Abstract Algebra: Abstract algebra is the study of algebraic structures. Algebraic structures include group, ring, field, module, vector space, lattices and algebras. The term abstract algebra was coined in the 20th century to distinguish this area of study from the other parts of algebra. Other part of mathematics, concrete problems and examples have played important role in the development of abstract algebra.

Group theory has extensive applications in mathematics, science, and engineering. Many algebraic structures such as fields and vector spaces may be defined concisely in terms of groups, and group theory provides an important tool for studying symmetry, since the symmetries of any object form a group. Groups are thus essential abstractions in branches of physics involving symmetry principles, such as relativity, quantum mechanics, and particle physics. Furthermore, their ability to represent geometric transformations finds applications in chemistry, computer graphics, material sciences, cryptography and other fields.

Binary Operation: Let A and B be two sets. A function from $A \times A$ to B is called a binary operation on A. In simple words binary operation is a process that combines two elements of a set to obtain an element of a set. Binary operations are mostly denoted by $*, \#, +, \times, \cdot, o, \cup, \cap, \odot, \otimes, \oplus$ etc.... If $*$ is a binary operation on a set A and $a, b \in A$, then $*\,(a, b)$ is generally written as $a * b$.

Algebraic Structure: A nonempty set S with binary operation $*$ is called an algebraic system or algebraic structure and it is denoted by $(S,*)$.

Example: Addition, subtraction, and multiplication are binary operations on the set of integers.

Closure Property: A binary operation $*$ on a set A is called closed if $a * b \in A$ for all $a, b \in A$.

Example: Addition '+'on set of natural numbers $\mathbb{N}$ is a closed binary operation, since sum of two natural number is always a natural number. But subtraction '−' is not a closed binary operation on $\mathbb{N}$. Since, $1, 2 \in N$ but $1 - 2 \notin \mathbb{N}$.

Example: Set of irrational number under multiplication is not closed. $i.e.$ Multiplication is not closed on $\mathbb{R} - \mathbb{Q}$. Since $\sqrt{3} \times \sqrt{3} = 3 \notin \mathbb{R} - \mathbb{Q}$.

Semigroup: A non-empty set S together with a binary operation $*$ is said to be a semigroup, if it satisfies the following properties:

(i) Closure: $a * b \in S, \ \forall\, a, b \in S$.
(ii) Associativity: $a * (b * c) = (a * b) * c, \forall\, a, b, c \in S$.

Examples

(i) Set of natural number under usual addition is a semigroup.
(ii) Set of even integers under addition is a semigroup.

(iii) The set of integers under subtraction is not a semigroup. Subtraction is not associative. If we take, $1, 2, 3 \in \mathbb{Z}$, then $1 - (2 - 3) \neq (1 - 2) - 3$

(iv) A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is said to be a 2× 2 matrix. The set of all 2×2 matrices with real entries form a semigroup under component wise addition. That is

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

Clearly, it holds closure and associative properties.

Monoid: A non-empty set M together with a binary operation $*$ is said to be a monoid, if satisfies the following conditions:

(i) Closure: $a * b \in M$; $\forall\ a, b \in M$.

(ii) Associativity: $a * (b * c) = (a * b) * c;\ \forall\ a, b, c \in M$.

(iii) Identity: There exist an element $e \in M$ such that $a * e = e * a = a$, $\forall\ a \in M$.

Examples

(i) Set of integers $\mathbb{Z}$ under usual multiplication $\times$ form a monoid. As we know that multiplication of two integers is an integer, multiplication is closed on $\mathbb{Z}$. Since for any three integers k, l, m we have $(k \times l) \times m = k \times (l \times m)$, multiplication is associative on $\mathbb{Z}$. The integer 1 is the identity element as $k \times 1 = 1 \times k = k$. Hence $\mathbb{Z}$ is a monoid under usual multiplication.

(ii) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ are monoids.

(iii) The set of complex number $\mathbb{C}$ is a monoid under addition $+$, where addition is defined as $(\boldsymbol{a + bi}) + (\boldsymbol{c + di}) = (\boldsymbol{a + b}) + (\boldsymbol{c + d})\boldsymbol{i}$.

(iv) Set of natural number under addition is not a monoid.

(v) Set of even integers under multiplication is not a monoid.

(vi) The set of all 2×2 matrices with real entries form a monoid under usual matrix multiplication

Group: A non empty set G, together with a binary operation $*$ is said to be form a group, if it satisfies the following postulates:

(i) Closure: $a * b \in G, \forall\ a, b \in G$.

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

(iii) Identity: There exists an element $e \in G$ such that $a * e = e * a = a$, $\forall a \in G$.

(iv) Existence of Inverse: $\forall a \in G$, $\exists b \in G$ (depending on a) such that $a * b = b * a = e$. Here, b is said to be inverse of a and is denoted by a^{-1}.

Examples

(i) $(\mathbb{Z}, +)$ is a group under usual addition. Inverse of an integer m is $-m$. But $(\mathbb{Z}, \times)$ is not a group. **:** Product of two integers is always an integer. Therefore, closure property hold. Since, $(a.b).c = a.(b.c) \; \forall \; a, b, c \in \mathbb{Z}$. So, associative hold. 1 is the identity element of $\mathbb{Z}$. Now, $2 \in \mathbb{Z}$ but 2 has no inverse in $\mathbb{Z}$. There does not exist $a \in \mathbb{Z}$ such that $a \times 2 = 2 \times a = 1$. Therefore, inverse property does not hold. Thus, set of integers under multiplication is not a group.

(ii) $(\mathbb{C}, +)$ is a group. But $(\mathbb{C}, \times)$ is not a group where $\times$ is the multiplication defined by
$(a + ib).(c + id) = (ac - bd) + i(ad + bc)$.

(iii) Let G be the set $\{1, -1\}$. It is a group under usual multiplication.

$\times$	1	-1
1	1	-1
-1	-1	1

(iv) The set of nonzero real numbers is a group under ordinary multiplication. The identity element is 1. The inverse of a is $\frac{1}{a}$.

(v) $\mathbb{C}^* = \mathbb{C} = \{0\}$ form a group under usual multiplication. $1 = 1 + 0i$ is the identity element and $\frac{a-ib}{a^2+b^2}$ is the inverse of $a + ib$.

(vi) The set of all 2×2 matrices with real entries form a group under component wise addition. That is

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

The identity element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

(vii) The set $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ for $n \geq 1$ is a group under addition modulo n. The identity element is 0 and for any $j > 0 \in \mathbb{Z}_n$, the inverse of j is $n - j$. For the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, we can form a table of operations as bellow:

mod 4	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(viii) The set $\{1, 2, 3, \dots, n-1\}$ is a group under multiplication modulo n if and only if n is prime. That is $\mathbb{Z}_p - \{0\}$ is a group under multiplication modulo p if and only if p is a prime. $\mathbb{Z}_7$ is a group under multiplication modulo 7. This can verify by the table:

mod 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

From the above table it is observed that 1 is the identity element and $2^{-1} = 4, 3^{-1} = 3, 5^{-1} = 5$.

(ix) Let $U(n)$ the set of all positive integer less than n and relatively prime to n. That is $U(n) = \{m: 1 \leq m < n,$ and $gcd\ (m, n) = 1\ \}$. Then $U(n)$ is a group under multiplication modulo n. For $n = 10$, $U(10) = \{1, 3, 7, 9\}$ is a group under multiplication modulo 10. The Cayley table for $U(10)$ is

mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(x) $G = \{1, -1, i, -i\}$ is a group under multiplication. This can be verified by the bellow table:

×	**1**	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
1	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	-1

(xi) The set $G = \{2, 4, 6, 8\}$ is a group under multiplication modulo 10. This can be shown in bellow table:

mod 10	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

(xii) The set $G = \{1, 2, 3\}$ under multiplication modulo 4 is not a group as $(2 \times 2) \bmod 4 = 0 \notin G$.

Example: Check whether the following operation $*$ on real number form a group or not.

$$a * b = a + b - ab, \forall a, b \in \mathbb{R}.$$

Solution: (i) Closure:

$$a * b = a + b - ab \in \mathbb{R}, \qquad \forall a, b \in \mathbb{R}$$

(ii) Associative: We have to prove, $a * (b * c) = (a * b) * c$

$$a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$$
$$a * (b * c) = a + b + c - bc - ab - ac + abc$$
$$a * (b * c) = a + b + c - ab - bc - ac + abc$$

Now,

$$(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c$$
$$(a * b) * c = a + b + c - ab - ac - bc + abc$$
$$(a * b) * c = a + b + c - ab - bc - ac + abc$$

Clearly, $a * (b * c) = (a * b) * c$, $\forall a, b, c \in \mathbb{R}$. Hence, associative property hold.

(iii) Identity: 0 is the identity element as

$$a * 0 = 0 * a = a + 0 - a.0 = a, \forall a \in \mathbb{R}.$$

(iv) Inverse: Let $a \in \mathbb{R}$, and $b \in \mathbb{R}$ such that

$$a * b = b * a = 0.$$
$$\Rightarrow a + b - ab = b + a - ba = 0$$
$$\Rightarrow a + b - ab = a + b - ab = a + b(1 - a) = 0$$
$$\Rightarrow b = \frac{-a}{1-a}, \text{ provided } a \neq 1.$$

Thus, inverse of 1 does not exist and hence $\mathbb{R}$ is not a group under the given binary operation $*$. It is a monoid.

########## upto this I have edited

Abelian Group: A group $(G, *)$ is said to be an abelian group if $a * b = b * a$, $\forall$ $a, b \in G$. It is also called commutative group.

Example: $(Z, +)$ is an abelian group. Since, $a + b = b + a, \forall\ a, b \in G$. Therefore, Z is an abelian group under addition.

Example: Set of all 2×2 matrices over integers under addition form an abelian group.

Example: Let $G = R - \{0\}$ and $a * b = \frac{ab}{2}, \quad \forall$ a, b $\in G$. Show that (G, *) is an abelian group.

Solution: (1) Closure: $a * b = \frac{ab}{2}, \forall\ a, b \in G$.

(2) Associative: $(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4}$.

$$a * (b * c) = a * (\frac{bc}{2}) = \frac{abc}{4}.$$

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

(3)Identity: $a * 2 = \frac{a.2}{2} = a, \quad \forall\ a \in G$.

$$2 * a = \frac{2.a}{2} = a, \quad \forall\ a \in G.$$

Hence 2 is an identity element of G.

(4) Inverse: Let $a \in G, \exists\ b \in G$ such that

$$a * b = b * a = 2.$$

$$\Rightarrow \frac{ab}{2} = \frac{ba}{2} = 2.$$

$$\Rightarrow \text{b} = \frac{4}{a}.$$

Hence inverse of a is $\frac{4}{a}$.

So, G is a group.

$a * b = \frac{ab}{2}, \quad b * a = \frac{ba}{2}.\ (ab = ba, \forall\ a, b \in R)$

$$\Rightarrow \quad a * b = b * a, \ \forall \ \ a, b \in G.$$

Thus, G is an abelian group.

Example: Show that in a group $G, if\ a^2 = e\ \forall a \in G$, then G is a commutative group.

Proof: $ab = eab = (ba)^2 ab = babaab$

$$= baba^2 b = babeb = bab^2 = bae = ba.$$

$$\Rightarrow \quad ab = ba, \ \forall a, b \in G.$$

$\Rightarrow$ G is an abelian group.

Example: One can verify that $(Q, +)$ and $(R, +)$ is an abelian group.

Example: $G = \{0, 1, 2, 3, 4\}$ defined on a operation $(*)$ on G by

$a * b = c$, where c is least nonnegative integer obtained as remainder when $a + b$ divided by 5.

For example $3 * 4 = 2$. Then * is a binary operation.

Now, we can verify G is a group under binary operation $*$.

Example: $G = \{1, -1, i, -i\}$ is a group under multiplication.

Lemma: In a group G

(i) Identity element is unique.
(ii) Inverse of each element $a \in G$ is unique.
(iii) $(a^{-1})^{-1} = a$, ∀ a ϵ G.
(iv) $(ab)^{-1} = b^{-1}a^{-1}$, ∀ a, b ϵ G.
(iv) $ab = ac$ implies $\boldsymbol{a = c}$, and $ba = ca$ implies $\boldsymbol{a = c}$ $\forall\, a, b, c \in G$.

Proof: (i) Suppose e and e' be two identity elements of a group G. Let e be an identity and $e' \in G$.

Then $ee' = e'e = e'$ (1)

Let e' be an identity and $e \in G$. Then

$e'e = ee' = e$ (2)

Then from (1) and (2), we have $e = e'$.

(ii) Let **a ϵ G** be any element and let **a'** and **a"** be two inverse of **a**, then

$$aa' = a'a = e$$
$$aa'' = a''a = e$$

Now, $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. Hence, inverse of a is unique.

(iii) Since $a^{-1}$is inverse of a.

$aa^{-1} = a^{-1}a = e$

a is inverse of a^{-1}. Thus, $(a^{-1})^{-1} = a$.

(i) We have to prove ab is inverse of $b^{-1}a^{-1}$.

$$(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$$

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$. Similarly,

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e.$$

(ii) Let $ab = ac$. Then

$$b = eb = (a^{-1}a)b = a^{-1}(ac) = (a^{-1}a)c = ec = c.$$

$\Rightarrow b = c.$

Subgroup: A non empty subset H of a group G is said to be subgroup of G, if H forms a group under the binary operation of G.

Example: $(Z, +)$ is a subgroup of $(R, +)$.

Theorem: Intersection of two subgroup is a subgroup.

Theorem: Union of two subgroup is a subgroup if and only if one of them is contained in the other.

Coset: Let H be a subgroup of G and let $a \epsilon G$ be any element. Then $Ha = \{ha : h \epsilon H\}$ is called a right Coset of H in G. $aH = \{ah: h\epsilon H\}$ is said to be left Coset of H in G.

Theorem: Let aH and bH be two cosets of H. Then either aH and bH are disjoint or they are identical.

Note: Union of all the right coset of H in G will equal G.

Remark: Note that a coset is not essentially a subgroup.
For example $G = \{1, -1, i, -i\}$ is a group under multiplication. $H = \{1, -1\}$ is a subgroup under multiplication but $Hi = \{i, -i\}$ is not a subgroup.

Order of a Group: Order of a group is number of elements of a group. It is denoted by $O(G)\ or\ |G|$.

Example: $G = \{1, -1\}$ is a group under multiplication. Then $O(G) = 2$.

Order of an Element: Let G be a group and $a \epsilon G$ be any element. We say a is of order n if n is least positive integer such that $a^n = e$.

Example: $G = \{1, -1, i, -i\}$ is a group under multiplication. Since, $(-1)^2 = 1$, therefore $o(-1) = 2$. And $O(i) = 4, o(-i) = 4$.

LAGRENGE'S THEOREM : If G is a finite group and H is a subgroup of G then $o(H)$ divides $o(G)$.

Prove: If G is a finite group and H is a subgroup, then $O(H)$ divides $O(G)$.
Let $O(G) = n$. Since corresponding to each element in G, we can define a right coset of H in G. So the number of distinct right coset of H in G less than or equal to n.
By equivalence classes $= H_{a_1} \cup H_{a_2} \cup H_{a_3} \ldots \cup H_{a_t}$, where t is number of distinct cosets of H in G.

$$\Rightarrow \quad O(G) = O(H_{a_1}) + O(H_{a_2}) + O(H_{a_3}) + \cdots + o(H_{a_t}).$$

As we know two right cosets are either equal or have no element common.

$$\Rightarrow \quad O(G) = O(H) + O(H) + O(H) + \cdots + O(H) \quad (t\ times)$$
$$\Rightarrow \quad O(G) = t.O(H)$$
$$\Rightarrow \quad O(H)/O(G).$$

Definition: Let G be a group and H, a subgroup of G. The index of H in G is the number of distinct right (left) coset of H in G. It is dented by $i_{G(H)}$ or $[G:H]$.

$$[G:H] = o(G)/O(H)$$

Cyclic Group: A group G is said to be cyclic if $\exists\ a \in G$ such that every element of G can be expressed as a power of a. a is said to be generator of group G and denoted as $G = < a >$.

$$i.e.$$

G is said to be cyclic group if there exist an element $a \in G$ such that $G = \{a^n : n \in N\}$.

Example: $G = \{1, -1, i, -i\}$ is a cyclic group under multiplication.

$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$. Here, $-i$ is also generator of group G. Thus, i and $-i$ are generator of G.

Example: $Z_5 = \{0, 1, 2, 3, 4\}$ is a group under addition modulo 5. One can verify that it is a cyclic group.

Theorem: Order of a cyclic group is equal to the order of its generator.

Theorem: A subgroup of a cyclic group is cyclic.

Normal Subgroup: A subgroup of a group G is said to be normal subgroup of G if $aH = Ha\ \forall\ a \in G$.

Example: $H = \{1, -1\}$ is a normal subgroup of group $G = \{1, -1, i, -i\}$. It is clear that $Ha = aH\ \forall\ a \in G$.

NOTE: All subgroup of an abelian group is normal.

Example: $(Q *, .)$ is a normal subgroup of $(R *, .)$. Since, $(R *, .)$ is an abelian group and $(Q *, .)$ is subgroup of $(R *, .)$. $Qa = aQ, \forall\ a \in R$.

Group Homomorphism: Let $< G, * >$ and $< G', O >$ be two groups. A mapping $f: G \to G'$ is called homomorphism if

$$f(a * b) = f(a)\ o\ f(b).$$

Example: Let $(Z, +)$ and $(E, +)$ be the group of integers and even integers. Define a map $f : Z \to E$ such that $f(x) = 2x, \forall\ x \in Z$. Check f is a homomorphism or not.

Proof: First, we check f is well defined.

$$x = y$$
$$2x = 2y$$
$$f(x) = f(y)$$

f is well defined.

Now, $f(x + y) = 2(x + y)$

$$f(x + y) = 2x + 2y$$
$$f(x + y) = f(x) + f(y)$$

Hence, f is a homomorphism.

Example: Let $G = (Z, +)$. $f: G \to G$ defined by $f(x) = x + 3$. Examine f is a homomorrphism or not.

Solution: $f(x + y) = x + y + 3 = x + 3 + y = f(x) + y$
$f(x + y) \neq f(x) + f(y)$. Hence, f is not a homomorphism.

Example: Let $G = (R *, .)$ be a group. A map $f: G \to G$ defined by $f(x) = |x|$. Check f is a homomorphism or not.
Solution: $f(xy) = |xy| = |x||y| = f(x)f(y)$. Hence, f is a homomorphism.

Theorem: *If* $f: G \to G'$ is a homomorphism, then
(i) $f(e) = e'$
(ii) $f(x^{-1}) = (f(x))^{-1}$
(iii) $f(x^n) = (f(x))^n$
Proof: (i) We have,

$$e.e = e$$
$$f(e.e) = f(e)$$
$$f(e)f(e) = f(e)e'$$
$$f(e) = e' \qquad (by\ cancellation).$$

(ii) Again, $xx^{-1} = e = x^{-1}x$
$f(xx^{-1}) = f(e) = f(x^{-1}x)$
$f(x)f(x^{-1}) = e = f(x^{-1})f(x)$
$(f(x))^{-1} = f(x^{-1})$

(i) Let n be a positive integer such that
$x^n = x.x \ldots x\ (n\ times)$
$f(x^n) = f(x).f(x) \ldots f(x)\ (n\ times)$
$f(x^n) = (f(x))^n$

Example: Let $G = (R *, .)$ and $G' = (R, +)$ be two groups. A map $f: G \to G'$ by $f(x) = x^2$. Check f is a homomorphism or not.
Solution: $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$
$f(xy) \neq f(x) + f(y)$
Therefore, f is not a homomorphism.

Example: If $G = (R, *, .)$ is a group and a map $f: G \to G$ defined by $f(x) = x^2$ then check f is a homomorphism or not.

Solution: $f(x.y) = (xy)^2 = x^2y^2 = f(x).f(y)$. Hence, f is a homomorphim.

Example: Let $G = (R, +)$ and $G' = (R, .)$ be two groups. A map $f: G \to G'$ defined by $f(x) = x + 2$. Check whether f is homomorphism or not.
Solution: $f(x + y) = x + y + 2 \neq f(x).f(y)$. Hence, f is not a homomorphism.

RING: A non empty set **R** together with two composition (operation) + and . is said to form a ring if the following axioms are satisfied:
(i) $a + b \in R\ \forall\ a, b \in R$.

(ii) $a + (b + c) = (a + b) + c, \forall\, a, b, c \in R$.
(iii) $\exists\, e \in R$ such that $a + 0 = 0 + a = a, \forall\, a \in R$.
(iv) For each $a \in R, \exists -a \in R$ such that $a + (-a) = (-a) + a = 0$.
(v) $a + b = b + a, \forall a, b \in R$.
(vi) $a.b \in R, \forall\, a, b \in R$.
(vii) $a.(b.c) = (a.b).c, \forall\, a, b, c \in R$.
(viii) $a.(b + c) = a.b + a.c$
$(b + c).a = b.a + c.a \;\forall\, a, b, c \in R$.

Definition: A ring R is said to be commutative ring if $ab = ba \;\forall\, a, b \in R$.

Note: If $\exists$ e $\in$ R such that $a.e = e.a = a, \forall\, a \in R$. Then R is said to be ring with unity**.**

Example: $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ form rings with usual addition and multiplication. These all are commutative rings with unity 1.

Example: Set of all even integers form a commutative ring without unity.

Example: The set $Z_n = \{0, 1, \ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring with unity 1. The set of units is $U(n)$.
Example: The set $Z[x]$ of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$.
Theorem: In a ring, the following results hold:
(1) $a.0 = 0.a = 0, \forall\, a \in R$.
(2) $a(-b) = (-a)b = -ab, \forall\, a, b \in R$.
(3) $a(b - c) = ab - ac, \;\forall\, a, b \in R$.
(4) $(-a)(-b) = ab, \;\forall\, a, b \in R$.
Proof: (1) $a.0 = a.(0 + 0) \quad (since\ 0 \in R)$
$\Rightarrow a.0 = a.0 + a.0 \quad (by\ distributive)$
$\Rightarrow a.0 + 0 = a.0 + a.0$
$\Rightarrow 0 = a.0 \;(by\ cancellation\ with\ respect\ to\ (R, +))$
$\Rightarrow a.0 = 0$
(2) by (1), $a.0 = 0$.
$\Rightarrow a\big(b + (-b)\big) = a.b + a.(-b) = 0 \quad (by\ distributive)$
$\Rightarrow a.(-b) = -ab$.
(3) $a(b - c) = a\big(b + (-c)\big) = a.b + a.(-c) \quad (by\ distributive)$
$\Rightarrow a(b - c) = ab - ac$.
(4) $(-a)(-b) = -(a(-b)) = -(-ab)$.

Zero divisor: Let R be a ring. An element $0 \neq a \in R$ is said to be a zero divisor if there exists an element $0 \neq b \in R$ such that $ab = 0$, then either $a = 0$ or $b = 0$.

Example: Let $Z_4 = \{0, 1, 2, 3\}$ be ring under addition and multiplication modulo 4. ***Here 2.2 = 0*** but $2 \neq 0$. Therefore 2 is a zero divisor.

Example: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is a ring under addition and multiplication modulo 7. There is no any $0 \neq a, 0 \neq b \in Z_7$such that $ab = 0$. Hence, there is no any zero divisor in Z_7.

Integral domain: A commutative ring R is said to be an integral domain if $ab = 0$, then either $a = 0$ or $b = 0$. i.e. An integral domain is commutative ring with unity $(1 \neq 0)$ with no zero-divisor.

Example: Z is an integral domain. Z is a commutative ring with unity 1 and $ab = 0$ implies $a = 0$ or $b = 0, \forall\, a, b \in Z$.

Example: $Z_5 = \{0, 1, 2, 3, 4\}$ is an integral domain. There is no any 0 ≠ a, 0 ≠ b $\in Z_5$ such that $ab = 0$.

Example: The ring of Gaussian integers $Z[i] = \{a + ib : a, b \in Z\}$ is an integral domain.

Example: The ring $Z[x]$ of polynomials with integer coefficients is an integral domain.

Example: The ring Z_p of integers modulo a prime p is an integral domain.

Example: The ring Z_n of integers modulo n is not a integral domain when n is not a prime.

Example: The ring $M_2(Z)$ of matrices of order 2 over the integers is not a integral domain.

Definition: A ring with unity is called a divison ring or skew field if non-zero element of R form a group with respect to multiplication.

Field: A commutative divison ring is said to be field.

Or

A non empty set F is said to be field under under two composition (operation) addition and multiplication if it is abelian group under addition and also an abelian group under multiplication, and distributive property with addition and multiplication.

$i.e.$

$(i)\ a + b \in F, \forall\, a, b \in F.$

$(ii)\ a + (b + c) = (a + b) + c, \forall\, a, b, c \in F.$

(iii) There exist some element $0 \in F$ such that $a + 0 = 0 + a = a, \forall\, a \in F.$

(iv) For each $a \in F$ there exist $-a \in F$ such that $a + (-a) = (-a) + a = 0$.

(v) $a + b = b + a \; \forall \; a, b \in F$.

(iii) $a.b \in F \; \forall \; a, b \in F$.

(iv) $a.(b.c) = (a.b).c, \forall a, b, c \in F$.

(v) There exist $1 \in F$ such that $a.1 = 1.a = a, \forall \; a \in F$.

(vi) For each $a \in F$, $\exists \; b \in F$ such that $a.b = b.a = 1$.

(vii) $a.b = b.a, \forall \; a, b \in F$.
$a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a, \forall \; a, b, c \in F$.

Example: $(R *, +, .)$ is a field. Since $(R, +)$ is an abelian group and $(R *, .)$ is also abelian group and property (xi) is hold.

Question. Let N be set of natural numbers. For each of the following determine whether (*) is an associative operation.

(1) $a * b = a$
(2) $a * b = max\,(a, b)$
(3) $a * b = min\,(a, b + 2)$
(4) $a * b = a + b + 3$
(5) $a * b = a + 2b$

Solution: (1) $(a * b) * c = a * c = a$.

$$a * (b * c) = a * b = a.$$

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

(2) Let $a * b = max\,(a, b)$

Suppose, $a, b, c \in N$ such that $a < b < c$.

$(a * b) * c = max(a, b) * c = b * c = max(b, c) = c$.

$a * (b * c) = a * max\,(b, c) = a * c = max(a, c) = c$.

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

(3) $a * b = min\,(a, b + 2)$

Consider, $a, b, c \; N$ such that $a < b < c$.

$$(a * b) * c = min(a, b + 2) * c = a * c = min(a, c + 2) = a.$$

$$a * (b * c) = a * min\,(b, c + 2) = a * c = min(a, c + 2) = a.$$

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

(4) $a * b = a + b + 3$.

$$(a * b) * c = (a + b + 3) * c = (a + b + 3) + c + 3 = a + b + c + 6.$$

$a * (b * c) = a * (b + c + 3) = a + (b + c + 3) + 3 = a + b + c + 6.$

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

(6) $a * b = a + 2b.$

$(a * b) * c = (a + 2b) * c = a + 2b + 2c$

$a * (b * c) = a * (b + 2c) = a + 2(b + 2c) = a + 2b + 4c$

$\Rightarrow (a * b) * c \neq a * (b * c).$

$\Rightarrow$ It is not associative.