Project Report

On

APPLICATIONS OF GROUP THEORY

Submitted

In partial fulfilment of the requirement for the degree of

BACHELOR OF SCIENCE

In

MATHEMATICS

By

ASHNA K (AB23AMAT010)

Under the supervision of

Ms. ANNA SHEETHAL V S



DEPARTMENT OF MATHEMATICS AND STATISTICS

ST. TERESA'S COLLEGE (AUTONOMOUS)

ERNAKULAM, KOCHI – 682011

MARCH 2026

ST.TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

CERTIFICATE

This is to certify that the dissertation entitled, **APPLICATIONS OF GROUP THEORY** is a Bonafide record of the work done by **ASHNA K** under my guidance as partial fulfilment of the award of the degree of **Bachelor of Science in Mathematics** at St. Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Date:

Place: Ernakulam

Ms. Anna Sheethal V S

Assistant Professor,

Department of Mathematics and Statistics

St. Teresa's College (Autonomous)

ST. TERESA'S COLLEGE (AUTONOMOUS) DEPARTMENT OF MATHEMATICS AND STATISTICS ERNAKULAM

Dr. Elizabeth Reshma M T

Assistant Professor and Head,

Department of Mathematics and Statistics

ST. Teresa's College (Autonomous)

External Examiners

1:..... 30/01/26

2:.....

DECLARATION

I hereby declare that the work presented in this project is based on the original work done by under the guidance of Ms. Anna Sheethal V S, Assistance Professor, Department of Mathematics and Statistics, St. Teresa's College (Autonomous), Ernakulam and has not been included in any other project submitted previously for the award of any degree.

Place: Ernakulam

Date: 03/10/2025

Ashna

ASHNA K (AB23AMAT010)

ACKNOWLEDGEMENT

I take the opportunity to express my sincere gratitude towards Ms. Anna Sheethal V S of the Department of Mathematics and Statistics, St. Teresa's College (Autonomous), Ernakulam who encouraged me to carry out this work. Her continuous evaluable knowledgeable guidance throughout this study helped me to complete the work up to this stage. I will always be thankful to you in this regard. I also express my thanks to all those who have indirectly guided and helped me in the completion of this project.

Place: Ernakulam

Date: 03/10/2025

ASHNA K (AB23AMAT010)

CONTENTS

CERTIFICATE……2

DECLARATION……3

ACKNOWLEDGMENT……4

CONTENT……5

INTRODUCTION…….. 7

1 PRELIMINARIES

1.1 History of Group Theory…….……....…....8

1.2 Introduction to Algebraic Structures.……..8

1.3 Definition of a Group……...……..…….……..8

1.4 Importance of Group Theory…….……10

1.5 Applications of Group Theory……..……...10

1.6 Objectives of the Study…….…..…10

2 GROUP THEORY IN SUDOKU

2.1 Abstract……...…….……...…11

2.2 Introduction to Sudoku……...……...……11

2.3 Objectives. ……..……...11

2.4 Basics of Sudoku…….……..12

2.5 Method of Solving Sudoku using Group Theory

2.5.1Circular Permutation Algorithm to solve Sudoku …….. 12

2.5.2 Sudoku solving using Algebra and Group Theory……..……16

2.6 Significance……19

3 GROUP THEORY IN CRYPTOGRAPHY

3.1Abstract……...…20

3.2 RSA Algorithm……..……..……. 20

3.3 Diffie- Hellman Key exchange. ……...……..…….……..23

3.4 Hill Cipher…….……..……..25

3.5 Significance…….……..……26

4 COUNTING WITH BURNSIDE'S LEMMA

4.1 Colouring of points on a square using n colours…….……...…27

4.2 Colouring the corners of the Equilateral Triangle using k colours……..…29

4.3 Applying Burnside's Lemma to a 4 ×4 Sudoku…….…....30

4.4 Applying Burnside's Lemma to Tic -Tac –Toe……..……..…31

4.5 Significance……...….33

5 GROUP THEORY IN BIOLOGY

5.1 Abstract ……..…….…….……...…....34

5.2 DNA and Group Theory…….……..…..……...34

5.3 Group Theory and Protein……..……...…….……37

5.4 Significance……..…….…….…39

CONCLUSION……..……...…….……..…40

REFERENCE ……41

INTRODUCTION

Mathematics serves as a vital bridge connecting abstract concepts to practical applications in the real world. One of its most powerful branches, Group Theory, provides a systematic framework for studying symmetry, structure, and transformations. Though abstract in nature, group theory finds wide-ranging applications across diverse fields. In recreational mathematics, it plays a significant role in solving puzzles such as Sudoku, where the arrangement of numbers can be analysed through group actions. In the field of cryptography, group theory underpins some of the most important algorithms such as the RSA algorithm, the Diffie–Hellman key exchange, and the Hill cipher, ensuring the security of digital communication. Beyond puzzles and cryptography, the Burnside Lemma offers elegant solutions to counting symmetrical configurations, such as in games like tic-tac-toe. Furthermore, group-theoretic ideas extend into the natural sciences, with significant applications in biology, where symmetry and structural analysis help explain molecular organization and genetic patterns.

Thus, group theory is not merely an abstract mathematical discipline, but a unifying tool that bridges logic, security, recreation, and science.

MODULE 1

PRELIMINARIES

1.1 History of Group Theory

The origins of group theory can be traced back to the late 18th century, when mathematicians began studying permutations and their role in solving polynomial equations.

The development of group theory began with Joseph-Louis Lagrange in the 1770s, who studied permutations of equation roots. It was later advanced by Evariste Galois (1811–1832), who introduced the modern concept of a group while investigating the solvability of equations, giving rise to Galois Theory. In 1854, Arthur Cayley provided the first abstract definition of a group and introduced Cayley tables. Towards the end of the 19th century, Sophus Lie developed Lie groups to study continuous symmetries. Since then, group theory has grown into a central branch of mathematics with applications across science, technology, and puzzles.

1.2 Introduction to Algebraic Structures

Mathematics gradually shifts from dealing with numbers to studying structures that describe patterns and symmetries. In this transition, concepts like sets, relations, and operations become important.Group theory is one such powerful structure in abstract algebra. It provides a way to study symmetry, transformations, and patterns in a systematic manner.

1.3 Definition of a Group

A group is a set G with a binary operation $*$ such that:

1. Closure: For all a, b $\in$ G, $a * b \in$ G.
1. Associativity: $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$.
1. Identity element: There exist e $\in$ G such that $a * e = a = a * e$ for all $a \in G$.
2. Inverse element: For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.

Examples:

- Integers (Z_n , +) form a group (identity = 0, inverse = -n).
- Non-zero rational number $(Q,\times)$ form a group. (identity= 1, inverse = reciprocal).
- Rotational symmetries of a square (90°, 180°, 270°, 360°).

Types of Groups

- Finite and Infinite Groups
    - Finite Group: Has a limited number of elements. Example: Rotational symmetries of a square (D, order 8).
    - Infinite Group: Has infinitely many elements. Example: Integers under addition (Z, +).
- Cyclic Groups
    - Groups generated by a single element.
    - Every element can be expressed as powers of this generator.
    - Example: (Z, +) is cyclic.
- Permutation Groups
    - Groups whose elements are permutations (rearrangements) of a set.
    - Example: S_n, the symmetric group on n elements.
- Dihedral Groups
    - Groups of symmetries of regular polygons (rotations + reflections).
    - Example: D_4 for a square, $D_6$for a hexagon.
- Matrix Groups
    - Groups formed by matrices under multiplication.
    - Example:$GL_n(R)$, the group of invertible $n \times n$ real matrices.
- Subgroups
    - A smaller group inside a group.

Group Notation and Terminology

- Order of a group |G|: Number of elements.
- Subgroup: Smaller group within a group.
- Generator: Element that produces the whole group by repeated operation $< a >$.
- Permutation groups: Groups formed by rearranging elements, written in cycle notation.

  Example: (1, 2, 3) means 1→2, 2→3, 3→1.

1.4 Importance of Group Theory

Group theory holds a central place in mathematics because it provides a unifying language to study symmetry, structure, and transformations. It connects different areas of mathematics and serves as a foundation for advanced studies in algebra, geometry, and number theory. Beyond pure mathematics, group theory is valued because it:

- Simplifies complex problems by focusing on structure rather than individual cases.
- Provides tools to classify and analyze symmetries in nature and science.
- Bridges abstract concepts with practical applications in diverse fields.
- Acts as a gateway to modern topics such as Galois theory, ring theory, and representation theory.

1.5 Applications of group theory

Group theory is not just theoretical—it has applications everywhere:

- Mathematics: Study of equations, number theory, combinatorics, and abstract algebra.
- Symmetry: in geometry, art, crystals, and molecules.
- Puzzles: Rubik's cube, Sudoku, sliding puzzles.
- Computer science & cryptography: modular arithmetic in RSA encryption.
- Physics & chemistry: molecular structures, quantum mechanics.

Thus, group theory acts as a bridge between abstract mathematics and real-world applications.

1.6 Objectives of the Study

The objectives of this study are:

1. Secure Communication – To design encryption systems (RSA, Diffie–Hellman, ElGamal) based on group structures like cyclic groups.
2. Systematic Solving – To use group actions and permutations instead of trial-and-error methods.
3. Count Solutions & Patterns – To apply group theory (example: Burnside's Lemma) for counting distinct puzzle configurations.
4. To explore the wide applications of group theory, with special focus on puzzles like the Sudoku.
5. To emphasize the importance of group theory in mathematics and other scientific fields.

MODULE 2
GROUP THEORY IN SUDOKU

2.1 Abstract

Sudoku is a popular number-placement puzzle that can be analyzed and solved using mathematical concepts, particularly group theory. The $n \times n$ Sudoku grid exhibits structural symmetries, permutations, and algebraic constraints that make it an excellent application of abstract algebra. In this module, we explore two group theory–based approaches to solving Sudoku. The first approach uses algebra and group theory, where the puzzle is represented as a system of algebraic constraints and solved through group actions and transformations. The second approach applies the circular permutation algorithm, making use of cyclic groups to arrange and generate valid Sudoku patterns. Both methods highlight the importance of group theory in simplifying logical structures, reducing complexity, and providing systematic solutions to the Sudoku puzzle.

2.2 Introduction to Sudoku

Sudoku is a popular logic-based number puzzle. The goal is to fill a grid so that every number appears only once in each row, column, and small box.

Sudoku is popularly known as a Japanese puzzle. Sudoku, as we know it today, originated in the 1970s, created by Howard Gams, a retired architect and puzzle constructor. It was first published in 1979 by Dell Magazines in the US under the name "Number Place". The puzzle gained global popularity after being introduced to Japan by Nikoli Publishing in 1984, where it was renamed "Sudoku," a Japanese abbreviation of "Süji wa dokushin ni kagiru," meaning "the digits must be single".

2.3 Objectives:

- To explain the mathematical connection between Sudoku and group theory.
- To study the role of algebraic structures, permutations, and symmetries in Sudoku solving.
- To demonstrate the use of circular permutation and cyclic groups in generating valid Sudoku solutions.
- To highlight the importance of group theory in simplifying logical puzzles like Sudoku.

2.4 Basics of Sudoku

Standard Sudoku puzzle is a logic-based, number-placement puzzle. The objective is to fill a 9×9 grid with digits from 1 to 9, such that each column, each row, and each of the nine 3×3 sub grids (also called blocks or regions) contain all the digits from 1 to 9 without repetition.

Generalized Sudoku is like a regular Sudoku, but instead of a 9×9 grid (which is $3^2 \times 3^2$), it can be any size like $4 \times 4, 16 \times 16$ or more. The size is $n^2\ x\ n^2$, where n ≥ 2. Instead of just numbers, you can use letters, symbols, or anything else.

Rules

- Each row and column should have each symbol only once.
- The large square is made up of n x n small boxes, and each small box must also contain all the symbols once.

2.5 Methods of Solving Sudoku Using Group Theory

2.5.1 Circular Permutation Algorithm to solve Sudoku

This method shows how group theory can help to solve Sudoku puzzles of any size, using circular permutation in a logical way.

The elementary solution of one of these generalized Sudoku, with elements (symbols) from the set:

S = $\{S_1, S_2, \ldots\ldots, S_n, S_{n+1}, \ldots\ldots, S_{2n}, \ldots\ldots S_{n^2}\}$

Row 1: all elements in ascending order

$$S_1, S_2, \ldots\ldots, S_n, S_{n+1}, \ldots\ldots, S_{2n}, \ldots\ldots, S_{n^2}$$

On the next rows we will use circular permutations, considering groups of elements from the first row as follows:

Row 2:

$$S_{n+1}, S_{n+2}, \ldots\ldots, S_{2n};\ S_{2n+1}, \ldots\ldots, S_{3n}; \ldots\ldots, S_{n^2};\ S_1, S_2, \ldots\ldots, S_n$$

Row 3:

$$S_{2n+1}, \ldots\ldots, S_{3n}; \ldots\ldots, S_{n^2}; \ldots\ldots, S_1, S_2, \ldots\ldots, S_n;\ S_{n+1}, S_{n+2}, \ldots\ldots, S_{2n}$$

……

Row n:

$$S_{n^2-n+1}, \ldots\ldots, S_{n^2}; S_1, \ldots\ldots, S_n; S_{n+1}, S_{n+2}, \ldots\ldots, S_{2n}, \ldots\ldots, S_{3n}; \ldots\ldots, S_{n^2-n}$$

Now we start permutations of the elements of row considering groups of elements.

Row n + 1

$$S_2, \ldots\ldots, S_n, S_{n+1}; S_{n+2}, \ldots\ldots, S_n, S_{n+1}; S_{n+2}, \ldots\ldots, S_{2n}, S_{(2n+1)}; \ldots\ldots; S_{\ n^2-n+2}, \ldots\ldots, S_{n^2}, S_1$$

Row n + 2:

$$S_{n+2}, \ldots\ldots, S_{2n}, S_{2n+1}; \ldots\ldots; S_{n^2-n+2}, \ldots\ldots, S_{n^2}, S_1; S_2, \ldots\ldots S_n, S_{n+1}$$

……

Row 2n:

$$S_{n^2-n+2}, \ldots\ldots, S_{n^2}, S_1; S_2, \ldots\ldots, S_n, S_{n+1}; S_{n+2}, \ldots\ldots, S_{2n}, S_{2n+1}; \ldots\ldots$$

Row 2n + 1

$$S_3, \ldots\ldots, S_{n+2}; S_{n+3}, \ldots\ldots, S_{2n+2}; \ldots\ldots; S_{n^2+3}, \ldots\ldots, S_{n^2}, S_1, S_2$$

and so on…

Replacing the set S by any permutation of its symbols, which we'll note by *S*', and applying the same procedure as above, we will obtain a new solution.

2.5.1.1 EXAMPLE:

The group-permutation idea works for a 2×2 Sudoku, which is actually a 4×4 grid with 2×2 smaller boxes (because n = 2, so $n^2 \times n^2 = 4 \times 4$ and blocks are $n \times n = 2 \times 2$). Imagine we're using numbers 1, 2, 3, 4 for this smaller puzzle, so our set of symbols $S = \{1,2,3,4\}$.

Steps:

Step 1: Understand the setup for a $2x2$ Sudoku. Add a little bit of body text.

Step 2: Construct the First Row.

According to the algorithm, the first row contains all elements in ascending order. (1, 2, 3, 4).

Step 3: Use Circular Permutations to Create Subsequent Rows within the First "Block Row".

Row 2: The rule states to take the second group from the previous row first, followed by the first group. (i.e., 3, 4, 1, 2).

Step 4: Permute Elements within Groups for Subsequent "Block Rows".

Take each group from the original first row and apply a circular permutation (shifting each element one place to the left, and moving the first element to the end of its group):

From (1, 2) get (2, 1)

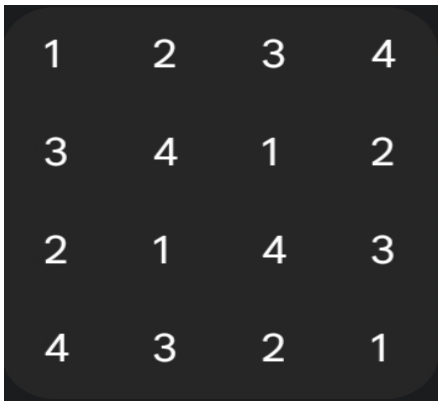
From (3, 4) get (4, 3)

Step 5: Create the Fourth Row using Circular Permutation of Groups from the Third Row.

Consider the third row as two groups: (2, 1) and (4, 3).

Swap the order of the group: 4, 3, 2, 1.

Final $2^2 \times 2^2$ Sudoku Grid



1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

The classical Sudoku is obtained for n = 3. (i.e., $3^2 \times 3^2 = 9 \times 9$ grid sudoku).

2.5.1.2 EXAMPLE:

Below example is the group-permutation algorithm for the classical case:

1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
2	3	4	5	6	7	8	9	1
5	6	7	8	9	1	2	3	4
8	9	1	2	3	4	5	6	7
3	4	5	6	7	8	9	1	2
6	7	8	9	1	2	3	4	5
9	1	2	3	4	5	6	7	8

2.5.2 Sudoku solving using Algebra and Group Theory

This introduces a formal, mathematical framework for solving Sudoku puzzles. Instead of relying on traditional methods like guesswork and exhaustive search (permutation), we leverage the concepts of group theory and abstract algebra. We show that a $n^2 \times n^2$ Sudoku grid can be modeled precisely as a system of algebraic equations operating over a finite group, offering a systematic approach to find the solution.

The set of symbols is $S = \{1, 2, \dots, n^2\}$.

Generalized Steps

I. Symbol Mapping:
   a) Map the symbols $S = \{1,2, \dots, n^2\}$ to the elements of the group $G = \{0,1, \dots, n^2 - 1\}$ under **addition modulo** n^2 (mod n^2). This is the group Z_{n^2}.
   b) A typical mapping might be: $k \rightarrow k - 1$.

II. Constraint Translation:

   a) For any complete row, column, or block with entries $(x_1, x_2, \dots, x_{n^2})$ the entries must be a permutation of G.
   b) Sum Constraint: The sum of the elements in G is,

$$x_1 + x_2 + \cdots + x_{n^2} \equiv \frac{[n^2(n^2 - 1)]}{2} (mod\ n^2)$$

   c) Product Constraints: The product of the element in G is,

$$x_1 . x_2 \dots \dots x_n^2 \equiv 0\ (mod\ n^2)$$

III. Equation Formation:

   a) Represent the blank cells with variable x_{ij}.
   b) Form a system of linear modular equations by applying the sum constraint to all n^2 rows, n^2 columns, n^2 blocks, substituting the values of the pre-filled cells.

IV. Solve Algebraically:

a) Solve the system of $3n^2$ equations with the unknown variables $x_{ij} \in G$ over the ring Z_{n^2}.
b) Apply the inverse mapping to get the final Sudoku solution.

This algebraic approach formalizes Sudoku solving as finding a solution to a system of equations, a powerful technique from abstract algebra.

2.5.2.1 EXAMPLE:

We illustrate the method using a $2^2 \times 2^2$ Sudoku puzzle and represent it as a system of algebraic equations over a finite group.

Steps:

Step 1: Symbols as numbers.

The standard digits {1, 2, 3, 4} used in the 4×4 Sudoku are mapped to the elements of the group G= {0,1,2,3} under addition modulo 4 (mod 4). This group is $\mathbb{Z}_4$, the integers modulo 4.

- $1 \rightarrow 0$
- $2 \rightarrow 1$
- $3 \rightarrow 2$
- $4 \rightarrow 3$

Step 2: Constraints as algebra.

The fundamental rules of Sudoku are translated into two types of algebraic constraints for any set of four entries (x_1, x_2, x_3, x_4) in a single row, column, or 2×2 block:

- Entries must be all different (Uniqueness Constraint): Since the set of entries must be a permutation of {1, 2, 3, 4}, their mapped values {x_1, x_2, x_3, x_4} must be a permutation of {1,2,3,4} in G.
- Sum of entries ≡ 2 (mod 4).
    - The Sum of the original digits 1+2+3+4 = 10 ≡ 2 (mod 4).
- The sum of the four entries in any complete row, column, or block must satisfy:

$$x_1 + x_2 + x_3 + x_4 \equiv 2 \ (mod\ 4)$$

- Product of entries ≡ 0 (mod 4).
    - The product of the mapped digits is 1×2×3×4 ≡ 0 (mod 4)
    - Therefore, the product of the four entries in any complete row, column, or block must satisfy:

$x_1 \times x_2 \times x_3 \times x_4 \equiv 0 \ (mod\ 4)$Step 3: Constructing Equations.The constraints are applied to the entries of the Sudoku grid, which has blanks represented by question marks (?). These blanks are treated as unknown variables.

- Example grid

? ? 2 ?

2 ? 0 ?

? 0 ? 2

? ? 1 ?

Note: The example grid uses {0, 1, 2, 3} as mapped digits, not {1, 2, 3, 4}.

- Forming Equations: For a row, say Row i with entries$(x_{i1}, x_{i2}, x_{i3}, x_{i4})$, the constraints generate the modular equations. For the given example, considering the first row's unknown entries (x_{11}, x_{12}, x_{13}, x_{14}).
- Sum equation: $x_{11} + x_{12} + x_{13} + x_{14} \equiv 2 \pmod 4$.
- Product equation: $x_{11} \cdot x_{12} \cdot x_{13} \cdot x_{14} \equiv 0 \pmod 4$.

A complete set of equations is generated by applying the constraints to all 4 rows, 4 columns, and 4 blocks. The values of the pre-filled cells are substituted into these equations.

Step 4: Solve algebraically

The system of linear and non-linear modular equations generated in Step 3 is solved systematically for the unknown variables. The solutions for the variables x_{ij} will be the elements of G = {1, 2, 3, 4}. Once the variables are solved, the 0 → 1, 1 → 2, 2 → 3, 3 → 4 inverse mapping is applied to fill the Sudoku grid with the original digits.

Final $2^2 \times 2^2$ Sudoku Grid



2.6 Significance

The study of Sudoku through group theory is significant because it connects recreational puzzles with abstract mathematics. By applying algebraic structures, permutations, and cyclic groups, Sudoku solving becomes more systematic and logical. This not only highlights the practical applications of group theory but also shows its importance in computer science, combinatorics, and problem-solving techniques beyond puzzles.

MODULE 3

GROUP THEORY IN CRYPTOGRAPHY

3.1 ABSTRACT

Cryptography is the mathematical science of securing communication, and group theory plays a fundamental role in its construction. The algebraic structures of groups, rings, and fields provide the backbone for many cryptographic algorithms. Classical ciphers such as the matrix cipher (hill cipher) rely on the concepts of invertible matrices and permutation groups, ensuring that messages can be systematically encrypted and decrypted. Modern public-key methods, including the RSA algorithm and the Diffie–Hellman key exchange, are deeply rooted in group theory. RSA depends on the multiplicative group of integers modulo n and Euler's totient function for key generation, while Diffie–Hellman uses the cyclic group structure of modular arithmetic to establish shared secret keys securely over public channels. Together, these systems highlight how abstract algebra, particularly group theory, provides the essential framework for both classical and modern cryptographic techniques, bridging pure mathematics with real-world data security.

3.2 RSA ALGORITHM

RSA Algorithm is an asymmetric or public-key cryptography algorithm which means it works on two different keys: Public Key and Private Key. The Public Key is used for encryption and is known to everyone, while the Private Key is used for decryption and must be kept secret by the receiver.

RSA Algorithm is based on factorization of large number and modular arithmetic for encrypting and decrypting data. It consists of three main stages:

1. Key Generation: Creating Public and Private Keys.
2. Encryption: Sender encrypts the data using Public Key to get cipher text.
3. Decryption: Decrypting the cipher text using Private Key to get the original data.

1. Key Generation

Choose two large prime numbers, say p and q. These prime numbers should be kept secret.

Calculate the product of primes, $n = p * q$. this product is part of the public as well as the private key.

Calculate Euler Totient Function $\Phi(n) = \Phi(p * q) = \Phi(p) * \Phi(q) = (p - 1) * (q - 1)$.

Choose encryption exponent e, such that $1 < e < \Phi(n)$, and $gcd(e, \Phi(n)) = 1$, that is e should be co-prime with $\Phi(n)$.

Calculate decryption exponent d, such that $(d * e) \equiv 1 \, mod \, \Phi(n)$, that is d is modular multiplicative inverse of e $mod \, \Phi(n)$.

We can have multiple values of d satisfying $(d * e) \equiv 1 \, mod \, \Phi(n)$ but it does not matter which value we choose as all of them are valid keys and will result into same message on decryption.

Finally, the Public Key = (n, e) and the Private Key = (n, d).

2. Encryption

To encrypt a message M, it is first converted to numerical representation. Now, use the public key (n, e) to encrypt the message and get the cipher text using the formula:

$C = M^e (mod \, n)$, C is the Cipher text and e and n are parts of public key.

3. Decryption

To decrypt the cipher text C, use the private key (n, d) and get the original data using the formula:

$M = C^d (mod \, n)$ here, M is the message and d and n are parts of private key.

Now, encrypt the message "**HELLO**" Using RSA algorithm.

Let's pick small primes:

p = 11, q = 13

n = p × q = 11 x 13 = 143

∅ (n) = (p - 1) (q - 1) = 10 × 12 = 120

Pick e such that $1 < e < \emptyset(n)$ and $gcd\ (e, \emptyset\ (n)) = 1$

Let's take e = 7

D is the modular inverse of e modulo p (n).

D. e ≡ 1(mod 120)

That means:

D. 7 = 1 (mod 120)

The solution is d = 103

We'll use simple mapping:

A = 1, B = 2……, Z = 26

So:

HELLO [8, 5, 12, 12, 15]

RSA encryption formula:

$C = M^e(mod\ n)$, Where M is the number (letter), C is the ciphertext.

For H = 8:

C = 8^7(mod 143) = 57

For E = 5:

C=5^7 (mod 143) = 47

For L = 12:

C =12^7 (mod 143) = 12

Again L = 12:

C = 12^7(mod 143) = 12

For O = 15

C = 15^7(mod 143) = 115

So, the cipher text is [57, 47, 12, 12, and 115]

RSA decryption formula:

Compute $M = C^d \ (mod\ n)$ on that ciphertext

57^{103} (mod143) = 8 → H

47^{103} (mod143) = 5 → E

12^{103} (mod143) = 12 → L

12^{103} (mod143) = 12 → L

115^{103}(mod143) = 15 → O

The RSA algorithm successfully encrypts and decrypts messages using modular arithmetic with public and private keys. In our example, the word "**HELLO**" was correctly recovered after encryption and decryption, demonstrating the reliability of RSA. In real applications, large prime numbers are used to ensure strong security.

3.3 DIFFE –HELLMAN KEY EXCHANGE

The Diffie-Hellman key exchange (also known as exponential key exchange) is a method for securely exchanging cryptographic keys over an insecure channel. It works by allowing two parties (Alice and Bob) to agree on a shared secret key without any other party being able to intercept the key or learn anything about it.

Two users (say Alice and Bob) agree on:

A prime number P

A primitive root (generator) g

These values are public.

Now, Alice chooses a secret a

Bob chooses a secret b

These numbers are kept secret.

Each computes a public key g^x(mod p).

Alice computes:

A= g^{as} (mod p)

Bob computes:

B= g^{ab} (mod p)

Alice sends A to Bob, and Bob sends B to Alice.

Now both compute the same secret key using each other's public value.

Alice computes:

S= B^a (mod p)

Bob computes:

S=A^b (mod p)

Both get the same shared secret.

Now, encrypt the message **"HELLO**" Using Daffier-Hellman key exchange.

p = 23

g = 5

a = 6

b = 15

A = 5^6(mod 23) = 8

B = 5^{15}(mod 23) = 19

Alice: S = 19^6(mod 23) = 2

Bob: S = 8^{15}(mod 23) = 2

So, the shared secret key = 2

Now, Map A= 1, Z= 26

Encrypting letters:

H (8) -- 8+2=10 → J

E (5) -- 5 +2=7 →G

L (12) -- 12+2=14 → N

L (12) -- 12 +2=14 → N

O (15) -- 15+2=17 → Q

Cipher text: JGNNQ

To decrypt subtract the shared secret key 2. We will get the message "**HELLO"**.

3.4 HILL CIPHER

The Hill cipher is a polygraphed substitution cipher built on concepts from Linear Algebra. The Hill cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses; hence, it is a more mathematical cipher than others.

We first convert the secret message into a string of numbers by arbitrarily assigning a number to each letter of the message. Next we convert this string of numbers into a new set of numbers by multiplying the string by a square matrix of our choice that has an inverse. This new set of numbers represents the coded message.

To decode the message, we take the string of coded numbers and multiply it by the inverse of the matrix to get the original string of numbers. Finally, by associating the numbers with their corresponding letters, we obtain the original message.

In the matrix cipher (Hill cipher) method, the plaintext is divided according to the size of the key matrix: pairs of letters for a 2×2 matrix and triplets of letters for a 3×3 matrix. The 2×2 matrix allows faster and simpler encryption but offers lower security due to smaller block size, whereas the 3×3 matrix increases security with more complex transformations, though calculations are slightly more involved. In both cases, the key matrix must be invertible modulo 26 to ensure that decryption is possible, highlighting the importance of algebraic structures in cryptography.

3.5 SIGNIFICANCE

Group theory is fundamental in cryptography, providing the algebraic structures that secure communication. The Hill cipher uses matrix groups for classical encryption; the RSA algorithm relies on modular arithmetic groups for secure public-key systems, and the Daffier-Hellman key exchange employs cyclic groups to establish shared secrets. These applications highlight the significance of group theory in building strong, reliable cryptographic methods for modern security

MODULE 4

COUNTING WITH BURNSIDE'S LEMMA

Introduction

Burnside's Lemma is a tool from group theory that helps count the number of distinct arrangements in problems like square colouring, triangle colouring, Sudoku and Tic Tac Toe, by removing duplicates caused by symmetry.

Burnside's Lemma

For a finite group G that acts on set$X$, let X/G be the set of orbits of$X$. Then, Burnside's Lemma states that

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Where,

G = finite group

X = set on which G acts

X/G = the set of orbits of X under g

g = One particular symmetry from group

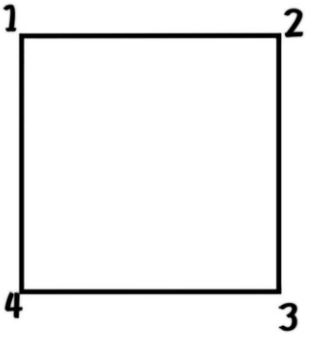
$|X^g|$ = number of elements of X fixed by g

4.1 Colouring of points on a square using n colors

Here, colourings that can be obtained from another through rotation are seen as the same. Similarly, one will set G to be the group of all rotations and reflections that can act on a square, and X to be the total number of ways to color the square, regardless of rotations.

To count $\sum_g \in G\ |X^g|$, there are 4 possible elements that act on: the identity (0°), 90° rotation, 180° rotation or 270° rotation (clockwise or counter clockwise).

Fig 4.1.1



- In identity case, the four vertices are obviously all fixed and there are n colors and 4 vertices,
  Cycles→ (1) (2) (3) (4) →4 cycles, so $|X^g|$ isn^4.
- In both the 90° and 270° rotation case, all four colours switched around, so the only way that for it to be a fixed point is for all the colours to be the same,
  Cycles → (1 2 3 4) → 1 cycle, so $|X^g| = n$
- In 180° rotation case, every vertex is switched with the one opposite to it, so as long as the two pairs of opposite vertices are of the same colour, the colouring will fixed under the 180° rotation. There are two pairs,
  Cycles→ (1 3) (2 4) → 2 cycles, so $|X^g| = n^2$

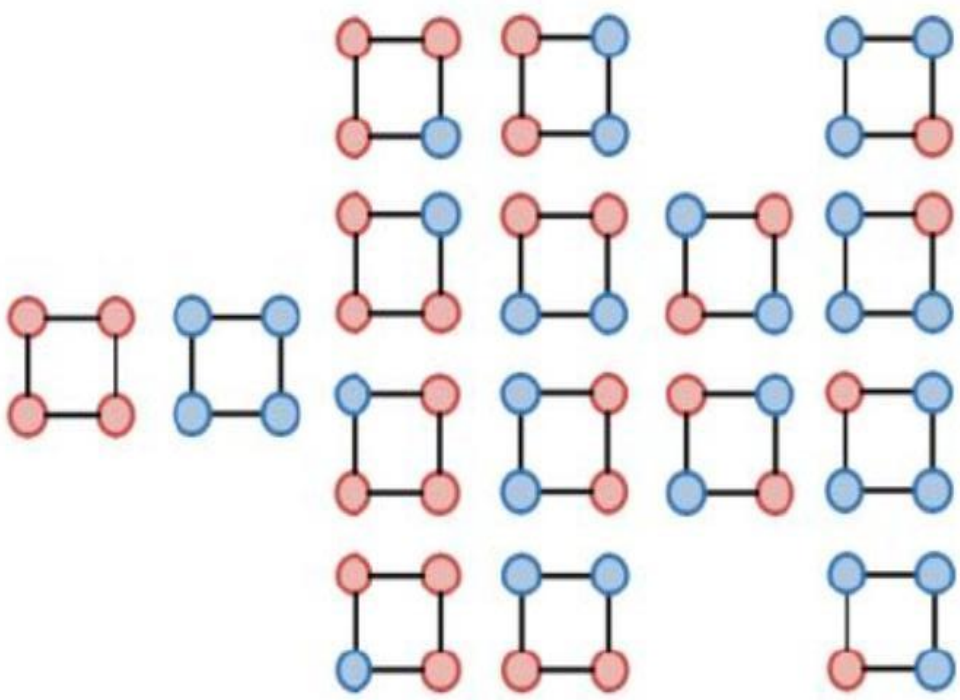
Therefore,

$$\frac{1}{|G|}\sum_{g\in G} |X^g| = \frac{1}{4}(n^4 + n^2 + n + n)$$

For example, if we are colouring the corners of square with two colours, so $n = 2$

That is,

$$\frac{1}{4}(2^4 + 2^2 + 2 + 2) = \frac{1}{4}(16 + 4 + 2 + 2) = 6$$



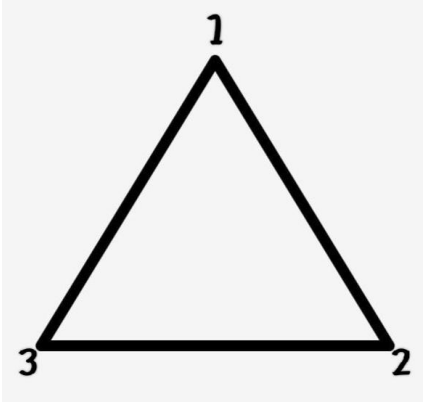
$Fig.$ 4.1.2 The coloring of four corners of a square with two colors

4.2 Colouring the corners of the equilateral triangle using k colors

We have an equilateral triangle and we want colour its 3 corners using k colors.

To count $\sum_{g} \in G \ |X^g|$, there are 6 possible elements that act on X: the identity (0°), 120° rotation, 240° rotation, and three reflections.

$Fig,$ 4.2.1



- In identity case, leaves all 3 vertices stays the same, cycles →(1)(2)(3)→3 cycles, $|X^g| = k^3$
- In both 120° and 240° rotation, the colouring to be invariant the colour at '1' must equal the colour at '2' and equal the colour at '3'. So all three must have the same colour, in 120°, cycles→ (1 2 3)→1 cycle and 240°, cycles→ (1 3 2), $|X^g| = k.\ ie, 2k$
- In reflection, it fixed one vertex and swap the other 2 vertices,
  Fix 1 and swap 2 and 3, cycles→ (1) (2 3)
  Fix 2 and swap 1 and 3, cycles→ (2) (1 3)
  Fix 3 and swap 1 and 2, cycles→ (3) (1 2)
  So, $|X^g| = k^2$, there are 3 reflections i.e., $3k^2$

Therefore,

$$\frac{1}{|G|}\sum_{g\in G} \quad |X^g| = \frac{1}{6}\,(k^3 + 2k + 3k^2)$$

When k = 2,

$$\frac{1}{6}(8 + 12 + 4) = \frac{24}{6} = 4$$

4.3 Applying Burnside's Lemma to a 4×4 Sudoku

Let $G = S_4$ = group of all permutations of the 4 symbols,

$$|G| = 4! = 24$$

In Burnside's Lemma, when you look at the identity symmetry the number of fixed grids is just the total number of valid 4x4 Sudoku solutions.

There are 288 valid 4x4 Sudoku solution grids.

The reason:

- First row – any permutations of (1, 2, 3, 4), that is 4! = 24 choices
- Second row – 12 valid choices
- Third row – 12 valid choices
- Fourth row – 1 choice
- Multiply – 24 x 12 x 12 x 1 = 288

Applying Burnside's Lemma

$$N_{distinct} = \frac{1}{|G|}\sum_{g \in G} |X^g|$$

- For the identity transformation, all Sudoku grids remain unchanged.
- For a 90° rotation, very few Sudoku grids remain unchanged.
- For digit relabelling, many can remain fixed depending on the permutation.

Identity permutation: $|X(e)| = 288$

Any non- identity permutation: $|X(g)| = 0$

$$\text{So, } N_{distinct} = \frac{1}{24}(288 + 0 + 0 + \cdots + 0)$$

$$= \frac{288}{24} = 12$$

4.4 Applying Burnside's Lemma to Tic TAC Toe

We want the number of legal Tic TAC Toe positions on 3 x 3 boards, where two positions are identified if one can be turned into the other by any symmetry of the square.

D_4 : 4 rotations + 4 reflections

Here $G = D_4(8\ elements)$ and $S =$ all legal Tic TAC Toe positions.

$X(g) =$ Number of elements of S fixed by symmetry g.

Counting $X(g)$ for legal positions:

1	**2**	**3**
4	**5**	**6**
7	**8**	**9**

- Identity
  Every cell maps to itself.
  Cycles: (1)(2)(3)(4)(5)(6)(7)(8)(9) – 9 cycles
  X (g) = 6046
- Rotation 90° clockwise
  Follow cell 1: 1 →3→9→7→1 – cycles (1 3 9 7)
  Follow cell 2: 2→6→8→4→2 – cycles (2 6 8 4)
  Centre 5 stays in place – cycles (5)
  Cycles: (1 3 9 7) (2 6 8 4) (5) → 3 cycles
  X (g) = 6
- Rotation 180°
  Follow cell 1: 1→9→1 – cycles (1 9)
  Follow cell 2: 2→8→2 – cycles (2 8)
  Follow cell 3: 3→7→3 – cycles (3 7)
  Follow cell 4: 4→6→4 – cycles (4 6)
  Centre 5 fixed – cycle (5)
  Cycles: (1 9) (2 8) (3 7) (4 6) (5) → 5 cycles
  X (g) = 54
- Rotation 270°
  Follow cell 1: 1→7→9→3→1 – cycles (1 7 9 3)
  Follow cell 2: 2→4→8→6→2 – cycles (2 4 6 8)
  Centre 5 fixed – cycles (5)
  Cycles: (1 7 9 3) (2 4 6 8) (5) → 3 cycles
  Same structure as 90°
  X (g) = 6

- Reflection about the vertical middle
  Pairs: 1→3, 4→6, 7→9 and fixed cells are 2, 5, and 8
  Cycles: (1 3) (4 6) (7 9) (2) (5) (8) → 6 cycles
  X (g) = 172
- Reflection about the horizontal middle
  Pairs: 1→7, 2→8, 3→9 and fixed cells are 4, 5, and 6
  Cycles: (1 7) (2 8) (3 9) (4) (5) (6) → 6 cycles
  X (g) = 172
- Reflection about main diagonal [top left – bottom right]
  Pairs: 2→4, 3→7, 6→8 and fixed cells are 1, 5, and 9
  Cycles: (2 4) (3 7) (6 8) (1) (5) (9) → 6 cycles

X (g) = 172

- Reflection about anti diagonal [top right – bottom left]
  Pairs: 1→9, 2→6, 4→8, and fixed cells are 3, 5, and 7

  Cycles: (1 9) (2 6) (4 8) (3) (5) (7) → 6 cycles
  X (g) = 172

Sum of $X(g)$ over all 8 group elements = 6800

Distinct legal positions up to symmetry = $\frac{1}{8}(6800) = 850$

4.5 Significance

Burnside's Lemma is significant in this project because it provides a systematic way to count distinct arrangements in problems involving symmetry. In square and triangle colouring, many colourings appear identical under rotations and reflections, and the lemma ensures that only the truly unique colourings are considered. Similarly, in Tic-Tac-Toe, different board positions can look the same when rotated or reflected, and Burnside's Lemma helps in counting only the distinct game states. In Sudoku, the enormous number of solution grids can often be reduced by noticing that many are equivalent under relabelling of digits or grid symmetries; here too, Burnside's Lemma allows us to calculate the number of essentially different solutions.

MODULE 5

GROUP THEORY IN BIOLOGY

5.1 ABSTRACT

Group theory, a branch of abstract algebra, provides a mathematical framework to describe symmetry and structure in biological systems. In DNA, the iconic double helix can be modelled using *helical symmetry groups*, which combine rotational and translational symmetries to explain its periodic structure. In proteins, group theory plays a central role in analysing folding patterns, quaternary structures, and functional assemblies. For instance, cyclic groups describe rotational symmetries in protein complexes. Thus, group theory acts as a bridge between mathematics and biology, offering powerful insights into the organization and function of DNA and protein structures.

5.2 DNA AND GROUP THEORY

The molecule that carries genetic instructions for the development, function, and reproduction of all living organisms. It has a twisted, ladder-like double helix shape, with its rungs made of paired chemical bases (adenine with thymine, and guanine with cytosine)

HOW GROUP THEORY COMES IN DNA

Provides mathematical tools to describe symmetries and patterns within DNA's structure and genetic code. DNA Double Helix Symmetry – DNA is shaped like a double helix, which means it repeats in a Spiral form.

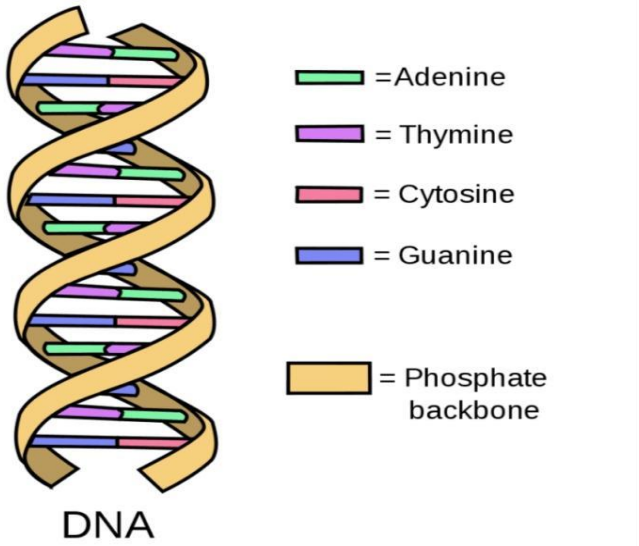


Fig 5.2.1

This spiral pattern can be described using helical groups (a combination of rotation + Translation). Example: Move a fixed distance along the axis (translation) and rotate by a fixed Angle → the structure looks the same. Group theory helps us mathematically describe these repeated symmetries.Step1 Imagine DNA as a spiral staircase, Each step = a base pair (A–T or G–C). To go from one step to the next, you must: 1. Rotate a fixed angle (about 36° in real DNA). 2. Move up a fixed Distance.

Step2 Define the 'moves', we call this move: T = (Rotate 36°) + (Move up one step)

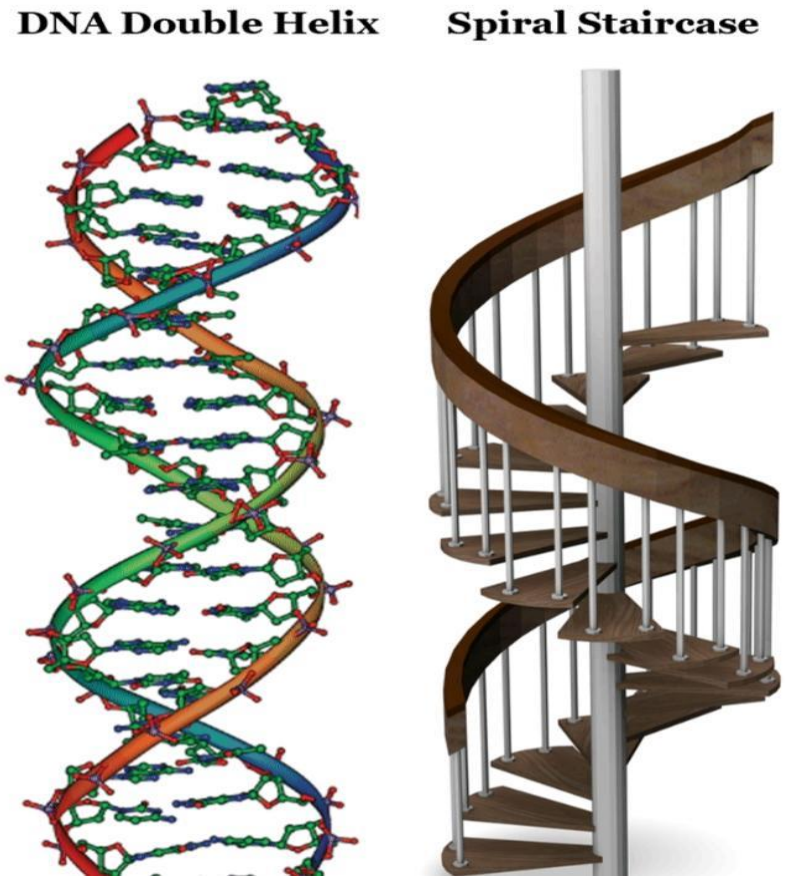


Fig 5.2.2

Step3 Repeat the move Apply T once → go from step 1 to step 2. Apply T twice → step 1 → Apply T 10 times → full 360° rotation, back to aligned position (but higher up). This repeating action forms a group (called helical group)

Step4 Group properties in DNA
Closure: Two moves in sequence stay in DNA's pattern.
Identity: Doing nothing (0° rotation, no shift) keeps you at the same step
Inverse: We can go backward (rotate -36° and move down)
Associativity: Combining moves works naturally. This is exactly the group structure.

5.3 GROUP THEORY AND PROTEIN

Protein is a vital macronutrient that's a building block for the body's bones, muscles, skin, cartilage, and blood. Group theory provides a mathematical language to describe and predict the symmetry of proteins.

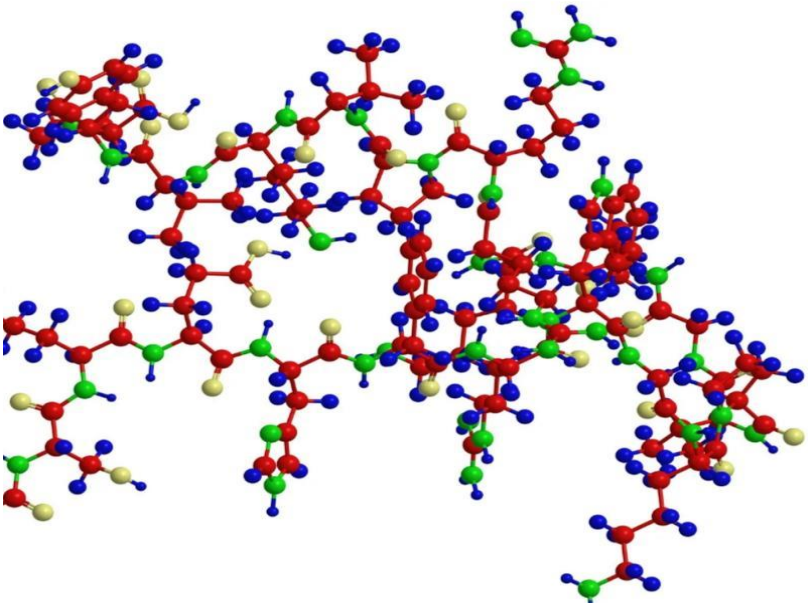


Fig 5.3.1

What is symmetry in a protein?

Many proteins are made of multiple, identical smaller protein units, called subunits. When these subunits come together, they often arrange in a repeating, symmetrical pattern.

Cyclic Symmetry

Cyclic symmetry (Cn) in proteins refers to the arrangement of identical subunits around a single axis of rotation, where the protein complex can be rotated by 360° around that axis to return to its original orientation.

ATP synthase

ATP synthase is a rotary molecular machine responsible for producing ATP in cells. Its Fo complex contains a ring of c-subunits, usually 10–14, which shows cyclic symmetry.

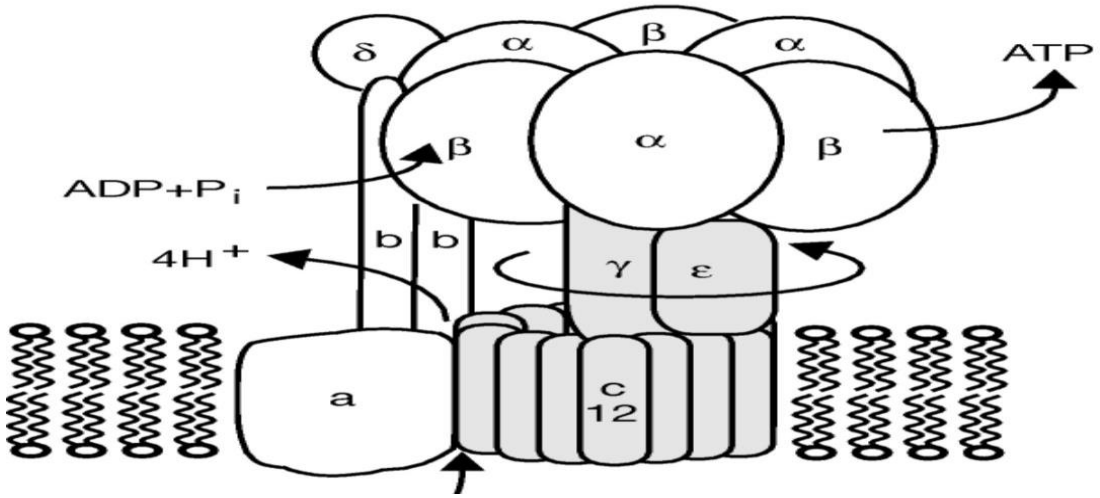


Fig 5.3.2

C12

Assuming 12 c-subunits, the ring has cyclic symmetry denoted as C12.Rotations of 30°, 60°, 90° … 330° map the structure onto itself. Think of it like a pizza of 12 slices, if we rotate the pizza by 30°, it looks the same. Group theory tells us the set of rotations that keep the pizza looking identical. ATP synthase's c-ring behave exactly like this, each "slice" is a protein subunit.



Fig 5.3.3

Group properties here come like:

Closure : Rotate by 30° then 90° rotation this is equivalent to a 120° which is still the part of this closure.
Identity : No rotation (0°) leaves the ring unchanged
Inverse : Rotating 30° forward can be undone by rotating 330° backward (360°-30°).

Associativity: Combining slices works naturally.

5.4 SIGNIFICANCE

Group theory offers a way to understand DNA and protein structures by analysing their underlying symmetries and algebraic relationships. Overall, group theory connects security, symmetry, problem-Solving, and innovation, making it a central pillar of modern Mathematics and its applications.

CONCLUSION

Starting from fundamental concepts, we explored how the abstract structures of groups can be applied to solve practical problems. In Sudoku, group theory helps analyse permutations and symmetries to understand solution strategies. In cryptography, it provides the foundation for secure encryption algorithms like RSA and Diffie-Hellman, ensuring safe communication through structured mathematical operations. The Burnside lemma further extends the power of group actions by simplifying complex counting problems, demonstrating how group theory reduces redundancy and reveals hidden patterns in combinatorial settings. In biology, group theory models molecular and structural symmetries, aiding in the study of chemical compounds and biological macromolecules. Overall, the study highlights how abstract algebraic concepts connect seamlessly to real-world applications, emphasizing the relevance and versatility of group theory across different disciplines.

REFERENCES

[1] Florentin Smarandache - A Group-Permutation Algorithm Permutation Algorithm to Solve the Generalized SUDOKU. [2] William Stallings, Cryptography and Network Security: Principles And Practice, Pearson.

[3] Tian Hao – Burnsides Lemma and its Application in Combinatorics Problems (2023)

[4] Jenny Jin – Analysis and Applications of Burnsides Lemma (2018)

[5] Michel Planat – DNA Sequence and Structure under the Prism of Group Theory and Algebraic Surfaces

[6] Ingemar Andre, Philip Bradley, Chu Wang, David Baker

