Algebraic Structures

Samarjit Kar

Department of Mathematics

National Institute of Technology

Durgapur

Algebraic Structures

- Algebraic systems Examples and general properties
- Semi groups
- Monoids
- Groups & Subgroups
- Rings and Subrings
- Integral Domain
- Fields

Abstract algebra

Algebra is about operations on sets. You have met many operations; for example:

- addition and multiplication of numbers;
- modular arithmetic;
- addition and multiplication of polynomials;
- addition and multiplication of matrices;
- union and intersection of sets;
- composition of permutations.

Many of these operations satisfy similar familiar laws. In all these cases, the “associative law” holds, while most (but not all!) also satisfy the “commutative law”.

Algebraic systems

- $\mathbb{N} = \{1, 2, 3, 4, \ldots\ldots \infty\}$ = Set of all natural numbers.

  $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\ldots \infty\}$ = Set of all integers.

  $\mathbb{Q}$ = Set of all rational numbers.

  $\mathbb{R}$ = 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).

If A is a nonempty set, a binary operation $*$ on A is a function $* : A \times A \rightarrow A$.

Ex: The set $\mathbb{N}$ 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: $(\mathbb{N}, +), (\mathbb{Z}, +, -), (\mathbb{R}, +, ., -)$ are 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
- $*$ is an associative operation, for all a, b, c in A.

Ex. $(\mathbb{N}, +)$ is a semi group.

Ex. $(\mathbb{N}, .)$ is a semi group.

Ex. $(\mathbb{N}, -)$ is not a semi group.

- **Monoid**: An algebraic system $(A,*)$ is said to be a monoid if the following conditions are satisfied.

  $*$ is an associative operation in A.

  There is an identity in A.

Group

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

  $*$ is an associative operation, i.e.,

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

  There is an identity in G, i.e.,

  $\exists e \in G : \forall a \in G : ea = a$

  Every element in G has inverse in G, i.e.,

  $\forall a \in G \; \exists \; a' \in G : \; a * a' = a' * a = e$

- **Abelian group** (Commutative group): A group $(G,*)$ is said to be abelian (or commutative) if $a * b = b * a$.
- The notion abelian, finite, infinite and order are introduced for semigroups and monoids in the same way as for groups. In this lecture we will not consider properties of semigroups or monoids any further. They were only mentioned for the sake of completeness.

Examples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are abelian groups with the usual addition as operation. In each of the cases the number zero is the identity (neutral) element, and for a number a the negative $-a$ is the inverse element.
- $(\mathbb{Q} - \{0\}, \cdot)$ and $(\mathbb{R} - \{0\}, \cdot)$ with the usual multiplication as operation are also abelian groups. The number one is in each case the neutral element, and for a number a the inverse is just $\frac{1}{a}$.
- In contrast to the last example $(\mathbb{Z} - \{0\}, \cdot)$ is only an abelian monoid with the number one as neutral element. The last axiom is not fulfilled, since only the integers $a = 1$ and $a = -1$ have inverses in $\mathbb{Z} - \{0\}$.
- $(\mathbb{N}, +)$ is also only an abelian monoid with the number zero as neutral element, since for a number $a > 0$ has no inverse in $\mathbb{N}$.
- The simplest group is a group containing only one element, $G = \{e\}$, with the group operation defined by $e \cdot e = e$.

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

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

   $a * c = b * c \implies a = b$ (Right cancellation law)
4. $(a * b)^{-1} = b^{-1} * a^{-1}$

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

Proof of (i): Let e_1 and e_2 are two identity elements in G. Now, $e_1 * e_2 = e_1 \ldots ... (1)$ (since e_2 is the identity)

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

From (1) and (2), we have $e_1 = e_2$. Identity element in a group is unique.

Proof of (ii): Suppose $a \in G$. By the third property of groups, there is one element $a' \in G$ such that $a * a' = a' * a = e$.

Suppose $a'' \in G$ also satisfy the same property, i.e $a * a'' = a'' * a = e$. Then, clearly $a * a' = a * a''$. So, by left cancellation $a' = a''$. So, the uniqueness of the "inverse" of a is established.

Proof of (iii): 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, $a * b = e \ldots ... (1)$ (Since, b is inverse of a)

Again, $a * c = e \ldots ... (2)$ (Since, c is also inverse of a) From (1) and (2), we have

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

In a group, the inverse of any element is unique.

Proof of (iv): 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, $(a * b)^{-1} = b^{-1} * a^{-1}$.

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

Solution: Let $\mathbb{R}^+ =$ set of all non zero real numbers. Let a, b, c are any three elements of $\mathbb{R}^+$.

1. Closure property: We know that, product of two nonzero real numbers is again a nonzero real number . i.e., $a \,.\, b \in \mathbb{R}^+$ for all $a, b \in \mathbb{R}^+$.

2. Associativity: We know that multiplication of real numbers is associative. i.e., $(a.b).c = a.(b.c)$ for all $a, b, c \in \mathbb{R}^+$.

3. Identity : We have $1 \in \mathbb{R}^+$ and $a.1 = a$ for all $a \in \mathbb{R}^+$. Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in \mathbb{R}^+$, we have $\frac{1}{a} \in \mathbb{R}^+$ such that $a.\frac{1}{a} = 1$ i.e., Each element in $\in \mathbb{R}^+$ has an inverse.

5. Commutativity: We know that multiplication of real numbers is commutative. i.e., $a \,.\, b = b.a$ for all $a, b \in \mathbb{R}^+$.

Hence, $(\mathbb{R}^+, .)$ is an abelian group.

Note: Set of all real numbers '$\mathbb{R}$' is not a group with respect to multiplication.

Example: 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. Closure property: 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. Associativity: $(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4}$

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

3. Identity : Let e be the identity element. We have

$$a * e = \frac{ae}{2} \quad \ldots\ldots (1)$$

By the definition of $*$ again, $a * e = a$ …… (2)

Since e is the identity. From (1)and (2), $\frac{ae}{2} = a \Longrightarrow e = 2$ and $2 \in A$. Identity element exists, and '2' is the identity element in A.

4. Inverse: Let $a \in A$ let us suppose b is inverse of a. Now,

$a * b = \frac{ab}{2}$ ….. (1) (By definition of inverse.)

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

From (1) and (2), it follows that $\frac{ab}{2} = 2 \Longrightarrow b = \frac{4}{a} \in A$

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

5. Commutativity: $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$.

Hence, $(A, *)$ is an abelian group.

Order of a group: The number of elements in a group G is called order of the group. It is denoted by $|G|$.

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

Obvioulsy, a group can have infinite order. For example $|\mathbb{Z}_n| = n$ and $|\mathbb{Z}| = \infty$.

Example: 1. Any singleton set $\{e\}$ can be given a group structure by defining $e * e = e$.

2. Also, the subset $\{0\}$ of $\mathbb{Z}$ is a group under addition.

3. Also, the subset $\{1\}$ of $\mathbb{Z}$ is a group under multiplication.

Note: Suppose $n \geq 0$ is a non-negative integer. In the additive notation, $na = a + a + \cdots + a$ denotes sum of a with itself n times. Also $-na = -(na)$. In multiplicative notation, $a^n = a \cdot a \cdots a$ product of a with itself n times. Also $a^{-n} = (a^{-1})^n$.

If $*$ is a binary operation on a finite set S, then properties of $*$ often correspond to properties of the **Cayley table**.

Example: $*$ is commutative if $x * y = y * x$ for all $x, y \in S$. This means that the (x, y)-entry in the Cayley table is equal to the (y, x)-entry. In other words, the Cayley table is symmetric (assuming that the rows and columns are labelled in the same order). Conversely, if $*$ is not commutative, then the Cayley table will not be symmetric. So the Cayley table of an abelian group is symmetric, while that of a non-abelian group is not symmetric. For example, below is the Cayley tables of the non-abelian group S_3, also known as the symmetry group of the equilateral triangle. Here e denotes the identity map, σ, τ are rotations, and α, β, γ are reflections.

Definition: A *Latin square* of order n is an $n \times n$ array, in which each entry is labelled by one of n labels, in such a way that each label occurs exactly once in each row, and exactly once in each column.

Examples of Latin squares appear every day in newspapers, in the form of Sudoku puzzles. They also have more serious applications in the theory of experimental design.

$*$	e	σ	τ	α	β	γ
e	e	σ	τ	α	β	γ
σ	σ	τ	e	β	γ	α
τ	τ	e	σ	γ	α	β
α	α	γ	β	e	τ	σ
β	β	α	γ	σ	e	τ
γ	γ	β	α	τ	σ	e

Lemma 1: The Cayley table of any finite group is a Latin square.

Example: Show that $G = \{1, -1, i, -i\}$ is an abelian group under multiplication.

Solution: The composition table of G is

$\cdot$	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 $1 \in G$.
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 '$\cdot$' is commutative. Hence, (G, .) is an abelian group.

Is $(\mathbb{Z}_n, +)$ a group?

Is $(\mathbb{Z}_n{}^*, *)$ a group?

Subgroups

Definition: A subgroup of a group $(G,*)$ is a subset of G which is also a group with respect to (the restriction of) the same binary operation $*$ as in G.

In particular, if H is a subgroup of $(G,*)$, then the restriction of $*$ is a binary operation on H, in other words H is closed with respect to $*$.

Examples:

1. $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are subgroups of $(\mathbb{C},+)$.

2. If n is a positive integer, then the set $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$ of all multiples of n is a subgroup of $(\mathbb{Z},+)$.

3. The special linear group $SL_n(R)$ of $n \times n$ matrices with real entries and determinant 1 is a subgroup of the general linear group $GL_n(R)$ of all invertible $n \times n$ matrices with real entries.

If H is a subgroup of G, we write $H \leq G$; if H is a proper subgroup of G, that is, $H \neq G$, then we write $H < G$. G is the improper subgroup of G. The subgroup $\{e\}$ is the trivial subgroup of G. All other subgroups are nontrivial.

Examples: 1. $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

2. $(\{-1,1\},.) \leq (\mathbb{Q}^*,.) \leq (\mathbb{R}^*,.) \leq (\mathbb{C}^*,.)$

There is a simple way of determining when a given subset of a group is in fact a subgroup.

The Subgroup Test

Theorem 1: Let $(G,*)$ be a group and $H \subset G$. Then H is a subgroup of G if and only if the following criteria are satisfied:

(i) H is closed with respect to $*$, that is $(\forall\, a,b \in H)\ a * b \in H$;

(ii) the identity element e of G is contained in H;

(iii) for each $a \in H$, the inverse a of a^{-1} in G is contained in H.

Theorem 2: A non empty sub set H of a group $(G,*)$ is a sub group of G iff

(i) $a * b \in H, \forall\, a,b \in H$

(ii) $a^{-1} \in H, \forall\, a \in H$

Theorem 3: A necessary and sufficient condition for a non empty subset H of a group $(G,*)$ to be a sub group is that $a,b \in H \Rightarrow a * b^{-1} \in H$.

Proof: Case 1: Let $(G,*)$ be a group and H is a subgroup of G.

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

$\Longrightarrow a * b^{-1} \in H$. (By closure property in H)

Case 2: Let H be a non empty set of a group $(G,*)$.

Let $a * b^{-1} \in H \quad \forall a,b \in H$

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

$\Longrightarrow e \in H$ i.e., identity exists in H.

Now, $e \in H, a \in H \Longrightarrow e * a^{-1} \in H \Longrightarrow \ a^{-1} \in H$.

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

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

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

$$\Longrightarrow a * b \in H.$$

$\therefore \ H$ is closed w.r.t $*$.

Finally, let $a,b,c \in H \Longrightarrow a,b,c \ \in G$ (since $H \ \in G$)

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

$\therefore *$ is associative in H.

Hence, H is a subgroup of G.

Example

The set of cardinality 4 may carry exactly two different group structures. The first is $(\mathbb{Z}_4, +)$

$+$	**0**	1	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

while the second is the Klein 4-group V

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\mathbb{Z}_4$ has only one nontrivial proper subgroup $\{\bar{0}, \bar{2}\}$, while V has three nontrivial proper subgroups, $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$.

Theorem: If $(H_1,*)$ and $(H_2,*)$ are both subgroups of the group $(G,*)$, then $(H_1 \cap H_2,*)$ is also a subgroup.

Proof: The set $H_1 \cap H_2 \neq \phi$, since $e \in H_1 \cap H_2$. Suppose that $a, b \in H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$, since $(H_1,*)$ and $(H_2,*)$ are subgroups of $(G,*)$.

Also $a, b \in H_1 \Longrightarrow a * b^{-1} \in H_1$ and $a, b \in H_2 \Longrightarrow a * b^{-1} \in H_2$.

i.e., $a * b^{-1} \in H_1 \cap H_2$

Thus $H_1 \cap H_2$ is a subgroup of $(G,*)$.

Note: $H_1 \cup H_2$ is not always a subgroup of $(G,*)$.

This can be illustrated through the following example.

Example: Let $H_1 = \{0, \pm 2, \pm 4, \pm 6, \ldots.\}$ and $H_2 = \{0, \pm 3, \pm 6, \pm 9, \ldots.\}$. Here, $(H_1, +)$ and $(H_2, +)$ are subgroups of $(\mathbb{Z}, +)$. Then $H_1 \cap H_2 = \{0, \pm 6, \pm 12, \ldots.\}$.

$(H_1 \cap H_2, +)$ is also a subgroup of $(\mathbb{Z}, +)$.

On the other hand, $(H_1 \cup H_2, +)$ is not a subgroup of $(\mathbb{Z}, +)$. Because $H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \ldots.\}$ and $2, 3 \in H_1 \cup H_2$; but $2 + 3 = 5 \notin H_1 \cup H_2$. Thus $H_1 \cup H_2$ is not closed under $+$.

Note: $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$ if either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Cyclic Subgroups

Theorem: Let G be group and $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G. In fact, H is the smallest subgroup of G that contains a.

Proof: First, recall for a negative integer $k < 0$ we define $a^k = (a^{-k})^{-1}$. Now H is closed under product: for $m, n \in \mathbb{Z}$ we have $a^m . a^n = a^{m+n} \in H$. The identity $e = e^0 \in H$. For $a^n \in H$, we have $(a^n)^{-1} = a^{-n} \in H$. So, H is a subgroup.

Now, suppose K is another subgroup of G that contains a. Since K is closed under multiplication $a^n \in K$ for all non-negative integers n. Again, for negative integers m we have $a^m = (a^{-m})^{-1} \in K$. So, $a^n \in K$, $\forall n \in \mathbb{Z}$. So, $H \subseteq K$. This establishes that H is the smallest subgroup of G that contains a. The proof is complete.

Definition. Let G be a group and $a \in G$.

1. Then, $H = \{a^n : n \in \mathbb{Z}\}$ is called the cyclic subgroup of G generated by a. This H is denoted by $\langle a \rangle$.

2. If $G = \langle a \rangle$ for some $a \in G$, then we say that G is a cyclic group.

Remark. So, a cyclic group is a group that is generated by one element.

Example: 1. $(\mathbb{Z}, +)$ is cyclic, generated by 1 or -1. i.e., $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

2. $(\mathbb{Z}_n, +) = \langle 1 \rangle$ is cyclic. In fact, given any integer k so that $\gcd(k, n) = 1$ we have $(\mathbb{Z}_n, +) = k$. (Exercise)

3. The Klein-4 group is not cyclic.(Exercise)

Theorem: Every cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by a. Then, for $x, y \in G$ we have $x = a^m$, $y = a^n$ for some $m, n \in \mathbb{Z}$. So, $xy = a^m \cdot a^n = a^{m+n} = a^n \cdot a^m = yx$.

Theorem: Let G be cyclic group. Then, any subgroup H of G is also cyclic.

Cosets

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

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

Note:- (i) Any two left (right) cosets of H in G are either identical or disjoint.

(ii) 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.

(iii) Lagrange's theorem: The order of each sub group of a finite group is a divisor of the order of the group.

(iv) The order of every element of a finite group is a divisor of the order of the group.

(v) The converse of the Lagrange's theorem need not be true.

Homomorphism

Homomorphism into: Let $(G,*)$ and $(G',\cdot)$ be two groups and f be a mapping from G into G'. If for $a,b \in G$, $f(a*b) = f(a)\cdot f(b)$, then f is called homomorphism G into G'.

Homomorphism onto: Let $(G,*)$ and $(G',\cdot)$ be two groups and f be a mapping from G onto G'. If for $a,b \in G$, $f(a*b) = f(a)\cdot f(b)$, then f is called homomorphism G onto G'. Also then G' is said to be a homomorphic image of G. We write this as $f(G) \cong G'$.

Isomorphism: Let $(G,*)$ and $(G',\cdot)$ be two groups and f be a one-one mapping of G onto G'. If for $a,b \in G$, $f(a*b) = f(a)\cdot f(b)$, then f is said to be an isomorphism from G onto G'.

Endomorphism: A homomorphism of a group G into itself is called an endomorphism.

Monomorphism: A homomorphism into is one-one, then it is called an monomorphism.

Epimorphism: If the homomorphism is onto, then it is called epimorphism.

Automorphism: An isomorphism of a group G into itself is called an automorphism.

Example 1: If R is the group of real numbers under the addition and R^+ is the group of positive real numbers under the multiplication. Let $f: R \to R^+$ be defined by $f(x) = e^x$, then show that f is an isomorphism.

Solution: Let $f: R \to R^+$ be defined by $f(x) = e^x$.

f is one-one: Let $a, b \in G$ and $f(a) = f(b) \Rightarrow e^a = e^b \Rightarrow \log e^a = \log e^b \Rightarrow a \log e = b \log e \Rightarrow a = b$. Thus f is one-one.

f is onto: If $c \in R^+$ then $\log c \in R$ and $f(\log c) = e \log c = c$. Thus each element of R^+ has a pre-image in R under f and hence f is onto.

f is Homomorphism: $f(a + b) = e^{a+b} = e^a . e^b = f(a) . f(b)$.

Hence f is an isomorphism.

Example 2: Let G be a group of positive real numbers under multiplication and G' be a group of all real numbers under addition. The mapping $f: G \to G'$ given by $f(x) = log_{10} x$. Show that f is an isomorphism. (Exercise)

Exercise

Problem 1: Prove that if $a^2 = a$, then $a = e$, a being an element of a group G.

Problem 2: In a group G having more than one element, if $x^2 = x$, for every $x \in G$.

Problem 3: Show that in a group G, for $a, b \in G$, $(ab)^2 = a^2b^2 \Leftrightarrow G$ is abelian. Also show that a group G such that $(ab)^n = a^n b^n$ for three consecutive integers n, and $\forall\, a, b \in G$ is a commutative group.

Problem 4: In a group G, a is an element of order 30. Find order of a^5.

Problem 5: Let $H = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq \mathbb{Z}_6$. Check that $(H, +)$ is a subgroup of $(\mathbb{Z}_6, +)$.

Problem 6: Let G be the group and $Z = \{x \in G \mid xy = yx \text{ for all } y \in G\}$. Prove that Z is a subgroup of G.

Problem 7: Let G be the additive group of integers and G' be the multiplicative group. Then mapping $f : G \to G'$ given by $f(x) = 2^x$ is a group homomorphism of G into G'.

Problem 8: Let G be a multiplicative group and $f: G \to G$ such that for $a \in G$, $f(a) = a^{-1}$. Prove that f is one-one and onto. Also, prove that f is homomorphism if and only if G is commutative.

Rings

- We can define more than one operation on a set.
- A ring is a set together with two operations (usually called $+$ and .). A ring is also called a system of double composition.

Definition: A ring R is a set together with two binary operations $+$ and ., satisfying the following properties:

1. $(R, +)$ is a commutative group.
2. '.' is associative.
3. The distributive laws hold in R:

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

Note: '$+$' refers to addition and '.' refers to multiplication although these operations need not necessarily have the meninges they have in arithmetic.

Examples

Example 1: Do the integers Z form a ring?

$(\mathbb{Z}, +)$ is a commutative group.

$(\mathbb{Z},.)$ is a semi-group. The distributive law also holds. So, $(\mathbb{Z}, +, .)$ is a ring.

Example 2: Ring of Integers modulo n

$(\mathbb{Z}_n, +, .)$ is a commutative group, where '$+$' is addition (mod n).

$(\mathbb{Z}_n, .)$ is a semi group here '.' denotes multiplication (mod n).

Also the distributive laws hold. So $(\mathbb{Z}_n, +, .)$ is a ring.

Many other examples also can be given on rings like $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ and so on.

Some Definitions

Trivial Ring: A set consists of only the null element 0 forms a ring called trivial ring.

Ring with Unity: If a ring $(R, +, .)$ has the multiplicative identity 1, it is called a ring with unity.

Example: $(\mathbb{Z}, +, .)$ is a ring with identity.

Commutative Ring: A ring $(R, +, .)$ is called a commutative ring if '.' is commutative.

Example: $(\mathbb{Z}, +, .)$ is a commutative ring.

Some Definitions

Division Ring: A ring $(R, +, *)$ with identity is called a division ring if all its non-zero elements are invertible.

Example: In the ring $(Z_6, +, .)$ $\bar{2}, \bar{3}, \bar{4}$ are divisors of zero since $\bar{2}.\bar{3} = \bar{6} = \bar{0}$, and $\bar{3}.\bar{4} = \overline{12} = \bar{0}$.

On the other hand the rings $(\mathbb{Z}, +, .)$, $(Q, +, .)$, $(\mathbb{R}, +, .)$ contains no divisor of zero.

Subring: A subring of the ring $(R, +, *)$ is a subset of R which by itself is a ring with respect to the same set of binary operations.

Example: $(\mathbb{Z}, +, .)$ is a subring of $(Q, +, .)$ and $(\mathbb{R}, +, .)$

Integral Domain: A commutative ring with identity but without zero divisor is called an integral domain.

Example: $(\mathbb{R}, +, .)$ is an integral domain

Fields

Definition: A field F is a set together with two binary operations $+$ and $*$, satisfying the following properties:

1. $(F, +)$ is a commutative group.

2. $(F - \{0\}, *)$ is a commutative group.

3. The distributive laws hold in F:

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

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

Example 1: Do the integers Z form a field?

$(\mathbb{Z}, +)$ is a commutative group.

but $(\mathbb{Z} - \{0\}, .)$ do not form a group!

there are no multiplicative inverses…

Examples

Example 2: The real numbers $\mathbb{R}$ form a field.

$(\mathbb{R}, +)$ is a commutative group.

$(\mathbb{R} - \{0\}, .)$ is a commutative group.

The distributive law holds.

Example 3: $\mathbb{Z}_p$ (for prime p) is a field.

$(\mathbb{Z}_p, +)$ is a commutative group.

$(\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}, .)$ is a commutative group.

The distributive law holds.

Problem 1: If in a ring R with unity $(xy)^2 = x^2y^2, \forall x, y \in R$ then R is commutative.

Problem 2: Prove that $(\mathbb{Z}, *, \circ)$ is a commutative ring, where '$*$' and '$\circ$' are defined as follows:

$a * b = a + b - 1, a \circ b = a + b - ab.$

Problem 3: Prove that every integral domain is a field.

Problem 4: Prove that in a field F the equations $a.x = b$ and $y.a = b$ have unique solutions.