Group theory

In abstract algebra, **group theory** studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces, can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have influenced many parts of algebra. Linear algebraic groups and Lie groups are two branches of group theory that have experienced advances and have become subject areas in their own right.

Definition:

A group is a triple (G, m, e) consisting of the following.

(1) G is a set and $e \in G$ is an element.

(2) $m : G \times G \to G$ is a map such that $m(a, m(b, c)) = m(m(a, b), c)$.

(3) For all $g \in G$ we have $m(g, e) = m(e, g) = g$.

(4) For all $g \in G$ there is an h such that $m(g, h) = e$.

The element $e \in G$ is referred to as the identity of the group. The map m is referred to as the multiplication law, or the group law. Let us now see some examples of groups.

Subgroups

• instead of writing, “Let (G, m, e) be a group”, we will simply say that G is a group,

• the group multiplication will be obvious from the context and it will often be suppressed. For elements $a, b \in G$ we will simply write ab instead of $a \cdot b$ or $m(a, b)$,

• when we take products of 3 or more elements, associativity allows us not to worry about the order in which the multiplication is done. Thus, for example, we will simply write abc for $(ab)c = a(bc)$.

Algebraic Structure

A non empty set S is called an algebraic structure w.r.t binary operation (*) if it follows the following axioms:

Closure:(a*b) belongs to S for all $a,b \in S$.

Example:
`S = {1,-1} is algebraic structure under *`

`As 1*1 = 1, 1*-1 = -1, -1*-1 = 1 all results belong to S.`

But the above is not an algebraic structure under + as 1+(-1) = 0 not belongs to S.

Semi Group

A non-empty set S, (S,*) is called a semigroup if it follows the following axiom:

- **Closure:**(a*b) belongs to S for all a, b ∈ S.
- **Associativity:** a*(b*c) = (a*b)*c ∀ a, b ,c belongs to S.

Note: *A semi-group is always an algebraic structure.*
Example: *(Set of integers, +), and (Matrix ,*) are examples of semigroup.*

Monoid

A non-empty set S, (S,*) is called a monoid if it follows the following axiom:

- **Closure:**(a*b) belongs to S for all a, b ∈ S.
- **Associativity:** a*(b*c) = (a*b)*c ∀ a, b, c belongs to S.
- **Identity Element:** There exists e ∈ S such that a*e = e*a = a ∀ a ∈ S

Note: *A monoid is always a semi-group and algebraic structure.*
Example:
(Set of integers,*) is Monoid as 1 is an integer which is also an identity element.
(Set of natural numbers, +) is not Monoid as there doesn't exist any identity element. But this is Semigroup.
But (Set of whole numbers, +) is Monoid with 0 as identity element.

Group

A non-empty set G, (G,*) is called a group if it follows the following axiom:

- **Closure:**(a*b) belongs to G for all a, b ∈ G.
- **Associativity:** a*(b*c) = (a*b)*c ∀ a, b, c belongs to G.
- **Identity Element:** There exists e ∈ G such that a*e = e*a = a ∀ a ∈ G
- **Inverses:**∀ a ∈ G there exists a^{-1} ∈ G such that a*a^{-1} = a^{-1}*a = e

Note:

- *A group is always a monoid, semigroup, and algebraic structure.*
- *(Z,+) and Matrix multiplication is example of group.*

Abelian Group or Commutative group

A non-empty set S, (S,*) is called a Abelian group if it follows the following axiom:

- **Closure:**(a*b) belongs to S for all a, b ∈ S.
- **Associativity:** a*(b*c) = (a*b)*c ∀ a ,b ,c belongs to S.
- **Identity Element:** There exists e ∈ S such that a*e = e*a = a ∀ a ∈ S
- **Inverses:**∀ a ∈ S there exists a^{-1} ∈ S such that $a*a^{-1} = a^{-1}*a = e$
- **Commutative:** a*b = b*a for all a, b ∈ S

For finding a set that lies in which category one must always check axioms one by one starting from closure property and so on.

Here are some important results-

	Must Satisfy Properties
Algebraic Structure	Closure
Semi Group	Closure, Associative
Monoid	Closure, Associative, Identity
Group	Closure, Associative, Identity, Inverse
Abelian Group	Closure, Associative, Identity, Inverse, Commutative

Note:
Every abelian group is a group, monoid, semigroup, and algebraic structure.

Here is a Table with different nonempty set and operation:

```
N=Set of Natural Number
```

```
Z=Set of Integer
```

```
R=Set of Real Number
```

```
E=Set of Even Number
```

```
O=Set of Odd Number
```

```
M=Set of Matrix
```

+,-,×,÷ are the operations.

Set, Operation	Algebraic Structure	Semi Group	Monoid	Group	Abelian Group
N,+	Y	Y	X	X	X

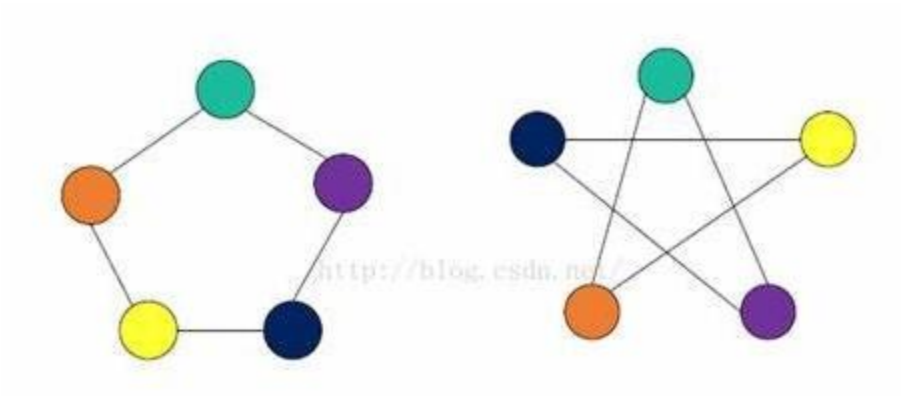
Set, Operation	Algebraic Structure	Semi Group	Monoid	Group	Abelian Group
N,-	X	X	X	X	X
N,×	Y	Y	Y	X	X
N,÷	X	X	X	X	X
Z,+	Y	Y	Y	Y	Y
Z,-	Y	X	X	X	X
Z,×	Y	Y	Y	X	X
Z,÷	X	X	X	X	X
R,+	Y	Y	Y	Y	Y
R,-	Y	X	X	X	X
R,×	Y	Y	Y	X	X
R,÷	X	X	X	X	X
E,+	Y	Y	Y	Y	Y
E,×	Y	Y	X	X	X
O,+	X	X	X	X	X

Set, Operation	Algebraic Structure	Semi Group	Monoid	Group	Abelian Group
O,×	Y	Y	Y	X	X
M,+	Y	Y	Y	Y	Y
M,×	Y	Y	Y	X	X

Isomorphism and homomorphism are concepts in mathematics.

- An isomorphism is a homomorphism that is also a bijection. It provides a perfect translation in both directions, with words corresponding one to one[12].
- A homomorphism is a “structure-preserving” map that can map many words in one language to the same word in another, effectively creating synonyms[1].
- A one-to-one group homomorphism is called a monomorphism. An onto group homomorphism is called an epimorphism. An isomorphism from a group G onto itself is called an automorphism[3].
- Isomorphism is a bijective homomorphism[4].
- Homomorphisms arise when one group is a subgroup of another or when one group is a quotient of another. The corresponding homomorphisms are called embeddings and quotient maps.

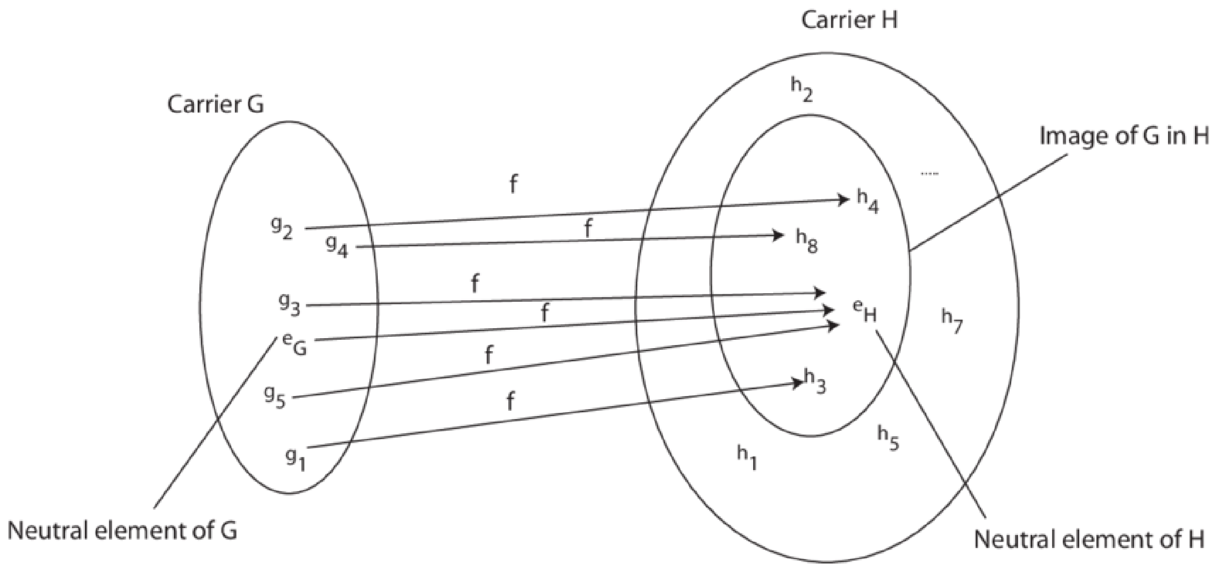
Isomorphism is a concept in mathematics that describes a structure-preserving mapping between two structures of the same type that can be reversed by an inverse mapping. Two mathematical structures are isomorphic if an isomorphism exists between them. Here are some examples of isomorphisms:



Graph Isomorphism

- **Logarithm and exponential**: The multiplicative group of positive real numbers and the additive group of real numbers are isomorphic. The logarithm function and the exponential function are homomorphisms that translate multiplication of positive real numbers into addition of real numbers, and vice versa. Since the logarithm function is bijective and has an inverse that is also a homomorphism, it is an isomorphism of groups.
- **Linear isomorphisms**: Linear isomorphisms between vector spaces are specified by invertible matrices .
- **Group isomorphisms**: Group isomorphisms between groups are defined for all algebraic structures. The classification of isomorphism classes of finite groups is an open problem.
- **Ring isomorphism**: Ring isomorphism between rings are defined for all algebraic structures.

Homomorphism is a concept in mathematics that describes a structure-preserving mapping between two structures of the same type that can be reversed by an inverse mapping. Homomorphisms are used to study the relationship between different algebraic structures . Here are some examples of homomorphisms:



- **Semigroup homomorphism**: A semigroup homomorphism is a map between semigroups that preserves the semigroup operation.
- **Monoid homomorphism**: A monoid homomorphism is a map between monoids that preserves the monoid operation and maps the identity element of the first monoid to that of the second monoid.
- **Group homomorphism**: A group homomorphism is a map between groups that preserves the group operation. This implies that the group homomorphism maps the identity element of the first group to the identity element of the second group, and maps the inverse of an element of the first group to the inverse of the image of this element .
- **Ring homomorphism**: A ring homomorphism is a map between rings that preserves the ring addition, the ring multiplication, and the multiplicative identity .

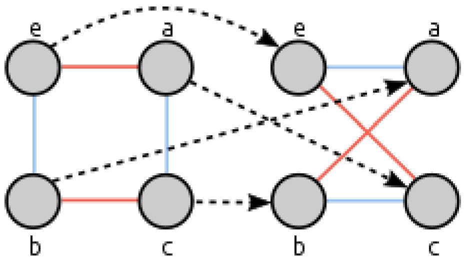
Definition:

A homomorphism is a function $\varphi: G \to H$ between two groups satisfying $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, b \in G$.

Note that the operation $a \cdot b$ is occurring in the domain while $\varphi(a) \cdot \varphi(b)$ occurs in the codomain.

Automorphism

In mathematics, an **automorphism** is an isomorphism from a mathematical object to itself. It is, in some sense, a symmetry of the object, and a way of mapping the object to itself while preserving all of its structure. The set of all automorphisms of an object forms a group, called the automorphism group. It is, loosely speaking, the symmetry group of the object.



$\phi(e) = e$
$\phi(a) = c$
$\phi(b) = a$
$\phi(c) = b$
$\phi = (acb)$

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

e	c	a	b
c	e	b	a
a	b	e	c
b	a	c	e

An automorphism of the Klein four-group shown as a mapping between two Cayley graphs, a permutation in cycle notation, and a mapping between two Cayley tables.

Integral domain

An **integral domain** is a nonzero commutative ring in which the product of any two nonzero elements is nonzero. In other words, it is a commutative ring with no zero divisors. Integral domains are generalizations of the ring of integers and provide a natural setting for studying divisibility .
Here are some equivalent definitions of integral domains:

- A nonzero commutative ring with no nonzero zero divisors.
- A commutative ring in which the zero ideal {0} is a prime ideal.
- A nonzero commutative ring for which every nonzero element is cancellable under multiplication.
- A ring for which the set of nonzero elements is a commutative monoid under multiplication (because a monoid must be closed under multiplication).
- A nonzero commutative ring in which for every nonzero element r, the function that maps each element x of the ring to the product xr is injective. Elements r with this property are called regular, so it is equivalent to require that every nonzero element of the ring be regular.
- A ring that is isomorphic to a subring of a field. (Given an integral domain, one can embed it in its field of fractions.)

Field:

In mathematics, a **field** is a set on which addition, subtraction, multiplication, and division are defined and behave as the corresponding operations on rational and real numbers do. A field is thus a fundamental algebraic structure which is widely used in algebra, number theory, and many other areas of mathematics.

Informally, a field is a set, along with two operations defined on that set: an addition operation written as $a + b$, and a multiplication operation written as $a \cdot b$, both of which behave similarly as they behave for rational numbers and real numbers, including the existence of an additive inverse $-a$ for all elements a, and of a multiplicative inverse b^{-1} for every nonzero element b. This allows one to also consider the so-called *inverse* operations of subtraction, $a - b$, and division, a / b, by defining:

$$a - b := a + (-b),$$
$$a / b := a \cdot b^{-1}.$$

Group theory is the study of symmetry and has many applications in various fields[123].Some examples of applications of group theory are[123]:

- Analyzing objects or systems that are invariant under transformations
- Solving Rubik’s cube using algorithms
- Expressing the fundamental symmetry of many physical laws using the Lorentz group

- Using harmonic analysis, combinatorics, algebraic topology, algebraic number theory, and algebraic geometry to solve mathematical problems
- Encrypting and decrypting messages using public key cryptography