5 Group Theory

Closure

A non-empty set G with operation * is said to be closed if $\forall$ a, b, $\in$ G, a * b $\in$ G

Example:

1. (N, +), Natural number is closed with respect to addition since
   $\forall$ a, b $\in$ N, a + b $\in$ N
2. (N, ×) Natural number is closed with respect to multiplication since
   $\forall$ a, b $\in$ N, a × b $\in$ N
3. (N, –) Natural number is not closed with respect to subtraction since
   $\forall$ a, b $\in$ N, a – b $\notin$ N for e.g. 3 $\in$ N, and 4 $\in$ N but 3 – 4 = –1 $\notin$ N.
4. Set of integers z is closed with respect to (+, ×, –).

Rack Your Brain

Is set of non-zero rational number Q_0 is closed with respect to {+, –}.

1. Which of the following satisfies closure property.

(A) a * b = a * b – 2020 $\forall$ a, b $\in$ z
(B) a * b = a + b – 2020 $\forall$ a, b $\in$ N
(C) a * b = a + b + 2021 $\forall$ a, b $\in$ N
(D) a * b = a^b $\forall$ a, b $\in$ N

Solution: (A), (C), (D)

- $\forall$ a, b $\in$ z, a * b – 2020 $\in$ z so closed.
- $\forall$ a, b $\in$ N, a + b – 2020 $\notin$ N so not closed.
  E.g. a = 1 $\in$ N, b = 2 $\in$ N. So, 1 + 2 – 2020 = – 2017 $\notin$N.
- $\forall$ a, b $\in$ N, a + b + 2021 $\in$ N so closed.
- $\forall$ a, b $\in$ N, a^b $\in$ N so closed.

Rack Your Brain

Check whether the following operations are closed or not.

1. a * b = a^b $\forall$ a, b $\in$ Q
2. a * b = a^b $\forall$ a, b $\in$ z

Note:

1. Set of vectors V is closed with respect to vector addition and cross product, but not with respect to the dot product.
2. Power set of a set A, i.e., P(A), is closed with respect to union, intersection and symmetric difference.

Binary operation:

- An operation * is said to be a binary operation on set G if a * b $\in$ G, $\forall$ a, b $\in$ G.
- A function f: G × G → G is said to be a binary operation, where G × G = {a, b | a $\in$ G and b $\in$ G}.

Algebraic structure:

- A non-empty set G along with one or more binary operations is called algebraic structure or algebraic system.
- If * is a binary operation, then (G, *) is said to be an algebraic structure.

Examples:

1. Set of natural numbers (N) with respect to addition is an algebraic structure (N, +).
2. (N, +, ×) is also an algebraic structure.
3. (Z, +, –, ×) is also an algebraic structure, where Z is a set of integers.

Note:
A non-empty set G is called an algebraic structure with respect to operation * if (a * b) $\in$ G $\forall$ a, b $\in$ G is satisfied closure property.

Groupoid or quasi group:

A non-empty set (G, *) is said to be groupoid if it satisfies the closure property.

Example: (N, +) is a groupoid.

Note:
An algebraic structure is also a groupoid.

Associative: A non-empty set G is associative with respect to * if.

a * (b * c) = (a * b) * c $\forall$ a, b, c $\in$ G.

Example: (N, +) satisfies associative property.

Semigroup: A non-empty set G is said to be semigroup with respect to * if it is satisfies.

1. Closure property
2. Associative property

Rack Your Brain

Is (N, –) is a semigroup?

Example: (N, +) is semigroup because

1. $\forall$ a, b $\in$ N, a + b $\in$ N so closure
2. $\forall$ a, b, c $\in$ N, a + (b + c) = (a + b) + c

Note:

- An algebraic structure (G, *) is a semigroup if it satisfies the associative property.
- Every semigroup is a groupoid, but the converse need not be true.

Identity element : A non-empty set G with * is a binary operation. If for every a $\in$ G, there exist an element e $\in$ G such that - $\boxed{a * e = e * a = a}$, then e is called the identity element in (G, *).

- If a * e = a, then e is called the right identity.
- If e * a = a, then e is called left identity.
- 'e' is called an identity element if both left and right identity exists.

2. Find identity element in a * b = $\frac{ab}{10}$ $\forall$ a, b $\in$ $R_{0,}$ where R_0 is a non-zero real number.

Solution:

Since $\forall$ a, b $\in$ R, a * b = $\frac{ab}{10}$ $\in$ R, So closure or *, is a binary operation.

Let e be the identity element.

a * e = e * a = a

Take right identity	Take left identity
a * e = a	e * a = a
$\frac{ae}{10} = a$	$\frac{ea}{10} = a$
e = 10 $\in$ R	e = 10 $\in$ R

Both left and right identity exists, and belong to the given domain (i.e., non-zero real number), so identity is 10.

Rack Your Brain

Find identity element in a * b = a^b $\forall$ a, b $\in$ N, where N is natural number.
Hint: (Only the right identity exists).

Monoid: A non-empty set G with operation *, is said to be monoid if it satisfies.

1. Closure
2. Associative
3. Identity

Rack Your Brain

Is (N, +) is a monoid?

Example: (z, +) is a monoid, where z is set of integers since,

1. $\forall$ a, b $\in$ z, a + b $\in$ z so closure.
2. $\forall$ a, b, c $\in$ z,
   a + (b + c) = (a + b) + c so associative.
3. $\exists$ e $\in$ G, $\forall$ a $\in$ G, a * e = e * a = a
   a + 0 = 0 + a = a. So 0 $\in$ z is an identity.
   So, (z, +) is a monoid.

Note:

- An algebraic structure (G, *) is a monoid if it satisfied associative and identity properties.
- An semigroup (G, *) is a monoid if it satisfies identity properties.
- G is a non-empty set, and * is an operation is called a loop if it satisfies closure and identity properties.
- Every monoid is a loop, but the converse need not be true.

Inverse property:

A non-empty set G with binary operation *, $\forall$ a $\in$ G $\exists$ b $\in$ G. Such that $\boxed{a * b = b * a = e}$,

where e is an identity element in G, then b is the inverse of a.

- If a * b = e, then b is called the right inverse of a.
- If b * a = e, then b is called the left inverse of a.

3. Find inverse in $a * b = \dfrac{ab}{10}$ $\forall$ a, b $\in$ R_0 (R_0 is a non-zero Real number).

Solution:

Since, identity e = 10 (calculated in identity example)

Let b is the inverse of a, i.e.

Let right inverse a * b = b * a = e

$$\begin{array}{l|l} a * b = e & b * a = e \text{ (left inverse)} \\ \dfrac{ab}{10} = 10 & \dfrac{ba}{10} = 10 \\ ab = 100 & ba = 100 \\ b = \dfrac{100}{a} \in R_0 & b = \dfrac{100}{a} \in R_0 \end{array}$$

$b = \dfrac{100}{a}$ is inverse of a.

Verification of inverse in the above problem:

a * b = e

$a * \dfrac{100}{a} = 10$

$\dfrac{a \cdot \dfrac{100}{a}}{10} = 10$

10 = 10

Rack Your Brain

Find inverse in a * b = a + b – ab $\forall$ a, b $\in$ Q – {–1}. Where Q is a rational number?

Group: A non-empty set G with operation *, is said to be group if it satisfies.

(A) Closure (B) Associative
(C) Identity (D) Inverse

Example: (z, +) is not only monoid, but also a group. Since $\forall$ a $\in$ G $\exists$ b $\in$ G such that

a * b = b * a = e

a + (–a) = (–a) + a = 0

Rack Your Brain

Is (Z, ×) is a group?

So the inverse of a is (–a); therefore, (z, +) is a group.

Note:

- A monoid (G, *) is a group if it satisfies the inverse property.
- Every group is a monoid, semigroup, and groupoid, but the converse need not be true.

Commutative property: A non-empty set G with respect to the operation * is said to be commutative.

If $\forall$ a, b $\in$ G a * b = b * a

Example: (N, +) is commutative.

Rack Your Brain

Is (Z, ×) is an abelian group?

Abelian group: A group (G, *) is said to be the Abelian group if it satisfies the commutative property.

Example: (Z, +) is not only a group, but also an abelian group since ∀ a, b ∈ Z a + b = b + a.

So it is commutative; hence (Z, +) is abelian.

Previous Years' Questions

Consider the set Σ* of all strings over the alphabet Σ = {0, 1}. Σ* with the concatenation operator for strings **[GATE CS 2003]**

(A) Does not form a group

(B) Forms a non-commutative group

(C) Does not have a right identity element

(D) Forms a group if the empty string is removed from Σ*

Solution: (A)

Previous Years' Questions

Let A be the set of all non-singular matrices over the real number, and let * be the matrix multiplication operation. Then

(A) A is closed under *, but (A, *) is not a semigroup

(B) (A, *) is a semigroup but not a monoid

(C) (A, *) is a monoid but not a group

(D) (A, *) is a group but not an abelian group

Solution: (D)

Previous Years' Questions

Some group (G, o) is known to be abelian. Then, which one of the following is true for G?

(A) $g = g^{-1}$ for every $g \in G$

(B) $g = g^2$ for every $g \in G$

(C) $(goh)^2 = g^2oh^2$ for every $g, h \in G$

(D) G is of finite order

Solution: (C)

Types of groups:

Group can be divided into two types.

1. Finite group
2. Infinite group

Finite and infinite group:

In a group G, if the number of elements is finite, the group is called finite; otherwise infinite group.

Order of group:

- The number of elements in a finite group is called the order of the group. It is represented by |G| or O|G|.

Example: G = {1, –1} is a group with respect to multiplication and 0(G) = 2.

- An infinite group has infinite order.

Example: (Z, +) is an infinite group and O(Z) = ∞.

Properties of a Group:

Let (G, *) is a group, then

1. In a group, the identity element is unique.
2. The inverse of every element in a group is unique.
3. In a group, the Identity element has its own inverse.
4. In a group, $\forall a \in G\ (a^{-1})^{-1} = a$ (i.e., The inverse of an element is equal to the element).
5. The inverse of the product of two elements of a group G is the product of the inverse in reverse order, ∀ a, b ∈ G $(ab)^{-1} = b^{-1}\ a^{-1}$.

6. In a group, if every element has its own inverse, then it is an abelian group, but the converse need not be true.
7. In a group G with multiplicative operation $\forall$ a $\in$ G, a^2 = e where e is the identity in G, then G is called an abelian group.
8. In an abelian group of odd order with respect to multiplication, the product of all elements in a group must be an identity element.
9. In an abelian group of odd order with respect to addition, the sum of all elements in a group G is an identity element.
10. Every group of prime order is always abelian.
11. Every group of the order less than 6 is always abelian (The smallest non-abelian group is of order 6).

Addition Modulo m:

Let a, b $\in$ z, and m is a fixed positive integer, r is a non-negative remainder then addition module m of (a, b) is denoted by a $+_m$ b, and it can be defined as a $+_m$ b = r, where $0 \le r < m$, r is a remainder obtained by dividing a + b with m.

Example: $3 +_2 4 = 1$

$3 +_2 (-4) = 1$

Solved Examples

1. Consider the set G = {0, 1, 2} under addition modulo 3. Is G an abelian group?

Solution:

G = $\{0, 1, 2\}_{+3}$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(Composition table)

- Since all the elements of the composition table belong to a given set, therefore closed.
- $(0 +_3 1) +_3 2 = 0 +_3 (1 +_3 2)$, so associative.
- In the composition table, the first-row element appearing against 0 is called the identity element.
- $(0)^{-1} = 0$ $(1)^{-1} = 2$ $(2)^{-1} = 1$, every element has a unique inverse.

So, G is a group.

Since in the composition table, the corresponding row, and corresponding column (1st row, 1st column, 2nd row, 2nd column, 3rd row, 3rd column) are the same, then it is abelian.

Note:

$z_m = G = \{0, 1, 2, 3 \ldots (m - 1)\}_{+m}$ is a finite abelian group of order m.

Rack Your Brain

Find the inverse of 2007 in the following group {0, 1, 2, ... 2021} with respect to addition modulo 2022.

Multiplication modulo:

Let a, b $\in$ z, and m is a fixed positive integer, r is a non-negative remainder then multiplication module m of (a, b) is denoted by a $\times_m$ b, and it can be defined as a $\times_m$ b = r, where $0 \le r < m$, r is a remainder obtained by dividing a × b with m.

Example: $2 \times_3 4 = 2$

2. Consider the set G = {1, 2, 3, 4} under multiplication modulo 5. Is G is an abelian group?

Solution:

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(Composition table)

- Since all the elements of the composition table belong to a given set, therefore closed.
- $(1 \times_5 2) \times_5 3 = 1 \times_5 (2 \times_5 3)$, so associative.
- In the composition table, the first-row element appearing against 1, is called the identity element.
- Every element has a unique inverse.
  $(1)^{-1} = 1$, $(2)^{-1} = 3$, $(3)^{-1} = 2$, $(4)^{-1} = 4$

So, G is a group.

Since in the composition table, corresponding row and column are the same, so it is an abelian group.

Note:
$Z_p = G = \{1, 2, 3 \ldots (p-1)_{\times_p}\}$ is an abelian group of order (p – 1), where p is a prime number.

Previous Years' Questions

The set {1, 2, 4, 7,8, 11, 13, 14} is a group under multiplication modulo 15. The inverses of 4 and 7 are respectively **[GATE CS 2005]**

(A) 3 and 13 (B) 2 and 11
(C) 4 and 13 (D) 8 and 14

Solution: (C)

Cayley table:

- Let (G, *) is a group, and the Cayley table of G is a table with rows and columns label led by the elements of the group.
- The binary operation table for a finite group is called the Cayley table.

Example: G = {1, –1} is form a group with respect to multiplication.

×	1	–1
1	1	–1
–1	–1	1

Properties of Cayley table:

1. All the entries of the Cayley table should belong to the given set otherwise the operation is not closed.
2. There should be one row in which the column label appears in order, indicating the presence of an identity element. (The column of this element should reflect the row labels); otherwise, there is no identity.
3. The identity element of the group should not only appear in every row and column (exactly once), but it should be distributed symmetrically about the main diagonal. Otherwise, one or more elements in the table do not have an inverse.
4. Every row and column of the table should contain each element exactly once.
5. If the Cayley table is symmetric along its diagonal, then the group is abelian group.

Examples of group's:

1. G = {0} is a group with respect to '+', '–' and 'x'.

+	0
0	0

–	0
0	0

×	0
0	0

It is also an abelian group with 0 as identity, and each element has its own inverse.

2. G = {1, –1} is a group with respect to '×' and '÷'.

×	1	–1
1	1	–1
–1	–1	+1

÷	1	–1
1	1	–1
–1	–1	1

(G, X), (G, ÷) is an abelian group with 1 as the identity, and each element has its own inverse.

3. G = {1, ω, ω²} is a group with respect to multiplication where $\omega^3 = 1$ (3rd root of unity)

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(G, ×) is an abelian group with 1 is the identity and $(1)^{-1} = 1$, $(\omega)^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$

Note:
If w represents the nth root of unity, i.e., $\omega^n = 1$, then the inverse of any element can be calculated $(\omega^r)^{-1} = \omega^{n-r}$.

4. G = {1, –1, i, –i} is a group with respect to multiplication where $i^2 = -1$

	1	–1	i	–i
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

(G, ×) is an abelian group with 1 as the identity and $(1)^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = -i$, $(-i)^{-1} = i$

Infinite order group:

1. (z, +) (2z, +), (3z, +) ... (nz, +) are an infinite abelian groups, where 0 is the identity.
2. (Q, +), (Q_0, ×), (Q^+, ×) are an infinite abelian group.
3. (R, +), (R_0, ×), (R^+, ×) are an infinite abelian group.
4. ($\mathbb{C}$, +), ($\mathbb{C}_0$, ×) are an infinite abelian group.
5. The set of all matrices of order n × n whose elements are rational (or) real or complex forms an infinite abelian group with respect to matrix addition.
6. The set of all non-singular matrices whose elements are rational, real, or complex. Forms an infinite non-abelian with respect to matrix multiplication.
7. $G = \left\{ A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \middle| (\alpha \in z) \right\}$ is an infinite abelian group with respect to the matrix multiplication.
8. $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \text{ and } ad - bc = 1 \mid \right\}$ forms an infinite non abelian group.
9. G = {cosθ + i sinθ | θ ∈ z or θ ∈ R, or θ ∈ Q} forms an infinite abelian group with respect to multiplication.
10. Let ‘s’ be a non-empty set, then G = {f | f : s → s is a bijection} forms a group with respect to the composition mapping.

Order of an element in a group:

Let G is a group. The order of an element a ∈ G defined as the least positive integer ‘n’ such that $a^n = e$, where e is the identity element.

Here a^n means n times operation on a (if the operation is addition, it means adding a, n times).

Example: Find the order of every element in the group G = {1, ω, ω²} with respect to multiplication where $\omega^3 = 1$.

Solution: In a group (1, ω, ω²), the identity element is 1.

$O(1) = (1)^1 = 1$

$O(\omega) = (\omega)^3 = 1$

$O(\omega^2) = (\omega^2)^3 = 3$

Rack Your Brain

Find the order of every element in the group G
$G = \{0, 1, 2, 3, 4\}_{+5}$

Properties of order of an element in a group:

- Every element of a finite group has a finite order that is less than or equal to the group’s order.
- An element of a group has the same order as its inverse.
- The order of identity elements in a group is always 1.
- In a group, if the order of every element is ‘2’ except the identity element, then the group is abelian.

Rack Your Brain

If a is an element in a group G such that O(a) = 6, then find the value of a^{2022}.

Cyclic Group's:

- A group (G, *) is called a cyclic group if, there exists an element $g \in G$ such that every element of G, can be written as g^n for some integer n (so, g is a generator of group G.)
- An element $g \in G$ such that $O(g) = O(G)$, then g is called the generator of the group and it is represented by <g>.
- A group having atleast one generator is called a cyclic group.

Example: G = ({1, –1, *i*, –*i*}, x) is a cyclic group generated by <*i*>.

$(i)^1 = i$	$(-i)^1 = -i$
$(i)^2 = -1$	$(-i)^2 = -1$
$(i)^3 = i^2 \times i = -1 \times i = -i$	$(-i)^3 = i$
$(i)^4 = i^2 \times i^2 = -1 \times -1 = 1$	$(-i)^4 = 1$

Solution:

Here, i, –i can generate all the elements of the given group, so <i>, <–i> are generators.

Rack Your Brain

In the above problem $0(i) = 0(-i) = 0(G) = 4$ so you can also say <i>, <–i> are generators and as the group has at least one generator so, it is called cyclic group.

Rack Your Brain

Whether the given group $G = \{0, 1, 2, 3\}_{+4}$ is a cyclic group or not?

Properties of cyclic group

1. Every cyclic group is also an abelian group.
2. If a is a generator of cyclic group G, then a^{-1} is also a generator of G.
3. The order of a cyclic group, as well as its generator, should be the same.
4. Every group of prime order is always cyclic.
5. If a group is cyclic, then every subgroup of that group is also cyclic.
6. If G is a cyclic group with an order n and generator g. If m < n, then the order of the element g^m is described by $|g^m| = \dfrac{n}{\gcd(m,n)}$.

Finding number of generators in cyclic group:

Let (G, *) be a cyclic group of order n with generator 'a' then

- The number of generators in G = $\phi(n)$ (Euler totient function where $\phi(n)$ is the cardinality of numbers from 1 to n, which are relatively prime to n.)

Example: If n is 7 then $\phi(n) = 6$, because relative prime numbers are {1, 2, 3, 4, 5, 6}, it means if the given number is prime, let's say p, then it's a relative prime number is always p-1.

- a^m is also a generator of G if gcd(m, n) = 1.

Example: Find the number of generators of a cyclic group of order 77.

Solution: The number of numbers from 1 to n, which are relatively prime to

$$77 = \phi(77) = \phi(7) \times \phi(11) = 6 \times 10 = 60$$

So the number of generators of a cyclic group is exactly 60.

Note:
If $\phi(n)$, if n is written into its prime factors as = $n = p_1^{n_1} \cdot p_2^{n_2} \ldots$ where p_1 p_2 are prime numbers, then

$$\phi(p^n) = p^n - p^{n-1}$$

For example,

$$\phi(7^1) = 7^1 - 7^{1-1} = 7 - 7^0 = 7 - 1 = 6$$

$$\phi(5^2) = 5^2 - 5^{2-1} = 25 - 5 = 20$$

Subgroup:

Let (G, *) is a group, A non-empty subset H of G is said to be a subgroup if:

1. $a \in H, b \in H \Rightarrow a * b \in H$ (satisfies closure)
2. $a * (b * c) = a * (b * c)\ \forall\ a, b, c \in H$. (Associative)
3. $\exists\ e \in H\ a * e = e * a = a\ \forall\ a \in H$ (Existence of identity)

4. $\forall$ a $\in$ H $\exists$ b $\in$ H a * b = b * a = e, b is the inverse of a.

   In other words, (H, *) is a subgroup of (G, *) if H $\subseteq$ G and (H, *) is itself a group.

Example: Let G = {1, –1, *i*, –*i*} is a group with multiplication, which of the following is a subgroup with respect to the given group.

1. {1, *i*}	2. {1, –*i*}
3. {1, –1}	4. {1}

Solution:

(H, *) is a subgroup of (G, *) if

1. H $\subseteq$ G
2. H itself is a group

Option:

1. H = {1, i}, H $\subseteq$ G, but H is not a group with respect to '×' because it is not closed (–1 $\notin$ H). So not a subgroup.
2. H = {1, –*i*}, H $\subseteq$ G, but H is not a group with respect to '×', because it is not closed (–1 $\notin$ H), so not a subgroup.
3. H = {1, –1}, H $\subseteq$ G and H is also a group with respect to '×' so subgroup.
4. H = {1}, H $\subseteq$ G and H is also a group with respect to '×'.

Note:

For any group (G, *), the identity element ({e}, *) and the group itself are called trivial subgroups, and other subgroups (if any) are called proper subgroups. In above example the group itself i.e. G = ({1, –1, *i*, –*i*}, ×) and the identity element ({1}, ×) are trivial subgroups and ({1, –1}, ×) is a proper subgroup.

- If G is a group of prime order, then G has only two subgroups, and those are trivial subgroups.
- The identity of the subgroup is the same as that of the group.

Lagrange's theorem:

The order of each subgroup of a finite group is the divisor of the group. (O(H) divides O(G)).

Note:

Converse of Lagrange's theorem need not be true.

Example: Find all subgroups of group G {0, 1, 2, 3 ... 11}$_{+12}$

H_1 = {0}$_{+12}$

H_2 = {0, 2, 4, 6, 8, 10}$_{+12}$

H_3 = {0, 3, 6, 9}$_{+12}$

H_4 = {0, 4, 8}$_{+12}$

H_5 = {0, 6}$_{+12}$

H_6 = G

Since the order of each subgroup divides the order of the group. So it satisfies Lagrange's theorem. But if we take one set H = {0, 3}$_{+12}$ of the given group G = {0, 1, 2, 3 ... 11}$_{+12}$, here also 0(H) i.e. 2 divides 0(G) i.e. 12, but H = {0, 3} is not a subgroup (since it is not closed). So the converse of Lagrange's theorem need not be true.

Previous Years' Questions

Let G be a group of 35 elements. Then the largest possible size of a subgroup of G other than G itself is ______.

Note: This question was numerical type.

(A) 1	(B) 5
(C) 7	(D) 35

Solution: (C) **[GATE CS 2020]**

Previous Years' Questions

Let G be a group of order 6, and H be a subgroup of G such that 1

(A) Both G and H are always cyclic

(B) G may not be cyclic, but H is always cyclic

(C) G is always cyclic, but H may not be cyclic

(D) Both G and H may not be cyclic

Solution: (B) **[GATE CS 2021]**

Properties of subgroup:

1. A non-empty subset 'H' of a group (G, o) is a subgroup of G if and only if
   a) $a, b \in H$, $\forall\ a \in H, b \in H$
   b) $a^{-1} \in H$, $\forall\ a \in H$
2. A non-empty subset (H) of a group (G, +) is said to be subgroup if and only if
   a) $a + b \in H$ $\forall\ a \in H, b \in H$
   b) $-a \in H$ $\forall\ a \in H$
3. A non-empty subset H of a group (G, o) is a subgroup if and only if $ab^{-1} \in H\ \forall\ a \in H$, $b \in H$
4. If H is a subgroup of G, then $H^{-1} = H$, but the converse need not be true i.e. if $H = H^{-1}$, H may not be a subgroup.
5. If H is any subgroup of G, then $H \cdot H = H$, but the converse need not be true.
6. If H and K are two subgroups of G, then H(K) is a subgroup of G if HK = KH.
7. The intersection ($\cap$) of any two subgroups of a group G is a subgroup.
8. The union ($\cup$) of two subgroups of a group G need not be a subgroup.
9. Union of two subgroup, H, K is again a subgroup if and only if one contains the other, i.e., $H \subseteq K$ or $K \subseteq H$.

Chapter Summary

- An non-empty set G with operation * satisfies:
  Closure → (G, *) is an algebraic structure
  Closure + Associative → (G, *) is a semigroup
  Closure + Associative + Identity → (G, *) is monoid
  Closure + Associative + Identity + Inverse → (G, *) is group
  Closure + Associative + Identity + Inverse + Commutative → (G, *) is abelian group
- Existence of identity $\exists\ e \in G\ \forall\ a \in G$ $a * e = e * a = a$
- Existence of inverse $\forall\ a \in G\ \exists\ b \in G$ $a * b = b * a = e$
- Modulo m operation $a +_m b$ = the remainder when m divides a + b
  $a \times_m b$ = the remainder when m divides a × b
- Set $G = \{0, 1, 2 \ldots (m - 1)\}_{+m}$ is an abelian group with identity 0 and the inverse of a is (m − a) mod m.
- Set $G = \{1, 2, 3 \ldots (p - 1)\}_{\times p}$ is an abelian group of prime order (p).
- An element $g \in G$ such that 0(g) = 0(G), then g is called the generator of the group and it is represented by <g>.
- A group having at least one generator is called a cyclic group.
- (H, *) is a subgroup of (G, *) if $H \subseteq G$ and (H, *) is itself a group.
- If H is a subgroup of a finite group G, then O(H) divides O(G).