$$W_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Step 5. Construct W_4.

$$W_4 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Step 6. Construct W_5.

$$W_5 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

From W_5, we can conclude that the transitive closure of R is:

$$\{(a,a),(a,c),(b,b),(b,d),(c,a),(c,c),(d,b),(d,d),(e,b),(e,d)\}.$$

Equivalence Relations

Definition: A relation on a set A is called an *equivalence relation* if it is reflexive, symmetric, and transitive. Two elements a and b that are related by an equivalence relation are called *equivalent*. The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

Example: Let R be the relation on the set of integers such that $(a,b) \in R$ if and only if $a = b$ or $a = -b$. Then R is reflexive, symmetric, and transitive. It follows that R is an equivalence relation.

Example: Let R be the relation on the set of real numbers such that $(a,b) \in R$ if and only if $a - b$ is an integer. Is R an equivalence relation?

Solution: Because $a - a = 0$ is an integer for all real numbers a, $(a,a) \in R$ for all real numbers a. Hence, R is reflexive. Now suppose that $(a,b) \in R$. Then $a - b$ is an integer, so $b - a$ is also an integer. Hence, $(b,a) \in R$. It follows that R is symmetric. If $(a,b) \in R$ and $(b,a) \in R$, then

$a - b$ and $b - c$ are integers. Therefore, $a - c = (a - b) + (b - c)$ is also an integer. Hence, $(a, c) \in R$. Thus, R is transitive. Consequently, *R* is an equivalence relation.

Example: Congruence Modulo *m*. Let m be an integer with $m > 1$. Show that the relation $R = \{(a, b) \mid a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers.

Solution: We know that $a \equiv b \pmod{m}$ if and only if m divides $a - b$. Note that $a - a = 0$ is divisible by m, because $0 = 0 \cdot m$. Hence, $a \equiv a \pmod{m}$, i.e. $(a, a) \in R$. So, congruence modulo m is reflexive. Let $(a, b) \in R$. So, $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m, so $a - b = km$, where *k* is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Thus, $(b, a) \in R$, and hence, congruence modulo m is symmetric. Next, suppose $(a, b), (b, c) \in R$. That is $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then m divides both $a - b$ and $b - c$. Therefore, there are integers k and l with $a - b = km$ and $b - c = lm$. Adding these two equations shows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Thus, $a \equiv c \pmod{m}$. Thus, $(a, c) \in R$. Therefore, congruence modulo m is transitive. It follows that congruence modulo m is an equivalence relation.

Example: Show that the "divides" relation on the set of positive integers is not an equivalence relation.

Example: Let R be the relation on the set of real numbers such that $(x, y) \in R$ if and only if x and y are real numbers that differ by less than 1, that is $|x - y| < 1$. Showthat R is not an equivalence relation.

Example: Let R be a reflexive relation on a set A such that

$$(a, b) \in R, (a, c) \in R \Longrightarrow (b, c) \in R.$$

Show that R is an equivalence relation.

Equivalence Classes and Partitions

Equivalence Classes: Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the *equivalence class* of a. The equivalence class of a with respect to R is denoted by $[a]_R$. When only one relation is under consideration, we may not use the subscript R and write $[a]$ for this equivalence class. In other words, if R is an equivalence

relation on a set A, the equivalence class of the element a is $[a]_R = \{x \in A \mid (a, x) \in R\}$. If $b \in [a]_R$, then b is called a **representative** of this equivalence class. Any element of a class can be used as a representative of this class. That is, there is nothing special about the particular element chosen as the representative of the class.

Example: What are the equivalence classes of 0 and 1 for congruence modulo 4?

Solution: The equivalence class of 0 contains all integers a such that $a \equiv 0 \pmod 4$. The integers in this class are those divisible by 4. Hence, the equivalence class of 0 for this relation is

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

The equivalence class of 1 contains all the integers a such that $a \equiv 1 \pmod 4$. The integers in this class are those that have a remainder of 1 when divided by 4. Hence, the equivalence class of 1 for this relation is

$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}.$$

Example: Suppose that R is the relation on the set of strings of English letters such that $a\ R\ b$ if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x. Is R an equivalence relation?

Example: Let n be a positive integer and S a set of strings. Suppose that R_n is the relation on S such that $s\ R_n\ t$ if and only if $s = t$, or both s and t have at least n characters and the first n characters of s and t are the same. That is, a string of fewer than $n + 1$ characters is related only to itself; a string s with at least $n + 1$ characters is related to a string t if and only if t has at least n characters and t begins with the n characters at the start of s. For example, let $n = 3$ and let S be the set of all bit strings. Then $s\ R_3\ t$ either when $s = t$ or both s and t are bit strings of length 3 or more that begin with the same three bits. For instance, $01\ R_3\ 01$ and $00111\ R_3\ 00101$, but not $01\ R_3\ 010$, and $01011\ R_3\ 01110$. Then for every set of strings S and every positive integer n, R_n is an equivalence relation on S.

Example: What is the equivalence class of the string 0111 with respect to the equivalence relation R_3 on the set of all bit strings?

Solution: The bit strings equivalent to 0111 are the bit strings with at least three bits that begin with 011. These are the bit strings $011, 0110, 0111, 01100, 01101, 01110, 01111$, and so on. Consequently,

$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \dots\}.$$

Let A be the set of students at your school who are majoring in exactly one subject, and let R be the relation on A consisting of pairs (x, y), where x and y are students with the same major. Then R is an equivalence relation, as the reader should verify. We can see that R splits all students in A into a collection of disjoint subsets, where each subset contains students with a specified major. For instance, one subset contains all students majoring (just) in computer science and a second subset contains all students majoring in history. Furthermore, these subsets are equivalence classes of R. This example illustrates how the equivalence classes of an equivalence relation partition a set into disjoint, nonempty subsets. We will make these notions more precise in the following discussion.

Let R be a relation on the set A. The following theorem shows that the equivalence classes of two elements of A are either identical or disjoint.

Theorem: Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

(i) $(a, b) \in R$ (ii) $[a] = [b]$ (iii) $[a] \cap [b] \neq \emptyset$.

Proof: We first show that (i) implies (ii). Assume that $(a, b) \in R$. We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then $(a, c) \in R$. Because $(a, b) \in R$ and R is symmetric, $(b, a) \in R$. Furthermore, because *R* is transitive and $(b, a) \in R$ and $(a, c) \in R$, it follows that $(b, c) \in R$. Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar.

Second, we will show that (ii) implies (iii). Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because $_R$ is reflexive).

Next, we will show that (iii) implies (i). Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$. In other words, $(a, c) \in R$ and $(b, c) \in R$. By the symmetric property, $(c, b) \in R$. Then by transitivity, because $(a, c) \in R$ and $(c, b) \in R$, we have $(a, b) \in R$. Because (i) implies (ii), (ii) implies (iii), and (iii) implies (i), the three statements, (i), (ii), and (iii) are equivalent.

Partition of a set: A partition of a set S is a collection of disjoint nonempty subsets of S that have S as their union.

Example: Suppose that $S = \{1, 2, 3, 4, 5, 6\}$. The collection of sets $A_1 = \{1, 2, 3\}, A_2 = \{4, 5\}$, and $A_3 = \{6\}$ forms a partition of *S*, because these sets are disjoint and their union is *S*.

We are now in a position to show how an equivalence relation gives a partition of a set. Let R be an equivalence relation on a set A. The union of the equivalence classes of R is all of A, because an element a of A is in its own equivalence class, namely, $[a]_R$. In other words,

$$\bigcup_{a \in A} [a]_R = A.$$

In addition, these equivalence classes are either equal or disjoint, so $[a]_R \cap [b]_R = \emptyset$, when $[a]_R \neq [b]_R$. These two observations show that the equivalence classes form a partition of A, because they split A into disjoint subsets.

Theorem: Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S, there is an equivalence relation R that has the sets $A_i, i \in I$, as its equivalence classes.

Example: List the ordered pairs in the equivalence relation R produced by the partition $A_1 = \{1, 2, 3\}, A_2 = \{4, 5\}$, and $A_3 = \{6\}$ of $S = \{1, 2, 3, 4, 5, 6\}$.

Solution: The subsets in the partition are the equivalence classes of R. The pair $(a, b) \in R$ if and only if a and b are in the same subset of the partition. The pairs $(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2)$, and $(3, 3)$ belong to R because $A_1 = \{1, 2, 3\}$ is an equivalence class; the pairs $(4, 4), (4, 5), (5, 4)$, and $(5, 5)$ belong to R because $A_2 = \{4, 5\}$ is an equivalence class; and

finally the pair $(6, 6)$ belongs to R because $\{6\}$ is an equivalence class. No pair other than those listed belongs to *R* and hence

$R = \{(1, 1),(1, 2),(1, 3),(2, 1),(2, 2),(2, 3),(3, 1),(3, 2),(3, 3),(4, 4),(4, 5),(5, 4),(5, 5),(6, 6)\}$.

Example: What are the sets in the partition of the integers arising from congruence modulo 4?

Solution: There are four congruence classes, corresponding to $[0]_4$, $[1]_4$, $[2]_4$, and $[3]_4$. They are the sets

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$
$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$
$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

These congruence classes are disjoint, and every integer is in exactly one of them. In other words, these congruence classes form a partition of set of integers.

Example: What are the sets in the partition of the set of all bit strings arising from the relation R_3 on the set of all bit strings? (Recall that $s\ R_3\ t$, where s and t are bit strings, if $s = t$ or s and t are bit strings with at least three bits that agree in their first three bits.)

Solution: Note that every bit string of length less than three is equivalent only to itself. Hence $[\lambda]_{R_3} = \{\lambda\}$, $[0]_{R_3} = \{0\}$, $[1]_{R_3} = \{1\}$, $[00]_{R_3} = \{00\}$, $[01]_{R_3} = \{01\}$, $[10]_{R_3} = \{10\}$, and $[11]_{R_3} = \{11\}$. Note that every bit string of length three or more is equivalent to one of the eight bit strings $000, 001, 010, 011, 100, 101, 110$, and 111.We have

$$[000]_{R_3} = \{000, 0000, 0001, 00000, 00001, 00010, 00011, \ldots\},$$
$$[001]_{R_3} = \{001, 0010, 0011, 00100, 00101, 00110, 00111, \ldots\},$$
$$[010]_{R_3} = \{010, 0100, 0101, 01000, 01001, 01010, 01011, \ldots\},$$
$$[[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\},$$
$$[100]_{R_3} = \{100, 1000, 1001, 10000, 10001, 10010, 10011, \ldots\},$$
$$[101]_{R_3} = \{101, 1010, 1011, 10100, 10101, 10110, 10111, \ldots\},$$
$$[110]_{R_3} = \{110, 1100, 1101, 11000, 11001, 11010, 11011, \ldots\},$$
$$[111]_{R_3} = \{111, 1110, 1111, 11100, 11101, 11110, 11111, \ldots\}.$$

These 8 equivalence classes are disjoint and every bit string is in exactly one of them. So, these equivalence classes partition the set of all bit strings.

Partial Ordering Relations

We often use relations to order some or all of the elements of sets. For instance, we order words using the relation containing pairs of words (x, y), where x comes before y in the dictionary. We schedule projects using the relation consisting of pairs (x, y), where x and y are tasks in a project such that x must be completed before y begins. We order the set of integers using the relation containing the pairs (x, y), where x is less than y. When we add all of the pairs of the form (x, x) to these relations, we obtain a relation that is reflexive, antisymmetric, and transitive. These are properties that characterize relations used to order the elements of sets.

Definition: A relation R on a set A is called a *partial ordering* or *partial order* if it is reflexive, antisymmetric, and transitive. A set A together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (A, R). Members of A are called *elements* of the poset.

Example: Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Example: Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set A.

Example: The divisibility relation is a partial ordering on the set of positive integers.

Customarily, the notation $a \preccurlyeq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset (A, R). This notation is used because the "less than or equal to" relation on the set of real numbers is the most familiar example of a partial ordering and the symbol $\preccurlyeq$ is similar to the $\leq$ symbol. (Note that the symbol $\preccurlyeq$ is used to denote the relation in *any* poset, not just the "less than or equals" relation.) The notation $a \prec b$ denotes that $a \preccurlyeq b$, but $a \neq b$. Also, we say "*a* is less than *b*" or "*b* is greater than *a*" if $a \prec b$.

Definition: The elements a and b of a poset $(A, \preccurlyeq)$ are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When a and b are elements of A such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, a and b are called *incomparable*. If every two elements of A are comparable, A is called a *totally ordered* or *linearly ordered set*, and $\preccurlyeq$ is called a *total order* or a *linear order.* A totally ordered set is also called a *chain*.

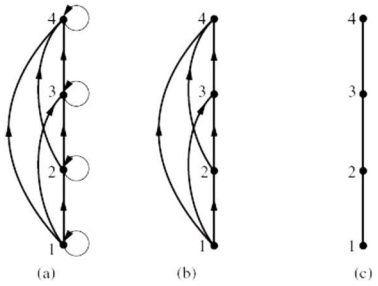
Example: The poset $(\mathbb{Z}, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.

Example: In the poset $(\mathbb{Z}^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

Solution: The integers 3 and 9 are comparable, because $3 \mid 9$. The integers 5 and 7 are incomparable, because $5 \nmid 7$ and $7 \nmid 5$.

Hasse Diagrams

Many edges in the directed graph for a finite poset do not have to be shown because they must be present. For instance, consider the directed graph for the partial ordering $\{(a, b) \mid a \leq b\}$ on the set {1, 2, 3, 4}, shown in bellow Figure (a).



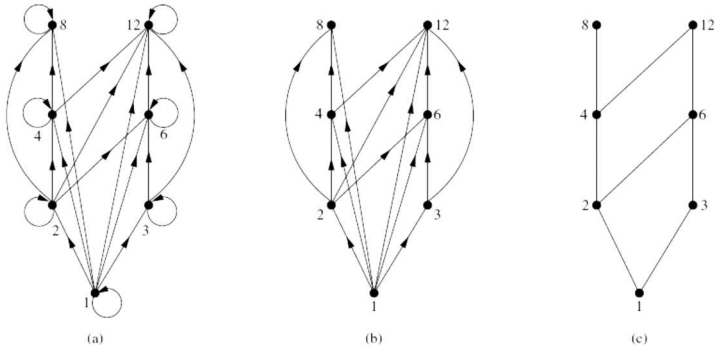
Because this relation is a partial ordering, it is reflexive, and its directed graph has loops at all vertices. Consequently, we do not have to show these loops because they must be present; in Figure (b) loops are not shown. Because a partial ordering is transitive, we do not have to show those edges that must be present because of transitivity. For example, in Figure (c) the edges $(1, 3)$, $(1, 4)$, and $(2, 4)$ are not shown because they must be present. If we assume that all edges are pointed "upward" (as they are drawn in the figure), we do not have to show the directions of the edges; Figure (c) does not show directions. In general, we can represent a finite poset $(S, \preccurlyeq)$ using this procedure: Start with the directed graph for this relation. Because a partial ordering is reflexive, a loop (a, a) is present at every vertex a. Remove these loops. Next, remove all edges that must be in the partial ordering because of the presence of other edges and transitivity. That is, remove all edges (x, y) for which there is an element $z \in S$ such that $x \preccurlyeq z$ and $z \preccurlyeq y$. Finally, arrange each edge so that its initial vertex is below its terminal vertex. Remove all the arrows on the directed edges, because all edges point "upward" toward their terminal vertex. These steps

are well defined, and only a finite number of steps need to be carried out for a finite poset. When all the steps have been taken, the resulting diagram contains sufficient information to find the partial ordering. The resulting diagram is called the **Hasse diagram** of $(S, \preccurlyeq)$, named after the twentieth-century German mathematician Helmut Hasse who made extensive use of them.

****

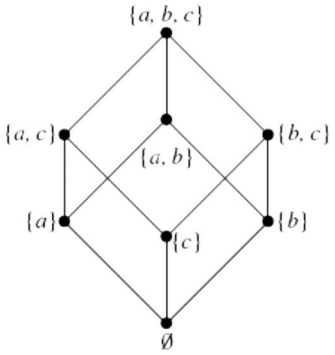
Example: Draw the Hasse diagram representing the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

Solution: Begin with the digraph for this partial order, as shown in Figure (a). Remove all loops, as shown in Figure (b). Then delete all the edges implied by the transitive property. These are $(1, 4), (1, 6), (1, 8), (1, 12), (2, 8), (2, 12)$, and $(3, 12)$. Arrange all edges to point upward, and delete all arrows to obtain the Hasse diagram. The resulting Hasse diagram is shown below.



Example: Draw the Hasse diagram for the partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set $P(S)$ where $S = \{a, b, c\}$.

Solution: The Hasse diagram for this partial ordering is obtained from the associated digraph by deleting all the loops and all the edges that occur from transitivity, namely $(\emptyset, \{a, b\}), (\emptyset, \{a, c\}), (\emptyset, \{b, c\}), (\emptyset, \{a, b, c\}), (\{a\}, \{a, b, c\}), (\{b\}, \{a, b, c\})$, and $(\{c\}, \{a, b, c\})$. Finally all edges point upward, and arrows are deleted. The resulting Hasse diagram is illustrated in below Figure.

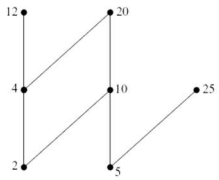


Maximal and Minimal Elements

Elements of a poset that have certain extremal properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset. That is, a is **maximal** in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \prec b$. Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is, a is **minimal** if there is no element $b \in S$ such that $b \prec a$. Maximal and minimal elements are easy to spot using a Hasse diagram. They are the "top" and "bottom" elements in the diagram.

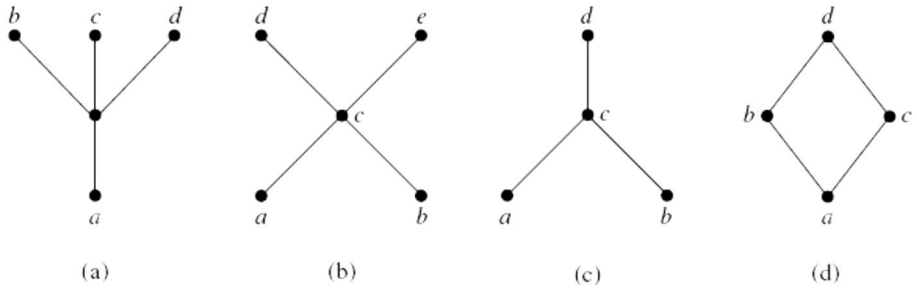
Example: Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ are maximal, and which are minimal?

Solution: The Hasse diagram in bellow Figure for this poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5. As this example shows, a poset can have more than one maximal element and more than one minimal element.



Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element. That is, a is the **greatest element** of the poset $(S, \preccurlyeq)$ if $b \preccurlyeq a$ for all $b \in S$. The greatest element is unique when it exists. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is, a is the **least element** of $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$. The least element is unique when it exists.

Example: Determine whether the posets represented by each of the Hasse diagrams in bellow figure have a greatest element and a least element.



Solution: The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least nor a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is d. The poset with Hasse diagram (d) has least element a and greatest element d.

Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset A of a poset $(S, \preccurlyeq)$. If u is an element of *S* such that $a \preccurlyeq u$ for all elements $a \in A$, then u is called an **upper bound** of A. Likewise, there may be an element less than or equal to all the elements in A. If l is an element of *S* such that $l \preccurlyeq a$ for all elements $a \in A$, then l is called a **lower bound** of A.

The element x is called the **least upper bound** of the subset A if x is an upper bound that is less than every other upper bound of A. Because there is only one such element, if it exists, it makes sense to call this element *the* least upper bound. That is, x is the least upper bound of A if $a \preccurlyeq x$ whenever $a \in A$, and $x \preccurlyeq z$ whenever z is an upper bound of A. Similarly, the element y is called the **greatest lower bound** of A if y is a lower bound of A and $z \preccurlyeq y$ whenever z is a lower bound of A. The greatest lower bound of A is unique if it exists. The greatest lower bound and least upper bound of a subset *A* are denoted by glb(A) and lub(A), respectively.

Unit III--Recurrence Relation and their solutions

Consider the numeric sequence $\{a_n\}$ given as $3, 5, 7, 9 \ldots$. We can find a formula for the n^{th} term of the sequence i.e. discrete numeric function by observing the pattern of the sequence

$$a_1 = 3 = 2 \times 1 + 1.$$

$a_2 = 5 = 2 \times 2 + 1.$

$a_3 = 7 = 2 \times 3 + 1.$

Thus, for the sequence $\{a_n\}$, n^{th} term of the sequence is $a_n = 2n + 1$ for $n \geq 1$.This type of formula is called **explicit formula** or discrete numeric function for the sequence, because we can find any term of the sequence directly from the above derived formula. For example, $a_{100} = 2 \times 100 + 1 = 201.$

Let us take another example of a sequence defined as

$$1, 1, 2, 3, 8, 5, 13, 21, \ldots .$$

For this sequence, the explicit formula is not obvious. If we observe closely however, we find that pattern of the sequence is such that any term after the second term is the sum of the preceding two terms. That is,

3rd term = 1st term + 2nd term.

4th term = 2nd term + 3rd term.

5th term = 3rd term + 4th term.

Here, the n^{th} term of the sequence sequence can be expressed in the form of an equation

$$a_n = a_{n-1} + a_{n-2};\ n \geq 3, \text{ where, } a_1 = 1, a_2 = 1.$$

Recurrence Relation

A recurrence relation for the sequence $\{a_n\}$ is an equation that express a_n in terms one or more of the previous terms $a_0, a_1, \ldots, a_{n-1}$ for all integers n with $n \geq k$, where k is a non negative integer. A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation. The initial conditions for the recurrence relation are a set of values that explicitly define some of the members $a_0, a_1, .., a_{k-1}$. We say that we have solved the recurrence relation together with the initial conditions when we find an explicit formula, called a **closed formula**, for the terms of the sequence.

Example: The equation

$$a_n = a_{n-1} + a_{n-2}, n \geq 2 \text{ with } a_0 = 0, a_1 = 1$$

relates a_n to a_{n-1} and a_{n-2}. Here $k = 2$. So, this is a recurrence relation with initial conditions. The sequence defined by this recurrence relation is known as the **Fibonacci sequence**, after the Italian mathematician Fibonacci.

Example: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$, and suppose that $a_0 = 2$. What are a_1, a_2, and a_3 ?

Solution: We see from the recurrence relation that $a_1 = a_0 + 3 = 2 + 3 = 5$. It then follows that $a_2 = a_1 + 3 = 5 + 3 = 8$ and $a_3 = a_2 + 3 = 8 + 3 = 11$.

Example: Determine whether the sequence $\{a_n\}$, where $a_n = 3n$ for every nonnegative integer n, is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$. Answer the same question where $a_n = 2^n$ and where $a_n = 5$.

Solution: Suppose that $a_n = 3n$ for every nonnegative integer n. Then, for $n \geq 2$, we see that $2a_{n-1} - a_{n-2} = 2 \times 3 \times (n-1) - 3 \times (n-2) = 3n = a_n$. Therefore, $\{a_n\}$, where $a_n = 3n$, is a solution of the recurrence relation.

Suppose that $a_n = 2^n$ for every nonnegative integer n. Note that $a_0 = 1, a_1 = 2$, and $a_2 = 4$. Because $2a_1 - a_0 = 2 \times 2 - 1 = 3 \neq a_2$, we see that $\{a_n\}$, where $a_n = 2^n$, is not a solution of the recurrence relation.

Suppose that $a_n = 5$ for every nonnegative integer n. Then for $n \geq 2$, we see that $a_n = 2a_{n-1} - a_{n-2} = 2 \times 5 - 5 = 5 = a_n$. Therefore, $\{a_n\}$, where $a_n = 5$, is a solution of the recurrence relation.

Example: Show that

(i) For the Recurrence Relation $a_n = 2a_{n-1}, n \geq 1, a_n = 2^n$ is the solution.

(ii) For the Recurrence Relation $a_n - 7a_{n-1} + 10a_{n-2} = 0, n \geq 2, a_n = c_1 2^n + c_2 5^n$ is a solution, where $c_1$and $c_2$arbitrary constants.

Linear Recurrence Relation

A Recurrence Relation of the form

$$c_0(n)a_n + c_1(n)a_{n-1} + \cdots + c_k(n)a_{n-k} = f(n), n \geq k$$

where, $c_0(n), c_1(n), \ldots, c_k(n)$ and $f(n)$ are functions of n, is called a linear recurrence relation.

Note 1: If $c_0(n), c_k(n)$ are not identically equal to zero, then the recurrence relation is said to be **recurrence relation of order k**. In other words, a recurrence relation is said to be of order k if a_n is expressed as function of $a_{n-1}, a_{n-2}, \dots, a_{n-k}$ that appears in the relation.

Note 2: If $c_0(n), c_1(n), \dots, c_k(n)$ are constants, then the Recurrence Relation is known as **Linear Recurrence Relation with constant coefficients.**

Note3: If $f(n) = 0$, then the Recurrence Relation is said to be **Homogenous**; otherwise, it is **Non-homogenous**.

Example: Consider the following recurrence relation:

(i) $a_n = a_{n-1} + a_{n-2}, n \geq 2$

(ii) $a_n = n + a_{n-1}, n \geq 1$

(iii) $a_n - 3a_{n-1} + 2a_{n-2} = 0, n \geq 2$

(iv) $a_n - 3a_{n-1} + 2a_{n-2} = n^2 - 1, n \geq 2$

(v) $a_n - (n-1)a_{n-1} - (n-2)a_{n-2} = 0, n \geq 2$

(vi) $a_n - 9a_{n-1} + 26a_{n-2} - 24a_{n-3} = 4^n, n \geq 3$

(vii) $a_n - 3a_{n-1}^2 + 2a_{n-2} = n^2, n \geq 2$

(viii) $a_n = a_0 a_{n-1} + a_1 a_{n-2} + \cdots + a_{n-1} a_0, n \geq 1$

(ix) $a_n^2 + a_{n-1}^2 = -1, n \geq 1$

(x) $a_n = 3a_{n-1}, n \geq 1$

Clearly, All the above examples are linear recurrence relations except (vii), (viii) and (ix); the relation (vii) is not linear because of the squared term a_{n-1}^2. The relations (i), (ii), (iii), (iv), (vi), and (x) are linear with constant coefficients. Relations (ii) and (x) have order 1; (iii), (iv) and (v) have order 2; and (vi) has order 3. Relations (i), (iii), (v) and (x) are homogenous.

Solving Linear Recurrence Relation with constant coefficients

A wide variety of recurrence relations occur in models. Some of these recurrence relations can be solved using iteration or some other ad hoc technique. It is not possible to solve all Recurrence Relations. Also, there is no general technique to solve all Recurrence Relation. However, one important class of recurrence relations can be explicitly solved in a systematic way. These are recurrence relations that express the terms of a sequence as linear combinations of previous

terms, i.e. linear Recurrence Relations with constant coefficients. Nonlinear Recurrence Relations can be solved by converting them into linear Recurrence Relations.

We are going to discuss two methods of solving Linear Recurrence Relation with constant coefficients. They are

(i) By Characteristic roots.

(ii) By Generating function method.

Solving of Linear Homogenous Recurrence Relations with constant coefficients

Recurrence relations may be difficult to solve, but fortunately this is not the case for linear homogenous recurrence relations with constant coefficients. We already said that a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

where, $c_1, c_2, \ldots, c_k$, are real numbers and $c_k \neq 0$ is called a **linear homogenous Recurrence Relation of order k** with constant coefficients.

The above recurrence relation is linear since each a_i has power 1 and no terms of the type $a_i a_j$ occurred. The order of the Recurrence Relation is k, since a_n is expressed in terms of the previous k terms of the sequence i.e., order is the difference between the greatest and lowest subscripts of the members of the sequence occurring in the Recurrence Relation. The coefficients of the terms of the expression are all constants, not functions of n. The recurrence relation is **homogeneous** because no terms occur that are not multiples of the a_js.

Solution of Recurrence Relation by Characteristic Polynomial: We can use two key ideas to find all their solutions. First, these recurrence relations have solutions of the form $a_n = r^n$, where r is a constant. The other key observation is that a linear combination of two solutions of a linear homogeneous recurrence relation is also a solution.

Note: This method of solving linear homogenous recurrence relation is similar to solving linear homogenous differential equation.

Let $a_n = r^n; r \neq 0$, be a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$
$$\Rightarrow r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k}$$
$$\Rightarrow r^n - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_k r^{n-k} = 0$$
$$\Rightarrow r^{n-k}(r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k) = 0$$
$$\Rightarrow r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k r^k = 0, \text{ since } \quad r^{n-k} \neq 0$$

Consequently, the sequence $\{a_n\}$ with $a_n = r^n$ where $r \neq 0$ is a solution if and only if r is a solution of the last equation. We call this the **characteristic equation** of the recurrence relation. That is, the characteristic equation of the recurrence relation is

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0$$

The solutions of the characteristic equation are called the **characteristic roots** of the recurrence relation. We will now state the general result about the solution of linear homogeneous recurrence relations with constant coefficients, under the assumption that the characteristic equation has distinct roots.

Theorem: Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0$$

has k distinct roots $r_1, r_2, \ldots, r_k$, then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

for $n = 0,1,2, \ldots$,where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are constants.

Example: Find the solution of the recurrence relation

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

with initial conditions $a_0 = 2, a_1 = 5, a_2 = 15$.

Solution: The characteristic polynomial of this recurrence relation is

$$r^3 - 6r^2 + 11r - 6.$$

The characteristic roots are $r = 1, r = 2, r = 3$ and they are distinct.

Thus, the solution is of the form

$$a_n = \alpha_1 . 1^n + \alpha_2 . 2^n + \alpha_3 . 3^n.$$

To find the constants $\alpha_1, \alpha_2$and α_3, we use the given initial conditions. This gives

$$a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3,$$

$$a_1 = 5 = \alpha_1 + 2\alpha_2 + 3\alpha_3$$
$$a_2 = 15 = \alpha_1 + 4\alpha_2 + 9\alpha_3$$

After solving three equations, the values of the constants are as follows.

$$\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = 2.$$

Then

$$a_n = 1 - 2^n + 2 \times 3^n.$$

Hence, the unique solution to this recurrence relation and the given initial conditions is the sequence $\{a_n\}$ with $a_n = 1 - 2^n + 2 \times 3^n$.

We now state the most general result about linear homogeneous recurrence relations with constant coefficients, allowing the characteristic equation to have multiple roots. The key point is that for each root r of the characteristic equation, the general solution is of the form $P(n)\, r^n$, where $P(n)$ is a polynomial of degree $m\ -\ 1$, with m the multiplicity of this root r.

Theorem: Let $c_{1,}c_2, \dots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0$$

has t distinct roots $r_1, r_2, \dots, r_t$ with multiplicities $m_1, m_2, \dots, m_t$, respectively, so that $m_i \geq 1$for $i = 1,2, \dots, t$ and $m_1 + m_2 + \cdots + m_t = k$.Then a sequence$\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$a_n = \left(\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1}\, n^{m_1-1}\right) r_1^n + \left(\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha n^{m_2-1}\right) r_2^n + \cdots$$
$$+ \left(\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1}\, n^{m_t-1}\right) r_t^n$$

for $n = 0,1,2$ …, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

Example: Find the solution of the recurrence relation

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3},$$

with initial conditions $a_0 = 1, a_1 = -2$ and $a_2 = -1$.

Solution: The characteristic polynomial of this recurrence relation is

$$r^3 + 3r^2 + 3r + 1 = 0.$$

The roots are$-1, -1, -1$. Then $r = -1$ with multiplicity 3. Thus, the solutions of the recurrence relation are of the form

$$a_n = (\alpha_{1,0} + \alpha_{1,1}n + \alpha_{1,2}n^2)(-1)^n.$$

To find the constants $\alpha_{1,0}$, $\alpha_{1,1}$and $\alpha_{1,2}$, use the initial conditions. This gives

$$a_0 = 1 = \alpha_{1,0}$$
$$a_1 = -2 = -\alpha_{1,0} - \alpha_{1,1} - \alpha_{1,2}$$
$$a_2 = -1 = \alpha_{1,0} + 2\alpha_{1,1} + 4\alpha_{1,2}$$

The simultaneous solution of these three equations is $\alpha_{1,0} = 1, \alpha_{1,1} = 3$ and $\alpha_{1,2} = -2$. Hence, the unique solution to this Recurrence Relation and the given initial conditions is the sequence $\{a_n\}$ with

$$a_n = (1 + 3n - 2n^2)(-1)^n.$$

Solving Linear Non- Homogenous Recurrence Relations with Constant Coefficients

Linear non- homogenous recurrence relations with constant coefficients is a recurrence relation of the form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + f(n)$$

where, $c_1, c_2, \ldots, c_k$ are real numbers and $f(n)$ is a function not identically zero depending only on n. The Recurrence Relation

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$$

is called the associated homogenous recurrence relation. It plays an important role in solving the given non-homogenous recurrence relation with constant coefficients.

Examples: The following are examples of non-homogenous recurrence relation with constant coefficients.

(i) $a_n = a_{n-1} + 2^n$

(ii) $a_n = a_{n-1} + a_{n-2} + n^2 + n + 1$

(iii) $a_n = 3a_{n-1} + n3^n$

The key fact about linear nonhomogeneous recurrence relations with constant coefficients is that every solution is the sum of a particular solution and a solution of the associated linear homogeneous recurrence relation.

Note: This method of solving linear non-homogenous recurrence relation is similar to solving linear non-homogenous differential equation.

Theorem: If $\left\{a_n^{(p)}\right\}$ is a particular solution of the non-homogenous linear recurrence relation with constant coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n),$$

then every solution is of the form $\left\{a_n^{(p)} + a_n^{(h)}\right\}$, where $a_n^{(h)}$ is a solution of the associated homogenous recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}.$$

There is no general procedure for finding the particular solution of a recurrence relation. However, if $f(n)$ has any one of the forms (i) polynomials in n, (ii) a constant or power of a constant, then we may guess the forms of particular solution and exactly find out it by the method of undetermined coefficients.

$f(n)$	**Form of a particular solution**
A constant, c	A constant , d
A linear function, $c_0 + c_1 n$	A linear function, $d_0 + d_1 n$
n^2	$d_0 + d_1 n + d_2 n^2$
An m^{th} degree polynomial $c_0 + c_1 n + c_2 n^2 + \cdots + c_m n^m$	An m^{th} degree polynomial $d_0 + d_1 n + d_2 n^2 + \cdots + d_m n^m$
power of a constant c^n	For a constant d dc^n

Example: Solve the recurrence relation $a_n = 3a_{n-1} + 2^n, a_0 = 1$

Solution: The associated homogenous recurrence relation is $a_n - 3a_{n-1} = 0$. The characteristic equation is

$$r - 3 = 0 \Rightarrow r = 3.$$

∴ The homogenous solution is

$$a_n^{(h)} = \alpha 3^n$$

where α is a constant. Since $f(n)$ of the recurrence relation is 2^n, the particular solution of the recurrence relation is

$$a_n^{(p)} = a_n = d2^n.$$

Using this equation in the given recurrence relation, we get

$$d2^n - 3d2^{n-1} = 2^n \Longrightarrow d - \frac{3}{2}d = 1 \Longrightarrow 2d - 3d = 2 \Longrightarrow d = -2.$$

$\therefore a_n^{(p)} = -2(2)^n = -2^{n+1}$.

Hence, the general solution is $a_n = a_n^{(h)} + a_n^{(p)}$

$$\Rightarrow a_n = \alpha 3^n - 2^{n+1}$$

Using the condition$a_0 = 1$, we get $a_0 = \alpha 3^0 - 2^1 = 1 \Rightarrow \alpha = 3$.

The required solution is

$$a_n = 3(3)^n - 2^{n+1} = 3^{n+1} - 2^{n+1}.$$

Example: Solve the recurrence relation

$$a_n - 7a_{n-1} + 10a_{n-2} = 6 + 8n, a_0 = 1, a_1 = 2.$$

Solution: The associated homogenous recurrence relation is $a_n - 7a_{n-1} + 10a_{n-2} = 0$. Then the characteristic equation is $r^2 - 7r + 10 = 0 \Rightarrow (r-5)(r-2) = 0 \Rightarrow r = 2, 5$. Therefore, homogenous solution is $a_n^{(h)} = c_1 2^n + c_2 3^n$.

Let $a_n^{(p)} = d_0 + d_1 n$ be the particular solution, since $f(n)$ is a linear polynomial in n. Using this equation in the given recurrence relation, we get

$$(d_0 + d_1 n) - 7\big(d_0 + d_1(n-1)\big) + 10\big(d_0 + d_1(n-2)\big) = 6 + 8n.$$

Equating the corresponding coefficients on both sides, we get

$4d_0 - 13d_1 = 6$ and $4d_1 = 8. \Rightarrow d_1 = 2$ and $d_0 = 8$.

Thus,

$$a_k^{(p)} = 8 + 2n.$$

Hence, the general solution is $a_n = a_n^{(h)} + a_n^{(p)}$

$$\Rightarrow a_n = c_1 2^n + c_2 5^n + 8 + 2n$$

Given that,$a_0 = 1, a_1 = 2$. Thus,

$$a_0 = 1 \Rightarrow c_1 + c_2 + 8 = 1 \text{ and } a_1 = 2 \Rightarrow 2c_1 + 5c_2 + 8 + 2 = 2.$$

Solving the equations, we get

$$c_1 = -9,\ c_2 = 2.$$

The required solution is $a_n = a_n^{(h)} + a_n^{(p)} = -9(2^n) + 2(5^n) + 8 + 2n$.

In both Examples we were able to find the particular solutions. Now we have to select the particular solution in more general way. When $f(n)$ is the product of a polynomial in n and the n^{th} power of a constant, we have to select the particular solution which is stated in the below theorem.

Theorem: Suppose that $\{a_n\}$ satisfies the linear non-homogenous recurrence relation

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + f(n),$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$f(n) = (b_tn^t + b_{t-1}n^{t-1} + \cdots + b_1n + b_0)s^n,$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers.

(i) When s is not root of the characteristic equation of the associated homogenous linear recurrence relation, there is a particular solution of the form

$$(p_tn^t + p_{t-1}n^{t-1}n + \cdots + p_1n + p_0)s^n.$$

(ii) When s is a root of this associated homogenous characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m(p_tn^t + p_{t-1}n^{t-1}n + \cdots + p_1n + p_0)s^n.$$

Example: Solve the recurrence relation

$$a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n.$$

Solution: The associated homogenous recurrence relation is

$$a_n - 4a_{n-1} + 4a_{n-2} = 0.$$

The characteristic equation is $r^2 - 4r + 4 = 0$.

i.e, $(r-2)^2 = 0 \Rightarrow r = 2, 2.$

∴ The homogenous solution is

$$a_n^{(h)} = (d_1 + d_2n)2^n.$$

Since, the $f(n)$ of the recurrence relation is $(n+1)2^n$and the characteristic root 2 is repeated twice, we assume the particular solution of the recurrence relation to be

$$a_n^{(p)} = (c_1 + c_2n)n^22^n.$$

Using this equation in the given recurrence relation, we get

$$(c_1 + c_2n)n^22^n - 4(c_1 + c_2(n-1)(n-1)^22^{n-1}) + 4\big(c_1 + c_2(n-2)\big)(n-2)^22^{n-2} = (n+1)2^n.$$

$$\Rightarrow (c_1 + c_2n)n^2 - 2\big(c_1 + c_2(n-1)\big)(n-1)^2\big) + \big(c_1 + c_2(n-2)\big)(n-2)^2 = (n+1).$$

Putting $n = 0$, we get

$$-2(c_1 - c_2) + 4(c_1 - 2c_2) = 1 \Rightarrow 2c_1 - 6c_2 = 4 \Rightarrow c_1 - 3c_2 = \frac{1}{2}.$$

Putting $n = 1$,

$$(c_1 + c_2) + (c_1 - c_2) = 2 \Rightarrow 2c_1 = 2 \Rightarrow c_1 = 1.$$

Thus, $c_2 = \frac{1}{6}$. And

$$a_n^{(p)} = \left(1 + \frac{1}{6}n\right) n^2 2^n = \left(n^2 + \frac{n^3}{6}\right) 2^n.$$

Thus, the general solution of the recurrence relation is

$$a_n = a_n^{(h)} + a_n^{(p)} = \left(d_1 + d_2 n + n^2 + \frac{n^3}{6}\right) 2^n.$$

Example: Solve the recurrence relation

$$a_n = 4a_{n-1} - 4a_{n-2} + 3n + 2^n,\ a_0 = 1, a_1 = 1.$$

Solution: The associated homogenous recurrence relation is

$$a_n - 4a_{n-1} + 4a_{n-2} = 0.$$

The characteristic equation is

$$r^2 - 4r + 4 = 0.$$

i.e., $(r-2)^2 = 0 \Rightarrow r = 2, 2.$

∴ The homogenous solution is

$$a_n^{(h)} = (c_1 + c_2 n)2^n.$$

Since $f(n) = 3n + 2^n$, the particular solution is of the form

$$a_n^{(p)} = a_n^{(p_1)} + a_n^{(p_2)}.$$

Where, $a_n^{(p_1)} = d_0 + d_1 n$ and $a_n^{(p_2)} = dn^2 2^n$.

Using the solution $a_n^{(p_1)}$ in the recurrence relation, we get

$$(d_0 + d_1 n) - 4\big(d_0 + d_1(n-1)\big) + 4\big(d_0 + d_1(n-2)\big) = 3n.$$

$$\Rightarrow (d_0 - 4d_1) + d_1 n = 3n.$$

Equating the coefficient of n on both the sides, we get

$$d_1 = 3.$$

Equating the constant terms on both the sides, we get

$$d_0 - 4d_1 = 0 \Rightarrow d_0 = 12.$$

Therefore, the particular solution corresponding to $3n$ is

$$a_n^{(p_1)} = 12 + 3n$$

Let $= dn^2 2^n$

Using the solution $a_n^{(p_2)}$ in the recurrence relation, we get

$$dn^2 2^n - 4d(n-1)^2 2^{n-1} + 4d(n-2)^2 2^{n-2} = 2^n.$$

Putting $n = 0$, we get

$$-2d + 4d = 1.$$

$$\Rightarrow d = \frac{1}{2}.$$

Therefore, $a_n^{(p_2)} = \frac{1}{2}n^2 2^n = n^2 2^{n-1}$.

Therefore, the particular solution is $a_n^{(p)} = a_n^{(p_1)} + a_n^{(p_2)} = 12 + 3n + n^2 2^{n-1}$.

Hence, the general solution is

$$a_n = (c_1 + c_2 n)2^n + 12 + 3n + n^2 2^{n-1}.$$

Given that, $a_0 = 1, a_1 = 1$.

Now, $a_0 = 1 \Rightarrow c_1 + 12 = 1 \Rightarrow c_1 = -11$.

Also, $a_1 = 1 \Rightarrow (c_1 + c_2)2 + 12 + 3 + 2^2 = 1 \Rightarrow 2c_1 + 2c_2 = -18 \Rightarrow c_1 + c_2 = -9 \Rightarrow c_2 = 2$.

Thus, the required solution is

$$a_n = (2n - 11)2^n + 12 + 3n + n^2 2^{n+1}.$$

Example: Solve the recurrence relation

$$a_n - 2a_{n-1} + a_{n-2} = 2, a_0 = 25, a_1 = 16.$$

The associated homogenous recurrence relation is

$$a_n - 2a_{n-1} + a_{n-2} = 0.$$

The characteristic equation is $r^2 - 2r + 1 = 0 \Rightarrow r = 1,1$.

∴ The homogenous solution is $a_n^{(h)} = (c_1 + c_2 n)1^n = c_1 + c_2 n$.

Since $f(n) = 2 = 2(1)^n$, 1 is the root of the characteristic equation of multiplicity 2,

So, the particular solution is $a_n^{(p)} = Dn^2$.

Using this solution in the recurrence relation, we get

$$Dn^2 - 2D(n-1)^2 + D(n-2)^2 = 2.$$

$$\Rightarrow Dn^2 - 2D(n^2 + 1 - 2n) + D(n^2 + 4 - 4n) = 2.$$

Comparing the like coefficients of n on both the sides, we get

$$2D = 2 \Rightarrow D = 1.$$

So, $a_n^{(p)} = n^2$. And hence,

$$a_n = a_n^{(h)} + a_n^{(p)} = c_1 + c_2 n + n^2.$$

Now, $a_0 = 25 \Rightarrow c_1 = 25$ and $a_1 = 16 \Rightarrow c_1 + c_2 + 1 \Rightarrow c_2 = -10$.

So, $a_n = 25 - 10n + n^2$.

Generating Functions

Definition: The generating function for the sequence $\{a_n\}$ of real numbers is the infinite series

$$G(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots = \sum_{n=0}^{\infty} a_nx^n.$$

The generating function of $\{a_n\}$ given in this definition is sometimes called the ordinary generating function of $\{a_n\}$ to distinguish it from other types of generating functions for the sequence.

Example: The generating function for the sequences $\{a_n\}$ with $a_n = 3$ is given by

$$G(x) = 3 + 3.x + 3.x^2 + 3.x^3 + \cdots + 3.x^n + \cdots + .. = \sum_{n=0}^{\infty} 3x^n = \frac{3}{1-x}$$

when $|x| < 1$.

Similarly, if $a_n = n + 1$,

$$G(x) = \sum_{n=0}^{\infty} (n+1)x^n = \frac{1}{(1-x)^2} \; ; \; |x| < 1.$$

We can define generating functions for finite sequence of real numbers by extending a finite sequence $a_0, a_1, \ldots, a_n$ into an infinite sequence by setting $a_{n+1} = 0$, $a_{n+2} = 0$, and so on. The generating function $G(x)$ of this infinite sequence $\{a_n\}$ is a polynomial of degree n because no terms of the form $a_jx^j, j > n$ occur, that is, $G(x) = a_0 + a_1x + \cdots + a_nx^n$.

Example: What is the generating function for the sequence 1,1,1,1,1,1?

Solution: The generating function for the sequence1,1,1,1,1,1is

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5.$$

Example: Find the closed form expression of the generating function for the sequence $1, a, a^2, \ldots$.

Solution: The closed form expression of the generating function for the sequence $1, a, a^2, ..$ can be written as

$$G(x) = 1 + ax + a^2x^2 + \cdots = 1 + ax + (ax)^2 + (ax)^3 + \cdots = \frac{1}{1-ax}$$

when $|ax| < 1$.

Example: Find the closed form expression of the generating function for the Fibonacci sequence

$$F_n = F_{n-1} + F_{n-2}, n \geq 2, F_0 = 0, F_1 = 1.$$

The generating function of a Fibonacci sequence $\{F_n\}$ is given by

$$F(z) = F_0 + F_1z + F_2z^2 + F_3z^3 + \cdots = \sum_{n=0}^{\infty} F_nz^n.$$

Multiplying both sides of above equation by $z^n$and summing over all $n \geq 2$, we get

$$\sum_{n=2}^{\infty} F_n z^n = \sum_{n=2}^{\infty} F_{n-1} z^n + \sum_{n=2}^{\infty} F_{n-2} z^n.$$

$$\Rightarrow \sum_{n=2}^{\infty} F_n z^n = z \sum_{n=2}^{\infty} F_{n-1} z^{n-1} + z^2 \sum_{n=2}^{\infty} F_{n-2} z^{n-2}.$$

$$\Rightarrow F(z) - F_0 - F_1 z = z[F(z) - F_0] + z^2 F(z).$$

Since $F_0 = 0, F_1 = 1$, we have

$$F(z) - 0 - z = z[F(z) - 0] + z^2 F(z).$$

$$\Rightarrow (1 - z - z^2) F(z) = z.$$

$$\Rightarrow F(z) = \frac{z}{1 - z - z^2}.$$

Properties of Generating functions

Let $\{a_n\}$ and $\{b_n\}$ be two sequences and $G(z)$ and $F(z)$ be the corresponding generating functions. That is,

$$G(z) = \sum_{n=0}^{\infty} a_n z^n \quad \text{and} \quad F(z) = \sum_{n=0}^{\infty} b_n z^n.$$

1. The sum of two generating functions is a generating function.

The sum of the generating functions $G(z)$ and $F(z)$ is defined as

$$H(z) = G(z) + F(z) = \sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} (a_n + b_n) z^n = \sum_{n=0}^{\infty} c_n z^n$$

where $c_n = a_n + b_n$.

2. The scalar product of any generating function, i.e., if λ is any scalar, then $\lambda G(z)$is a generating function.

$$H(z) = \lambda G(z) = \lambda \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} (\lambda a_n) z^n = \sum_{n=0}^{\infty} c_n z^n$$

Where $c_n = \lambda a_n$.

Some Useful Generating Functions

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k) x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k) = \frac{n!}{k!\,(n-k)!}$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k) a^k x^k$ $= 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)a^k$

$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$\begin{cases} C\left(n,\frac{k}{r}\right) & if\ r\|k \\ 0 & \text{otherwisre} \end{cases}$
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	$\begin{cases} 1 & \text{if } k \le n \\ 0 & \text{otherwisre} \end{cases}$
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	$\begin{cases} 1 & if\ r\|k \\ 0 & \text{otherwisre} \end{cases}$
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k = 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k)$ $C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k$ $= 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k)$ $(-1)^k C(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} (n+k-1,k)a^k x^k$ $= 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k$ $C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$\frac{1}{k!}$
$\ln(1+x) = \sum_{k=0}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$\frac{(-1)^{k+1}}{k}$

Solving of Leaner Homogeneous Recurrence Relation using generating function

Example: Use generating function to solve the recurrence relation $a_n = 3a_{n-1}, n \ge 1$ with $a_0 = 1$.

Solution: Let the generating function of the sequence $\{a_n\}$ be $G(z) = \sum_{n=0}^{\infty} a_n z^n$. Given the recurrence relation is

$$a_n = 3a_{n-1}.$$

Multiplying both the sides by z^n and summing over all $n \geq 1$, we have

$$\sum_{n=1}^{\infty} a_n z^n = 3 \sum_{n=1}^{\infty} a_{n-1} z^n.$$

$$= 3z \sum_{n=1}^{\infty} a_{n-1} z^{n-1}.$$

$$\Rightarrow G(z) - a_0 = 3zG(z).$$

$$\Rightarrow G(z) - 1 = 3zG(z) \Rightarrow (1 - 3z)G(z) = 1.$$

$$\therefore G(z) = \frac{1}{1-3z} = \sum_{n=0}^{\infty} (3z)^n = \sum_{n=0}^{\infty} 3^n z^n.$$

Hence

$$a_n = 3^n.$$

Example: Given $a_0 = 2, a_1 = 7$, solve the recurrence relation

$$a_n = 5a_{n-1} - 6a_{n-2}; \text{ for all } n \geq 2$$

by using generating function.

Solution: Let $G(t)$ be the generating function of the sequence $\{a_n\}$. Then

$$G(t) = \sum_{n=0}^{\infty} a_n t^n .$$

Given that,

$$a_n = 5a_{n-1} - 6a_{n-2}; \text{ for all } n \geq 2.$$

Multiplying t^n in both sides, we get

$$a_n t^n = 5a_{n-1} t^n - 6a_{n-2} t^n.$$

Now taking the sum over n from 2 to ∞, we have

$$\sum_{n=2}^{\infty} a_n t^n = \sum_{n=2}^{\infty} 5a_{n-1} t^n - \sum_{n=2}^{\infty} 6a_{n-2} t^n.$$

Simplifying,

$$\Rightarrow \sum_{n=0}^{\infty} a_n t^n - a_0 - a_1 t = 5t \sum_{n=2}^{\infty} a_{n-1} t^{n-1} - 6t^2 \sum_{n=2}^{\infty} a_{n-2} t^{n-2}$$

$$\Rightarrow G(t) - 2 - 7t = 5t \sum_{m=1}^{\infty} a_m t^m - 6t^2 \sum_{s=0}^{\infty} a_s t^s$$

$$\Rightarrow G(t) - 2 - 7t = 5t \left(\sum_{m=0}^{\infty} a_m t^m - a_0 \right) - 6t^2 G(t)$$

$$\Rightarrow G(t) - 2 - 7t = 5t(G(t) - 2) - 6t^2 G(t)$$

$$\Rightarrow (1 - 5t + 6t^2) G(t) = 2 - 3t$$

$$\Rightarrow G(t) = \frac{2 - 3t}{1 - 5t + 6t^2}.$$

Thus, generating function $G(t)$ of $\{a_n\}$ is $\frac{2-3t}{1-5t+6t^2}$. Now a_n is the coefficient of t^n in the expansion of $G(t)$. Thus,

$$G(t) = \frac{2 - 3t}{(1 - 2t)(1 - 3t)} = \frac{3}{1 - 3t} - \frac{1}{1 - 2t} = 3 \sum_{n=0}^{\infty} (3t)^n - \sum_{n=0}^{\infty} (2t)^n = \sum_{n=0}^{\infty} (3^{n+1} - 2^n) t^n.$$

Therefore, $a_n = 3^{n+1} - 2^n$.

Example: Use generating function to solve the recurrence relation $a_n - 2a_{n-1} - 3a_{n-2} = 0, n \geq 2$ with $a_0 = 3, a_1 = 1$.

Solution: Let the generating function of the sequence $\{a_n\}$ be $G(z) = \sum_{n=0}^{\infty} a_n z^n$.

Multiplying both the sides of recurrence relation by z^n and summing over all $n \geq 2$, we have

$$\sum_{n=2}^{\infty} a_n z^n - 2 \sum_{n=2}^{\infty} a_{n-1} z^n - 3 \sum_{n=2}^{\infty} a_{n-2} z^n = 0.$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n - 2z \sum_{n=2}^{\infty} a_{n-1} z^{n-1} - 3z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} = 0.$$

$$\Rightarrow [G(z) - a_0 - a_1 z] - 2z[G(z) - a_0] - 3z^2 G(z) = 0.$$

$$\Rightarrow (1 - 2z - 3z^2) G(z) - 3 - z - 2z(-3) = 0.$$

$$\Rightarrow (1-2z-3z^2)G(z) = 3-5z.$$

$$\Rightarrow G(z) = \frac{(3-5z)}{(1-2z-3z^2)} = \frac{(3-5z)}{(1-3z)(1+z)}.$$

Let $\frac{(3-5z)}{(1-3z)(1+z)} = \frac{A}{(1-3z)} + \frac{B}{(1+z)}$.

Equating the numerators on both the sides, we get

$$3-5z = A(1+z) + B(1-3z).$$

From this, we get $A = 1, B = 2$ and

$$\therefore G(z) = \frac{1}{1+3z} + \frac{2}{1+z} = 1(3)^n + 2(-1)^n.$$

Thus, the required solution is $a_n = 3^n + 2(-1)^n$.

Example: Use generating function to solve the recurrence relation $a_n - 4a_{n-1} + 4a_{n-2} = 0, n \geq 2$ with $a_0 = 2, a_1 = 8$.

Solution: Multiplying both the sides of recurrence relation by z^n and summing over all $n \geq 2$, we have

$$\sum_{n=2}^{\infty} a_n z^n = 4\sum_{n=2}^{\infty} a_{n-1}z^n - 4\sum_{n=2}^{\infty} a_{n-2}z^n.$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n = 4z\sum_{n=2}^{\infty} a_{n-1}z^{n-1} - 4z^2\sum_{n=2}^{\infty} a_{n-2}z^{n-2} + \sum_{n=2}^{\infty} 4^n z^n.$$

$$\Rightarrow [G(z) - a_0 - a_1 z] - 4z[G(z) - a_0] + 4z^2 G(z) = 0.$$

$$\Rightarrow [G(z) - 2 - 8z] - 4z[G(z) - 2] + 4z^2 G(z) = 0.$$

$$\Rightarrow [1 - 4z + 4z^2]G(z) = 2$$

$$\Rightarrow G(z) = \frac{2}{(1-2z)^2}.$$

$$G(z) = 2\sum_{n=0}^{\infty}(n+1)(2z)^n = \sum_{k=0}^{\infty}(n+1)2^{n+1}z^n$$

The required solution is $a_n = (n+1)2^{n+1}$.

Unit—IV Algebraic Structure

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 $a * b$.

Example: Addition, subtraction, multiplication and division 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 $\sqrt{3} \times \sqrt{3} = 3 \notin \mathbb{R} - \mathbb{Q}$.

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

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 matrice with real enteries form a semigroup under component wise addition. That is

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

Cleary, 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 $(a + bi) + (c + di) = (a + c) + (b + d)i$.

(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 matrice with real enteries 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 properties:

(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 $a * b = b * a = e$. The element b is called inverse of a.

Note: In a group $(G,*)$ identity element is unique and generally denoted by e. Inverse of an element a is unique and is denoted by a^{-1}. The element $a * a$ is denoted by a^2 and $a^n * a = a^{n+1}$ for any integer n. Also $a^0 = e$. We can write $a * b$ as ab, when the operation is well understood. **Order of a group G** is number of elements in G and it is denoted by $o(G)$ or $|G|$. **Order of an element a** is the least positive integer n such that $a^n = e$, where e is the identity element and is denoted by $o(a)$.

Examples

(i) $(\mathbb{Z}, +)$ is a group under usual addition. In verse of an integer m is $-m$.

(ii) $(\mathbb{Z}, \times)$ 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.

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

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

$\times$	**1**	**−1**
1	1	−1
−1	−1	1

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

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

(vii) The set of all 2×2 matrice with real enteries 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 $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

(viii) 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

(ix) 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 $2^{-1} = 4, 3^{-1} = 3, 5^{-1} = 5$.

(x) Let $U(n)$ the set of all positive integer less than n and relatively prime to n. That is $U(n) = \{m: 1 \leq m < n, \text{and } gcd\ (m, n) = 1\ \}$. 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

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

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	1

From the table it is observed that the identity element is 1 and inverse of -1 is -1, inverse of i is $-i$.

(xii) 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

(xiii) 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.

Some properties of Groups: In a group $(G,*)$

(i) Identity element is unique.

(ii) Inverse of an element is unique.

(iii) $(a^{-1})^{-1} = a, \forall\, a \in G$.

(iv) $(a * b)^{-1} = b^{-1} * a^{-1}$, $\forall\, a, b \in G$.

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

Proof: (i) Suppose e and e' be two identity elements of the group G. As, e is an identity and $e' \in G$,

$$e * e' = e' * e = e' \qquad (1)$$

Also, as e' is an identity and $e \in G$,

$$e' * e = e * e' = e \qquad (2)$$

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

(ii) Let $a \in G$ be any element and let a' and a'' be two inverses of a, then

$$a * a' = a' * a = e.$$

$$a * a'' = a'' * a = e.$$

Now,

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

Hence, inverse of a is unique.

(iii) Since $a^{-1}$is inverse of a, $a * a^{-1} = a^{-1} * a = e$. Thus, a is inverse of a^{-1}. That is $(a^{-1})^{-1} = a$.

(iv) We have to prove $a * b$ has inverse $b^{-1} * a^{-1}$. That is

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

Now,

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

Similarly,

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

Thus, $(a * b)^{-1} = b^{-1} * a^{-1}$, $\forall\, a, b \in G$.

(v) Let $a * b = a * c$. Then

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

Thus, $a * b = a * c \Rightarrow b = c$.

Similarly, $b * a = c * a$ implies $a = c$.

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

Examples:

(i) The set $(\mathbb{Z}, +)$ is an abelian group. Since, $a + b = b + a$, $\forall\, a, b \in \mathbb{Z}$.

(ii) Set of all 2×2 matrices over integers under addition form an abelian group.

(iii) Set of all 2×2 real matrices with non-zero determinant under matrix multiplication is a non-abelian group.

(iv) Let $G = \{0, 1, 2, 3, 4\}$ and define a binary operation $*$ on G by $a * b = (a + b) \bmod 5$. That is $a * b = c$, where c is least nonnegative integer obtained as remainder when $a + b$ divided by 5. Then G is an abelian group under the binary operation $*$.

(v) The set $G = \{1, -1, i, -i\}$ is an abelian group under multiplication.

(vi) The set of all permutations on a set of n elements is a non-abelian group under composition of functions.

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

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

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

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

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

(iii) 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 the identity element of G.

(iv) Inverse: Let $a \in G$, and $b \in G$ such that

$$a * b = b * a = 2. \qquad \Rightarrow \frac{ab}{2} = \frac{ba}{2} = 2. \qquad \Rightarrow b = \frac{4}{a}.$$

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

So, G is a group.

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

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

Thus, G is an abelian group.

Example: Show that in a group $(G,*)$, if $a^2 = e$. $\forall a \in G$, where e is the identity element, then G is a commutative group.

Solution: $a * b = e * a * b = (b * a)^2 * a * b = b * a * b * a * a * b$

$= b * a * b * a^2 * b = b * a * b * e * b = b * a * b * b$

$= b * a * b^2 = b * a * e = b * a.$

$\Rightarrow a * b = b * a, \ \forall a, b \in G,$ $\Rightarrow$ G is an abelian group.

Alternative: Let $x \in G$, then

$$x^2 = e \Rightarrow x * x = e \Rightarrow x * x * x^{-1} = e * x^{-1} \Rightarrow x * e = x^{-1} \Rightarrow x = x^{-1}.$$

Thus, $\forall x \in G, x = x^{-1}$. Now for $a, b \in G$, we have,

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

Therefore, $(G,*)$ is an abelian group.

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, i.e. $b = a^k$ for $b \in G$ and $k \in \mathbb{N}$. Then a is called a generator of group G and we write $G = < a >$. In other words, G is said to be a cyclic group if there exist an element $a \in G$ such that $G = \{a^n : n \in \mathbb{N}\}$.

Example: $G = \{1, -1, i, -i\}$ is a cyclic group under multiplication and i is a generator, as $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$. Here, $-i$ is also a generator of G. Thus, i and $-i$ are generators of G.

Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is a group under addition modulo 5. One can verify that it is a cyclic group.

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

Rings, integral domains and Fields

Let R be a non empty set. Let there be two binary compositions, called addition and multiplication, defined on it. Then R is called a **ring** if it is

(i) an abelian group with respect to addition

(ii) a semigroup with respect to multiplication

(iii) the two distributive laws hold: for $a, b, c \in R$

$a(b + c) = ab + ac$

$(b + c)a = ba + ca$

If we write explicitly, then the definition of ring will read as follows: A nonempty set $R$with two binary operations, addition and multiplication, defined on it is called a ring if for all $a, b, c \in R$

(i) $a + b \in R$

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

(iii) There is an element $0 \in R$ (called zero element) such that $a + 0 = 0 + a = a$

(iv) There is an element $-a \in R$ such that $a + (-a) = (-a) + a = 0$

(v) $a + b = b + a$

(vi) $ab \in R$

(vii) $a(bc) = (ab)c$

(viii) $a(b + c) = ab + ac; \quad (b + c)a = ba + ca$

A ring R is said to be a **ring with unit element** (or a ring with identity) if there is an element $1 \in R$ called the multiplicative identity, such that

$$a1 = 1a = a \,; \forall a \in R.$$

A ring R is called a **commutative ring** if the multiplication in R satisfies the commutative property, i.e. if

$$ab = ba; \ \forall a, b \in R.$$

A ring R is called a **division ring** (or a skew field) if all its nonzero elements form a group under multiplication.

A commutative division ring is called a **field**. In other words, a ring R is called a field if all its nonzero elements form an abelian group under multiplication.

If R is a commutative ring, then $0 \neq a \in R$ is said to be a **zero divisor** if there exists an element $0 \neq b \in R$ such that $ab = 0$.

A commutative ring is called an **integral domain** if it has no zero divisors.

Examples of Rings, integral domains and Fields

(a) The following are rings with respect to usual addition and multiplication

(i) The singleton set consisting only of the number 0

(ii) The set $\mathbb{Z}$ of all integers

(iii) The set of all even integers

(iv) The set $\mathbb{Q}$ of all rational numbers

(v) The set $\mathbb{R}$ of all real numbers

(vi) The set $\mathbb{C}$ of all complex numbers

It should be noted that the set in (ii) is an integral domain and the sets in (iv), (v) and (vi) are in fact fields.

(b) Any ring of subsets of a set U is a ring with respect to addition and multiplication defined by $A + B = A \triangle B$ and $AB = A \cap B$. The fact that a ring of sets is actually a ring is the reason for the name ring of sets.

(c) Let m be a positive integer and $\mathbb{Z}_m = \{0,1, \dots, m-1\}$. In $\mathbb{Z}_m$define a sum $a + b$ and the product ab to be the remainders obtained when their usual sum and product are divided by m. Then $\mathbb{Z}_m$ is a ring with respect to the addition and multiplication define as above. If m is any positive integer, then $\mathbb{Z}_m$ is not always an integral domain. For example, if $m = 6$, then observe that $2 \cdot 3 = 0$ and also $3 \cdot 4 = 0$.

(d) The set $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$is a ring under usual addition and multiplication of real numbers

(e) Let $\mathbb{Z}(i) = \{a + ib : a, b \in \mathbb{Z}\}$. Note that a complex number of the form $a + ib$ where $a, b \in \mathbb{Z}$, is called a Gaussian integer and $\mathbb{Z}(i)$ is called the set of all Gaussian integers. $\mathbb{Z}(i)$ is a ring under the usual addition and multiplication of complex numbers. More precisely it is an integral domain called the domain if Gaussian integers.

(f) The set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$is a ring under usual addition and multiplication of real numbers

(g) Let $\mathbb{R}$ denote the field of all real numbers. Then $\mathbb{R} \times \mathbb{R}$ is a field with respect to addition and multiplication of real defined as follows

$(a, b) + (c, d) = (a + c, b + d)$;

$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Note that $(0,0)$ and $(1,0)$ are the additive and multiplicative identity respectively.

If $(a, b) \neq (0,0) \in \mathbb{R} \times \mathbb{R}$, then $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ since

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1,0).$$

(h) The set $\mathbb{R} \times \mathbb{R}$ is a ring under addition and multiplication defined as follows:

$(a, b) + (c, d) = (a + c, b + d)$;

$(a, b) \cdot (c, d) = (ac, bd)$

It is neither an integral domain nor a field. It is not an integral domain because

$(1,0) \cdot (0,1) = (0,0)$, but $(1,0) \neq (0,0)$ and $(0,1) \neq (0,0)$.

(i) The set of all n −rowed square matrices form a ring under addition and multiplication of matrices. This is not an integral domain. First observe that matrix multiplication is not commutative. For if $n = 2$ then

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \text{ but } \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

Also, by taking $n = 2$ we observe that

$$\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix}\begin{pmatrix}-1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

This set is also not a skew field. Because any non-zero square matrix A need not have a multiplicative inverse. This holds if and only if A is non-singular.

(j) Let M be the set of all 2×2 matrices of the form $\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}$ where α, β are complex numbers and $\bar{\alpha}$, $\bar{\beta}$ are respectively the complex conjugates of α and β. Then M is skew-field under addition and multiplication of matrices. If $A = \begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}$ is a nonzero element of M and if $D = \alpha\bar{\alpha} + \beta\bar{\beta}$, then the matrix $B = \frac{1}{D}\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}$ is the inverse of A and belongs to M.

Example: Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ be ring under addition and multiplication modulo $4. 2.2 = 0$ but $2 \neq 0$. Therefore 2 is a zero divisor.

Example: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ 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 $\mathbb{Z}_7$.

Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is an integral domain. There is no any $0 \neq a, 0 \neq b \in \mathbb{Z}_5$ such that $ab = 0$.

Example: The ring $\mathbb{Z}_p$ of integers modulo a prime p is an integral domain.

Example: The ring $\mathbb{Z}_n$ of integers modulo n is not a integral domain when n is not a prime.

Example: The ring $M_2(\mathbb{Z})$ of matrices of order 2 over the integers is not an integral domain.

Theorem: In a ring, the following results hold:

(i) $a.0 = 0.a = 0, \forall\, a \in R$. (ii) $a(-b) = (-a)b = -ab, \forall\, a, b \in R$.

(iii) $a(b - c) = ab - ac, \ \forall\, a, b, c \in R$. (iv) $(-a)(-b) = ab, \ \forall\, a, b \in R$.

Proof: (i) $a.0 = a.(0 + 0)$ (since $0 \in R$)

$\Rightarrow a.0 = a.0 + a.0$ (by distributive)

$\Rightarrow a.0 + 0 = a.0 + a.0$

$\Rightarrow 0 = a.0$ (by cancellation with respect to $(R, +)$)

$\Rightarrow a.0 = 0$

(ii) By (i), $a.0 = 0$.

$\Rightarrow a\big(b + (-b)\big) = a.b + a.(-b) = 0$ (by distributive)

$\Rightarrow a.(-b) = -ab$.

(iii) Now, $a(b - c) = a\big(b + (-c)\big) = a.b + a.(-c)$ (by distributive)

$\Rightarrow a(b - c) = ab - ac$.

(iv) Finally, $(-a)(-b) = -(a(-b)) = -(-ab)$.

Unit V: Graph Theory

****