$ are distinct elements of S and $r \in \mathbb{N}$. We also identify this cycle in (2.12) with the permutation $\theta \in A(S)$ which maps

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

We shall refer to this permutation as the cycle $(i_1, i_2, i_3, \dots, i_r)$. 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 2.3.5. 1. In S_5 , $(1, 4, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

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

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

Solution.

$$\begin{aligned}
 (i_1, i_2, i_3, \dots, i_r) &= (i_2, i_3, \dots, i_r, i_1) \\
 &= (i_3, i_4, \dots, i_r, i_1, i_2) \\
 &\quad \dots \\
 &= (i_k, i_{k+1}, \dots, i_r, i_1, i_2, \dots, i_{k-1}) \\
 &\quad \dots \\
 &= (i_r, i_1, i_2, \dots, i_{r-1})
 \end{aligned} \tag{2.13}$$

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

Definition 2.3.7

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 2.3.8.

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.

Definition 2.3.9

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 2.3.10

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

Proof. Let $a, b, c \in S$. Clearly, $a \equiv_{\theta} a$ because $a = a\theta^0$. Thus \equiv_{θ} is reflexive. Next

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

Thus \equiv_{θ} is symmetric. Finally,

$$a \equiv_{\theta} b, b \equiv_{\theta} c$$

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

Hence \equiv_{θ} is transitive. □

Definition 2.3.11

Let $\theta \in S_n$, and $a \in S$. The equivalence class of \equiv_{θ} containing a is called the *orbit* of “ a ” under θ . Thus the orbit of a under θ is the set

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

Lemma 2.3.12

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

Proof. Since $a\theta, a\theta^2, a\theta^3, \dots \in S$ and S is finite, there must be a repetition in the list, say $a\theta^k = a\theta^m$, with $m > k$. Hence $a = a\theta^{m-k}$. By the well ordering principal, the set

$$\{n \in \mathbb{N} : a\theta^n = a\}$$

has the least element, say l .

Claim 1: $a, a\theta, \dots, a\theta^{l-1}$ are all distinct.

Let $1 \leq i < j \leq l-1$ be two integers such that $a\theta^i = a\theta^j$.

$\therefore a\theta^{j-i} = a$ and $1 \leq j-i \leq l-i$, contradicting to the minimality of l . Hence $a, a\theta, a\theta^2, \dots, a\theta^{l-1}$ are all distinct. □

Definition 2.3.13

Let S be a finite set and $\theta \in A(S)$. By a *cycle* of θ we mean

$$(a, a\theta, a\theta^2, \dots, a\theta^{l-1}) \tag{2.14}$$

for some $a \in S$ and l , the smallest positive integer such that $a\theta^l = a$.

Example 2.3.14. 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.

$$1\theta = 3, 1\theta^2 = 3\theta = 1$$

$$\therefore \text{orb}(1) = \{1, 3\}, l(1) = 2$$

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

$$2\theta = 4, 2\theta^2 = 4\theta = 6, 2\theta^3 = 6\theta = 7, 2\theta^4 = 7\theta = 2$$

$$\therefore \text{orb}(2) = \{2, 4, 6, 7\}, l(2) = 4$$

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

$$5\theta = 5$$

$$\therefore \text{orb}(5) = \{5\}, l(5) = 1.$$

Consequently,

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

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

Lemma 2.3.15

Two disjoint cycles in S_n commute.

Proof. Let $\theta = (i_1, i_2, \dots, i_r)$ and $\sigma = (j_1, j_2, \dots, j_t)$ be disjoint cycles in $A(S)$. Let $a \in S$.

Case I: $a = i_k$ for some $1 \leq k \leq r$

Clearly

$$a\theta\sigma = i_k\theta\sigma = \begin{cases} i_{k+1}\sigma, & \text{if } k < r \\ i_1\sigma, & \text{if } k = r. \end{cases}$$

$$= \begin{cases} i_{k+1} & \text{if } k < r \\ i_1, & \text{if } k = r. \end{cases}$$

and

$$a\sigma\theta = i_k\sigma\theta = i_k\theta = \begin{cases} i_{k+1}, & \text{if } k < r \\ i_1, & \text{if } k = r. \end{cases}$$

Case II: $a = j_k$ for some $1 \leq k \leq t$

The argument similar to the above works in this case also.

Case III: $a \neq i_k$ for any $1 \leq k \leq r$ and $a \neq j_k$ for any $1 \leq k \leq t$.

In this case, $a\sigma\theta = a\theta = a$ and $a\theta\sigma = a\sigma = a$. This completes the proof. \square

Lemma 2.3.16

A cycle of length 1 is identity.

Proof. Let S be a finite set and $a \in S$. Then (a) maps a to a and b to b for all other b . Thus $(a) = e$, the identity permutation. \square

Proposition 2.3.17

Let $n \in \mathbb{N}$ and $\theta \in S_n$. Then θ can be written as a product of disjoint cycles in a unique way except

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

Proof. Let us start with $s_1 = 1$. Let $\theta_1 = (s_1, s_2, \dots, s_{k_1})$ be a cycle of θ . If $k_1 = n$, then $\theta = (s_1, s_2, \dots, s_{k_1})$ and we are done.

Suppose $k_1 < n$.

$\therefore \{s_1, s_2, \dots, s_{k_1}\} \subsetneq S$. Choose $s_{k_1+1} \in S \setminus \{s_1, s_2, \dots, s_{k_1}\}$. Let $\theta_2 = (s_{k_1+1}, s_{k_1+2}, \dots, s_{k_2})$ be a cycle of θ . If $k_1 = n$, then $\theta = \theta_1 \theta_2$ and we are done.

Continuing in this way, we get $k_m = n$ in finitely many steps to get $\theta = \theta_1 \theta_2 \cdots \theta_m$. Note that the following will be considered as the same way of writing this.

1. Since the disjoint cycles commute, change of order of $\theta_1, \theta_2, \dots, \theta_m$, is considered to be the same as the original.³
2. If any cycle is rewritten as described in (2.13), they are considered to be the same.
3. If any 1-cycle is written or omitted, then there is no effect, as a 1-cycle is the identity. \square

Definition 2.3.18

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

Example 2.3.19. Now that we know how to multiply the cycles, the following, which expresses some cycles as a product of transpositions, is apparent.⁴

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 2.3.20

Every cycle can be written as a product of transpositions.

³Just like $2 \times 4 \times 7$ and $7 \times 2 \times 4$ are considered to be the same ways.

⁴Verify!

Proof. For a cycle $\theta = (i_1, i_2, \dots, i_r)$, we claim that

$$\theta = (i_1, i_2)(i_1, i_3)(i_1, i_4) \cdots (i_1, i_r) \quad (2.15)$$

Case I: $k = 1$.

$i_1\theta = i_2$. On the right hand side, the first transposition (i_1, i_2) maps i_1 to i_2 and each of the transpositions $(i_1, i_3), (i_1, i_4), \dots, (i_1, i_r)$ maps i_2 to i_2 . Thus i_1 is mapped to i_2 .

Case II: $1 < k < r$.

$i_k\theta = i_{k+1}$. On the right hand side, each of the transpositions $(i_1, i_2), \dots, (i_1, i_{k-1})$ maps i_k to i_k . The transposition (i_1, i_k) maps i_k to i_1 . The transposition (i_1, i_{k+1}) maps i_1 to i_{k+1} . Each of the transpositions $(i_1, i_{k+2}), (i_1, i_{k+3}), \dots, (i_1, i_r)$ maps i_{k+1} to i_{k+1} . Thus i_k is mapped to i_{k+1} .

Case III: $k = r$.

$i_r\theta = i_1$. On the right hand side, each of the transpositions $(i_1, i_2), \dots, (i_1, i_{r-1})$ maps i_r to i_r . The last transposition (i_1, i_r) maps i_r to i_1 . Thus i_r is mapped to i_1 .

Thus in each case, image of i_k under θ and under $(i_1, i_2)(i_1, i_3)(i_1, i_4) \cdots (i_1, i_r)$ are the same. So, (2.15) follows. \square

Corollary 2.3.21

Every permutation can be written as a product of two cycles.

Proof. Proof in seminar/assignment \square

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

Definition 2.3.22

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.

In what follows, p_n denotes the polynomial ⁵

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

in n variables x_1, x_2, \dots, x_n .

⁵Write p_1, p_2, p_3, p_4

Definition 2.3.23

Let $\theta \in S_n$. Define

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

i.e.,

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

Lemma 2.3.24

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

Proof. Step I: We show that for $i \neq j$, one and only one of $(x_i - x_j)$ and $(x_j - x_i)$ appears in θp_n .

Consider the permutation $\psi = \theta^{-1}$. Let $i_1 = i\psi$ and $j_1 = j\psi$. Consequently, $i_1\theta = i$ and $j_1\theta = j$. (Equivalently since θ is onto, there exists, i_1, j_1 such that $i_1\theta = i, j_1\theta = j$.)

Case I: $i_1 < j_1$.

$\therefore (x_{i_1} - x_{j_1})$ appears as a factor in p_n .

$\therefore (x_{\theta(i_1)} - x_{\theta(j_1)})$ appears in θp_n as one of the factors.

But $(x_i - x_j) = (x_{\theta(i_1)} - x_{\theta(j_1)})$.

$\therefore (x_i - x_j)$ appears in θp_n as one of the factors.

On the other hand, (x_{j_1}, x_{i_1}) does not appear in p_n .

$\therefore (x_j - x_i) = (x_{\theta(j_1)} - x_{\theta(i_1)})$ does not appear in θp_n .

Case II: $j_1 < i_1$.

The argument made by interchanging i_1, j_1 in the Case I proves see that $(x_j - x_i)$ appears but $(x_i - x_j)$ does not appear in θp_n as one of the factors.

Step II: Sign change in θp_n .

Now let i, j be distinct. Assume that $i < j$.

Case III: $(x_i - x_j)$ appears in θp_n .

Thus $(x_i - x_j)$ appears on both the sides and it does not contribute to change of sign.

Case IV: $(x_j - x_i)$ appears in θp_n .

Thus $(x_i - x_j)$ appears in p_n but $(x_j - x_i) = -(x_i - x_j)$ appears in θp_n , and so, it contributes to change of sign.

So, depending upon number of times the sign is changed $\theta p_n = \pm p_n$. This completes the proof. \square

Lemma 2.3.25

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

Proof. Let $\varphi = (i, j)$. Without loss of generality, we assume that $i < j$. Note that $(x_i - x_j)$ appears in p_n and $(x_j - x_i) = (x_{\varphi(i)} - x_{\varphi(j)})$ appears in φp_n that contributes to the change of sign.

Next we make couples from all the possible sign changing pairs, so that the change of sign is made even number of times.

Fix k other than i, j .

Case I: $i, j < k$.

In this case, $(x_i - x_k)$ and $(x_j - x_k)$ appear in p_n . Also, $(x_{\varphi(i)} - x_{\varphi(k)}) = (x_j - x_k)$ and $(x_{\varphi(j)} - x_{\varphi(k)}) = (x_i - x_k)$ appear in p_n contributing nothing to the change of sign.

Case II: $k < i, j$.

In this case, $(x_k - x_i)$ and $(x_k - x_j)$ appear in p_n . Also, $(x_{\varphi(k)} - x_{\varphi(i)}) = (x_k - x_j)$ and $(x_{\varphi(k)} - x_{\varphi(j)}) = (x_k - x_i)$ appear in p_n contributing nothing to the change of sign.

Case III: $i < k < j$.

In this case, $(x_i - x_k)$ and $(x_k - x_j)$ appear in p_n . Also, $(x_{\varphi(i)} - x_{\varphi(k)}) = (x_j - x_k)$ and $(x_{\varphi(k)} - x_{\varphi(j)}) = (x_k - x_i)$ appear in p_n contributing two times the change of sign, nullifying the effect.

Thus the gross effect of φ on p_n is a sign change. Thus $\varphi p_n = -p_n$ □

Corollary 2.3.26

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 $\theta = \psi_1 \psi_2 \cdots \psi_r$, where each ψ_i is a transposition, then $p_n = \theta p_n = \psi_1 \psi_2 \cdots \psi_r p_n$. So, $\psi_1 \psi_2 \cdots \psi_r$ does not change sign of p_n . But each ψ_i changes the sign of p_n . So, $\psi_1 \psi_2 \cdots \psi_r$ must change the sign of p_n even number of times. So, r is even. □

Definition 2.3.27

Let $n \in \mathbb{N}$. We define the *alternating group* A_n of order $2n$ to be

$$A_n = \{\theta \in S_n : \theta \text{ is even}\} \tag{2.16}$$

Proposition 2.3.28

A_n is a subgroup of S_n

Proof. Let $\theta_1, \theta_2 \in A_n$. If $\theta_1 = \sigma_1\sigma_2 \cdots \sigma_{2k}$ and $\theta_2 = \eta_1\eta_2 \cdots \eta_{2m}$, where each of σ_i, η_j is a transposition ($1 \leq i \leq 2k, 1 \leq j \leq 2m$), then $\theta_1\theta_2 = \sigma_1\sigma_2 \cdots \sigma_{2k}\eta_1\eta_2 \cdots \eta_{2m}$ is an even permutation. Also $\theta_1^{-1} = \sigma_{2k} \cdots \sigma_2\sigma_1$ is an even permutation. Thus A_n is a subgroup of S_n \square

Lemma 2.3.29

Define $\psi : S_n \rightarrow \{-1, 1\}$ 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. Proof in seminar/assignment \square

Corollary 2.3.30

1. A_n is normal in S_n
2. $o(A_n) = \frac{o(S_n)}{2}$.

Proof. Proof in seminar/assignment \square

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

The relation of being “conjugate of” is an equivalence relation.

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,

$$a \sim b, b \sim c \Rightarrow b = x^{-1}ax, c = y^{-1}by \quad \text{for some } x, y \in G \quad (2.17)$$

$$\Rightarrow c = y^{-1}x^{-1}axy = (xy)^{-1}a(xy) \quad (2.18)$$

$$\Rightarrow a \sim c. \quad (2.19)$$

This completes the proof. \square

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,

$$C(a) = \{x \in G : a \sim x\} = \{y^{-1}ay : y \in G\}. \quad (2.20)$$

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 ,

$$o(G) = \sum c_a, \quad (2.21)$$

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. Let us recall the Definition 2.4 restated below.

Notation Let H be a subgroup of a group G and $a \in G$. We define

$$aHa^{-1} = \{aha^{-1} : h \in H\}.$$

Example 2.4.3. Let H be a subgroup of a group G and $a \in G$. Then aHa^{-1} is a subgroup of G .

Solution.

Step I: To show that aHa^{-1} is closed under multiplication.

$$\begin{aligned} &aha^{-1}, aka^{-1} \in G, && \text{(with } h, k \in H) \\ \Rightarrow &hk \in H, && \text{(because } H \text{ is a group)} \\ \Rightarrow &aha^{-1}aka^{-1} = ahka^{-1} \in aHa^{-1}. \end{aligned}$$

Step II: To show that aHa^{-1} is closed under inversion.

$$\begin{aligned} &aha^{-1} \in G, && \text{(with } h \in H) \\ \Rightarrow &h^{-1} \in H, && \text{(because } H \text{ is a group)} \\ \Rightarrow &(aha^{-1})^{-1} = ah^{-1}a^{-1} \in H, \end{aligned}$$

Thus aHa^{-1} is a subgroup of G . \square

Definition 2.4.4

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

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

Lemma 2.4.5

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

Proof.

$$\begin{aligned} x, y \in N(a) &\Rightarrow xy^{-1}a = xy^{-1}a yy^{-1} = xy^{-1}yay^{-1} = xay^{-1} = axy^{-1} \\ &\Rightarrow xy^{-1} \in N(a). \end{aligned}$$

This completes the proof. □

Definition 2.4.6

Let G be a group, H be a subset of G and $a \in G$. Then we define the following

1. The *normalizer of H* is the set

$$N(H) = \{a \in G : aHa^{-1} = H\}.$$

2. The *centralizer of H* is the set

$$C(H) = \{x \in G : xh = hx \text{ for all } h \in H\}.$$

The centralizer of G , given by

$$Z(G) = \{x \in G : xg = gx \forall g \in G\},$$

is called the *centre of G* . Usually we shall write Z for $Z(G)$.

Lemma 2.4.7

Let G be a group and $a \in G$. The following are equivalent.

1. $a \in Z$, that is, $ab = ba$ for all $b \in G$.
2. $C(a) = \{a\}$.
3. $c_a = 1$.
4. $N(a) = G$.

Further, when G is finite, then each of the above is equivalent to

$$5. o(N(a)) = o(G).$$

Proof. Step I: (1) \Rightarrow (2)

Assume (1).

$$\begin{aligned} C(a) &= \{y^{-1}ay : y \in G\} \\ &= \{y^{-1}ya : y \in G\} \{asa \in Z\} \\ &= \{a\}. \end{aligned}$$

Step II: (2) \Rightarrow (3) is clear.

Step III: (3) \Rightarrow (4)

Assume (3). Since $c_a = 1$ is singleton and $a \in C(a)$, we get $C(a) = \{a\}$. Now

$$\begin{aligned} b \in G &\Rightarrow b^{-1}ab \in C(a) = \{a\} \\ &\Rightarrow b^{-1}ab = a \\ &\Rightarrow ab = ba \\ &\Rightarrow b \in N(a). \end{aligned}$$

Step IV: (4) \Rightarrow (1)

$b \in G \Rightarrow b \in N(a) \Rightarrow ab = ba$. Thus $ab = ba$ for all $b \in G$. So, $a \in Z$.

Step V: (4) \Leftrightarrow (5) when G is finite.

If $N(a) = G$, then clearly $o(N(a)) = o(G)$. Conversely, G is finite and $N(a) \subset G$ having the same number of elements as G clearly implies that $G = N(a)$. \square

Theorem 2.4.8

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

$$c_a = i_{GN(a)} = o(G)/o(N(a)). \quad (2.22)$$

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

$$\begin{aligned} N(a)x = N(a)y &\Leftrightarrow x \equiv y \pmod{N(a)} \\ &\Leftrightarrow yx^{-1} \in N(a) \\ &\Leftrightarrow yx^{-1}a = ayx^{-1} \\ &\Leftrightarrow x^{-1}ax = y^{-1}ay \end{aligned} \quad (2.23)$$

$N(a)x = N(a)y \Rightarrow x^{-1}ax = y^{-1}ay$ in (2.23) 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. \square

Corollary 2.4.9

For a finite group G ,

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

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. \square

The equation (2.24) is called the *class equation of G* . It is clear from the definition of $N(a)$ that $a \in Z \Leftrightarrow N(a) = G$. Thus 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

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

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

Example 2.4.10. We shall compute all entities discussed above 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 $\psi = (1, 2, 3)$.

: $N(e), C(e)$:

$$e \in Z \Rightarrow N(e) = G, \text{ and } C(e) = e. \tag{2.26}$$

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

$$\begin{aligned} \varphi\psi &= \psi^{-1}\varphi = \psi^2\varphi \neq \psi\varphi \\ \Rightarrow \varphi &\notin N(\psi), \psi \notin N(\varphi). \end{aligned} \tag{2.27}$$

$$\begin{aligned} \varphi\psi^2 &= \psi\varphi \neq \psi^2\varphi \\ \Rightarrow \varphi &\notin N(\psi^2), \psi^2 \notin N(\varphi). \end{aligned} \tag{2.28}$$

$$\begin{aligned} \varphi(\varphi\psi) &= \varphi^2\psi = \psi \neq \psi^2 = \psi^{-1} = (\psi^{-1}\varphi)\varphi = (\varphi\psi)\varphi \\ \Rightarrow \varphi\psi &\notin N(\varphi), \varphi \notin N(\varphi\psi). \end{aligned} \quad (2.29)$$

$$\begin{aligned} \varphi(\varphi\psi^2) &= \varphi^2\psi^2 = \psi^2 \neq \psi = (\psi\varphi)\varphi = (\varphi\psi^2)\varphi \\ \Rightarrow \varphi\psi^2 &\notin N(\varphi), \varphi \notin N(\varphi\psi^2). \end{aligned} \quad (2.30)$$

Collecting all the above we get,

$$N(\varphi) = \{e, \varphi\}. \quad (2.31)$$

Now,

$$e^{-1}\varphi e = \varphi \quad (2.32)$$

$$\varphi^{-1}\varphi\varphi = \varphi \quad (2.33)$$

$$\psi^{-1}\varphi\psi = \varphi\psi^2 \quad (2.34)$$

$$(\psi^2)^{-1}\varphi\psi^2 = \varphi\psi^4 = \varphi\psi \quad (2.35)$$

$$(\varphi\psi)^{-1}\varphi(\varphi\psi) = \psi^{-1}\varphi^{-1}\psi = \psi^{-1}\varphi\psi = \varphi\psi^2 \quad (2.36)$$

$$(\varphi\psi^2)^{-1}\varphi(\varphi\psi^2) = (\psi^2)^{-1}\varphi\psi^2 = \psi\psi\varphi = \varphi\psi \quad (2.37)$$

Collecting all the above we get,

$$C(\varphi) = \{\varphi, \varphi\psi, \varphi\psi^2\}. \quad (2.38)$$

$:N(\psi), C(\psi):$

Clearly, $e, \psi, \psi^2 \in N(\psi)$. By (2.27) $\varphi \notin N(\psi)$. Now $\varphi\psi \in N(\psi) \Rightarrow \varphi = (\varphi\psi)\psi^2 \in N(\psi)$, a contradiction to (2.27). Also, $\varphi\psi^2 \in N(\psi) \Rightarrow \varphi = (\varphi\psi^2)\psi \in N(\psi)$, a contradiction to (2.27). Thus $N(\psi) = \{e, \psi, \psi^2\}$.

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

Clearly, $\psi \in C(\psi)$. So, we need only to check if $\psi^2 \in C(\psi)$.

Suppose, if possible, that $\psi^2 \notin C(\psi)$. Then $C(\psi) = \{\psi\} \Rightarrow \psi \in Z \Rightarrow \psi\varphi = \varphi\psi$, a contradiction. Thus $\psi^2 \in C(\psi)$. Thus $C(\psi) = \{\psi, \psi^2\}$.⁶

Hide me:

Direct computation reveals that $e^{-1}\psi e = \psi$ and $(\varphi\psi)^{-1}\psi(\varphi\psi) = \psi^2\varphi\psi\varphi\psi = \psi^2$.

In the same way, one can easily prove that $N(\varphi\psi) = \{e, \varphi\psi\}$ and $N(\varphi\psi^2) = \{e, \varphi\psi^2\}$. \square

Finally in this section, we give two applications of counting principle.

Application 1:

Theorem 2.4.11

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. Let $z = o(Z)$. Recall the Class Equation (2.25),

$$o(G) = o(Z) + \sum \frac{o(G)}{o(N(a))}, \quad (2.39)$$

⁶Directly compute $C(\psi)$.

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,

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

Hide me:

Since in the sum, $o(N(a)) < o(G)$, $p \mid \frac{o(G)}{o(N(a))}$. Hence $p \mid o(Z)$ also. Since $o(Z) > 0$, $o(Z)$ is at least p . Thus $Z \neq \{e\}$. □

Corollary 2.4.12

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 2.4.13. 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 2.4.14: Cauchy's Theorem

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

Proof. If G is abelian, then we have already proved this result. So we assume that G is nonabelian, that is, $G \neq Z(G)$. We prove this result by induction on $o(G)$.

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

Suppose $o(G) = 1$. Then the result is vacuously true.⁷

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 we are done. So we assume that G does not have any proper subgroup W such that $p \mid o(W)$.

Note that

$$a \notin Z(G) \Rightarrow N(a) \neq G \Rightarrow p \nmid o(N(a)) \Rightarrow p \mid \frac{o(G)}{o(N(a))}.$$

Hence 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. 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. \square

Now we turn to computation of conjugate classes of S_n .

Definition 2.4.15

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

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

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

Example 2.4.16.

$$n = 1.$$

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

⁷Give me a prime p such that $p \mid 1$ and I will give you a such that $o(a) = p$.

$$n = 2.$$

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

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

$$\theta = (1, 3, 4)(2, 5, 6)(7, 9). \quad (2.40)$$

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,

$$\theta = (10)(8)(7, 9)(1, 3, 4)(2, 5, 6). \quad (2.41)$$

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

$$10 = 1 + 1 + 2 + 3 + 3. \quad (2.42)$$

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 2.4.18. Two different permutations may give rise to the same partition. To see this observe that the permutations

$$\begin{aligned} \sigma &= (7)(9)(1, 2)(3, 4, 5)(6, 8, 10) \\ \theta &= (1, 3, 4)(2, 5, 6)(7, 9). \end{aligned}$$

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 2.4.19

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

$$1 \leq n_1 < n_2 < \cdots < n_k \leq n \quad (2.43)$$

is the *cycle decomposition* of σ if there are disjoint cycles $\sigma_1, \sigma_2, \dots, \sigma_k \in S_n$ 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 2.4.20

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

$$i\sigma = j, i\theta = s, j\theta = t \Rightarrow s\theta^{-1}\sigma\theta = t. \quad (2.44)$$

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

Remark 2.4.21. If (i_1, i_2, \dots, i_k) is a cycle of σ , if and only if $(i_1\theta, i_2\theta, \dots, i_k\theta)$

Corollary 2.4.22

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

Example 2.4.23. 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 2.4.21

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

□

Corollary 2.4.24

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

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

$$\sigma = (i_1, i_2, \dots, i_{n_1})(i_{n_1+1}, i_{n_1+2}, \dots, i_{n_1+n_2}) \cdots (i_{n_1+n_2+\dots+n_{k-1}}, \dots, i_n) \quad (2.45)$$

and

$$\psi = (j_1, j_2, \dots, j_{n_1})(j_{n_1+1}, j_{n_1+2}, \dots, j_{n_1+n_2}) \cdots (j_{n_1+n_2+\dots+n_{k-1}}, \dots, j_n) \quad (2.46)$$

Define $i_t\theta = j_t, t = 1, 2, \dots, n$. Then from Lemma 2.4, it is clear that

$$\theta^{-1}\sigma\theta = \psi \quad (2.47)$$

□

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

Theorem 2.4.25

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, Corollary 2.4 and Corollary 2.4. □

Lemma 2.4.26

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 $1 \leq n_1 \leq n_2 < n_3 < \dots < n_k$ of n , define

$$\sigma = (1, 2, \dots, n_1)(n_1 + 1, n_1 + 2, \dots, n_1 + n_2) \cdots (n_1 + n_2 + \dots + n_{k-1}, \dots, n). \quad (2.48)$$

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

Exercises

In Exercise 2.8 to Exercise 2.12, H, K, N are subgroups of G be a group.

Exercise 2.1

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 .

Exercise 2.2

Let H be a subgroup of a group G and $a \in G$. Show that

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

Exercise 2.3

Show that in Definition 2.4, $C(H)$ is a subgroup of G .

Exercise 2.4

Show that in Definition 2.4, $N(H)$ is a subgroup of G . Further, if H is a subgroup of G , then show that $H \subset N(H)$.

Exercise 2.5

Show that in Definition 2.4, $N(a)$ is a subgroup of G and $a \in N(a)$.

Exercise 2.6

For $a, b \in \mathbb{R}$, define $\tau_{ab} : \mathbb{R} \rightarrow \mathbb{R}$ 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 2.7

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

1. 3

2. 4

3. 6

4. 7

Exercise 2.8

If $o(G) = 36 = 4o(H)$, then show that H has a nontrivial normal subgroups. (This group could be of order 3 or 9).

Exercise 2.9

If $o(G) = 77 = 7o(K)$, then show that the action of G on $S = \{xH : x \in G\}$ is the trivial action. (You may need to use many results like first isomorphism theorem, Lagrange's theorem et cetera.)

Exercise 2.10

For $g \in G$, define $\lambda_g : G \rightarrow G$ 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 2.11

Let λ_g be defined as in (2.10) above and τ_g be defined as in Definition 2.2. Show that $\lambda_g \tau_h = \tau_h \lambda_g$ for $g, h \in G$.

Exercise 2.12

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

Exercise 2.13

Find the smallest possible group containing a, b satisfying

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

Exercise 2.14

Find all the normal subgroups of S_3 .

Exercise 2.15

Find the centre of S_3 .

Exercise 2.16

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

Exercise 2.17

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 2.18

Write each cycle of permutations in (2.17) as a product of transpositions in more than one ways.

Exercise 2.19

Prove that two transpositions (i_1, i_2) and (i_3, i_4) commute with each other if and only if they are either the same or disjoint.

Exercise 2.20

Show that two transpositions are the same if and only if all their orbits are the same.

Exercise 2.21

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

Exercise 2.22

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

Exercise 2.23

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

Exercise 2.24

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 2.25

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

Exercise 2.26

Show that two distinct cycles θ and σ may have the same orbits.

Exercise 2.27

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 2.28

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

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

Exercise 2.29

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

Exercise 2.30

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

Exercise 2.31

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

Exercise 2.32

Find the order of the normalizer of a transposition in S_n .

Exercise 2.33

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

Exercise 2.34

Find the number of r -cycles in S_n .

Exercise 2.35

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 2.36

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

Exercise 2.37

Compute the conjugate classes in A_5 .

Exercise 2.38

Compute all automorphisms of a finite cyclic group.

Exercise 2.39

Compute all automorphisms of an infinite cyclic group.

Exercise 2.40

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

Exercise 2.41

Find all automorphisms of the Klein four-group.

Exercise 2.42

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

Exercise 2.43

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.

Sylow's Theorem

In this unit, we shall study the following.

Sylow's theorem and applications. Simple groups, solvable 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 3.1.1) 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 $\binom{n}{r} = \frac{n!}{k!(n-k)!}$.

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,

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

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. \square

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. Let \mathcal{M} denote the set of all subsets of G having exactly p^α elements. Since $p^\alpha \mid o(G)$, there is $m \in \mathbb{N}$ such that $o(G) = p^\alpha m$. Assume that

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

Note that there are $\binom{p^\alpha m}{p^\alpha}$ elements in \mathcal{M} .

Claim 1: Equivalence relation on \mathcal{M}

For $M_1, M_2 \in \mathcal{M}$, define $M_1 \sim M_2$ if $M_1 = M_2g$ for some $g \in G$. We show that \sim is an equivalence relation on \mathcal{M} . Indeed $M = Me$ for all $M \in \mathcal{M}$. 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 \mathcal{M} , a contradiction to the above lemma, as \mathcal{M} has $\binom{p^\alpha m}{m}$ 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

$$[M] = \{M_1, M_2, \dots, M_n\}. \quad (3.3)$$

Clearly,

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

Define

$$H = \{g \in G : M_1 g = M_1\}. \quad (3.4)$$

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

Claim 4: The map $\psi : [M] \rightarrow \{Hg : g \in G\}$, 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 . Clearly for Hg , we choose $M_1 g$ and $\psi(M_1 g) = Hg$. Thus ψ is bijective. Thus $n = i_G(H) = o(G)/o(H)$. So, $no(H) = o(G) = p^\alpha m$. Recall that $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid o(G)$. So, $p^{\alpha+r} \mid no(H)$. So, $p^\alpha \mid o(H)$. So, $p^\alpha \leq o(H)$. On the other hand, for any $m \in M$, $mH \subset M_1$. So, M_1 has at least as many element as $o(H)$. Thus $p^\alpha =$ number of elements in $M_1 \alpha o(H)$. This proves that $o(H) = p^\alpha$. \square

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 3.1.1 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 3.1.1.

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 (2.25) of G ,

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

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 $p^m \mid o(G)$ but $p^m \nmid o(N(a))$. Therefore we must have

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

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

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

This implies $p \mid \left(o(G) - \sum \frac{o(G)}{o(N(a))} \right)$. Hence by the class equation of G , $p \mid z$. 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 $p^m \mid o(G)$ but $p^{m+1} \nmid o(G)$, it is clear that $p^{m-1} \mid o(G')$ 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 $p^\alpha \mid o(G)$ instead of $p^m \mid o(G)$ 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 .

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

Definition 3.1.7

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 3.1.8

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

$$[x] = \{y \in G \mid x \sim y\}$$

$$\begin{aligned}
&= \{y \in G \mid y = axb, \text{ for some } a \in A, b \in B\} \\
&= \{axb \mid a \in A, b \in B\} = AxB.
\end{aligned}$$

Thus, the equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$. \square

Definition 3.1.9

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 3.1.10

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 $T : AxB \rightarrow AxBx^{-1}$ 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 1.2, we have

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

\square

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 3.1.11

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, $p^{m+1} \mid o(GxQ)$. 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,

$$p^{m+1} \mid o(GxQ) \Rightarrow p^{m+1} \mid \sum o(GxQ) \Rightarrow p^{m+1} \mid o(M)$$

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 . \square

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.

$$p^{n(k)} \mid (p^k)! \text{ but } p^{n(k)+1} \nmid (p^k)!.$$

The following lemma determines $n(k)$.

Lemma 3.1.12

$$n(k) = 1 + p + \cdots + p^{k-1}.$$

Proof. Let $k = 1$. Since $p! = 1 \cdot 2 \cdots (p-1) \cdot p$, it is clear that $p|p!$ but $p^2 \nmid p!$. Therefore $n(1) = 1$.

Our goal is to find the largest power $n(k)$ such that $p^{n(k)}|(p^k)!$. Now, consider the expansion of $(p^k)!$, i.e.

$$(p^k)! = p^k(p^k - 1) \cdots p(p-1) \cdots 2 \cdot 1.$$

Observe that, in the above expansion, the terms that contribute to the powers of p dividing $(p^k)!$ are all multiples of p , i.e. $p, 2p, \dots, p^{k-1}p$. Thus, finding $n(k)$ such that $p^{n(k)}|(p^k)!$ is equivalent to finding $n(k)$ such that $p^{n(k)}|p(2p)(3p) \cdots (p^{k-1}p)$. In other words, $n(k)$ must be the power of p dividing $p(2p)(3p) \cdots (p^{k-1}p) = (p^{k-1})! p^{k-1}$. Therefore

$$n(k) = n(k-1) + p^{k-1} \quad \text{or} \quad n(k) - n(k-1) = p^{k-1}.$$

Similarly, $n(k-1) - n(k-2) = p^{k-2}$ and so on. We write all these together as follows:

$$\begin{aligned} n(k) - n(k-1) &= p^{k-1}, \\ n(k-1) - n(k-2) &= p^{k-2}, \\ &\vdots \\ n(2) - n(1) &= p, \\ n(1) &= 1. \end{aligned}$$

Adding the above expressions along with the cancellations, we get

$$n(k) = 1 + p + \cdots + p^{k-1}.$$

Hence, the lemma. □

We shall need the following lemma.

Lemma 3.1.13

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 $\psi : S_m \rightarrow A$ by

$$\psi(\theta) = \begin{pmatrix} 1 & 2 & \cdots & m & m+1 & \cdots & n \\ 1\theta & 2\theta & \cdots & m\theta & m+1 & \cdots & n \end{pmatrix} \tag{3.6}$$

Then it is easy to verify that ψ is an onto isomorphism. Thus $A \approx S_m$. □

Lemma 3.1.14

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. $\psi : H \rightarrow x^{-1}Hx$ defined by $\psi(h) = x^{-1}hx$, ($h \in H$) is an onto isomorphism.

3. $\varphi : H \rightarrow xHx^{-1}$ defined by $\varphi(h) = xhx^{-1}$, ($h \in H$) is an onto isomorphism.

Proof. Proof in seminar. □

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. We prove the result by induction on k .

Step I: $k = 1$

If $k = 1$, then the p -cycle $(1, 2, 3, \dots, p) \in S_{p^1}$ and it has order p . Consequently, it generates a subgroup of order p . Since $n(1) = 1$, the result holds for $k = 1$.

Step II: Induction hypothesis: Suppose that the result is true for all integers up to $k - 1$, i.e. S_{p^r} has a subgroup of order $p^{n(r)}$ for all $r \leq k - 1$.

Now, we show that the result holds for k . Consider the following sets distributing the numbers $1, 2, \dots, p^k$.

$$\begin{aligned} & \{ \quad \quad \quad 1, \quad \quad \quad 2, \dots, \quad \quad \quad j, \dots, p^{k-1} \}, \\ & \{ \quad \quad \quad p^{k-1} + 1, \quad \quad \quad p^{k-1} + 2, \dots, \quad \quad \quad p^{k-1} + j, \dots, 2p^{k-1} \}, \\ & \{ \quad \quad \quad 2p^{k-1} + 1, \quad \quad \quad 2p^{k-1} + 2, \dots, \quad \quad \quad 2p^{k-1} + j, \dots, 3p^{k-1} \}, \\ & \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ & \{ (p-1)p^{k-1} + 1, (p-1)p^{k-1} + 2, \dots, (p-1)p^{k-1} + j, \dots, p^k \} \end{aligned}$$

Using this we define the following disjoint p -cycles $\sigma_1, \sigma_2, \dots, \sigma_{p^{k-1}}$ and σ as their product.

$$\begin{aligned} \sigma_1 &= (1, p^{k-1} + 1, 2p^{k-1} + 1, \dots, (p-1)p^{k-1} + 1). \\ \sigma_2 &= (2, p^{k-1} + 2, 2p^{k-1} + 2, \dots, (p-1)p^{k-1} + 2). \\ &\quad \vdots \\ \sigma_j &= (j, p^{k-1} + j, 2p^{k-1} + j, \dots, (p-1)p^{k-1} + j). \\ &\quad \vdots \\ \sigma_{p^{k-1}} &= (p^{k-1}, 2p^{k-1}, 3p^{k-1}, \dots, p^k). \end{aligned}$$

and

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_{p^{k-1}}.$$

Then σ has the following properties:

1. $\sigma^p = e$.

Reason: Note that $\sigma_1, \sigma_2, \dots, \sigma_{p^{k-1}}$ are disjoint p -cycles. So, that they commute. Also, $\sigma_j^p = e$ for all $j = 1, 2, \dots, k-1$. Hence $\sigma^p = \sigma_1^p \sigma_2^p \cdots \sigma_{p^{k-1}}^p = e$.

2. If τ is a permutation that leaves all $i > p^{k-1}$ fixed, i.e. $i\tau = i, \forall i > p^{k-1}$, then $\sigma^1 \tau \sigma^{-1}$ affects only elements in $\{p^{k-1} + 1, p^{k-1} + 2, \dots, 2p^{k-1}\}$.

More generally, $\sigma^j \tau \sigma^{-j}$ affects only elements in $\{jp^{k-1} + 1, jp^{k-1} + 2, \dots, (j+1)p^{k-1}\}$.

Reason: Verification left as a seminar exercise.

Now define

$$A = \{\tau \in S_{p^k} : i\tau = i \text{ for all } i > p^{k-1}\}.$$

Then by Lemma 3.1.1, $A \approx S_{p^{k-1}}$. By induction, A has a subgroup P_1 of order $p^{n(k-1)}$. Now, let

$$T = P_1(\sigma P_1 \sigma^{-1})(\sigma^2 P_1 \sigma^{-2}) \cdots (\sigma^{(p-1)} P_1 \sigma^{-(p-1)}) = P_1 P_2 \cdots P_{p-1} P_p,$$

where $P_{i+1} = \sigma^i P_1 \sigma^{-i}$, for $i = 0, 1, 2, \dots, p-1$. Then by Lemma 3.1.1, $P_1 \approx P_j$ for all $j = 1, 2, \dots, p-1$ and hence each of them has order $p^{n(k-1)}$. Observe (from property (2) of σ stated above) that, elements from distinct P_i 's affects disjoint sets of integers. Hence they commute with each other. Then by Lemma 1.2, T is a subgroup of S_{p^k} . Also since $P_i \cap P_j = \{e\}$ for $i \neq j$, by Lemma 1.2,

$$o(T) = o(P_1)o(P_2) \cdots o(P_{p-1}) = o(P_1)^p = p^{pn(k-1)}.$$

Since $\sigma^p = e$ and $P_i = \sigma^i P_1 \sigma^{-i}$, we have $\sigma T \sigma^{-1} = T$ (**Verify!**). Let

$$P = \{\sigma^j t \mid t \in T, 0 \leq j \leq p-1\} = \bigcup_{j=0}^{p-1} \sigma^j T.$$

Since $\sigma \notin T$, $\sigma^p = e$ and $\sigma T \sigma^{-1} = T$ (or $\sigma T = T \sigma$), we conclude that

1. P is a subgroup of S_{p^k} (**Verify!**).

$$2. o(P) = \sum_{j=0}^{p-1} o(\sigma^j T) = p \cdot o(T) = p p^{pn(k-1)} = p^{pn(k-1)+1}.$$

Note, that $n(k-1) = 1 + p + \cdots + p^{k-2}$. Therefore

$$\begin{aligned} pn(k-1) + 1 &= p[1 + p + \cdots + p^{k-2}] + 1 \\ &= [p + p^2 + \cdots + p^{k-1}] + 1 = n(k). \end{aligned}$$

Thus, $o(P) = p^{n(k)}$ and hence P is the p -Sylow subgroup of S_{p^k} . □

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 3.1.1, S_{p^k} has a p -Sylow subgroup. Hence, by Lemma 3.1.1, 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 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. \square

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.

Lemma 3.2.3

The number of p -Sylow subgroups in G is equal to $\frac{o(G)}{o(N(P))}$, where P is any p -Sylow subgroup of G . In particular, this number is a divisor of $o(G)$.

Proof. Let \mathcal{P} be the collection of all p -Sylow subgroups of G and $P \in \mathcal{P}$ be any p -Sylow subgroup of G . Since any two p -Sylow subgroups are conjugate to each other, every element of \mathcal{P} can be written of the form xPx^{-1} for some $x \in G$.

Let $N(P)$ denote the normalizer of P . Define $\phi : \mathcal{P} \rightarrow G/N(P)$ 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 $xPx^{-1}, yPy^{-1} \in \mathcal{P}$, 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. $xPx^{-1} \in \mathcal{P}$ 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 $P \cap xPx^{-1} \neq P$ is a proper subgroup of P and hence $o(P \cap xPx^{-1} \neq P) \leq p^{n-1}$. Therefore, $p^{n+1} | o(PxP)$.

Now, $P \cap xPx^{-1} \neq P \neq p \Rightarrow xP \neq Px \Rightarrow x \notin N(P)$. 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

$$p^{n+1} \left| \sum_{x \notin N(P)} o(PxP) \right|$$

Then we can write the second sum as

$$\sum_{x \notin N(P)} o(PxP) = p^{n+1}u \quad (\text{for some } u).$$

Therefore, $o(G) = o(N(P)) + p^{n+1}u$ and so

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}. \quad (3.7)$$

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, $p \left| \frac{p^{n+1}u}{o(N(P))} \right|$. 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 . \square

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 Simple group and Solvable group

Now we turn to what is called a solvable group. In passing we also define what is called a simple group.

Definition 3.3.1

A group G is said to be *simple* if it does not have any proper nontrivial normal subgroup.

Definition 3.3.2

A group G is called *solvable* if there exist subgroups N_0, N_1, \dots, N_r of G such that $G = N_0 \supset N_1 \supset \dots \supset N_r = \{e\}$ such that N_i is normal in N_{i-1} and N_{i-1}/N_i is abelian for every $i = 1, 2, \dots, r$.

Since every subgroup of a commutative group is normal, it follows directly from the definition that a commutative group is solvable.

Example 3.3.3. S_3 is solvable.

Solution. Let $N_1 = \{e, \psi, \psi^2\}$ and $N_2 = \{e\}$. Then $N_0 = S_3, N_1, N_2$ satisfy the requirement of the preceding definition. \square

3.4 Applications of Sylow's theorem

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 3.4.1. 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, we know that, the number of 11-Sylow subgroups in G is of the form $1 + 11k$. Also by Lemma 3.2, this number divides $o(G)$. Thus,

$$1 + 11k \mid 11^2 \cdot 13^2.$$

Note that $(1 + 11k, 11^2) = 1$ and therefore $1 + 11k \mid 13^2$. 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, 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, 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,

$$o(AB) = \frac{o(A)o(B)}{o(A \cap B)} = 11^2 \times 13^2 = o(G).$$

Finally, we show that G is abelian, by showing that 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. \square

Example 3.4.2. 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, 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, N must contain a non-trivial normal subgroup of G . Thus, G cannot be simple. \square

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 3.1.1, 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 order $5^2 \cdot 7 \cdot 11$.

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.

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.

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 4.1.1: External Direct Product

Let G_1, G_2, \dots, G_n be any n groups. Let

$$G = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}$$

be the Cartesian product of G_1, G_2, \dots, G_n , i.e. set of all ordered n -tuples. Then G is a group with componentwise multiplication defined by

$$(g_1, g_2, \dots, g_n)(g'_1, g'_2, \dots, g'_n) = (g_1g'_1, g_2g'_2, \dots, g_ng'_n).$$

We call this group G the *external direct product* of groups G_1, G_2, \dots, G_n .

Remark 4.1.2. 1. The product in the i th 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, \dots, e_n) , where e_i is the unit element in the group G_i . The inverse of the element (g_1, g_2, \dots, g_n) in G is given by $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$, i.e.

$$(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}).$$

3. In $G = G_1 \times G_2 \times \dots \times G_n$ let $\bar{G}_i = \{(e_1, e_2, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \mid g_i \in G_i\}$. 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 $G = \bar{G}_1 \bar{G}_2 \dots \bar{G}_n$ and every $g \in G$ can be uniquely written as $g = \bar{g}_1 \bar{g}_2 \dots \bar{g}_n$, where $\bar{g}_i \in \bar{G}_i$, $i = 1, 2, \dots, n$. (Verify!)

Here, we have realized G as an internal direct product of normal subgroups $\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n$. More precisely, we have the following definition.

Definition 4.1.3: Internal Direct Product

Let G be a group and N_1, N_2, \dots, N_n be normal subgroups of G such that

1. $G = N_1 N_2 \dots N_n$.
2. Every $g \in G$ can be uniquely written as $g = m_1 m_2 \dots m_n$, $m_i \in N_i$.

Then we say that G is the *internal direct product* of N_1, N_2, \dots, N_n .

Example 4.1.4. 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, $H_1 H_2 = H_2 H_1$ and hence $H_1 H_2$ 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

$$o(H_1 H_2) = \frac{o(H_1) o(H_2)}{o(H_1 \cap H_2)} = \frac{2 \cdot 2}{1} = 4 = o(G).$$

Thus, $G = H_1 H_2$. Observe that every element $g \in G$ can be uniquely written as $g = h_1 h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$ as follows:

$$e = e \cdot e, \quad a = a \cdot e, \quad b = e \cdot b, \quad c = a \cdot b.$$

Hence $G = K_4$ is internal direct product of its normal subgroups H_1 and H_2 defined above.

Example 4.1.5. Let G be a finite abelian group of order $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where p_1, p_2, \dots, 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 , \dots , 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, \dots, P_k (see Exercise 4.2).

Before we prove that external direct product and internal direct product are isomorphic, we have the following lemma.

Lemma 4.1.6

Suppose G is the internal direct product of N_1, N_2, \dots, 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 $e_i = e$. 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 $e_j = e$. Since G is internal direct product of N_1, N_2, \dots, N_n , every element $x \in G$ has a unique representation of the form $m_1 m_2 \cdots m_n$, 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 i th or the j th 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 and 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 $ab = ba$. \square

Remark 4.1.7. The converse of the above lemma is not true. That is if K_1, K_2, \dots, K_n are normal subgroups of G such that $G = K_1 K_2 \cdots K_n$ 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, \dots, K_n (see Exercise 4.3). **An example is already provided. Find another example yourself.**

A more stronger condition is needed for it to be true (see Exercise 4.4). **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 4.1.8

Let G be a group and suppose that G is the internal direct product of N_1, N_2, \dots, N_n . Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G is isomorphic to T .

Proof. Define the map $\psi : T \rightarrow G$ by

$$\psi((b_1, b_2, \dots, b_n)) = b_1 b_2 \cdots b_n,$$

where $b_i \in N_i$ for $i = 1, 2, \dots, n$. We show that ψ is an isomorphism of T onto G .

First we show that ψ is a homomorphism. Let $X = (a_1, a_2, \dots, a_n), Y = (b_1, b_2, \dots, b_n) \in T$. Then

$$\begin{aligned} \psi(XY) &= \psi((a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)) \\ &= \psi((a_1 b_1, a_2 b_2, \dots, a_n b_n)) \end{aligned}$$

$$= a_1 b_1 a_2 b_2 \cdots a_n b_n.$$

Since G is the internal direct product of N_1, \dots, N_n , by above lemma, $a_i b_j = b_j a_i$ for $i \neq j$. Thus,

$$\begin{aligned} a_1 b_1 a_2 b_2 \cdots a_n b_n &= a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n \\ &= \psi((a_1, a_2, \dots, a_n)) \psi((b_1, b_2, \dots, b_n)) \\ &= \psi(X) \psi(Y). \end{aligned}$$

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

$$\begin{aligned} \psi(X) &= \psi(Y) \\ \Rightarrow \psi((a_1, a_2, \dots, a_n)) &= \psi((b_1, b_2, \dots, b_n)) \\ \Rightarrow a_1 a_2 \cdots a_n &= b_1 b_2 \cdots b_n, \end{aligned}$$

where $a_i, b_i \in N_i$ for $i = 1, 2, \dots, n$. Since G is the internal direct product of N_1, \dots, N_n every element in G has a unique representation as product of elements from N_1, N_2, \dots, N_n . Therefore, $a_i = b_i$ for all $i = 1, 2, \dots, n$ and hence $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$, 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, \dots, N_n , $x = a_1 a_2 \cdots a_n$, where $a_i \in N_i$ for $1 \leq i \leq n$. But then $(a_1, a_2, \dots, a_n) \in T$ and $\psi((a_1, a_2, \dots, a_n)) = a_1 a_2 \cdots a_n = x$. Thus, ψ is onto. Hence ψ is isomorphism of T onto G , i.e. $T \approx G$. \square

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 $\phi : G \rightarrow G'$ 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 $n \mid m$. \square

Example 4.2.2. Let G be a group and A_1 be a subgroup of G . Then the map $\pi : G \rightarrow G/A_1$ defined by $\pi(b) = \bar{b} = bA_1$, $b \in G$, is a homomorphism.

Solution. Let $a, b \in G$. Then

$$\pi(a)\pi(b) = \overline{ab} = (aA_1)(bA_1) = abA_1 = \overline{ab} = \pi(ab).$$

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 (4.2), 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 be 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 $A_1 = \langle a_1 \rangle$. Then $o(A_1) = o(a_1) = p^{n_1}$. Let $b_2 \in G$ be such that its image (under the map $\pi : G \rightarrow G/A_1$), $\overline{b_2} = b_2A_1$ in G/A_1 has maximal order p^{n_2} , i.e. $o(\overline{b_2}) = p^{n_2}$. Then (by above two exercises) we have $o(\overline{b_2}) \mid o(b_2)$ and since a_1 has maximal order in G ,

$$p^{n_2} = o(\overline{b_2}) \leq o(b_2) \leq o(a_1) = p^{n_1}.$$

This gives $n_1 \geq n_2$. In order to write G as direct product of cyclic groups, we need $A_1 \cap \langle b_2 \rangle = \{e\}$. If this is true then we proceed further. However, this may not be the case, i.e. $A_1 \cap \langle b_2 \rangle \neq \{e\}$. 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. $b_2^{p^{n_2}} \in A_1 \cap \langle b_2 \rangle$. Then we have $b_2^{p^{n_2}} = a_1^i$ for some i . Therefore

$$a_1 i p^{n_1 - n_2} = (a_1^i)^{p^{n_1 - n_2}} = (b_2^{p^{n_2}})^{p^{n_1 - n_2}} = b_2^{p^{n_1}} = e.$$

Since $o(a_1) = p^{n_1}$, we have $p^{n_1} \mid i p^{n_1 - n_2}$. Now,

$$\begin{aligned} p^{n_1} \mid i p^{n_1 - n_2} &\Rightarrow p^{n_2} p^{n_1} \mid i p^{n_1} && (\because a \mid b \Rightarrow ac \mid bc) \\ &\Rightarrow p^{n_2} \mid i && (\because ac \mid bc \Rightarrow a \mid b) \\ &\Rightarrow i = j p^{n_2} \text{ for some } j. \end{aligned}$$

Substituting this value of i above, we get

$$b_2^{p^{n_2}} = a_1^i = a_1^{j p^{n_2}} \tag{4.1}$$

Take $a_2 = a_1^{-j} b_2$. Then a_2 is an required element such that $A_1 \cap \langle a_2 \rangle = \{e\}$. First observe that, by equation (4.1)

$$a_2^{p^{n_2}} = a_1^{-j} b_2^{p^{n_2}} = a_1^{-j p^{n_2}} b_2^{p^{n_2}} = e. \tag{4.2}$$

Claim 1: Let $A_2 = \langle a_2 \rangle$. Then $A_1 \cap A_2 = \{e\}$.

Suppose $a_2^t \in A_1$ for some t . Then

$$\begin{aligned}
 a_2^t \in A_1 &\Rightarrow (a_1^{-j}b_2)^t \in A_1 \\
 &\Rightarrow a_1^{-jt}b_2^t \in A_1 \\
 &\Rightarrow b_2^t \in A_1 && (\because a_1^{-jt} \in A_1) \\
 &\Rightarrow (b_2A_1)^t = b_2^tA_1 = A_1 && (\text{where } A_1 \text{ is the identity in } G/A_1) \\
 &\Rightarrow (\bar{b}_2)^t = A_1 && (\because \bar{b}_2 = b_2A_1) \\
 &\Rightarrow p^{n_2} \mid t && (\because o(\bar{b}_2) = p^{n_2}) \\
 &\Rightarrow t = sp^{n_2} \text{ for some } s.
 \end{aligned}$$

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 $A_1 = (a_1), A_2 = (a_2), \dots, A_k = (a_k)$ of order $p^{n_1}, p^{n_2}, \dots, p^{n_k}$ respectively with $n_1 \geq n_2 \geq \dots \geq n_k$ 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 4.4) G is the direct product of cyclic subgroups A_1, A_2, \dots, A_k . \square

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, \dots, 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

$$\begin{aligned}
 o(G) &= o(A_1)o(A_2) \cdots o(A_k) \\
 \Rightarrow p^n &= p^{n_1}p^{n_2} \cdots p^{n_k} = p^{n_1+n_2+\cdots+n_k} \\
 \Rightarrow n &= n_1 + n_2 + \cdots + n_k.
 \end{aligned}$$

Thus, n_1, n_2, \dots, 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, \dots, A_k and their generators a_1, a_2, \dots, 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 $H_1 = \langle a \rangle = \{e, a\}$, $H_2 = \langle b \rangle = \{e, b\}$ and $H_3 = \langle c \rangle = \{e, c\}$ be subgroups of G of order 2.

As seen in Example 4.1.4, $G = K_4$ 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 $A_i = \langle a_i \rangle$ 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 $B_1, \dots, B_t, A_{t+1}, \dots, A_k$ is contained in $G(p^m)$.

For this we begin by showing that A_{t+1}, \dots, 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

$$a_j^{p^m} = \left(a_j^{p^{n_j}}\right)^{p^{m-n_j}} = (e)^{p^{m-n_j}} = e \quad (\because o(a_j) = p^{n_j}).$$

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, \dots, 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 $B_1, \dots, B_t, A_{t+1}, \dots, A_k$ 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, \dots, 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

$$a_1^{\lambda_1 p^m} = e, \dots, a_k^{\lambda_k p^m} = e.$$

Since $o(a_i) = p^{n_i}$, we have $p^{n_i} \mid p^m$ for all $i = 1, 2, \dots, k$. 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

$$p^{n_i} \mid \lambda_i p^m \Rightarrow p^{n_i-m} \mid \lambda_i \Rightarrow \lambda_i = v_i p^{n_i-m} \quad \text{for some } v_i.$$

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, 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 $\phi : G \rightarrow G'$ 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

$$\phi(gh) = \phi\left(\left(a_1^{\alpha_1} \cdots a_k^{\alpha_k}\right)\left(a_1^{\beta_1} \cdots a_k^{\beta_k}\right)\right)$$

$$\begin{aligned}
&= \phi \left(a_1^{\alpha_1 + \beta_1} \cdots a_k^{\alpha_k + \beta_k} \right) && (\because G \text{ is direct product, by Lemma 4.1}) \\
&= (b'_1)^{\alpha_1 + \beta_1} \cdots (b'_k)^{\alpha_k + \beta_k} && (\text{by definition of } \phi) \\
&= ((b'_1)^{\alpha_1} \cdots (b'_k)^{\alpha_k}) \left((b'_1)^{\beta_1} \cdots (b'_k)^{\beta_k} \right) && (\because G' \text{ is direct product, by Lemma 4.1}) \\
&= \phi(g)\phi(h).
\end{aligned}$$

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 $i = 1, 2, \dots, k$ 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 $\alpha_1, \alpha_2, \dots, \alpha_k$, 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 4.6). 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 $C_r = (a_i^{p^m})$ is cyclic of order $p^{n_i - m}$. Thus, the invariants of H are $n_1 - m, n_2 - m, \dots, n_r - m$ 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 $D'_i = ((b'_i)^{p^m})$ is cyclic of order $p^{h_i - m}$. Thus, the invariants of H' are $h_1 - m, h_2 - m, \dots, h_{t-1} - m$ 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 exist i such that $n_i \neq h_i$, i.e. $n_i = h_i$ for all i . \square

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 $n_1 \geq \dots \geq n_k > 0$, $n = n_1 + \dots + n_k$ be a partition of n . Then let A_i be the cyclic group of order p^{n_i} and $G = A_1 \times \dots \times A_k$. Then G is an abelian group of order p^n with invariants n_1, \dots, 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 . \square

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 $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, where p_i are distinct primes and each $\alpha_i > 0$, is $p(n) = p(\alpha_1)p(\alpha_2) \dots p(\alpha_r)$.

Exercises

Exercise 4.1

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

$$(a_1, b_1)(a_2, b_2) := (a_1 a_2, b_1 b_2), \quad \forall (a_1, b_1), (a_2, b_2) \in G.$$

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 $\phi : A \rightarrow \bar{A}$ 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} .

Exercise 4.2

Show that G is isomorphic to the direct product of its Sylow subgroups.

Exercise 4.3

Give an example of a group G and normal subgroups N_1, \dots, 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, \dots, N_n .

Exercise 4.4

Prove that G is the internal direct product of the normal subgroups N_1, \dots, 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 $i = 1, 2, \dots, n$.

Exercise 4.5

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 4.6

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 4.7

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].

Exercise 4.8

Describe all the finite abelian groups of order

1. 2^6 .

2. 11^6 .

3. 7^5 .

4. $2^4 \cdot 3^4$.

Exercise 4.9

Show how to obtain all abelian groups of order $2^3 \cdot 3^4 \cdot 5$.

Exercise 4.10

Let G is an abelian group of order p^n with invariants $n_1 \geq \dots \geq n_k > 0$ and $H \neq \{e\}$ is a subgroup of G . Show that if $h_1 \geq \dots \geq h_s > 0$ are invariants of H , then $k \geq s$ and $h_i \leq n_i$ for each $i = 1, 2, \dots, s$.

Index

Symbols

p -Sylow subgroup 62

A

alternating group 43
 $A(S)$ 11
 automorphism 27
 inner 29
 outer 30

C

centralizer 45
 see also normalizer 45
 class equation 47
 conjugate
 of an element 43
 coset
 double 15, 65
 left 14
 right 14
 counting principle 18, 19
 cycle 35
 r -cycle 35
 disjoint 36
 length of 35
 of θ 37
 order of 35

E

element of a group
 inverse 10

F

First isomorphism theorem 23

function
 Euler's totient 17

G

Group
 solvable 73
 group 9
 abelian 9
 centre of 45
 commutative 9
 cyclic 13, 17
 identity of 9
 isomorphic 22
 non-abelian 10
 simple 73
 the factor 22
 the quotient 22

H

homomorphism 22
 automorphism 27
 isomorphism 22
 kernel of 22

I

isomorphic 22
 isomorphism 22

L

law
 associative 9

N

normalizer 45
 see also centralizer 45

O

operation	
associative	9
orbit	
of an element	37
order	
finite	17
infinite	17
of a group	16
of an element	17

P

partition	
of an integer	50
permutation	12, 34
cycle	35
cycle decomposition of	52
product	12
transposition	39

Q

quotient	22
----------------	----

R

relation

equivalence	36
-------------------	----

S

S_3	12
S_n	12, 34
subgroup	14
characterization	14
index of	16
left coset	14
normal	21
quotient by	22
right coset	14

T

Theorem	
Sylow	
first part, 62	
Cauchy	23
abelian, 23	
general, 50	
Cayley	31
Euler	17
Fermat	18
Langrage	16
Sylow	60
transposition	39