Algebraic Structures

- Algebraic systems Examples and general properties
- Semi groups
- Monoids
- Groups
- Sub groups

Algebraic systems

- **N = {1,2,3,4,…..$\propto$ } = Set of all natural numbers.**

  Z = { 0, $\pm$1, $\pm$2, $\pm$3, $\pm$4 , ….. $\propto$} = Set of all integers.

  Q = Set of all rational numbers.

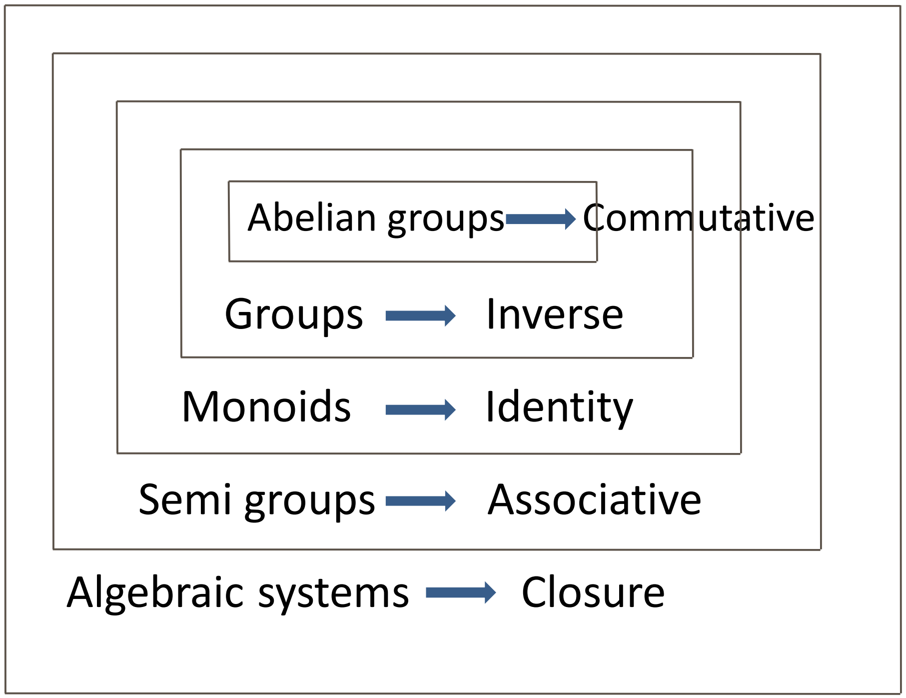
  R = Set of all real numbers.
- **Binary Operation:** The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if

  $a * b \in A$ for all $a, b \in A$ (Closure property).

  Ex: The set N is closed with respect to addition and multiplication but not w.r.t subtraction and division.
- **Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

  Ex: (N, +), (Z, +, $-$), (R, +, **. , –**) are algebraic systems.

Algebraic systems



Properties

- **Commutative:** Let * be a binary operation on a set A.

  The operation * is said to be commutative in A if

  $a * b = b * a$ for all a, b in A

- **Associativity:** Let * be a binary operation on a set A.

  The operation * is said to be associative in A if

  $(a * b) * c = a * (b * c)$ for all a, b, c in A

- **Identity:** For an algebraic system (A, *)**,** an element 'e' in A is said to be an identity element of A if

  $a * e = e * a = a$ for all $a \in A$.

- **Note:** For an algebraic system (A, *), the identity element, if exists, is unique.

- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

  $$a * b = b * a = e$$

Semi group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
  1. * is closed operation on A.
  2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, −) is not a semi group.

- **Monoid:** An algebraic system (A, *) is said to be a **monoid** if the following conditions are satisfied.
  1) * is a closed operation in A.
  2) * is an associative operation in A.
  3) There is an identity in A.

Monoid

- Ex. Show that the set 'N' is a monoid with respect to multiplication.
- Solution: Here, N = {1,2,3,4,……}

1. Closure property : We know that product of two natural numbers is again a natural number.

i.e., $a.b = b.a$ for all $a,b \in N$

$\therefore$ Multiplication is a closed operation.

2. Associativity : Multiplication of natural numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

   $a.1 = 1.a = a$ for all $a \in N$.

   $\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Subsemigroup & submonoid

Subsemigroup : Let (S, *) be a semigroup and let T be a subset of S. If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

Submonoid : Let (S, *) be a monoid with identity e, and let T be a non- empty subset of S. If T is closed under the operation * and e $\in$ T, then (T, *) is called a submonoid of (S, *).

Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.

  1) * is a closed operation.

  2) * is an associative operation.

  3) There is an identity in G.

  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $$a * b = b * a \quad \text{for all } a, b \in G.$$

Theorem

- In a Group (G, *) the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

$a * b = a * c \Rightarrow b = c$ (left cancellation law)

$a * c = b * c \Rightarrow a = b$ (Right cancellation law)

4. $(a * b)^{-1} = b^{-1} * a^{-1}$

- In a group, the identity element is its own inverse.

- ***Order of a group*** : The number of elements in a group is called order of the group.

- Finite group: If the order of a group G is finite, then G is called a finite group.

Ex. Show that, the set of all integers is a group with respect to addition.

- Solution: Let Z = set of all integers.

  Let a, b, c are any three elements of Z.

1. Closure property : We know that, Sum of two integers is again an integer.

   i.e., $a + b \in Z$ for all $a,b \in Z$

2. Associativity: We know that addition of integers is associative.

   i.e., $(a+b)+c = a+(b+c)$ for all $a,b,c \in Z$.

3. Identity : We have $0 \in Z$ and $a + 0 = a$ for all $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

4. Inverse: To each $a \in Z$, we have $-a \in Z$ such that

   $a + (-a) = 0$

   Each element in Z has an inverse.

Contd.,

- 5. Commutativity: We know that addition of integers is commutative.

  i.e., $a + b = b + a$ for all $a, b \in Z$.

  Hence, $(Z, +)$ is an abelian group.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

- Solution: Let R^* = set of all non zero real numbers.

  Let a, b, c are any three elements of R^* .

1. <u>Closure property</u> : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a . b \in R^*$ for all $a,b \in R^*$.

2. <u>Associativity</u>: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. <u>Identity</u> : We have $1 \in R^*$ and $a .1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. <u>Inverse</u>: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a .(1/a) = 1$ i.e., Each element in R^* has an inverse.

Contd.,

- 5.<u>Commutativity</u>: We know that multiplication of real numbers is commutative.

  i.e., $a . b = b . a$ for all $a,b \in R^*$.

  Hence, $(R^* , .)$ is an abelian group.

- <u>Ex:</u> Show that set of all real numbers 'R' is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

  The multiplicative inverse of 0 does not exist.

  Hence. R is not a group.

Example

- Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by $n * m = \text{maximum of } (n, m)$.
  Show that (Z, *) is a semi group.
  Is (Z, *) a monoid ?. Justify your answer.
- Solution: Let a , b and c are any three integers.

Closure property: Now, $a * b = \text{maximum of } (a, b) \in Z$ for all $a,b \in Z$

Associativity : $(a * b) * c = \text{maximum of } \{a,b,c\} = a * (b * c)$

$\therefore$ (Z, *) is a semi group.

Identity : There is no integer x such that

$a * x = \text{maximum of } (a, x) = a$ for all $a \in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Example

- Ex. Let S be a finite set, and let F(S) be the collection of all functions $f: S \to S$ under the operation of composition of functions, then show that F(S) is a monoid.

  Is S a group w.r.t the above operation? Justify your answer.

- Solution:

  Let f_1, f_2, f_3 are three arbitrary functions on S.

Closure property: Composition of two functions on S is again a function on S.

i.e., $f_1 o f_2 \in F(S)$

Associativity: Composition of functions is associative.

i.e., $(f_1 o f_2) o f_3 = f_1 o (f_2 o f_3)$

Contd.,

- Identity: We have identity function $I : S \to S$

  such that $f_1 \circ I = f_1$.

  $\therefore$ F(S) is a monoid.

- Note: F(S) is not a group, because the inverse of a non bijective function on S does not exist.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition * defined by

$$a * b = (ab)/2 .$$

- Solution: Let A = set of all positive rational numbers.

  Let a,b,c be any three elements of A.

1. <u>Closure property:</u> We know that, Product of two positive rational numbers is again a rational number.

   i.e., $a * b \in A$ for all $a,b \in A$.

2. <u>Associativity</u>: $(a*b)*c = (ab/2) * c = (abc) / 4$

   $a*(b*c) = a * (bc/2) = (abc) / 4$

3. <u>Identity</u> : Let e be the identity element.

   We have $a*e = (a\,e)/2$ ...(1) , By the definition of *

   again, $a*e = a$ .....(2) , Since e is the identity.

   From (1)and (2), $(a\,e)/2 = a \Rightarrow e = 2$ and $2 \in A$.

$\therefore$ Identity element exists, and '2' is the identity element in A.

Contd.,

- 4. <u>Inverse:</u> Let $a \in A$

  let us suppose b is inverse of a.

  Now, $a * b = (a\,b)/2$ ….(1) (By definition of inverse.)

  Again, $a * b = e = 2$ …..(2) (By definition of inverse)

  From (1) and (2), it follows that

  $(a\,b)/2 = 2$

  $\Rightarrow \quad b = (4 / a) \in A$

$\therefore$ (A ,*) is a group.

- Commutativity: $a * b = (ab/2) = (ba/2) = b * a$
- Hence, (A,*) is an abelian group.

Theorem

- Ex. In a group (G, *) , Prove that the identity element is unique.
- <u>Proof </u>:

a) Let e_1 and e_2 are two identity elements in G.

Now, $e_1 * e_2 = e_1$ ...(1) (since e_2 is the identity)

Again, $e_1 * e_2 = e_2$ ...(2) (since e_1 is the identity)

From (1) and (2), we have $e_1 = e_2$

$\therefore$ Identity element in a group is unique.

Theorem

- Ex. In a group (G, *) , Prove that the inverse of any element is unique.
- <u>Proof</u>:
- Let $a, b, c \in G$ and e is the identity in G.
- Let us suppose, Both b and c are inverse elements of a .
- Now, $a * b = e$ ...(1) (Since, b is inverse of a)
- Again, $a * c = e$ ...(2) (Since, c is also inverse of a)
- From (1) and (2), we have
- $a * b = a * c$
- $\Rightarrow \quad b = c$ (By left cancellation law)
- In a group, the inverse of any element is unique.

Theorem

- Ex. In a group $(G, *)$, Prove that
  $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a,b \in G$.
- <u>Proof :</u>
- Consider,
- $(a * b) * (b^{-1} * a^{-1})$
- $= (a * (b * b^{-1}) * a^{-1})$ (By associative property).
- $= (a * e * a^{-1})$ (By inverse property)
- $= (a * a^{-1})$ (Since, e is identity)
- $= e$ (By inverse property)
- Similarly, we can show that
- $(b^{-1} * a^{-1}) * (a * b) = e$
- Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Ex. If $(G, *)$ is a group and $a \in G$ such that $a * a = a$, then show that $a = e$, where e is identity element in G.

- Proof: Given that, $a * a = a$
- $\Rightarrow a * a = a * e$ (Since, e is identity in G)
- $\Rightarrow \quad a = e$ (By left cancellation law)
- Hence, the result follows.

Ex. If every element of a group is its own inverse, then show that the group must be abelian .

- Proof: Let (G, *) be a group.
- Let a and b are any two elements of G.
- Consider the identity,
- $(a * b)^{-1} = b^{-1} * a^{-1}$
- $\Rightarrow$ $(a * b) = b * a$ (Since each element of G is its own
- inverse)
- Hence, G is abelian.

Note: $a^2 = a * a$

$a^3 = a * a * a$ etc.

- Ex. In a group $(G, *)$, if $(a * b)^2 = a^2 * b^2 \quad \forall a,b \in G$ then show that G is abelian group.
- <u>Proof</u>: Given that $(a * b)^2 = a^2 * b^2$
- $\Rightarrow (a * b) * (a * b) = (a * a) * (b * b)$
- $\Rightarrow a * (b * a) * b = a * (a * b) * b$ (By associative law)
- $\Rightarrow (b * a) * b = (a * b) * b$ (By left cancellation law)
- $\Rightarrow (b * a) = (a * b)$ (By right cancellation law)
- Hence, G is abelian group.

Finite groups

- Ex. Show that G = {1, -1} is an abelian group under multiplication.
- Solution: The composition table of G is

$\cdot$	1	-1
1	1	-1
-1	-1	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are real numbers, and we know that multiplication of real numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of

   1 and -1 are 1 and -1 respectively.

Contd.,

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication..

Ex. Show that $G = \{1, \omega, \omega^2\}$ is an abelian group under multiplication. Where $1, \omega, \omega^2$ are cube roots of unity.

- Solution: The composition table of G is

.	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of $1\ \omega, \omega^2$ are $1, \omega^2, \omega$ respectively.

Contd.,

- Hence, G is a group w.r.t multiplication.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.
- Hence, G is an abelian group w.r.t. multiplication.

Ex. Show that G = {1, –1, i, –i } is an abelian group under multiplication.

- Solution: The composition table of G is

.	1	–1	i	-i
1	1	-1	i	- i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.

Contd.,

- 4. Inverse: From the composition table, we see that the inverse elements of

  1 -1, i, -i are 1, -1, -i, i respectively.

- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative. Hence, (G, .) is an abelian group.

Modulo systems.

- <u>Addition modulo m</u> ($+_m$)
- let m is a positive integer. For any two positive integers a and b
- $a +_m b = a + b$ if $a + b < m$
- $a +_m b = r$ if $a + b \geq m$ where r is the remainder obtained
- by dividing (a+b) with m.
- <u>Multiplication modulo p</u> ($\times_p$)
- let p is a positive integer. For any two positive integers a and b
- $a \times_p b = a\,b$ if $a\,b < p$
- $a \times_p b = r$ if $a\,b \geq p$ where r is the remainder obtained
- by dividing (ab) with p.
- Ex. $3 \times_5 4 = 2$, $5 \times_5 4 = 0$, $2 \times_5 2 = 4$

Ex.The set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

- Solution: The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- 1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Contd.,

- 2. Associativity: The binary operation $+_6$ is associative in G.

  for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

  $2 +_6 (3 +_6 4) = 2 +_6 1 = 3$
- 3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.
- 4. . Inverse: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.
- Hence, $(G, +_6)$ is an abelian group.

Ex.The set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

- Solution: The composition table of G is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- 1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under $\times_7$.

Contd.,

- 2. Associativity: The binary operation $\times_7$ is associative in G.

  for ex. $(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$ and

  $2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$
- 3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 1 is the identity element.
- 4. . Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4, 5 ,6 are 1, 4, 5, 2, 5, 6 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $\times_7$ is commutative.
- Hence, $(G, \times_7)$ is an abelian group.

More on finite groups

- In a group with 2 elements, each element is its own inverse
- In a group of even order there will be at least one element (other than identity element) which is its own inverse
- The set G = {0,1,2,3,4,…..m-1} is a group with respect to addition modulo m.
- The set G = {1,2,3,4,….p-1} is a group with respect to multiplication modulo p, where p is a prime number.
- **Order of an element of a group:**
- Let (G, *) be a group. Let 'a' be an element of G. The smallest integer n such that $a^n = e$ is called order of 'a'. If no such number exists then the order is infinite.

Examples

- Ex. G = {1, -1, i, -i } is a group w.r.t multiplication. The order –i is
  a) 2 b) 3 c) 4 d) 1
- Ex. Which of the following is not true.
- a) The order of every element of a finite group is finite and is a divisor of the order of the group.

  b) The order of an element of a group is same as that of its inverse.
- c) In the additive group of integers the order of every element except 0 is infinite
- d) In the infinite multiplicative group of nonzero rational numbers the order of every element except 1 is infinite.
- Ans. d

Sub groups

- Def. A non empty sub set H of a group (G, *) is a sub group of G,
- if (H, *) is a group.

Note: For any group {G, *}, {e, * } and (G, *) are trivial sub groups.

- Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.

  H_1 = { 1, -1 } is a subgroup of G .

  H_2 = { 1 } is a trivial subgroup of G.

- Ex. (Z , +) and (Q , +) are sub groups of the group (R +).
- Theorem: A non empty sub set H of a group (G, *) is a sub group of G iff
- i) $a * b \in H \quad \forall\, a, b \in H$
- ii) $a^{-1} \in H \quad \forall\, a \in H$

Theorem

- Theorem: A necessary and sufficient condition for a non empty subset H of a group (G, *) to be a sub group is that

  $a \in H,\ b \in H \Rightarrow a * b^{-1} \in H.$
- Proof: Case1: Let (G, *) be a group and H is a subgroup of G

  Let $a,b \in H \Rightarrow b^{-1} \in H$ (since H is is a group)

  $\Rightarrow a * b^{-1} \in H.$ (By closure property in H)
- Case2: Let H be a non empty set of a group (G, *).

  Let $a * b^{-1} \in H \quad \forall\, a, b \in H$
- Now, $a * a^{-1} \in H$ (Taking b = a)

  $\Rightarrow e \in H$ i.e., identity exists in H.
- Now, $e \in H,\ a \in H \Rightarrow e * a^{-1} \in H$

  $\Rightarrow a^{-1} \in H$

Contd.,

- $\therefore$ Each element of H has inverse in H.

  Further, $a \in H, \ b \in H \Rightarrow a \in H, \ b^{-1} \in H$

  $\Rightarrow a * (b^{-1})^{-1} \in H.$

  $\Rightarrow a * b \in H.$

  $\therefore$ H is closed w.r.t $*$.
- Finally, Let $a,b,c \in H$

  $\Rightarrow a,b,c \in G$ (since $H \subseteq G$)

  $\Rightarrow (a * b) * c = a * (b * c)$

  $\therefore$ $*$ is associative in H
- Hence, H is a subgroup of G.

Ex. Show that the intersection of two sub groups of a group G is again a sub group of G.

- Proof: Let (G, *) be a group.
- Let H_1 and H_2 are two sub groups of G.
- Let $a, b \in H_1 \cap H_2$.
- Now, $a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$ (Since, H_1 is a subgroup of G)
- again, $a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$ (Since, H_2 is a subgroup of G)
- $\therefore\ a * b^{-1} \in H_1 \cap H_2$.
- Hence, $H_1 \cap H_2$ is a subgroup of G .

Ex. Show that the union of two sub groups of a group G need not be a sub group of G.

- Proof: Let G be an additive group of integers.
- Let $H_1 = \{ 0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}$
- and $H_2 = \{ 0, \pm 3, \pm 6, \pm 9, \pm 12, \ldots\}$
- Here, H_1 and H_2 are groups w.r.t addition.
- Further, H_1 and H_2 are subsets of G.
- $\therefore$ H_1 and H_2 are sub groups of G.
- $H_1 \cup H_2 = \{ 0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$
- Here, $H_1 \cup H_2$ is not closed w.r.t addition.
- For ex. $2 , 3 \in G$
- But, $2 + 3 = 5$ and 5 does not belongs to $H_1 \cup H_2$.
- Hence, $H_1 \cup H_2$ is not a sub group of G.

Homomorphism and Isomorphism.

- **Homomorphism :** Consider the groups $(G, *)$ and $(G^1, \oplus)$

  A function $f : G \to G^1$ is called a homomorphism if

  $$f(a * b) = f(a) \oplus f(b)$$

- **Isomorphism** : If a homomorphism $f : G \to G^1$ is a bijection then f is called isomorphism between G and G^1 .

  Then we write $G \equiv G^1$

Example

- Ex. Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R \rightarrow R^+$ defined by $f(x) = 2^x$ for all $x \in R$ is an isomorphism.
- Solution: First, let us show that f is a homomorphism.
- Let $a, b \in R$.
- Now, $f(a+b) = 2^{a+b}$
- $= 2^a \; 2^b$
- $= f(a).f(b)$
- $\therefore$ f is an homomorphism.
- Next, let us prove that f is a Bijection.

Contd.,

- For any a , b $\in$ R, Let, f(a) = f(b)
- $\Rightarrow 2^a = 2^b$
- $\Rightarrow a = b$
- $\therefore$ f is one.to-one.
- Next, take any c $\in$ R^+.
- Then $\log_2 c \in R$ and $f(\log_2 c) = 2^{\log 2\ c} = c$.
- $\Rightarrow$ Every element in R^+ has a pre image in R.
- i.e., f is onto.
- $\therefore$ f is a bijection.
- Hence, f is an isomorphism.

Example

- Ex. Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R^+ \rightarrow R$ defined by $f(x) = \log_{10} x$ for all $x \in R$ is an isomorphism.
- <u>Solution</u>: First, let us show that f is a homomorphism.
- Let $a , b \in R^+$.
- Now, $f(a.b) = \log_{10} (a.b)$
- $= \log_{10} a + \log_{10} b$
- $= f(a) + f(b)$
- $\therefore$ f is an homomorphism.
- Next, let us prove that f is a Bijection.

Contd.,

- For any a , b $\in R^+$,   Let,   f(a) = f(b)
- $\Rightarrow \log_{10} a = \log_{10} b$
- $\Rightarrow a = b$
- $\therefore$ f is one.to-one.
- Next, take any c $\in$ R.
- Then $10^c \in R$ and $f(10^c) = \log_{10} 10^c = c$.
- $\Rightarrow$ Every element in R has a pre image in R^+ .
- i.e., f is onto.
- $\therefore$ f is a bijection.
- Hence, f is an isomorphism.

Theorem

- Theorem: Consider the groups (G_1, $*$) and (G_2, $\oplus$) with identity elements e_1 and e_2 respectively. If $f : G_1 \to G_2$ is a group homomorphism, then prove that

  a) $f(e_1) = e_2$

  b) $f(a^{-1}) = [f(a)]^{-1}$

  c) If H_1 is a sub group of G_1 and $H_2 = f(H_1)$,

  then H_2 is a sub group of G_2.

  d) If f is an isomorphism from G_1 onto G_2,

  then f^{-1} is an isomorphism from G_2 onto G_1.

Proof

- Proof: a) we have in G_2,

$e_2 \oplus f(e_1) = f(e_1)$ (since, e_2 is identity in G_2)

$= f(e_1 * e_1)$ (since, e_1 is identity in G_1)

$= f(e_1) \oplus f(e_1)$ (since f is a homomorphism)

$e_2 = f(e_1)$ (By right cancellation law)

- b) For any $a \in G_1$, we have

$f(a) \oplus f(a^{-1}) = f(a * a^{-1}) = f(e_1) = e_2$

and $f(a^{-1}) \oplus f(a) = f(a^{-1} * a) = f(e_1) = e_2$

$\therefore$ $f(a^{-1})$ is the inverse of $f(a)$ in G_2

i.e., $[f(a)]^{-1} = f(a^{-1})$

Contd.,

- c) $H_2 = f(H_1)$ is the image of H_1 under f; this is a subset of G_2.
- Let $x, y \in H_2$.
- Then $x = f(a)$, $y = f(b)$ for some $a,b \in H_1$
- Since, H_1 is a subgroup of G_1, we have $a * b^{-1} \in H_1$.
- Consequently,
- $x \oplus y^{-1} = f(a) \oplus [f(b)]^{-1}$
- $\quad = f(a) \oplus f(b^{-1})$
- $\quad = f(a * b^{-1}) \in f(H_1) = H_2$
- Hence, H_2 is a subgroup of G_2.

Contd.,

- d) Since $f : G_1 \rightarrow G_2$ is an isomorphism, f is a bijection.
- $\therefore\ f^{-1} : G_2 \rightarrow G_1$ exists and is a bijection.
- Let $x, y \in G_{2.}$ Then $x \oplus y \in G_2$
- and there exists $a, b \in G_1$ such that $x = f(a)$ and $y = f(b)$.
- $\therefore\ f^{-1}(x \oplus y) = f^{-1}(f(a) \oplus f(b))$
- $= f^{-1}(f(a * b))$
- $= a * b$
- $= f^{-1}(x) * f^{-1}(y)$
- This shows that $f^{-1} : G_2 \rightarrow G_1$ is an homomorphism as well.
- $\therefore\ f^{-1}$ is an isomorphism.

Cosets

- If H is a sub group of(G, *) and $a \in G$ then the set $Ha = \{ h * a \mid h \in H\}$ is called a right coset of H in G.

Similarly $aH = \{a * h \mid h \in H\}$ is called a left coset of H is G.

- ***Note:-*** 1) Any two left (right) cosets of H in G are either identical or disjoint.
- 2) Let H be a sub group of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a sub group H is equal to G.

  3) <u>Lagrange's theorem</u>: The order of each sub group of a finite group is a divisor of the order of the group.
- 4) The order of every element of a finite group is a divisor of the order of the group.
- 5) The converse of the lagrange's theorem need not be true.

Example

- Ex. If G is a group of order p, where p is a prime number. Then the number of sub groups of G is
- a) 1 b) 2 c) p – 1 d) p
- Ans. b
- Ex. Prove that every sub group of an abelian group is abelian.
- <u>Solution</u>: Let (G, *) be a group and H is a sub group of G.
- Let $a , b \in H$
- $\Rightarrow a , b \in G$ (Since H is a subgroup of G)
- $\Rightarrow a * b = b * a$ (Since G is an abelian group)
- Hence, H is also abelian.

State and prove Lagrange's Theorem

- <u>Lagrange's theorem</u>: The order of each sub group H of a finite group G is a divisor of the order of the group.
- <u>Proof</u>: Since G is finite group, H is finite.
- Therefore, the number of cosets of H in G is finite.
- Let $Ha_1, Ha_2, \ldots, Ha_r$ be the distinct right cosets of H in G.
- Then, $G = Ha_1 \cup Ha_2 \cup \ldots, \cup Ha_r$
- So that $O(G) = O(Ha_1)+O(Ha_2) \ldots + O(Ha_r)$.
- But, $O(Ha_1) = O(Ha_2) = \ldots\ldots = O(Ha_r) = O(H)$
- $\therefore\ O(G) = O(H)+O(H) \ldots + O(H)$. (r terms)
- $= r \,.\, O(H)$
- This shows that O(H) divides O(G).

Hass Diagram, Lattices and Boolean Algebra

Hasse Diagram

- A Hasse diagram is a graphical representation of a poset.
- Since a poset is by definition reflexive and transitive (and antisymmetric), the graphical representation for a poset can be compacted.
- For example, why do we need to include loops at every vertex? Since it’s a poset, it *must* have loops there.

Constructing a Hasse Diagram

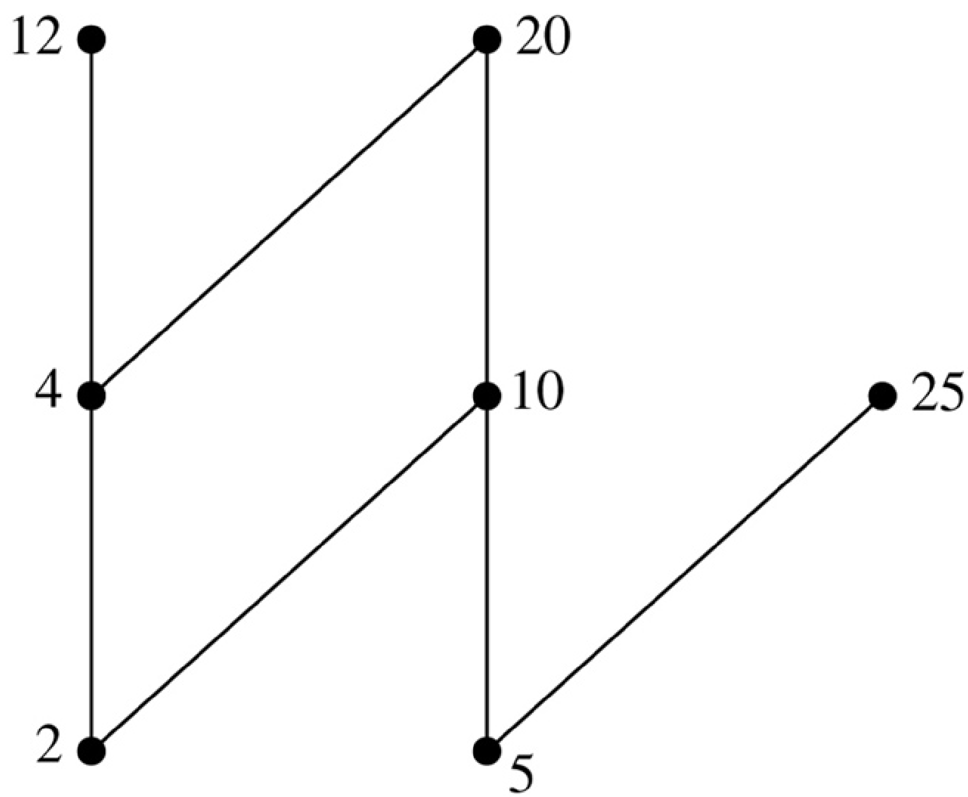
- Start with the digraph of the partial order.
- Remove the loops at each vertex.
- Remove all edges that *must* be present because of the transitivity.
- Arrange each edge so that all arrows point up.
- Remove all arrowheads.

Hasse Diagram Terminology

- Let $(S, \preccurlyeq)$ be a poset.
- a is *maximal* in $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \preccurlyeq b$. (top of the Hasse diagram)
- a is *minimal* in $(S, \preccurlyeq)$ if there is no $b \in S$ such that $b \preccurlyeq a$. (bottom of the Hasse diagram)

Hasse Diagram Terminology

Which elements of the poset ({, 2, 4, 5, 10, 12, 20, 25}, |) are maximal? Which are minimal?

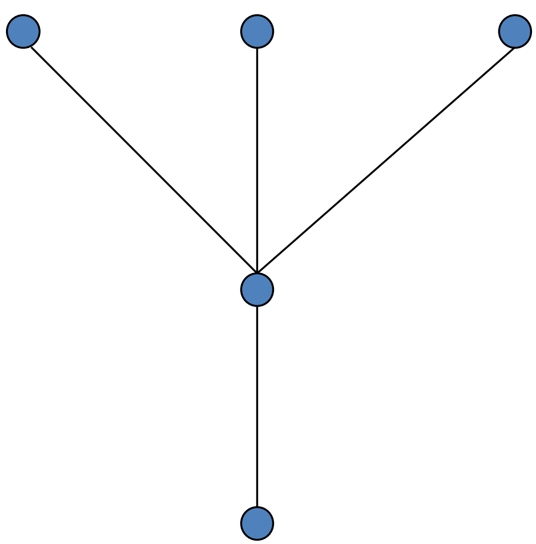


Hasse Diagram Terminology

- Let $(S, \preccurlyeq)$ be a poset.
- a is the *greatest element* of $(S, \preccurlyeq)$ if $b \preccurlyeq a$ for all $b \in S$…
  - It must be unique
- a is the *least element* of $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$.
  - It must be unique

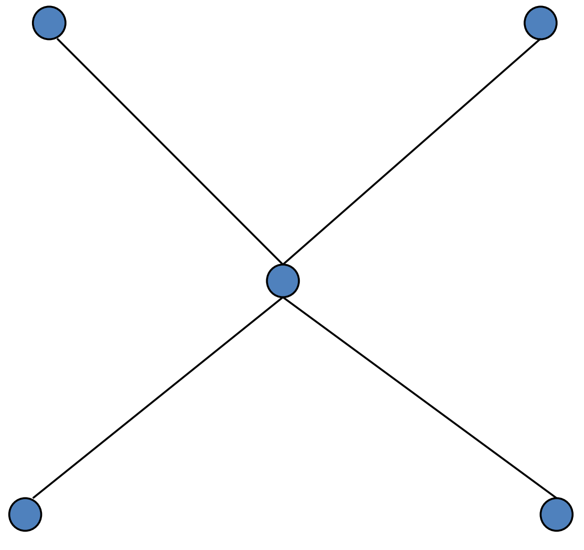
Hasse Diagram Terminology

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?



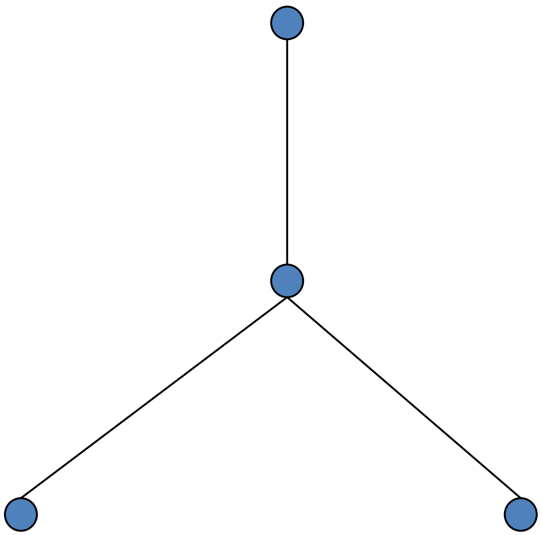
Hasse Diagram Terminology

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?



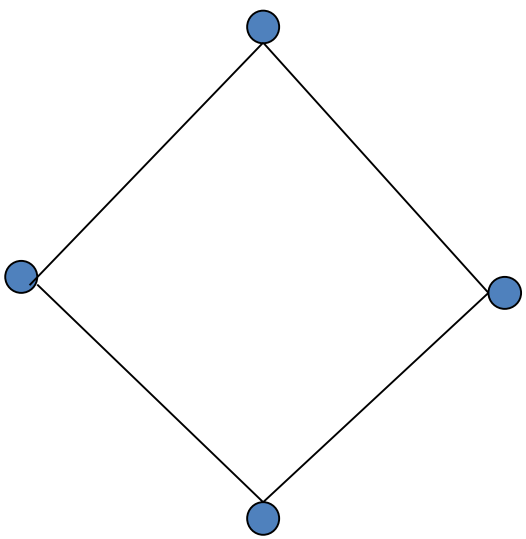
Hasse Diagram Terminology

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?



Hasse Diagram Terminology

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?

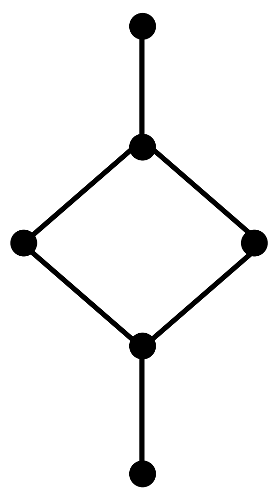


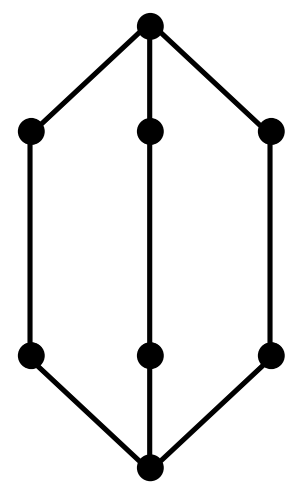
Hasse Diagram Terminology

- Let A be a subset of $(S, \preccurlyeq)$.
- If $u \in S$ such that $a \preccurlyeq u$ for all $a \in A$, then u is called an *upper bound* of A.
- If $l \in S$ such that $l \preccurlyeq a$ for all $a \in A$, then l is called an *lower bound* of A.
- If x is an upper bound of A and $x \preccurlyeq z$ whenever z is an upper bound of A, then x is called the *least upper bound* of A.
  - It must be unique
- If y is a lower bound of A and $z \preccurlyeq y$ whenever z is a lower bound of A, then y is called the *greatest lower bound* of A.
  - It must be unique

Lattices

- A *lattice* is a partially ordered set in which every pair of elements has both a *least upper bound* and *greatest lower bound*.





Lattice example

- Are the following three posets *lattices?*