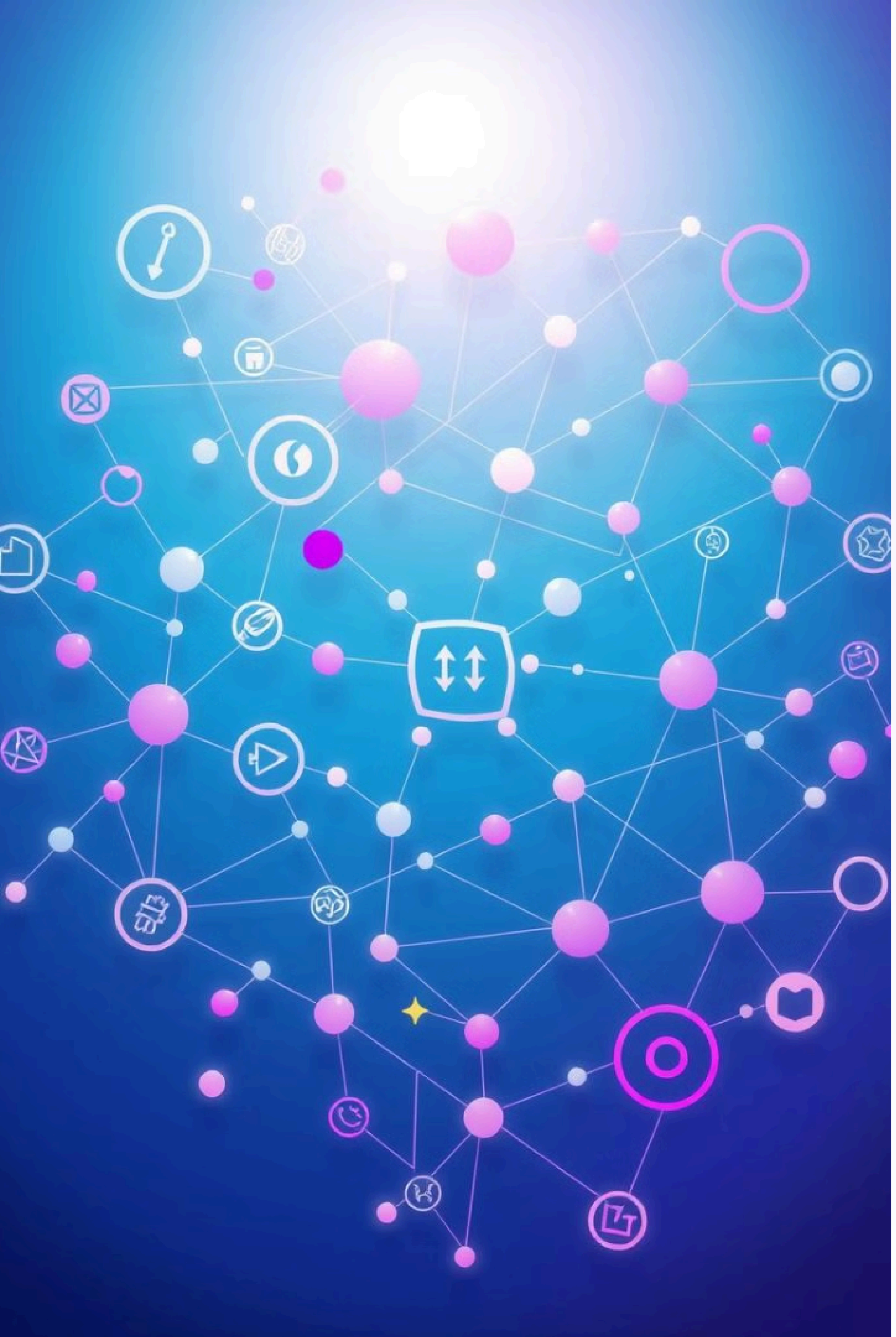
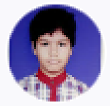


Introduction to Group

This presentation will introduce the fundamental concepts of group theory, an important branch of abstract algebra.



by Satangat

What is a group?

Definition

A group is a set with a binary operation that satisfies four axioms: closure, associativity, identity, and inverse.

Example

The set of integers under addition forms a group. The operation is addition, and the identity element is 0.

Closure

For all x, $y \in G$, the result of the operation, $x * y$, is also in G

Associativity

For all x, y, and $z \in G$, $(x * y) * z = x * (y * z)$

Identity

For any $a \in G$, if there exists an element $e \in G$ such that the equation $e * x = x * e = x$ holds, then 'e' is the identity element of 'G'

Invertibility

For any $x \in G$, if there exists an element $y \in G$ such that the equation $x * y = y * x = e$ holds, then 'y' is the inverse of 'x' in 'G.'

Group axioms and

1 **Closure**

The result of applying the operation to any two elements in the set is also in the set.

2 **Associativity**

The order of operations does not affect the result.

3 **Identity**

There exists an element that does not change the result when combined with any other element.

4 **Inverse**

For every element, there exists another element that, when combined with the first element, gives the identity element.

A Set of Integers ($\mathbb{Z}$) with Addition Operation

Closure: The sum of two integers is always an integer. Thus, the closure property holds.

Associativity: The addition of integers holds the associative property.

Identity: For all integers x ∈ G, 0 + x = x + 0 = x. Thus, 0 is an identity element of $\mathbb{Q}$ under multiplication.

Invertibility: For all integers x ∈ G, we get x + (-x) = (-x) + x = 0, where -x is an integer. Thus, -x is the inverse of x in $\mathbb{Z}$ under multiplication.

Hence, the set of integers ($\mathbb{Z}$) forms the group under addition.

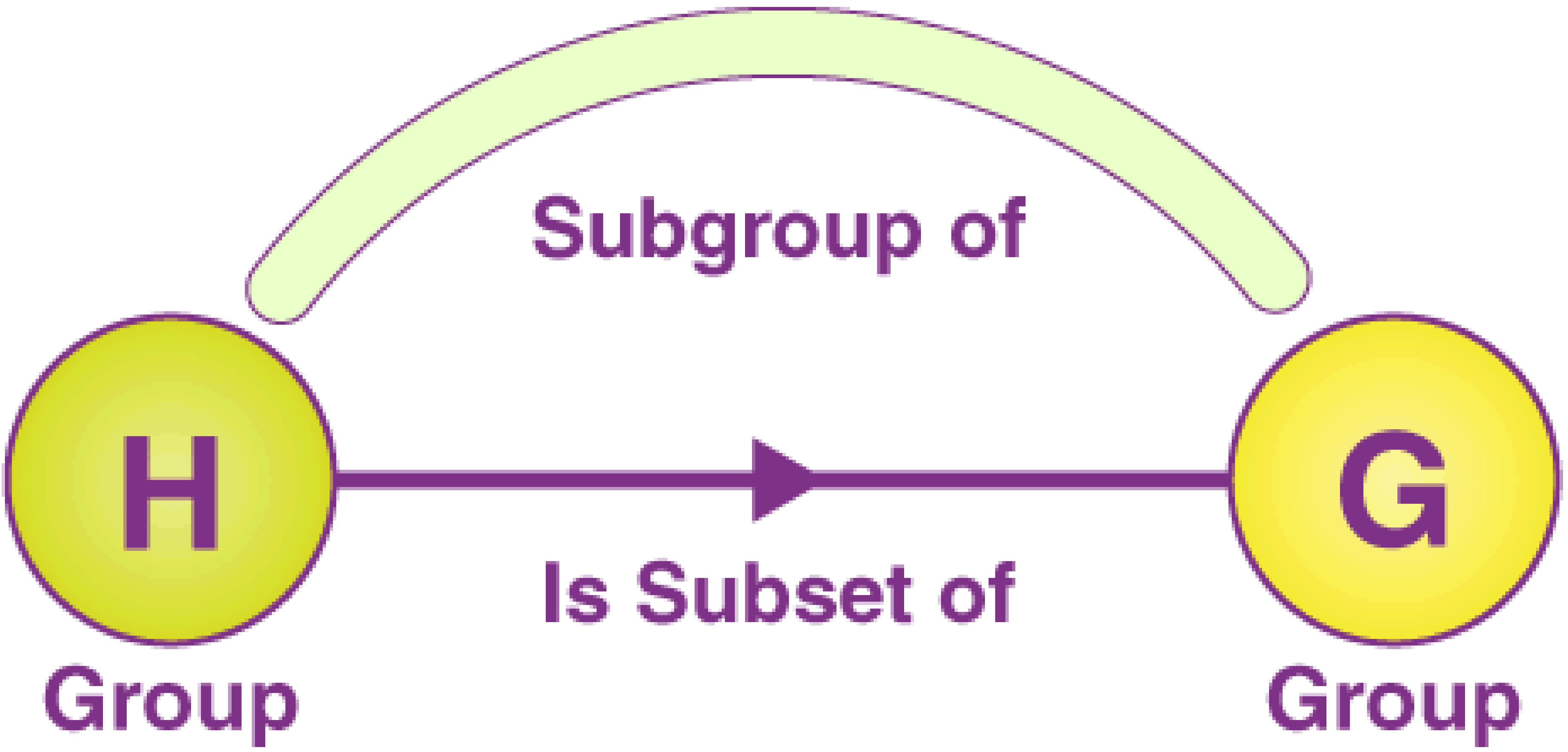
Subgroups and

Subgroups

Subsets of a group that themselves form groups under the same operation.

Cosets

Sets formed by multiplying all elements of a subgroup by a fixed element in the group.


Subgroup of
H
Is Subset of
G
Group
Group

Subgroups

A subgroup is a subset of a group but is also a group in itself.

If $(G, \ast)$ is a group and a non-empty set $H \subseteq G$ such that

- $e \in H$, where ‘e’ is the identity element of G
- If for all $x, y \in H$, $x \ast y \in H$
- If $x \in H$, $x^{-1} \in H$

Then, group H is a subgroup of G and $H \leq G$.

Lagrange’s group theory connects a group’s order to the order of its subgroups.

Cosets

If 'G' is a finite group and 'H' is a subgroup of 'G,' such that g ∈ G, then

gH = {gh: h ∈ H} is the left coset of 'H' in 'G' with respect to the element of 'G,' and Hg = {hg: h ∈ H} is the right coset of 'H' in 'G' with respect to the element of 'G.'

For example,

The 3-cycle (0, 1, 2) ∈ S_3 has order 3, so H = ⟨(0, 1, 2)⟩ equals to {e, (0, 1, 2), (0, 2, 1)}

Thus,

(1,2)H = {(1, 2), (1, 2) (0, 1, 2), (1, 2) (0, 2, 1)} = {(1, 2), (0, 1), (0, 2)}

(0, 1)H = {(0, 1), (0, 1) (0, 1, 2), (0, 1) (0, 2, 1)} = {(0, 1), (0, 2), (1, 2)}

We conclude that (1,2)H = (2,3)H.

Homomorphisms and isomorphisms

1

Homomorphism

A function between two groups that preserves the group operation.

2

Isomorphism

A bijective homomorphism between two groups.

Homomorphism

- If (G, •) and (H, *) are groups, then a function f:G→ H is a homomorphism if

$$f(x \bullet y) = f(x) * f(y) \text{ for all } x, y \text{ in } G$$

Example

- Let $f: \langle R, + \rangle \rightarrow \langle R^{+}, \cdot \rangle$ be the function such that $f(x) = e^x$

- Show f is a homomorphism.

$f(x+y) = f(x) \cdot f(y)$

$e^{x+y} = e^x \cdot e^y$ by properties of exponents

Isomorphism

- Bijective homomorphism
  - Let <G, +> and <H, *>
  - **Bijective-** f is one to one and onto
  - Homomorphism– $f(x + y) = f(x) * f(y)$ for all x, y in G

  - If <G, +> is isomorphic to <H, *> then we write

$$G \cong H$$

Example

$<Z_6, +> \rightarrow <Z_7-\{0\}, \bullet>$

$f(x) = 3^x$

x	0	1	2	3	4	5
f(x)	1	3	2	6	4	5

Take any 2 elements a and b

$$f(a)\bullet f(b) = 3^a \bullet 3^b$$

$$= 3^{a+b}$$

Lagrange's Theorem

1

Statement

The order of a subgroup divides the order of the group.

States that if ‘H’ is a subgroup of the finite group ‘G,’ then the order of ‘H’ divides the order of ‘G’

$$\boxed{\begin{array}{l} |H| \text{ divides } |G| \\ \Rightarrow |G|/|H| \text{ or } o(G)/o(H) \end{array}}$$

here,

$|H|$ or $o(H)$ = order of the subgroup H

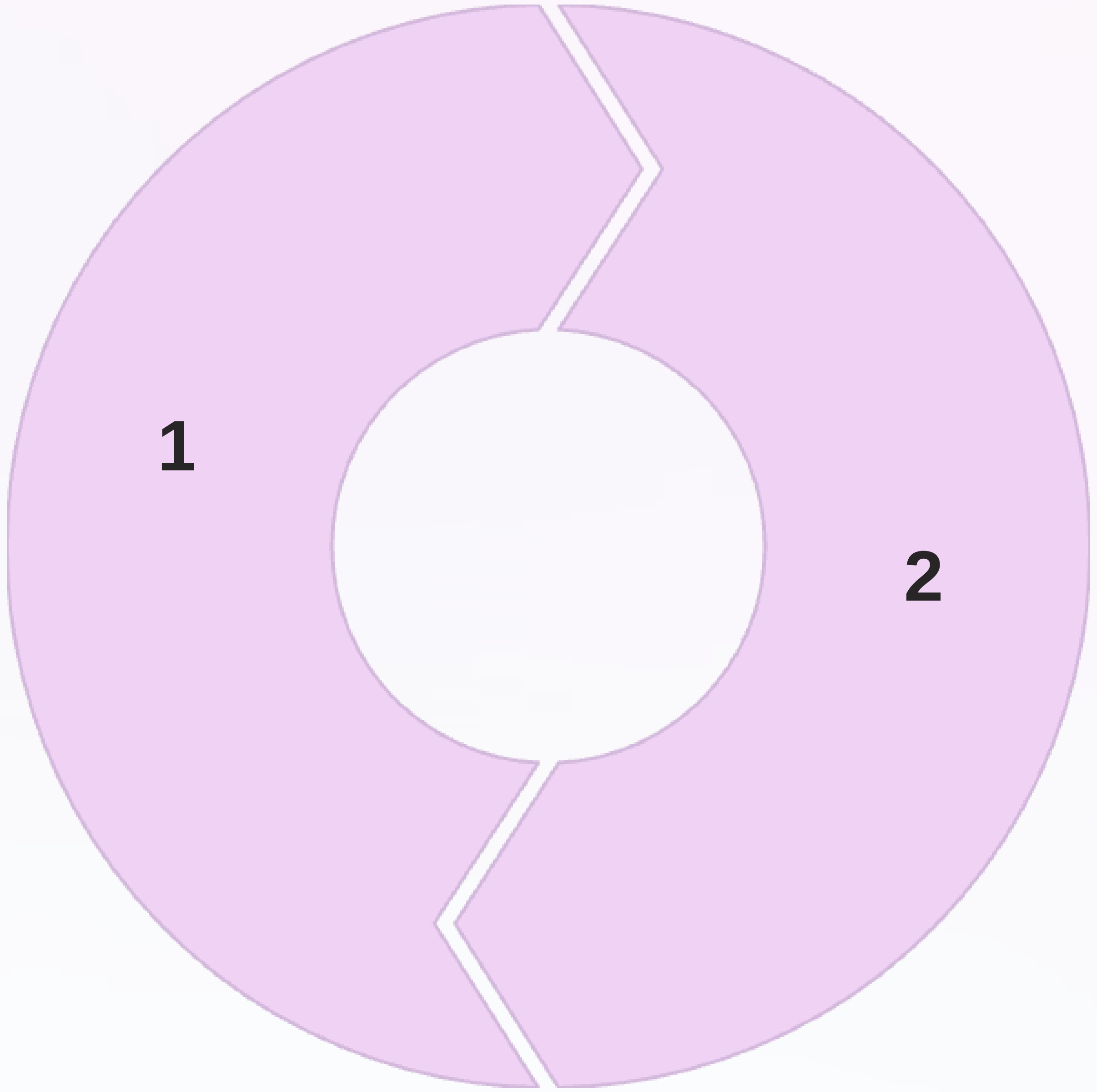
$|G|$ or $o(G)$ = order of the group G

Now Lagrange's theorem says that whatever groups $H \subset G$ we have, $|H|$ divides $|G|$. That's an amazing thing, because it's not easy for one number to divide another. For example, if we had a group $G1$ with $|G1| = 77$, then any subgroup of $G1$ could only have size 1, 7, 11 or 77.

Group actions

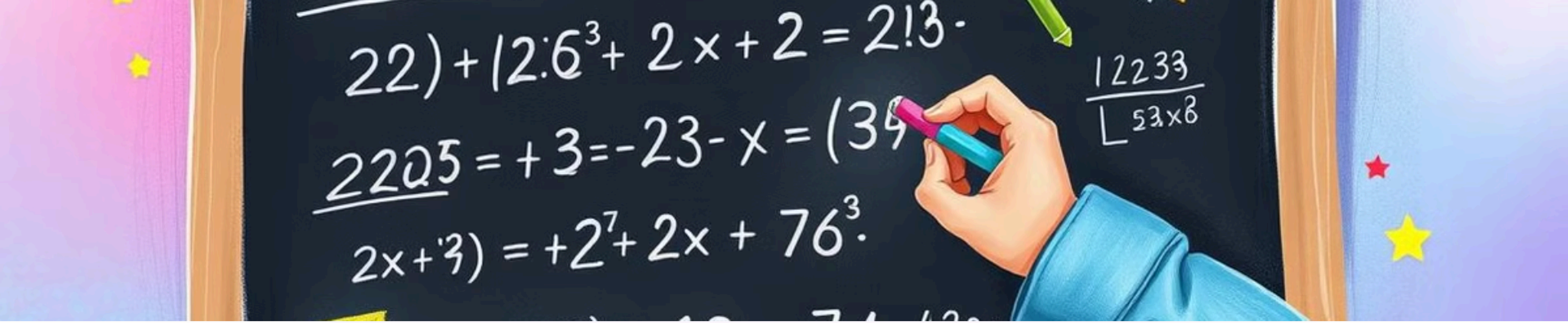
Definition

A group action is a way for a group to act on a set.



Example

The group of rotations of a square acts on the set of vertices of the square.



Sylow Theorems

Sylow p-subgroups

Subgroups whose order is a power of a prime number.

Existence

Every finite group has a Sylow p-subgroup for every prime p dividing the order of the group.

Conjugacy

All Sylow p-subgroups of a group are conjugate.

Applications of group

1

Cryptography

Group theory is used in public-key cryptography.

2

Physics

Used to study symmetries in physical systems.

3

Chemistry

Helps understand the structure of molecules.

Molecular structure and bonding

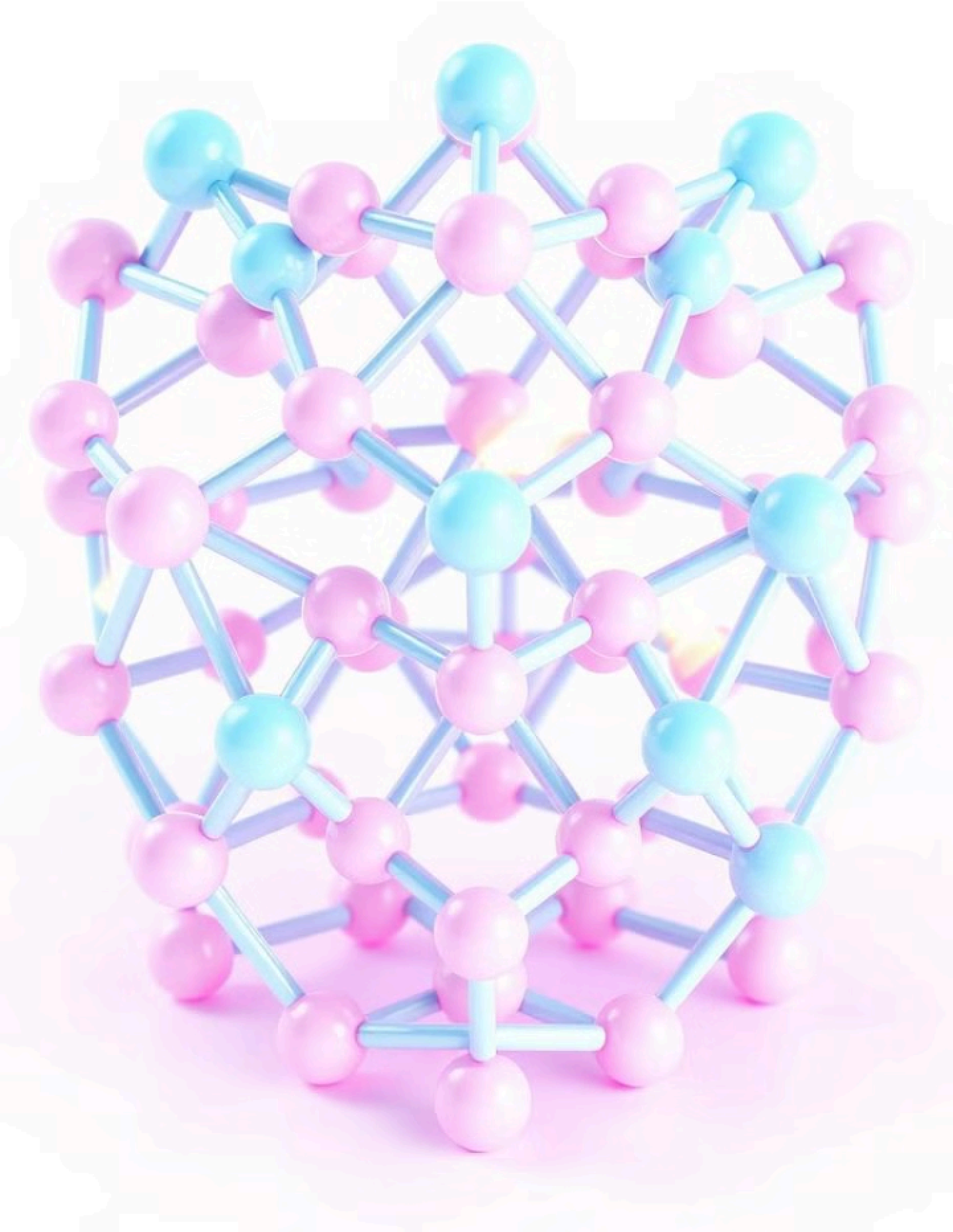
Group theory helps analyze the symmetry of molecules, predicting their properties and reactions.

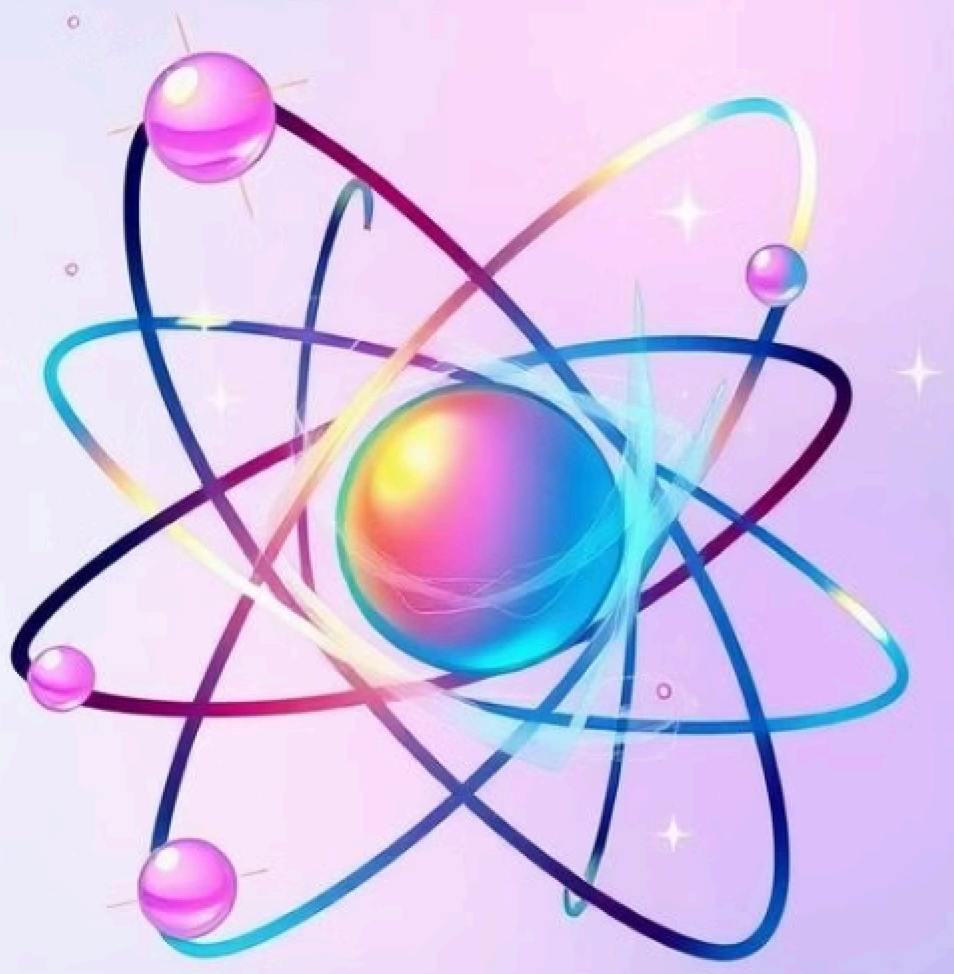
Understanding molecular symmetry is crucial in chemistry, enabling researchers to understand how molecules interact and form bonds.

Crystal structure and materials science

Group theory is used to classify and analyze crystal structures, which determine material properties.

It helps design materials with desired properties, like strength, conductivity, and optical characteristics.





Quantum mechanics and atomic structure

1. Group theory plays a critical role in understanding the symmetry of atoms and their behavior in quantum mechanics.
2. It helps predict the energy levels and transitions of electrons in atoms, explaining the periodic table and spectral lines.

Mathematical physics and particle theory

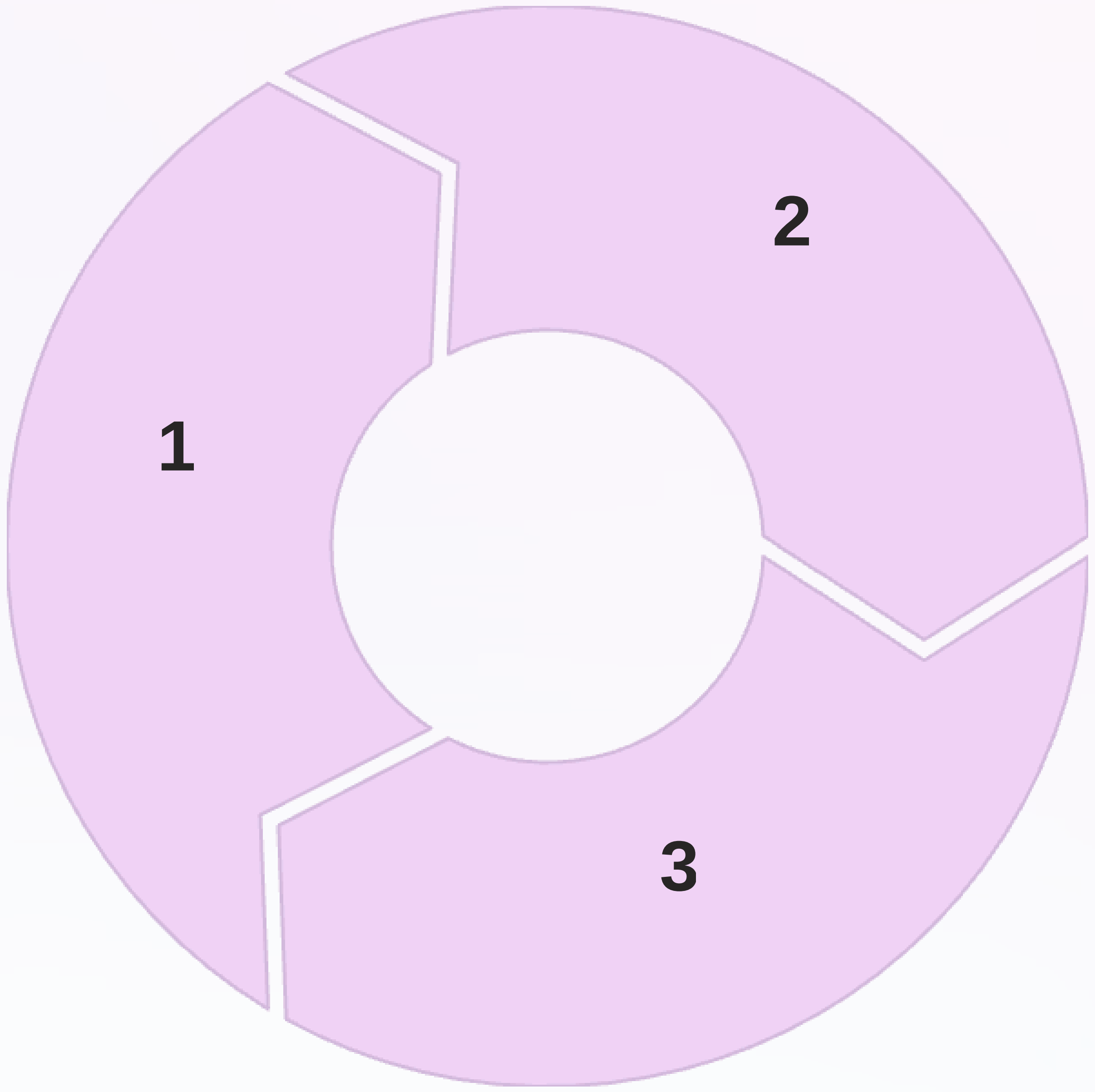
1. Group theory is widely used in mathematical physics, particularly in particle physics and quantum field theory.

2. It helps classify particles and their interactions, leading to the understanding of fundamental forces like the weak and strong forces.

Cryptography and coding theory

- Group theory is essential for designing secure encryption algorithms used to protect sensitive data.
- It enables the development of error-correcting codes for reliable communication, crucial in data transmission and storage.

Network analysis and graph



Structure

Understanding network structure

Flow

Analyzing data flow

Reliability

Assessing network resilience

Computer science and algorithms

1

Efficiency

Optimizing algorithms

2

Complexity

Analyzing algorithm performance

Thank you!