Lecture-(1-2)

Proposition: A proposition is a declarative sentence which is either true or false but not both. Propositions are generally expressed by small alphabets $p, q, r, \ldots$.

Examples: 1: Paris is in France (true),

2: London is in Denmark (false),

3: $2 < 4$ (true),

4: $4 = 7$ (false).

However the following are not propositions:

1: what is your name? (this is a question),

2: do your homework (this is a command),

3: this sentence is false (neither true nor false),

4: x is an even number (it depends on what x represents),

5: Socrates (it is not even a sentence).

The truth or falsehood of a proposition is called its truth value

Compound Proposition: A proposition that is constructed by combining one or more propositions is called a compound proposition. We denote compound propositions by capital alphabets $L, M, X, Y, \ldots$. The propositions in a compound proposition are called primitives.

1. P: If you work hard, then you will get A grade. Here primitives are: $p :=$ You work hard, and $q :=$ You will get A grade.
2. Q: Amit is good in study and he plays football every day. Here $p :=$ Amit is good in study, $q :=$ Amit plays football everyday.

Connective: Connectives are used for making compound propositions. The main ones are the following (p and q represent given propositions):

Name	Notation	Meaning
Negation	$\neg\, p$	not p
Conjunction	$p \wedge q$	p and q
Disjunction	$p \vee q$	p or q
Exclusive OR	$p \oplus q$	either p or q, but not both
Implication	$p \Rightarrow q$	p implies q
Bi-conditional	$p \Leftrightarrow q$	p if and only if q

Truth Table: A table showing ouput (truth or falsity) of a proposition from all possible inputs (all combinations of Truth and False for the inputs). Let p, q be propositions.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

Conditional statement: Let p and q be two propositions. The conditional proposition $p \Rightarrow q$ is the proposition "if p, then q". A conditional statement has two parts, one is hypothesis (p) and other is conclusion (q).

Example: If you do your homework, you will not be punished. Here, the hypothesis $p :=$ "you do your homework" and the conclusion $q :=$ "you will not be punished".

Inverse, Converse, Contra-positive: We can form new conditional propositions from an existing conditional proposition. These are: Inverse, Converse and Contra-positive. So if $p \Rightarrow q$ is a conditional proposition, then inverse is $\neg p \Rightarrow \neg q$, converse is $q \to p$, and contra-positive is $\neg q \Rightarrow \neg p$.

Tautology, Contradiction, Contingency: A compound statement which is always true is called a tautology. A compound statement which is always false, is called a contradiction. If a compound statement is neither tautology nor contradiction, then it is called contingency.

Example: Let p and q be propositions. Then $(p \wedge \neg p)$, $(p \vee \neg p)$ and $(p \wedge q)$ are contradiction, tautology and contingency respectively. To see this, construct their truth tables.

Example: Construct the truth table for compound proposition $(p \vee \neg q) \Rightarrow (p \wedge q)$.

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \Rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Propositional Equivalence: Two propositions X and Y are logically equivalent or equivalent, denoted as $X \equiv Y$, if the bi-conditional proposition $X \Leftrightarrow Y$ is a tautology or if the columns giving their truth values agree.

Example: Show that $\neg(p \vee q) \equiv [(\neg p) \wedge (\neg q)]$.

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
T	T	F	F	T	F	F	T
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	F	T	T	T

In the above truth table, we see that truth value of $\neg(p \vee q)$ and $[(\neg p) \wedge (\neg q)]$ are same (see columns six and seven) or $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ is a tautology. Therefore the propositions are equivalent.

Exercise: Show that $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$.

Laws of propositions: Let p, q, r be primitive statements.

1. **Double negation:** $\neg\neg p \equiv p$.
2. **De Morgan's Laws:** $\neg(p \wedge q) \equiv \neg p \vee \neg q$ and $\neg(p \vee q) \equiv \neg p \wedge \neg q$
3. **Commutative Laws:** $p \vee q \equiv q \vee p$ and $p \wedge q \equiv q \wedge p$.
4. **Associative Laws:** $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ and $p \vee (q \vee r) \equiv (p \vee q) \vee r$.
5. **Distributive Laws:** $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
6. **Idempotent Laws:** $p \wedge p \equiv p$ and $p \vee p \equiv p$
7. **Identity Laws:** $p \wedge T \equiv p$ and $p \vee F \equiv p$.
8. **Inverse Laws:** $p \wedge \neg p \equiv F$ and $p \vee \neg p \equiv T$
9. **Dominations Laws:** $p \vee T \equiv T$ and $p \wedge F \equiv F$,
10. **Absorption Laws:** $p \vee (p \wedge q) \equiv p$ and $p \wedge (p \vee q) \equiv p$

One can also show the equivalence of propositions by using the laws of propositions. Here are examples.

Example: Show that $(p \vee q) \wedge \neg(\neg p \wedge q) \equiv p$.

Solution: $(p \vee q) \wedge \neg(\neg p \wedge q)$

$\equiv (p \vee q) \wedge \neg\neg p \vee \neg q$ (by De Morgan's Law)

$\equiv (p \vee q) \wedge p \vee \neg q$ (by Double negation Law)

$\equiv p \vee (q \wedge \neg q)$ (by Distributive Law)

$\equiv p \vee F$ (by Inverse Law)

$\equiv p$ (by Identity law)

Example: Show that $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$.

Solution: $\neg(p \vee (\neg p \wedge q))$

$\equiv \neg p \wedge \neg(\neg p \wedge q)$ (by De Morgan's Law)

$\equiv \neg p \wedge (p \vee \neg q)$ (by De Morgan's Law and Double negation Law)

$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$ (by Distributive Law)

$\equiv F \vee (\neg p \wedge \neg q)$ (by Inverse Law)

$(\neg p \wedge \neg q)$. (by Identity Law)

Exercise: Show that $p \Rightarrow q \equiv \neg p \vee q$.

Example: Show that $(p \wedge q) \Rightarrow (p \vee q)$ is a tautology.

Solution: By above exercise: $(p \wedge q) \Rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q)$

$\equiv (\neg p \vee \neg q) \vee (p \vee q)$ (by De Morgan's Law)

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ (by Associative and Commutative Laws)

$\equiv T \vee T$ (by Inverse Law)

$\equiv T.$ (by Dominations Law)

Thus $(p \wedge q) \Rightarrow (p \vee q)$ is a tautology.

Argument and its validity: An argument is a sequence of statements in which the conjunction of the initial statements (called the premises/hypotheses) $p_1, p_2, \ldots, p_n$ is said to imply the final statement (called the conclusion) q.

An argument is valid if the truth of all its premises implies that the conclusion is true or $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$ is a tautology. Here p_i's are premises or hypothesis and q is conclusion.

Example: Let p, q be primitive propositions. Let $P : p$ and $Q : p \Rightarrow q$ be premises and q be conclusion. Check the validity of the argument.

Solution: Let us construct the truth table.

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$[p \wedge (p \Rightarrow q)] \Rightarrow q$
T	F	F	F	T
T	T	T	T	T
F	T	T	F	T
F	F	T	F	T

Method 1: In the above truth table, we see that there is only one case when both premises are two (see second row) and in this cases the conclusion is also true. Thus the argument is valid.

Method 2: Note that $[p \wedge (p \Rightarrow q)] \Rightarrow q$ is a tautology, therefore the argument is valid.

Exercise: Let $P : p \Rightarrow q$ and $Q : \neg p$ be premises and $\neg q$ be conclusion. Show that the argument is not valid.

Lecture-3

Note that the sentence "$P(x) := x + 2 = 2x$" is not a proposition. However, if we assign a value for x then it becomes a proposition. As for each value of x the sentence is either true or false. Thus the sentence can be treated as a function for which input is a value of x and the output is a proposition. Such sentence is an example of predicate or a propositional function. We define it more precise way as follows:

Predicate or Propositional function: Let A be a given set. A propositional function defined on A is an expression $P(x)$ which has the property that $P(a)$ is true or false for each $a \in A$. That is $P(x)$ becomes a statement whenever x is replaced by any value $a \in A$. In short, predicate is the part of a sentence that attributes a property to the subject.

The set A is called the domain of $P(x)$, and the set T_p of all elements of A for which $P(a)$ is true is called the truth set of $P(x)$. In other words, $T_p = \{x : x \in A, P(x) \text{ is true}\}$

Example: Find the truth set T_p of each propositional function $P(x)$ defined on the set $\mathbb{N}$.

1. Let $P(x)$ be "$x + 5 > 1$". Then $T_p = \{x : x \in \mathbb{N}, x + 5 > 1\} = \mathbb{N}$.
2. Let $P(x)$ be "$x + 2 > 7$". Then $T_p = \{x : x \in \mathbb{N}, x + 2 > 7\} = \{6, 7, 8, \ldots\}$ consists of all integers greater than 5.
3. Let $P(x)$ be "$x + 5 < 3$". Then $T_p = \{x : x \in \mathbb{N}, x + 5 < 3\} = \emptyset$.

Remark: The above example shows that if $P(x)$ is a propositional function defined on a set A then $P(x)$ could be true for all $x \in A$, for some $x \in A$ or for no $x \in A$. In the next paragraph, we discuss this quantifiers related notion to such proposition function.

A word which is usually used before noun to express the quantity of object is called quantifier. Here we discuss few quantifiers which are used in propositional functions.

Universal Quantifier:

Let $P(x)$ be a propositional function defined on a set A. Consider the expression

$$(\forall x \in A)\, P(x) \quad \text{or} \quad \forall x\, P(x)$$

which reads as "for every x in A, $P(x)$ is true statement. The symbol $\forall$ which reads "for all" or "for every" is called universal quantifier. In this case $T_p = A$ (the entire domain).

Existential Quantifier: Let $P(x)$ be a propositional function defined on a set A. Consider the expression

$$(\exists x \in A)\, P(x) \quad \text{or} \quad \exists x\, P(x)$$

which reads as "there exists x in A such that $P(x)$ is true statement. The symbol $\exists$ which reads "there exists" or "for some" or "for at least one" is called existential quantifier. In this case $T_p \neq \emptyset$.

Precedence of Quantifiers: The quantifiers $\forall$ (universal quantifier) and $\exists$ (existential quantifier) have higher precedence than all logical operators from propositional calculus. For example, $\forall x P(x) \vee Q(x)$ is the disjunction of $\forall x P(x)$ and $Q(x)$. In other words, it means $(\forall x P(x)) \vee Q(x)$ rather than $\forall x (P(x) \vee Q(x))$.

Negation of Quantified Statements

Consider the statement "All maps are linear". Its negation is either of the following equivalent statements:

"It is not the case that that all maps are linear"

"There exists at least one map which is not linear".

Symbolically, let S denote the set of all maps. Then the above negation can be written as

$$\neg(\forall x \in S)\,(x \text{ is linear}) \equiv (\exists x \in S)\,(x\,\text{is not linear}).$$

Or when $P(x)$ denotes " x is linear",

$$\neg(\forall x \in S)\,P(x) \equiv (\exists x \in S)\neg P(x) \quad \text{or} \quad \neg\forall x\, P(x) \equiv \exists x\, \neg P(x).$$

Thus we have **Negating Quantified Expressions:**

1. $\neg(\forall x \in S)\,P(x) \equiv (\exists x \in S)\neg P(x)$
2. $\neg(\exists x \in S)\,P(x) \equiv (\forall x \in S)\neg P(x)$

The above rules for negations for quantifiers are called De Morgan's laws for quantifiers.

Example: What are the negations of the statements $\forall x\ (x^2 > x)$ and $\exists x\ (x^2 = 2)$?
Solution: The negation of $\forall x\ (x^2 > x)$ is the statement $\neg\forall x\ (x^2 > x)$, which is equivalent to $\exists x\ \neg(x^2 > x)$, that is, $\exists x(x^2 \leq x)$. The negation of $\exists x(x^2 = 2)$ is the statement $\neg\,\exists x(x^2 = 2)$, which is equivalent to $\forall x\ \neg(x^2 = 2)$, that is, $\forall x(x^2 \neq 2)$.

Example: Show that $\neg\forall x(P(x) \rightarrow Q(x)) \equiv \exists x(P(x) \wedge \neg Q(x))$.

Solution: By De Morgan's law for universal quantifiers, we know that $\neg\forall x(P(x) \rightarrow Q(x))$ and $\exists x(\neg(P(x) \rightarrow Q(x)))$ are logically equivalent. Since $P(x) \rightarrow Q(x) \equiv \neg P(x) \vee Q(x)$, it follows that $\neg\forall x(P(x) \rightarrow Q(x)) \equiv \exists x(P(x) \wedge \neg Q(x))$.

Nested Quantifiers: Two quantifiers are nested if one is within the scope of the other.

Example: Assume that the domain for the variables x and y consists of all real numbers. The statement

$$\forall x\ \forall y\ (x + y = y + x)$$

says that $x+y = y+x$ for all real numbers x and y. This is the commutative law for addition of real numbers. Likewise, the statement

$$\forall x\ \exists y\ (x + y = 0)$$

says that for every real number x there is a real number y such that $x + y = 0$. This states that every real number has an additive inverse. Similarly, the statement

$$\forall x\ \forall y\ \forall z\ (x + (y + z) = (x + y) + z)$$

is the associative law for addition of real numbers.
Quantifications of Two Variables:

- **Statement:** $\forall x\ \forall y\ P(x, y)$ OR $\forall y\ \forall x\ P(x, y)$
  When True? $P(x, y)$ is true for every pair x, y.
  When False? There is a pair x, y for which $P(x, y)$ is false.
- **Statement:** $\forall x\ \exists y P(x, y)$
  When True? For every x there is a y for which $P(x, y)$ is true
  When False? There is an x such that $P(x, y)$ is false for every y.
- **Statement:** $\exists x\ \forall y\ P(x, y)$
  When True? There is an x for which $P(x, y)$ is true for every y.
  When False? For every x there is a y for which $P(x, y)$ is false.
- **Statement:** $\exists x\ \exists y\ P(x, y)$ OR $\exists y\ \exists x\ P(x, y)$
  When True? There is a pair x, y for which $P(x, y)$ is true.
  When False? $P(x, y)$ is false for every pair x, y.

Example: We can express that a function $f : X \to Y$ is one-to-one using quantifiers as

$$\forall a\ \forall b\ \big(f(a) = f(b) \to a = b\big).$$

Example: A function $f : X \to Y$ is onto if

$$\forall y\ \exists x\ (f(x) = y).$$

Example: Use quantifiers to express the definition of the limit of a real-valued function $f(x)$ of a real variable x at a point a in its domain.
Solution: Recall that the definition of the statement

$$\lim_{x \to a} f(x) = L$$

is: For every real number $\epsilon > 0$ there exists a real number $\delta > 0$ such that $|f(x) - L| < \epsilon$

whenever $0 < |x - a| < \delta$. This definition of a limit can be phrased in terms of quantifiers by

$$\forall\epsilon > 0 \; \exists\delta > 0 \; \forall x \; \Big(0 < |x - a| < \delta \to |f(x) - L| < \epsilon\Big).$$

Example: Negate each of the following statement:

1. $\exists x \; \forall y, \; P(x, y)$,
2. $\exists x \; \exists y \; \forall z, \; p(x, y, z)$

Solution:

1. $\neg(\exists x \; \forall y, \; P(x, y)) \equiv \forall x \; \exists y, \; \neg P(x, y)$.
2. $\neg(\exists x \; \exists y \; \forall z, \; P(x, y, z)) \equiv \forall x \; \forall y \; \exists z, \neg P(x, y, z)$

Example from "A basic course in Real Analysis by S Kumaresan": Suppose we have a sentence: "In each tree in the orchard, we can find a branch in which all the leaves are green".

Let us convert the above sentence as a mathematical sentence: Let T denote the set of all trees in the orchard. Let $t \in T$ be a tree. Let B_t denote the set of all branches of the tree t. Let $b \in B_t$ be a branch of tree t. Let l_b denote the set of all leaves on the branch b. Then the above sentence can be written as:

$\forall t \in T \, \exists \, b \in B_t \, \forall \, l \in L_b, l$ is green. The negation is:

$$\neg(\forall t \in T \, \exists \, b \in B_t \, \forall \, l \in L_b, l \text{ is green}) \equiv \exists \, t \in T \, \forall \, b \in B_t \, \exists \, l \in L_b, l \text{ is not green}.$$

Lecture-4

Set: A set is defined as a well defined collection of well defined distinct objects. The objects are called the elements or members of the set. We denote a set usually by capital letters, such as, $A, B, X, Y, \ldots$, whereas the lower-case letters $a, b, p, q, \ldots$ will usually be used to denote elements of sets. The set having no element is called empty set or nul set denoted by ϕ. If x is an element of a set X then we denote it by $x \in X$. The cardinality or the number of elements in a set S is denoted by $|S|$.

Let A and B be two sets such that elements of A are also the elements of B then we say that A is a subset of B, denoted as $A \subseteq B$. Two sets A and B are said to be equal, written as $A = B$, if $A \subseteq B$ and $B \subseteq A$. Let A be a set. A collection of all subsets of A is called power set of A, denoted as $P(A)$. If $|A| = n$, then $|P(A)| = 2^n$.

Examples:

1. Natural numbers $\mathbb{N}$, Integers $\mathbb{Z}$, Rationals $\mathbb{Q}$, Real numbers $\mathbb{R}$.
2. The solution of the equation $x^2 - 4x + 4$.
3. The set of nobel laureates in the world.
4. The set of points in $\mathbb{R}^2$.
5. The people living in India.

Operations on sets Let A and B be two sets. Then:

1. A union B, denoted as: $A \cup B = \{x : x \in A \,\text{or}\, x \in B\}$.
2. A intersection B, denoted as: $A \cap B = \{x : x \in A \,and\, x \in B\}$.
3. A minus B denoted as: $A - B = \{x : x \in A \,and\, x \notin B\}$.
4. A complement, denoted as: $A^c = \{x : x \in U \,and\, x \notin A\}$, where U is universal set.
5. The symmetric difference of A and B written as: $A \oplus B = (A \cup B) - (A \cap B)$.

Algebra of sets Let A and B be two sets and U be universal set. Then:

1. Associative Law: $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
2. Commutative Law: $A \cup B = B \cup A$ and $A \cap B = B \cap A$
3. Distributive Law: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. De Morgan's Law: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$.
5. Identity Law: $A \cup \phi = A$, $A \cup U = U$ and $A \cap \phi = \phi$, $A \cap U = A$.
6. Complement Law: $A \cup A^c = U$, $A \cap A^c = \phi$, $U^c = \phi$ and $\phi^c = U$
7. Involution Law: $(A^c)^c = A$

Inclusion and exclusion principle:

1. For two sets A_1 and A_2: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.
2. For three sets A_1, A_2 and A_3: $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.
3. General form: $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|$.

Multiset: A multiset is a set in which the multiplicity of an element may be one or more. The multiplicity of an element is the number of times the element repeated in the multiset.

Operations on multiset: Let A and B be two multisets. Then

1. Union of multisets: The union of two multiset A and B is a multiset C such that the multiplicity of an element in C is equal to the maximum of the multiplicity of the element in A and B.
2. Intersection of multisets: The intersection of two multiset A and B is a multiset C such that the multiplicity of an element in C is equal to the minimum of the multiplicity of the element in A and B.
3. Difference of multisets: The difference of two multisets A and B is a multiset C such that the multiplicity of an element in C is equal to the multiplicity of the element in A minus the multiplicity of the element in B if the difference if positive, and if the difference is negative multiplicity is considered as 0.
4. Sum of multisets: The sum of two multisets A and B is a multiset C such that the multiplicity of an element in C is the sum of multiplicity of the element in A and B.
5. Cardinality of multiset: The cardinality of a multiset is the number of distinct elements in the multiset without considering the multiplicity of an element.

Cartesian product: Let A and B be two sets. Then the cartesian product $A \times B$ of the sets is defined as $A \times B = \{(a, b) : a \in A, b \in B\}$. The elements of $A \times B$ are called ordered pairs. Note that if $|A| = n$, $|B| = m$, then $|A \times B| = n.m$.

Examples 1: Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Then $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$, $B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$, and $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

Example 2: Let $A = \mathbb{R}$. Then $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Lecture-5

Binary Relation: Let A and B be non-empty sets. A binary relation or simply a relation R from A to B is a subset of $A \times B$, that is, $R \subseteq A \times B$. If $(a, b) \in R$, then we also say that a is related to b by R or aRb. If $A = B$, then we say that R is a relation on A.

The domain of R is a subset of A which are related to some elements in B. The range of R is set of all element $b \in B$ for which there is some element $a \in A$ such that aRb. Let A, B be a sets with $|A| = m$ and $|B| = n$. Then there are 2^{mn} relations from A to B.

Examples:

1. Let $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$, and let $R = \{(1, y), (1, z), (3, y)\}$. Since $R \subseteq A \times B$, R is a relation from A to B. The domain of R is $\{1, 3\}$ and the range of R is $\{y, z\}$.
2. Let S be a collection of sets. Then set inclusion $\subseteq$ is a relation on A.
3. The divisibility of two numbers in $\mathbb{N}$ is a relation on $\mathbb{N}$.
4. Let L be the set of lines in the plane. Then perpendicularity of two lines l_1 and l_2 in the plane gives a relation on L.

Complement of relation: Let R be a relation from A to B. The complement of R, denoted by $\bar{R}$, is a relation from A to B such that $\bar{R} = \{(a, b) : (a, b) \notin R\}$.

Inverse of relation: Let R be a relation from A to B. The inverse of R, denoted by R^{-1} is a relation from B to A such that $R^{-1} = \{(b, a) : (a, b) \in R\}$.

Composition of relation: Let A, B and C be sets, and let R be a relation from A to B and S be a relation from B to C, that is, $R \subseteq A \times B$ and $S \subseteq B \times C$. Then

$R \circ S = \{(a, c) :$ there exists $b \in B$ for which $(a, b) \in R$ and $(b, c) \in S\}$.

Example: Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$. Let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$ and $S = \{(b, x), (b, z), (c, y), (d, z)\}$ be relations from A to B and from B to C respectively. Then $R \circ S = \{(2, z), (3, x), (3, z)\}$.

Types of relation: Let A be a set and R be a relation on A.

1. **Reflexive Relation:** R is reflexive if $(a, a) \in R$, that is, aRa for all $a \in A$.
2. **Symmetric Relation:** R is symmetrix if aRb then bRa.
3. **Antisymmetric Relation:** R is called antisymmetric if aRb and bRa then $a = b$.
4. **Transitive Relation:** R is called transitive: if aRb and bRc then aRc.

Example. Let $A = \{1, 2, 3, 4\}$. Consider the following relations on A.

$R_1 = \{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\}$,

$R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$,

$R_3 = \{(1, 3), (2, 1)\}$,

$R_4 = \emptyset$, the empty relation,

$R_5 = A \times A$.

Determine, which of the relations are: (a) reflexive, (b) symmetric, (c) antisymmetric, (d) transitive.

Solution: Since $(2,2) \notin R_1, R_3, R_4$. Hence, these relations are not reflexive. Since $(a,a) \in R_2, R_5$ for every $a \in A$, R_2 and R_5 are reflexive.

R_1 is not symmetric since $(1,2) \in R_1$ but $(2,1) \notin R_1$. Similarly R_3 is not symmetric. All other relations are symmetric.

R_2 is not antisymmetric since $(1,2),(2,1) \in R_2$ but $1 \neq 2$. Similarly R_5. All the other relations are antisymmetric.

R_3 is not transitive since $(2,1),(1,3) \in R_3$ but $(2,3) \notin R_3$. All the other relations are transitive.

Equivalence Relation: A relation R on a set S is called an equivalence relation if it is reflexive, symmetric, and transitive.

Examples:

1. Let S be a set of lines in the plane. The relation of parallel is an equivalence relation.
2. The relation of inclusion $\subseteq$ is not equivalence relation. It is reflexive and transitive but not symmetric, since $A \subseteq B$ does not imply $B \subseteq A$.
3. Let m be a fixed positive integer. Two integers a and b are said to be congruent moulo m, written as $a \equiv b \pmod{m}$, if m divides $a - b$. This relation of congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Equivalence Class: Let R be an equivalence relation on a set S. For $a \in S$, the set $[a] = \{x : (a,x) \in R\}$ is called the equivalence class of a.

The collection of all such equivalence classes is denoted by S/R, that is, $S/R = \{[a] : a \in S\}$. The set S/R is also called quotient set of S by R.

Example In the above Example 3, the relation of congruent modulo m on the set of integers $\mathbb{Z}$. Let $m = 5$. Then we see that

$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$, that is, $[0] = \{5k : k \in \mathbb{Z}\}$,

$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$, that is, $[1] = \{5k+1 : k \in \mathbb{Z}\}$,

$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$, that is, $[2] = \{5k+2 : k \in \mathbb{Z}\}$.

$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$, that is, $[3] = \{5k+3 : k \in \mathbb{Z}\}$.

$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$, that is, $[3] = \{5k+4 : k \in \mathbb{Z}\}$.

The above are the only distinct equivalence classes. Thus $\mathbb{Z}/R = \{[0], [1], [2], [3], [4]\}$.

Theorem 1: Let R be an equivalence relation on a set S.

1. For each $a \in S$, $a \in [a]$, that is, every element lies in its own equivalence class.

2. For each $a, b \in S$, $a\,R\,b$ if and only if $[a] = [b]$, that is, if any two elements are related by R then they have same equivalence class.

3. For each $a, b \in S$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Proof: Since R is reflexive, $a\,R\,a$ for each $a \in S$. So $a \in [a]$. This proves first part.

Second Part: Suppose $a\,R\,b$ and $x \in [a]$. Then $x\,R\,a$. Since $a\,R\,b$ and R is transitive, $x\,R\,b$. So $x \in [a]$, and $[a] \subseteq [b]$. Similarly we see that $[b] \subseteq [a]$. Combining both, we get $[a] = [b]$. Conversely, let $[a] = [b]$. This means, if $x \in [a]$ then $x \in [b]$ and therefore xRa (or aRx since R is symmetrix) and xRb. Since R is transitive, aRb.

Third Part: let $[a] \cap [b] \neq \emptyset$ and $x \in [a] \cap [b]$. Then xRa (so aRx) and xRb imples aRb. By second part, $[a] = [b]$.

Partition of a set: Let S be a non-empty set. A collection P, containing subsets $A_1, A_2, \ldots$ of S, is called a partition of S if: $\cup A_i = S$ and $A_i \cap A_j = \emptyset$ for $i \neq j$.

Example: Let $S = \{1, 2, \ldots, 9\}$. Consider the following collections of subsets of S.

$P_1 = [\{1, 3, 5\}, \{2, 6\}, \{4, 8, 9\}]$,

$P_2 = [\{1, 3, 5\}, \{2, 4, 6, 8\}, \{5, 7, 9\}]$,

$P_3 = [\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}]$.

P_1 is not a partition, since $7 \notin P_1$. P_2 is not a partition, since $\{1, 3, 5\}$ and $\{5, 7, 9\}$ are not disjoint. Note that P_3 is a partition of S.

Theorem 2: Let R be an equivalence relation on a nonempty set S. The collection S/R of all equivalence classes gives a partition of S.

Proof: Proof follows from Theorem 1.

Lecture-6

Partial order relation: Let R be a relation on a set X satisfying the following three properties:

Reflexive: For any $a \in S$, we have aRa.

Antisymmetric: If aRb and bRa, then $a = b$.

Transitive: If aRb and bRc, then aRc.

POSET

Then R is called partial order and the set X with such R is called partially ordered set.

Examples:

1. The relation ($\leq$) "less than or equal to" is partial order on $\mathbb{R}$.
2. The inclusion relation of sets ($\subseteq$) is partial order on a collection of sets.
3. The relation divisibility ($|$) is a partial order on $\mathbb{N}$.
4. The ralation divisibility ($|$) is not a partial order on $\mathbb{Z}$. As, $2|-2$ and $-2|2$ but $2 \neq -2$.

Totally ordered set: A partial order R on a set X is called total ordering if given every pair of $x, y \in X$, either xRy or yRx. A set X with total ordering is called totally ordered set or a chain.

Examples:

1. $\mathbb{R}$ is a chain with the relation $\leq$. What if we replace $\leq$ by $<$?

wont be POSET itself since not reflexive

2. A collection of sets with the inclusion relation $\subseteq$ is not a chain.
3. The set $S = \{2, 5, 6, 8, 9, 10\}$ is not a chain with the divisibility relation.

First and Last element: Let X be a partially order set with the relation R. If $a \in X$ such that aRx for every $x \in X$, then we say that a is the first element of X. Similarly if $b \in X$ such that xRb for every $x \in X$, then b is called the last element of X.

Well ordered set: A partially ordered set X is called well ordered if every non-empty subset of X contains the first element.

Example. $\mathbb{N}$ is well ordered set under the usual relation $\leq$.

Maximal and Minimal element: Let X be a partially ordered set with the ralation R. An element $a \in X$ is called a minimal element of X if no element of X related to a, that is, if xRa implies $x = a$.

An element $b \in X$ is called a maximal element of X if b is not related to any element of X, that is, if bRx implies $x = b$.

Example: Consider the divisibility relation on the set $S = \{2, 3, 4, 6, 9, 10, 12, 36\}$. Then 2 and 3 are minimal elements and 10 and 36 are maximal elements.

Upper and lower bounds: Let A be a subset of a partially orederd set X. An element $a \in X$ is called a lower bound of A if aRx for every $x \in A$. Similarly an element $b \in X$ is an upper bound of A if xRb for every $x \in A$. A set A may have no upper bound or lower bound.

Infimum and Supremum: Let A^* denote the collection of all upper bounds of A and A_* denote the collection of all lower bounds of A. Then the first element of A^*, if it exists, is called the least upper bound or the supremum of A. Similarly the last element of A_*, if it exists, is called the greatest lower bound or infimum of A.

Example: Let $\mathbb{R}$ with usual order relation $\leq$ and let $A = \{x \in \mathbb{R} : 1 < x < 2\}$. Here $A_* = \{x \in \mathbb{R} : x \leq 1\}$. and $A^* = \{x \in \mathbb{R} : x \geq 2\}$. So, the supremum is 2 and infimum is 1.

Order Completeness Axiom: A partial order set X is said to be order complete if every non-empty subset of X which has an upper bound (or which has a lower bound) has a supremum (or infimum).

Example: The sets $\mathbb{N}$ and $\mathbb{R}$ with usual oreder $\leq$ are order complete. The set $\mathbb{Q}$ is not order complete. Consider $A := \{x \in \mathbb{Q} : 2 < x^2 < 5\}$, has no supremum and infimum.

Function: A function f from A to B is an assignment which assigns each element of A to a unique element of B. Equivalentely, a function is a relation from A to B such that for each element $a \in A$ there is a unique element $b \in B$ such that aRb. A and B are called the domain and co-domain of the function respectively. The set of all those elements in B which are mapped by some elemets in A is called the range or image of f.

Types of Functions: Let $f : A \to B$.

1. **Injective (one-to-one):** If distinct elements of domain have distinct images. That is, f is one-to-one if $f(x) = f(y)$, then $x = y$. Or $x \neq y$ implies $f(x) \neq f(y)$. Find the number of injective functions from one set to another.
2. **Surjective (onto):** If every element of co-domain are mapped by some elements of domain. That is f is onto, if for each $b \in B$ there is $a \in A$ such that $f(a) = b$. Find the number of surjective functions from one set to another.
3. Bijective: If it is one one and onto. Find the number of bijective functions from one set to other.

Similar set: Sets A and B are called similar, if there is a bijective map between them.

Example: $\mathbb{N}$ and E (set of all even natural number) are similar. Define $f : \mathbb{N} \to E$ by $f(n) = 2n$.

Countable set: A set S is called countable if it is similar to $\mathbb{N}$.

Example: The set $S = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots\}$ is countable. Define $f : \mathbb{N} \to S$ as $f(n) = \frac{n}{(n+1)}$ for all $n \in N$.

Uncountable set: A set which is not countable is called uncountable set.

Example: The set of real numbers $\mathbb{R}$ is not countable, that is, an uncountable set.

Proof: Suppose $\mathbb{R}$ is countable. We know that a subset of a countable set is countable. consider $A = (0,\ 1) \subseteq \mathbb{R}$. We show that A is not countable. On the contrary, suppose A is countable. Then we can write elements of A as $r_1, r_2, r_3 \ldots$, where r_i can be written in the decimal expansion form as follows:

$r_1 = d_{11}d_{12}d_{13}\ldots$

$r_2 = d_{21}d_{22}d_{23}\ldots$

$r_3 = d_{31}d_{32}d_{33}\ldots$

....

$r_n = d_{n1}d_{n2}d_{n3}\ldots$

....

, where $d_{ij} \in \{0, 1, 2, \ldots, 9\}$. Now consider $r = d_1d_2d_3\ldots$ as follows:

$$d_i = \begin{cases} 1 & d_{ii} \neq 1 \\ 2 & d_{ii} = 1. \end{cases}$$

Then r is an element of A which is not equal to r_i. Thus A is uncountable and therefore $\mathbb{R}$ is uncountable.

Schröder-Bernstein Theorem: If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. In other words, if there are one-to-one functions f from A to B and g from B to A, then there is a one-to-one correspondence between A and B.

Example: Show that $|(0, 1)| = |(0, 1]|$

Solution: Let $A = (0, 1)$ and $B = (0, 1]$. Then consider $f : A \to B$ defined as $f(x) = x$ and $g : B \to A$ defined as $g(x) = \frac{x}{2}$. Then f and g are one-to-one. Therefore $|(0, 1)| = |(0, 1]|$.

Lecture-(7-9)

(Proof Techniques)

Mathematical system: A system consists of Axioms, Definitions, and Terms is called a Mathematical system. We prove or disprove any statement within a mathematical system. Let us define some terms which are related to a mathematical system directly or indirectly.

1. **Definition:** A precise description of meaning of a mathematical term.
2. **Theorem:** A proposition that has been proved to be true. A theorem is of two kinds: Lemma and Corollary.
3. **Lemma:** A theorem that is usually not too interesting in its own right but is useful in proving another theorem.
4. **Corollary:** A theorem that follows immediately from another theorem.
5. **Conjecture:** A statement that is suspected to be true but yet to prove.

   Example: The 4-color conjecture, the $3x+1$ conjecture, Goldbach's conjecture, Hadwiger conjecture, the abc conjecture, etc.
6. **Axiom:** A statement that is assumed to be true without proof.

   Example: 2+2=4.
7. **Paradox:** A statement that can be shown, using a given set of axioms and definitions, to be both true and false at the same time.

   Example: Nobody goes to Murphy's Bar anymore as it's too crowded.

1° Methods of Proof:

By a proof, of a proposition $p \Rightarrow q$, we mean an argument that establishes the truth value of the proposition. Since the argument can be given in different forms and hence we can have different proof techniques.

1. **Direct Method:** Using p is true and with the help of other axioms, definitions and previously derived theorems, we here show that q is true.

   (a) **Example:** If m is odd and n is even integer, then show that $m+n$ is odd integer.

   Proof: We use the definitions of even and odd integer.

   m is odd if there is an integer k_1 such that $m = 2k_1 + 1$ and n is even integer if there is an integer k_2 such that $n = 2k_2$.

   Then $m+n = 2k_1 + 1 + 2k_2 = 2(k_1+k_2)+1 = 2k+1$, where $k = k_1 + k_2$. So, $m+n$ is odd.

2. **Proof by Contradiction** In this technique, we assume that q is false, that is, $\neg q$ is true. Note that $\neg(p \to q) \equiv (p \wedge \neg q)$, that is to say, $p \to q$ is true if and only if $(p \wedge \neg q)$ is false. In other words, $p \wedge \neg q$ is a contradiction.

   (a) **Example:** For any integer x if x^2 is even, then x is even.

   Proof: Suppose x is not even and x^2 is even. So $x = 2k_1 + 1$ and $x^2 = 2k_2$ for some integers k_1, k_2. Then we have $(2k_1 + 1)^2 = 2k_2$. This implies $4(k_1^2 + k_1) + 1 = 2k_2$. But $4(k_1^2 + k_1) + 1$ is odd and $2k_2$ is even, so these cannot be equal. Thus we have a contradiction.

   (b) **Example:** Prove that $\sqrt{2}$ is irrational.

   gcd

   Proof: Suppose $\sqrt{2}$ is rational. Then we can write $\frac{p}{q} = \sqrt{2}$, where $(p, q) = 1$.

   Then squaring both sides, we get $p^2 = 2q^2$. This implies p is even, that is, $p = 2k$ for some integer k. But then $q^2 = 2k^2$, that is, q is even. This gives a contradiction that $(p, q) = 1$.

   (c) **Example:** Prove that primes are infinite.

   Proof: Suppose there are only k primes $p_1, p_2, \ldots, p_k$. Now consider $n = p_1 p_2 \ldots p_k + 1$. Since n is not a prime so there is some prime p_i such that p_i divides n. Also p_i divides $p_1 p_2 \ldots p_k$. This implies p_i divides $n - p_1 p_2 \ldots p_k = 1$. This is a contradiction as the smallest prime is 2.

   (d) **Example:** Prove that there are no integers x and y such that $x^2 = 4y + 2$.

   Proof: Suppose there are integers x and y such that $x^2 = 4y + 2 = 2(2y + 1)$. So x^2 is even and therefore x is even. Let $x = 2k$ for some integer k. Then substituting this, we get $2k^2 = 2y + 1$. But $2k^2$ is even while $2y + 1$ is odd, so these cannot be equal. Thus we have a contradiction.

3. **Proof by Contrapositive:** Note that $p \Rightarrow q \equiv \neg(p \wedge \neg q) \equiv \neg(\neg q \wedge p) \equiv \neg((\neg q) \wedge \neg(\neg p)) \equiv (\neg q \Rightarrow \neg p)$.

   Thus $p \Rightarrow q$ is logically equivalent to $\neg q \Rightarrow \neg p$. In other words, saying that if p is true then q is true is equivalent to if q is false then p is false.

   (a) **Example:** For any integer x if x^2 is even, then x is even.

   Proof: Suppose x is not even. So $x = 2k_1 + 1$ for some integer k_1. Then we have $x^2 = (2k_1 + 1)^2 = 4(k_1^2 + k_1) + 1$. This shows that x^2 is not even.

   (b) **Example:** Let a and b be integers. If $a + b$ is even, then a and b are either both odd or both even.

   Proof: Suppose that a and b are not both odd and both even. So one of a and b is odd and other is even. Without loss of generality, assume that a is even and b is odd. So $a = 2k$ and $b = 2l + 1$ for some integers k, l. Therefore $a + b = 2(k + l) + 1$. So $a + b$ is odd.

4. **Proof by Cases:** If $p \Rightarrow q$ and p is partitioned into cases r, s, that is, $p \equiv r \vee s$. Then from the below truth table, we see that $p \Rightarrow q \equiv (r \vee s) \Rightarrow q \equiv (r \Rightarrow q) \wedge (s \Rightarrow q)$.

r	s	q	$r \vee s$	$(r \vee s) \Rightarrow q$	$r \Rightarrow q$	$s \Rightarrow q$	$(r \Rightarrow q) \wedge (s \Rightarrow q)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	F	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

So if p as a proposition involves "or", it is sufficient to consider each of the possibilities for p separately.

(a) **Example:** Prove that there is no possible integer n such that $n^2 + n^3 = 100$.

Proof (Method 1): If $n^2 + n^3 = 100$ then we have

$n^2 \leq 100$ and $n^3 \leq 100$. This implies $n \leq 10$ and $n \leq 4$. So we have to check for the cases $n = 1, 2, 3, 4$. This gives the following cases:

For $n = 1$, $n^2 + n^3 = 1 + 1 = 2 \neq 100$,

For $n = 2$, $n^2 + n^3 = 4 + 8 = 12 \neq 100$,

For $n = 3$, $n^2 + n^3 = 9 + 27 = 36 \neq 100$,

For $n = 4$, $n^2 + n^3 = 16 + 64 = 80 \neq 100$.

Proof (Method 2): $n^2 + n^3 = 100$ is equivalent to $n^2(1 + n) = 100$. This is an expression of factors of 100 into two numbers n^2 and $1 + n$.

Note that possible divisors of 100 are : 2,4,5,10,25,50 and out of then for the possibility of $n^2 = 4$ and $n^2 = 25$.

Thus for $n^2 = 4$, $n = 2$ and $(1 + n) = 3$, then we get $n^2.(1 + n) = 4.3 = 12 \neq 100$,

Similarly, for $n^2 = 25$, $n = 5$ and $(1+n) = 6$, then we get $n^2.(1+n) = 25.6 = 150 \neq 100$.

5. **Proof by Counterexample:** Suppose we have problem: Prove or disprove $A \Rightarrow B$. Thus if the proposition $A \Rightarrow B$ is not true then to show that $\neg(A \Rightarrow B)$ is true for some instances.

If the problem is of the form $\forall x,\ A(x) \Rightarrow B(x)$, then its negation is $\exists x\ A(x) \not\Rightarrow B(x)$.

Recall that $A \Rightarrow B \equiv B \vee \neg A$. So

$\exists x\ A(x) \not\Rightarrow B(x)$

$\equiv \exists x \neg(A(x) \Rightarrow B(x))$

$\equiv \exists x \neg(B(x) \vee \neg A(x))$

$\equiv \exists x\, (\neg B(x) \wedge A(x))$.

Thus to prove the original statement is not true, we have to find an x such that $(\neg B(x) \wedge A(x))$ is true.

(a) **Example:** Prove or disprove: for all positive integetr n, $n^2 - n + 41$ is prime.

Solution: Let us disprove by counterexample. If the statement is not true then we have to find a positive integer n such that $n^2 - n + 41$ is not a prime.

Let $n = 41$. Then $n^2 - n + 41$ is equal to 1681, which is not a prime.

(b) **Example:** Prove or disprove: for all positive inetegrs n, $2^n + 1$ is a prime.

Solution: For $n = 1$, $2^n + 1 = 3$, which is prime.

For $n = 2$, $2^n + 1 = 5$, which is prime.

For $n = 3$, $2^n + 1 = 9$, which is not a prime.

6. **Existence Proofs:** An existence proof is a proof of a statement of the form $\exists x\, P(x)$. Such proofs are generally fall into one of the following two types:

(a) **Constructive Proof:** Establish $P(x_0)$ for some x_0 in the domain of P.

i. Example: Prove that If $f(x) = x^3 + x - 5$, then there exists a positive real number x_0 such that $f^{'}(x_0) = 7$.

Proof: Find $f^{'}(x) = 7$, this gives $x_0 = \sqrt{2}$.

(b) **Nonconstructive Proof:** Assume no x_0 exists that makes $P(x_0)$ true and derive a contradiction. In other words, use a proof by contradiction.

i. **Example: Pigeonhole Principle**: If $n+1$ pigeons are distributed into n holes, then some hole must contain at least 2 of the pigeons.

Proof: Assume $n + 1$ pigeons are distributed into n boxes. Suppose the boxes are labeled $B_1, B_2, \ldots, B_n$, and assume that no box contains more than 1 object. Let k_i denote the number of objects placed in B_i. Then $k_i \leq 1$ for $i = 1, \ldots, n$, and so $k_1 + k_2 + \ldots + k_n \leq 1 + 1 + \ldots + 1 \leq n$. But this contradicts the fact that $k_1 + k_2 + \ldots + k_n = n + 1$, the total number of objects we started with.

7. **Proof by Induction:** There are two form of mathematical induction. One is weak form and another is strong form. We discuss them separately.

(a) **Weak Form of Mathematical Induction:** Let $P(n)$ be a statement on positive integer n such that

1: $P(1)$ is true,

2: for all $k \geq 1$, $P(k+1)$ is true whenever one assumes that $P(k)$ is true.

Then $P(n)$ is true for all positive integer n.

i. **Example:** Prove that $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Proof: Let $P(n) = 1 + 2 + \ldots + n$. Then $P(n)$ holds for $n = 1$.

Suppose $P(n)$ holds for $n = k$, that is, $P(k) = 1 + 2 + \ldots + k = \frac{k(k+1)}{2}$. Now we show that $P(n)$ is true for $n = k + 1$.

$P(k+1) = 1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. Thus $P(n)$ holds for every n.

ii. **Exercise:** Prove that $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

iii. **Exercise:** Prove that for any positive integer n, $1 + 3 + \ldots + (n-1) = n^2$.

iv. **Exercise:** Let $n \in \mathbb{N}$ and suppose we are given real numbers $a_1 \geq a_2 \geq \ldots \geq a_n \geq 0$. Then Arithmetic mean (AM) $= \frac{a_1+a_2+\ldots a_n}{2} \geq (a_1 a_2 \ldots a_n)^{\frac{1}{n}} =$ GM (Geometric mean).

v. **Exercise:** Fix a positive integer n and let A be a set with $|A| = n$. Let $P(A)$ denote the power set of A. Then show that $|P(A)| = 2^n$.

Corollary of weak form of mathematical induction: Let $P(n)$ be a statement on positive integer n such that for some fixed positive integer n_0

1: $P(n_0)$ is true,

2: for all $k \geq n_0$, $P(k+1)$ is true whenever one assume that $P(k)$ is true.

Then $P(n)$ is true for all positive integer $n \geq n_0$.

(b) **Strong Form of the Principle of Mathematical Induction:** Let $P(n)$ be a statement on positive integer n such that

1: $P(1)$ is true,

2: $P(k+1)$ is true whenever one assumes that $P(m)$ is true, for all m, $1 \leq m \leq k$.

Then $P(n)$ is true for all positive integer n.

Corollary of strong form of mathematical induction: Let $P(n)$ be a statement on positive integer n such that for some fixed positive integer n_0,

1: $P(n_0)$ is true,

2: $P(k+1)$ is true whenever one assume that $P(m)$ is true, for all m, $n_0 \leq m \leq k$.

Then $P(n)$ is true for all positive integer $n \geq n_0$.

Lecture-(10-12)

(Counting Techniques)

How do you count the number of people in a crowded room? You could count heads, since for each person there is exactly one head. Alternatively, you could count ears and divide by two. Of course, you might have to adjust the calculation if someone lost an ear in a pirate raid or someone was born with three ears. The point here is that you can often count one thing by counting another, though some fudge factors may be required. This is a central theme of counting, from the easiest problems to the hardest.
Let us note that **every counting problem comes down to determining the size of some set.**

We first present basic counting rules. Then we will show how they can be used to solve many different counting problems.

The product rule: Suppose a task has $n \in \mathbb{N}$ **compulsory** parts and the i-th part can be completed in $m_i \in \mathbb{N}$ ways for $i = 1, 2, \ldots, n$. Then the task can be completed in $m_1 m_2 \ldots m_n$ ways.
In terms of sets, if $A_1, A_2, \ldots, A_n$ are sets, then

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1|.|A_2|.\ldots.|A_n|.$$

1. How many three digit natural numbers can be formed using digits $0, 1, \ldots, 9$?

   Solution: $9 \times 10 \times 10$ ways.

2. The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

   Solution: 100×26 ways.

3. There are 32 computers in a computer center. Each microcomputer has 24 ports. How many different ports to a computer in the center are there?

   Solution: 32×24 ports.

4. How many functions are there from a set with m elements to a set with n elements?

   Solution: $n \times n \times \ldots \times n (m \,\text{times})$, that is, n^m.

5. How many one-to-one functions are there from a set with m elements to one with n elements?

   Solution: $n \times (n-1) \times (n-2) \times \ldots \times (n-m+1)$.

6. Let $|S| = n$. $|P(S)| = 2^n$.

   Solution: consider the one-to-one correspondence between subsets of S and bit strings (each element takes on a value of 0 or 1) of length $|S|$. A susbset of S is associated with the bit string with a 1 in the ith position if the ith element in the list is in the subset. By the multiplication rule, there are $2^{|S|}$ bit strings of length $|S|$. Therefore, $|P(S)| = 2^{|S|}$.

The sum rule: Suppose a task consists of n **alternative** parts (either parts), and the i-th part can be completed in m_i ways, $i = 1, \ldots, n$. Then the task can be completed in $m_1 + m_2 + \ldots + m_n$ ways. Following examples illustrate the rule.
In terms of sets, if $A_1, A_2, \ldots, A_n$ are disjoint sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

1. Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

   Solution: 37+83= 110.

2. How many three digit natural numbers with distinct digits can be formed using digits $1, \ldots, 9$ such that each digit is odd or each digit is even?

   Solution: The task has two alternative parts. Part 1: form a three digit number with distinct digits using digits from $\{1, 3, 5, 7, 9\}$. Part 2: form a three digit number with distinct digits using digits from $\{2, 4, 6, 8\}$. Observe that Part 1 is a task having three compulsory subparts. Using multiplication rule, we see that Part 1 can be done in $5 \times 4 \times 3$ ways. Part 2 is a task having three compulsory subparts. So, it can be done in $4 \times 3 \times 2$ ways. Since our task has alternative parts, addition rule implies $60 + 24 = 84$.

The subtraction rule: If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.
In terms of sets, if A and B are finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

The subtraction rule is also known as the principle of inclusion-exclusion, especially when it is used to count the number of elements in the union of two sets.

1. How many bit strings of length eight either start with a 1 bit or end with the two bits 00?

   Solution: $2^7 + 2^6 - 2^5$.

2. A computer company receives 350 applications from computer graduates for a job. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

   Solution: Let A_1 be the set of students who majored in computer science and A_2 the set of students who majored in business. By the subtraction rule, the number of students who majored either in computer science or in business equals $A \cup B$

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316$. Thus, $350 - 316 = 34$ of the applicants majored neither in computer science nor in business.

The division rule: There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.
In terms of functions, if $f : A \to B$ is $k-$to-1, then $|A| = k|B|$. A $k-$to-1 function maps exactly k elements of the domain to every element of the codomain.

1. How many different ways are there to seat four people around a circular table, where two seatings are considered the same when each person has the same left neighbor and the same right neighbor?

   Solution: There are 4! seatings. Now any seating is similar to four seatings. For example $A-B-C-D$ is similar to $A-B-C-D$, $B-C-D-A$, $C-D-A-B$, $D-A-B-C$. Thus total number of different seatings is $4!/4 = 6$.

Bijection Rule: If there is a bijection $f : A \to B$ between A and B, then $|A| = |B|$.

The Subset Rule: The number of k-element subsets of an n-element set is

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Let A be an n-element set and $k_1, k_2, \ldots, k_m$ be nonnegative integers whose sum is n. A $(k_1, k_2, \ldots, k_m)$-split of A is a sequence

$$(A_1, A_2, \ldots, A_m),$$

where the A_i are disjoint subsets of A and $|A_i| = k_i$ for $i = 1, 2 \ldots, m$.

Subset Split Rule: The number of $(k_1, k_2, \ldots, k_m)$-splits of an n element set is

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!\ k_2!\ \ldots\ k_m!}.$$

The Bookkeeper Rule: Let $l_1, \ldots, l_m$ be distinct elements. The number of sequences with k_1 occurrences of l_1, and k_2 occurrences of l_2, $\ldots$, and k_m occurrences of l_m is

$$\frac{(k_1 + k_2 + \ \cdots + k_m)!}{k_1!\ k_2!\ \ldots\ k_m!}.$$

Example: Suppose you are planning a 20-mile walk, which should include 5 northward miles, 5 eastward miles, 5 southward miles, and 5 westward miles. How many different walks are possible?
Solution: There is a bijection between such walks and sequences with 5 N's, 5 E's, 5 S's, and

5 W's. By the Bookkeeper Rule, the number of such sequences is:

$$\frac{(5+5+5+5)!}{5!\ 5!\ 5!\ 5!} = \frac{20!}{(5!)^4}.$$

Pigeonhole Principle: If $n+1$ pigeons (resp. objects) are distributed into n holes (resp. boxes), then some hole (box) must contain at least 2 of the pigeons (objects).

Proof: Assume $n+1$ pigeons are distributed into n boxes. Suppose the boxes are labeled $B_1, B_2, \ldots, B_n$, and assume that no box contains more than 1 object. Let k_i denote the number of objects placed in B_i. Then $k_i \le 1$ for $i = 1, \ldots, n$, and so $k_1+k_2+\ldots+k_n \le 1+1+\ldots+1 \le n$. But this contradicts the fact that $k_1+k_2+\ldots+k_n = n+1$, the total number of objects we started with.

1. Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

2. In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

3. How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?

   Solution: There are 101 possible scores on the final. The pigeonhole principle shows that among any 102 students there must be at least 2 students with the same score.

The Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects, where $\lceil . \rceil$ denotes the ceiling function. In terms of functions, If $|X| > k|Y|$, then every function $f : X \to Y$ maps at least $k+1$ different elements of X to the same element of Y.

1. Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.

2. Show that among any $n+1$ positive integers not exceeding $2n$ there must be an integer that divides one of the other integers.

   Solution: Let us write each of the $n+1$ integers $a_1, a_2, \ldots, a_{n+1}$ as a power of 2 times an odd integer. In other words, let $a_j = 2^{k_j} q_j$ for $j = 1, 2, \ldots, n+1$, where k_j is a non-negative integer and q_j is odd. The integers $q_1, q_2, \ldots, q_{n+1}$ are all odd positive integers less than $2n$. Because there are only n odd positive integers less than $2n$, it follows from the pigeonhole principle that two of the integers $q_1, q_2, \ldots, q_{n+1}$ must be equal. Therefore, there are distinct integers i and j such that $q_i = q_j$. Let q be the common value of q_i and q_j. Then, $a_i = 2^{k_i} q$ and $a_j = 2^{k_j} q$. It follows that if $k_i < k_j$, then a_i divides a_j, while if $k_i > k_j$, then a_j divides a_i.

A permutation of a set of distinct objects is an ordered arrangement of these objects. An ordered arrangement of r elements of a set is called an r-permutation. The number of r-permutations of a set with n elements is denoted by $P(n,r) = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!}$.

1. Let $S = a, b, c$. The 2-permutations of S are the ordered arrangements a, b; a, c; b, a; b, c; c, a; c, b. Consequently, there are six 2-permutations of this set with three elements. We see that $P(3, 2) = 3.2 = 6$.

2. How many permutations of the letters ABCDEFGH contain the string ABC ?

   Solution: Because the letters ABC must occur as a block, we can find the answer by finding the number of permutations of six objects, namely, the block ABC and the individual letters D, E, F , G, and H . Because these six objects can occur in any order, there are $6! = 720$ permutations of the letters ABCDEFGH in which ABC occurs as a block

An r-combination of elements of a set is an unordered selection of r elements from the set. The number of r-combinations of a set with n distinct elements is denoted by $C(n, r)$. Note that $C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$, Here $\binom{n}{r}$ is called a **binomial coefficient**.

Example: How many poker hands of five cards can be dealt from a standard deck of 52 cards?
Solution: Because the order in which the five cards are dealt from a deck of 52 cards does not matter, there are

$$C(52, 5) = \frac{52!}{5!\ 47!}.$$

Corollary: Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n - r)$.

The Binomial Theorem: Let x and y be variables, and let n be a nonnegative integer. Then

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

Corollary: Let n be a nonnegative integer. Then

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \text{ and } \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Pascal's Identity: Let n and k be positive integers with $n \geq k$. Then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Vandermonde's Identity: Let $m, n,$ and r be nonnegative integers with r not exceeding either m or n. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k}.$$

Corollary: If n is a nonnegative integer, then $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$.

Lecture-(13-15)

Theorem (Permutations with Repetition): The number of $r-$permutations of a set of n objects with repetition allowed is n^r.
Proof: There are n ways to select an element of the set for each of the r positions in the r-permutation when repetition is allowed, because for each choice all n objects are available. Hence, by the product rule there are n^r r-permutations when repetition is allowed.

Example: How many strings of length r can be formed from the uppercase letters of the English alphabet?
Solution: By the product rule(or by the above theorem), because there are 26 uppercase English letters, and because each letter can be used repeatedly, we see that there are 26^r strings of uppercase English letters of length r.

Theorem (Combinations with Repetition): There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.
Proof: Each r-combination of a set with n elements when repetition is allowed can be represented by a list of $n-1$ bars and r stars. The $n-1$ bars are used to mark off n different cells, with the ith cell containing a star for each time the ith element of the set occurs in the combination.
For instance, a 6-combination of a set with four elements is represented with three bars and six stars. Here

$$* * | * || * **$$

represents the combination containing exactly two of the first element, one of the second element, none of the third element, and three of the fourth element of the set.

As we have seen, each different list containing $n-1$ bars and r stars corresponds to an r-combination of the set with n elements, when repetition is allowed. The number of such lists is $C(n-1+r, r)$, because each list corresponds to a choice of the r positions to place the r stars from the $n-1+r$ positions that contain r stars and $n-1$ bars. The number of such lists is also equal to $C(n-1+r, n-1)$, because each list corresponds to a choice of the $n-1$ positions to place the $n-1$ bars.

Example: How many solutions does the equation

$$x_1 + x_2 + x_3 = 11$$

have, where x_1, x_2, and x_3 are nonnegative integers?

Solution: To count the number of solutions, we note that a solution corresponds to a way of selecting 11 items from a set with three elements so that x_1 items of type one, x_2 items of type two, and x_3 items of type three are chosen. Hence, the number of solutions is equal to the number of 11-combinations with repetition allowed from a set with three elements. From the above theorem, it follows that there are

$$C(3 + 11 - 1, 11) = C(13, 11) = C(13, 2) = 78$$

solutions.

Generating Functions: The generating function for the sequence $a_0, a_1, \ldots, a_k, \ldots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k.$$

Example: What is the generating function for the sequence $1, 1, 1, 1, 1, 1$?
Solution: The generating function of $1, 1, 1, 1, 1, 1$ is $1 + x + x^2 + x^3 + x^4 + x^5$.

Example: The function $f(x) = 1/(1-x)$ is the generating function of the sequence $1, 1, 1, 1, \ldots$.

Theorem: Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k \quad \text{and} \quad f(x)g(x) = \sum_{k=0}^{\infty} \Big(\sum_{j=0}^{k} a_j b_{k-j} \Big) x^k.$$

Extended Binomial Coefficient: Let u be a real number and k a nonnegative integer. Then the extended binomial coefficient $\binom{u}{k}$ is defined by

$$\binom{u}{k} = u(u-1)\ldots(u-k+1)/k! \;\text{ if }\; k > 0,$$

and $\binom{u}{k} = 1$ if $k = 0$.
The Extended Binomial Theorem: Let x be a real number with $|x| < 1$ and let u be a real number. Then

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k.$$

Example(Counting Problems and Generating Functions): Find the number of solutions of $x_1 + x_2 + x_3 = 17$, where x_1, x_2, and x_3 are nonnegative integers with $2 \le x_1 \le 5, 3 \le x_2 \le 6$, and $4 \le x_3 \le 7$.
Solution: The number of solutions with the indicated constraints is the coefficient of x^17 in the expansion of $(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$.

Example (Using Generating Functions to Solve Recurrence Relations): Solve the recurrence relation $a_k = 3a_{k-1}$ for $k = 1, 2, 3, \ldots$ and initial condition $a_0 = 2$.

Solution: Let $G(x)$ be the generating function for the sequence $\{a_k\}$, that is, $G(x) = \sum_{k=0}^{\infty} a_k x^k$ Now, let us observe that

$$xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1} x^k.$$

With the help of recurrence relation, we have

$G(x) - 3xG(x) = \sum_{k=0}^{\infty} a_k x^k - 3\sum_{k=1}^{\infty} a_{k-1}x^k = a_0 + \sum_{k=1}^{\infty}(a_k - 3a_{k-1})x^k = 2$, because $a_0 = 2$ and $a_k = 3a_{k-1}$. Further, we have that $G(x) = 2/(1-3x)$. Using the identity

$$1/(1-ax) = \sum_{k=0}^{\infty} a^k x^k,$$

we obtain

$$G(x) = 2\sum_{k=0}^{\infty} 3^k x^k = \sum_{k=0}^{\infty} 2.3^k x^k,$$

hence, $a_k = 2.3^k$.

Example(Proving Identities via Generating Functions): Use generating functions to show that

$$\sum_{k=0}^{n} C(n,k)^2 = C(2n,n),$$

whenever n is a positive integer.

Solution: Using the Binomial theorem, we have that $C(2n,n)$ is the coefficient of x^n in $(1+x)^{2n}$. However, we also have

$$(1+x)^{2n} = [(1+x)^n]^2 = [C(n,0) + C(n,1)x + C(n,2)x^2 + \cdots + C(n,n)x^n]^2.$$

The coefficient of x^n in this expression is

$$C(n,0)C(n,n) + C(n,1)C(n,n-1) + C(n,2)C(n,n-2) + \cdots + C(n,n)C(n,0) = \sum_{k=0}^{n} C(n,k)^2,$$

because $C(n,n-k) = C(n,k)$. Because both $C(2n,n)$ and $\sum_{k=0}^{n} C(n,k)^2$ represent the coefficient of x^n in $(1+x)^{2n}$, they must be equal.

Exercise: Prove Pascal's identity and Vandermonde's identity using generating functions.

Recurrence Relations: A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{x_n\}$ is a solution of the recurrence relation $x_n = c_1 x_{n-1} + c_2 x_{n-2}$ if and only if $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

Proof: Here we will do two things to prove the theorem. First, we will show that if r_1 and r_2 are the roots of the characteristic equation, and α_1 and α_2 are constants, then the sequence

$\{x_n\}$ with $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ is a solution of the recurrence relation. Second, we will show that if the sequence $\{x_n\}$ is a solution, then $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for some constants α_1 and α_2.

Now we will show that if $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, then the sequence $\{x_n\}$ is a solution of the recurrence relation. Because r_1 and r_2 are roots of $r^2 - c_1 r - c_2 = 0$, it follows that $r_1^2 = c_1 r_1 + c_2, r_2^2 = c_1 r_2 + c_2$. From these equations, we see that

$$\begin{aligned}
c_1 x_{n-1} + c_2 x_{n-2} &= c_1 \left(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}\right) + c_2 \left(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2}\right) \\
&= \alpha_1 r_1^{n-2} \left(c_1 r_1 + c_2\right) + \alpha_2 r_2^{n-2} \left(c_1 r_2 + c_2\right) \\
&= \alpha_1 r_1^{n-2} r_1^2 + \alpha_2 r_2^{n-2} r_2^2 \\
&= \alpha_1 r_1^n + \alpha_2 r_2^n \\
&= x_n
\end{aligned}$$

This shows that the sequence $\{x_n\}$ with $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ is a solution of the recurrence relation.

To show that every solution $\{x_n\}$ of the recurrence relation $x_n = c_1 x_{n-1} + c_2 x_{n-2}$ has $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \ldots$, for some constants α_1 and α_2, suppose that $\{x_n\}$ is a solution of the recurrence relation, and the initial conditions $x_0 = C_0$ and $x_1 = C_1$ hold. It will be shown that there are constants α_1 and α_2 such that the sequence $\{x_n\}$ with $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ satisfies these same initial conditions. This requires that

$$\begin{aligned}
x_0 &= C_0 = \alpha_1 + \alpha_2, \\
x_1 &= C_1 = \alpha_1 r_1 + \alpha_2 r_2.
\end{aligned}$$

We can solve these two equations for α_1 and α_2. From the first equation it follows that $\alpha_2 = C_0 - \alpha_1$. Inserting this expression into the second equation gives

$$C_1 = \alpha_1 r_1 + \left(C_0 - \alpha_1\right) r_2.$$

Hence,

$$C_1 = \alpha_1 \left(r_1 - r_2\right) + C_0 r_2.$$

This shows that

$$\alpha_1 = \frac{C_1 - C_0 r_2}{r_1 - r_2}$$

and

$$\alpha_2 = C_0 - \alpha_1 = C_0 - \frac{C_1 - C_0 r_2}{r_1 - r_2} = \frac{C_0 r_1 - C_1}{r_1 - r_2},$$

where these expressions for α_1 and α_2 depend on the fact that $r_1 \neq r_2$. (When $r_1 = r_2$, this theorem is not true.) Hence, with these values for α_1 and α_2, the sequence $\{x_n\}$ with $\alpha_1 r_1^n + \alpha_2 r_2^n$ satisfies the two initial conditions.

We know that $\{x_n\}$ and $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ are both solutions of the recurrence relation $x_n = c_1 x_{n-1} + c_2 x_{n-2}$ and both satisfy the initial conditions when $n = 0$ and $n = 1$. Because there is a unique solution of a linear homogeneous recurrence relation of degree two with two initial conditions, it follows that the two solutions are the same, that is, $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for all nonnegative integers n. We have completed the proof by showing that a solution of the linear homogeneous recurrence relation with constant coefficients of degree two must be of the form $x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, where α_1 and α_2 are constants.

Example: Find the solution to the recurrence relation

$$x_n = 6x_{n-1} - 11x_{n-2} + 6x_{n-3}$$

with the initial conditions $x_0 = 2,\ x_1 = 5$, and $x_2 = 15$.

Solution:

(1) The characteristic polynomial of this recurrence relation is $r^3 - 6r^2 + 11r - 6$.

(2) The characteristic roots are $r = 1,\ r = 2$, and $r = 3$.

(3) The solutions to this recurrence relation are of the form

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

(4) Using intial conditions, we have $\alpha_1 = 1, \alpha_2 = -1$, and $\alpha_3 = 2$.

(5) After putting values of α_i's in Step-3, we have $x_n = 1 - 2^n + 2.3^n$. This completes the task.

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

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

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

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k}$$

if and only if

$$\begin{aligned} x_n =& (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1}\ n^{m_1-1}) r_1^n \\ &+ (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{1,m_2-1}\ n^{m_2-1}) r_2^n + \\ &\cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1}\ n^{m_t-1}) r_t^n \end{aligned}$$

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

Example: Find the solution to the recurrence relation $x_n = -3x_{n-1} - 3x_{n-2} - x_{n-3}$with initial conditions $x_0 = 1, x_1 = -2$, and $x_2 = -1$.
Solution:

(1) The characteristic polynomial of this recurrence relation is $r^3 + 3r^2 + 3r + 1 = (r+1)^3 = 0$

(2) The characteristic roots are $r = -1, -1, -1$. Here multiplicity of -1 is three.

(3) The solutions to this recurrence relation are of the form

(4) Using intial conditions, we have $\alpha_{1,0} = 1$, $\alpha_{1,1} = 3$, and $\alpha_{1,2} = -2$.

(5) After putting values of the constants in Step-3, we have $x_n = (1 + 3n - 2n^2)(-1)^n$. This completes the required job.

Lecture-16

(Graph Theory)

1 Basic Terminologies

Definition 1.1 A graph G consists of two sets V and E, where V is non-empty set, called the vertex set, and E is called the edge set. A graph G is also denoted as $G = (V, E)$. We define some terminologies in a graph G as follows.

1. Let $u, v \in V$. An edge $e \in E$ joining them is denoted as $e = uv$. In this cases, u and v are called adjacent vertices, also called the end vertices, of the edge e. We also say that e is incident at u and v. Two edges $e_1, e_2 \in E$ are called adjacent if they have a common end vertex.

2. Let $v \in V$. The neighborhood of v, denoted as $N(v)$, is the set of all the adjacent vertices to v. Similarly, if $A \subseteq V$, then $N(A)$ is the set of all the vertices which are adjacent to at least one vertex of A, that is, $N(A) = \cup_{v \in A} N(v)$.

3. The degree of a vertex $v \in V$, denoted as $\deg(v)$, is the number of edges incident at v. A vertex v is called isolated vertex if $\deg(v) = 0$ and pendent vertex if $\deg(v) = 1$. The minimum degree of a vertex in G is denoted by $\delta(G)$ and the maximum degree of a vertex in G is denoted by $\Delta(G)$.

4. A set of vertices or edges is said to be independent if no two of them are adjacent. The maximum size of an independent vertex set is called the independence number of G, denoted $\alpha(G)$.

5. If the end vertices of an edge $e \in E$ are same then the edge is called loop. If e_1, e_2 are two edges such that they have same end points, then the edges are called parallel edges or multiple edges. A graph is called simple if it has no loops or multiple edges.

In these notes, unless stated otherwise, all our graphs are simple graphs with finite number of vertices (and hence finite number of edges).

Lemma 1.0.1 **[Handshake Lemma:]** Let $G = (V, E)$ be a graph. Then $\sum_{v \in V} \deg(v) = 2|E|$, where $|E|$ denote the number of edges in E.

Proof: The proof is based on induction on the cardinality of edge set, that is, $|E|$. Clearly, the result holds for $|E| = 1$.

Suppose the result holds for any graph G with $|E| = k$.

Let G be a graph with $|E| = k + 1$. Then consider a graph $G' = (V, E')$, where $E' = E \setminus uv$. Then the number of edges in G' is k and therefore the result holds for G', that is

$\sum_{v \in V} \deg(v) = 2|E'|$.

the sum of degree counts the total number of times an edge is incident on a vertex. An edge is incident on exactly 2 vertex .

Now, add the removed edge back to G'. Because this edge is indecent on two vertices, we add two to the previous sum, that is, $\sum_{v \in V} \deg(v) + 2 = 2|E'| + 2$. Thus $\sum_{v \in V} \deg(v) = 2|E|$.

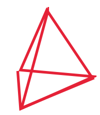
Corollary 1 *Let $G = (V, E)$. Then the number of odd degree vertices is even.*

Proposition 1 In a graph $G = (V, E)$ with $|V| = n \geq 2$, there are two vertices of equal degree.

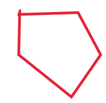
Proof: If G has two or more isolated vertices, then we are done. Suppose G has one isolated vertex. Then the remaining $n - 1$ vertices have degree between 1 to $(n - 2)$ and hence by PHP the result holds. Otherwise, G has no isolated vertices. Then there are n vertices whose degrees lies between 1 to $n - 1$. Again by PHP, the result holds.

2 Some Special Simple Graphs

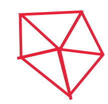
n(n-1)/2=e



1. **Complete graph:** A graph $G = (V, E)$ with $|V| = n$ is called a complete graph if each pair of vertices form an edge. We denote the G by K_n.



2. **Cycle:** A cycle C_n, $(n \geq 3)$, consists of n vertices $v_1, v_2, \ldots, v_n$ and the edges v_1v_2, $v_2v_3, \ldots, v_{n-1}v_n$, v_1.
e=n



3. **Wheel Graph:** A wheel graph W_n is obtained from cycle C_n, $(n \geq 3)$, when each v_i of C_n is adjacent to another vertex v.
an additional vertex v is added and each previous vertex is connected to v . |V|=n+1 and |E|=2n

4. **Bipartite Graph:** A graph $G = (V, E)$ is called bipartite graph if the vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that each edge $e \in E$ has one end vertex in V_1 and other in V_2. If $|V_1| = m$ and $|V_2| = n$, then we denote the graph G by $K_{m,n}$.

5. **Complete Bipartite Graph:** A bipartite graph $G = (V, E)$, with partition sets V_1 and V_2 of V, is called complete bipartite graph if each pair $\{u, v\}$, where $v \in V_1$ and $u \in V_2$ forms and edge.
e=mn

Theorem 2.1 A simple graph is bipartite if and only if it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.

Proof: First assume that $G = (V, E)$ is bipartite graph with bipartite subsets V_1 and V_2 of V. Then assign one color to each vertex of V_1 and a second color to each vertex of V_2 will give the desired condition.

Conversely, let it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color. Let V_1 be the set of vertices assigned one color and V_2 be the set of vertices assigned the other color. Then, V_1 and V_2 are disjoint and $V = V_1 \cup V_2$. $\square$

a single vertex of G is a subgraph of G
a single edge along with its end vertices in G is a subgraph of G

Lecture-(17-18)

every simple graph of n vertices is a subgraph of complete graph Kn

1 New Graphs from Old Graph

condition- each edge in G' must have the same end points as in G

1. **Subgraph:** A subgraph G' of a graph $G = (V, E)$ is a graph $G' = (V', E')$ such that $V' \subseteq V$ and $E' \subseteq E$.
2. **Spanning subgraph:** A subgraph $G' = (V', E')$ of $G = (V, E)$ is called spanning subgraph of G if $V = V'$.
3. **Induced subgraph:** A subgraph $G' = (V', E')$ of $G = (V, E)$ is called an induced subgraph of G if for every $u, v \in V'$, $e = uv \in E'$ whenever $e = uv \in E$.
4. If $v \in V$, then the graph $G - v$, called the **vertex deleted subgraph**, is obtained from G by deleting v and all the edges that are incident with v.
5. If $e \in E$, then the graph $G - e = (V, E \setminus \{e\})$ is called the **edge deleted subgraph**.
6. If $u, v \in V$, then $G + uv = (V, E \cup \{uv\})$ is called the graph obtained by edge addition.
7. The complement $\overline{G}$ of a graph G is defined as $(\overline{V}, \overline{E})$, where $\overline{V} = V$ and $\overline{E} = \{uv \,|\, u \neq v, uv \notin E\}$.

Definition 1.1 Let $G = (V(G), E(G))$ and $H = (V(H), E(H))$ be two graphs.

1. Then their intersection, denoted $G \cap H$, is defined as $(V(G) \cap V(H), E(G) \cap E(H))$.
2. Then their union, denoted $G \cup H$, is defined as $(V(G) \cup V(H), E(G) \cup E(H))$.

2 Representing Graph and Graph Isomorphism

Definition 2.1 Let $G = (V, E)$ be a graph with $V = \{v_1, v_2, \ldots, v_n\}$. Then the adjacency matrix with respect to the ordering $v_1, v_2, \ldots, v_n$ of V is the matrix $A_G = [a_{ij}]$, where

$$a_{ij} = \begin{cases} 1 & \text{if } v_i v_j \text{ is an edge of } G \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.2 Let $G = (V, E)$ be a graph. Suppose that $v_1, v_2, \ldots, v_n$ are the vertices and $e_1, e_2, \ldots, e_m$ are the edges of G. Then the incidence matrix with respect to this ordering of V and E is the $n \times m$ matrix $M = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.3 Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs. Then G_1 is said to be isomorphic to G_2, denoted as $G_1 \cong G_2$, if there is bijective map $f : V_1 \to V_2$ such that $\{f(u), f(v)\} \in E_2$ if and only if $\{u, v\} \in E_1$.

Definition 2.4 A graph G is called self-complementary if $G \cong \overline{G}$.

Definition 2.5 A graph invariant is a function which assigns the same value to isomorphic graphs. Observe that some of the graph invariants are: $|V|$, $|E|$, $\Delta(G)$ (maximum degree), $\delta(G)$ (minimum degree), $\omega(G)$ (clique number), $r(G)$ (radius), $e(G)$ (eccentricity).

Proposition 1 *Let G and H be graphs and let $f : G \to H$ be an isomorphism. For any $v \in V(G)$, $G - v \cong H - f(v)$.*

Proof: Consider the bijection $g : V(G - v) \to V(H - f(v))$ described by $g = f_V(G - v)$.

3 Connectedness

Definition 3.1 Let $G = (V, E)$ be a graph.

1. A u-v walk W is a finite sequence of vertices $(u = v_1, v_2, \ldots, v_n = v)$ such that $v_i v_{i+1} \in E$ for all $i = 1, 2, \ldots, n - 1$.
2. The length of a walk $W = (u = v_1, v_2, \ldots, v_n = v)$ is the number of edges in W, that is n. $n-1$
3. A walk $W = (v_1, v_2, \ldots, v_n)$ is called a trail if all the edges are distinct.
4. A walk $W = (u = v_1, v_2, \ldots, v_n = v)$ is called a path P if all the vertices, and hence the edges, are distinct. we call u and v as the end vertices of P and the remaining vertices on P as the internal vertices.

   path is also a trail
5. A walk $W = (u = v_1, v_2, \ldots, v_n = v)$ is called closed if $u = v$. vertex same
6. A cycle C is a closed path. trail $v_1 v_2 v_3 \ldots\ldots v_n v_1$

   special trail in which origin and terminating vertex are same but internal vertex are distinct
7. The graph G is called connected if for any vertices $u, v \in V$, there is a u-v path.

4 Some Graph Invariants

Let $G = (V, E)$ be a graph. Then we define some terms associated to G.

Definition 4.1 Let $u, v \in V$. The distance between u and v is denoted as $d(u, v)$ and is defined as the length of shortest path between u and v. If there is no such path then $d(u, v) = \infty$.

Definition 4.2 Let $u \in V$. The eccentricity of u, denoted as $e(u)$, is defined as $e(u) = \max\{d(u, v) \mid v \in V\}$. If G is disconnected then eccentricity of each vertex is ∞.

Definition 4.3 The radius of G, denoted as $r(G)$, is defined as $r(G) = \min\{e(v) \mid v \in V\}$. Since the eccentricity of every vertex in a disconnected graph is infinity, hence the radius of a disconnected graph will be infinity.

Definition 4.4 The diameter of G, denoted as $\text{diam}(G)$, is defined as $\text{diam}(G) = \max\{e(v) \mid v \in V\}$. The diameter of a disconnected graph is ∞.

Definition 4.5 A point $u \in V$ is called a center point of (G) if $e(u) = r(G)$. A collection of all the center points is called the center of G and is denoted as $C(G)$.

Definition 4.6 The number of edges in the longest cycle of G is called as the circumference of G.

Definition 4.7 The number of edges in the shortest cycle of G is called its girth and is denoted as $g(G)$. If G has no cycle then $g(G) = \infty$.

Definition 4.8 A complete subgraph of G is called a clique of G. The maximum order of a clique is called the clique number of G and is denoted as $\omega(G)$.

Definition 4.9 A graph which is not connected is called disconnected. If G is a disconnected graph, then a maximal connected subgraph of G is called a component or connected component of G.

Proposition 2 Let P and Q be two different u-v paths in G. Then, $P \cup Q$ contains a cycle.

condition for disconnected graph

Proposition 3 Every graph G containing a cycle satisfies $g(G) \leq 2\,\mathrm{diam}\,(G) + 1$.

Proposition 4 Let $G = (V, E)$ be a non-null graph. Then G is disconnected if and only if the vertex set V can be partitioned into two parts, say V_1, V_2, such that if $e = uv \in E$ then either both $u, v \in V_1$ or both $u, v \in V_2$.

Proof: Suppose V can be partitioned into two parts V_1 and V_2, satisfying the stated condition in the proposition. Since, V_1 and V_2 are non-empty, let $u \in V_1$ and $v \in V_2$. Let P be path joining u and v. There there is an edge $e = xy$ such that $x \in V_1$ and $y \in V_2$. This contradicts the assumption that either both $x, y \in V_1$ or $x, y \in V_2$. Hence no such P exists.

Conversely, let us assume that G is disconnected. Now fix a vertex $u \in V$ and consider $V_1 = \{x \in V \mid d(u, v) = \infty\}$. Since G is disconnected, V_1 is a proper subset of V and hence the set $V_2 = V \setminus V_1$ is non-empty subset of V. Clearly, V_1 and V_2 give a partition of V fulfilling the given condition. This completes the proof.

<u>Lecture-(19-21)</u>

1 Trees

Definition 1.1 A connected graph G is called a tree if it has no cycles. A collection of trees is called a forest.

We now prove that the following statements that characterize trees are equivalent.

Theorem 1.1 Let $G = (V, E)$ be a graph on n vertices and m edges. Then the following statements are equivalent for G.

1. G is a tree.
2. Let $u, v \in V$. Then there is a unique path from u to v.
3. G is connected and $n = m + 1$.

Proof: 1 implies 2: Since G is connected, for each $u, v \in V$, there is a path from u to v. On the contrary, let us assume that there are two distinct paths P_1 and P_2 that join the vertices u and v. Since P_1 and P_2 are distinct and both start at u and end at v, there exist vertices, say u_0 and v_0, such that the paths P_1 and P_2 take different edges after the vertex u_0 and the two paths meet again at the vertex v_0 (note that u_0 can be u and v_0 can be v). In this case, we see that the graph G has a cycle consisting of the portion of the path P_1 from u_0 to v_0 and the portion of the path P_2 from v_0 to u_0. This contradicts the assumption that G is a tree (it has no cycle).

2 implies 3: Since for each $u, v \in V$, there is a path from u to v, the connectedness of G follows. We need to prove that $n = m + 1$. We prove this by induction on the number of vertices of a graph. The result is clearly true for $n = 1$ or $n = 2$. Let the result be true for all graphs that have n or less than n vertices. Now, consider a graph G on $n + 1$ vertices that satisfies the conditions of Item 2. The uniqueness of the path implies that if we remove an edge, say $e \in E$, then the graph G will become disconnected. That is, $G \setminus e$ will have exactly two components. Let the number of vertices in the two components be n_1 and n_2. Then $n_1, n_2 \leq n$ and $n_1 + n_2 = n + 1$. Hence, by induction hypothesis, the number of edges in $G - e$ equals $(n_1 - 1) + (n_2 - 1) = n_1 + n_2 - 2 = n - 1$ and hence the number of edges in G equals $n - 1 + 1 = n$. Thus, by the principle of mathematical induction, the result holds for all graphs that have a unique path from each pair of vertices.

3 implies 1: It is already given that G is a connected graph. We need to show that G has no cycle. So, on the contrary, let us assume that G has a cycle of length k. Then this cycle has k vertices and k edges. Now, consider the $n - k$ vertices that do not lie of the cycle. Then for each vertex (corresponding to the $n - k$ vertices), there will be a distinct edge incident with it on the smallest path from the vertex to the cycle. Hence, the number of edges will be greater than or equal to $k + (n - k) = n$. A contradiction to the assumption that the number of edges equals $n - 1$. Thus, the required result follows.

As a next result in this direction, we prove that a tree has at least two pendant (end) vertices.

Theorem 1.2 Let G be a non-trivial tree. Then G has at least two vertices of degree 1.

Proof: Let $G = (V, E)$ with $|V| = n \geq 2$. Then, by above theorem, $|E| = n - 1$. Also, by handshake lemma, we know that $2|E| = \sum_{v \in V} \deg(v)$. Thus, $2(n-1) = \sum_{i=1}^{n} \deg(v_i)$. Now, G is connected implies that $\deg(v) \geq 1$, for all $v \in V$ and hence the above equality implies that there are at least two vertices for which $\deg(v) = 1$. This ends the proof of the result.

2 Eulerian Graphs

Definition 2.1 Let G be a graph. A closed trail $(v_0, v_1, \ldots, v_k, v_0)$ is called Eulerian trail if it contains all the edges of the graph. A graph G is said to be Eulerian if it has an Eulerian trail.

Theorem 2.1 Let G be a connected graph. Then the following statements are equivalent.

1. G is Eulerian.
2. Every vertex of G has even degree.
3. The set of edges can be partitioned into cycles.

Proof: $1 \Rightarrow 2$: Let G be Eulerian graph. Then G has an Eulerian trail T. Note that for each vertex v the trail enters through an edge and departs v from another edge. Thus at each stage, the process of coming in and going out contribute 2 to the degree of v. Since each edge appears exactly once, the degree of v is even.

$2 \Rightarrow 3$: Since G is connected and the degree of each vertex even, the graph is not a tree. So there is at least one cycle C_1 in G. If C_1 is not G. Let G_1 be the subgraph (possibly disconnected) of G after deleting the edges in C_1. Since each vertex in a cycle has degree 2, the degree of each vertex in G_1 has even and as before has a cycle C_2. Let $G_2 = G_1 - C_2$. We repeat the process of identifying the cycles until we get the graph $G_k = G - C_1 - C_2 - \cdots - C_k$ with no edges. Thus the set of edges of these cycles gives the required partition.

$3 \Rightarrow 1$: Suppose the set of edges in a connected graph G is the disjoint union of k cycles. Consider any one of these cycles, say cycle C_1. Since the graph is connected, there is a cycle, say C_2, such that the two cycles have a vertex v_1 in common. Let Q_{12} be the circuit that consists of all the edges in these two cycles. As before, there is a cycle C_3 such that this cycle and the circuit Q_{12} have no edge common but do have vertex v_2 in common. Let Q_{123} be the circuit that contains all the edges of these three edge-disjoint cycles. We repeat this process until we get a circuit that contains all the edges of the graph. Thus graph is Eulerian.

Theorem 2.2 Let G be a connected graph with exactly two vertices of odd degree. Then, there is an Eulerian walk starting at one of those vertices and ending at the other.

Proof: Let x and y be the two vertices of odd degree and let v be a symbol such that $v \notin V(G)$. Then, the graph H with $V(H) = V(G) \cup \{v\}$ and $E(H) = E(G) \cup \{xv, yv\}$ has each vertex of even degree and hence by Theorem 9.5.2, H is Eulerian. Let $\Gamma = (v, v_1 = x, \ldots, v_k = y, v)$ be an Eulerian tour. Then, $\Gamma - v$ is an Eulerian walk with the required properties.

3 Hamiltonian Graph

Definition 3.1 Let G be a graph. A cycle in G is said to be Hamiltonian if it contains all vertices of G. If G has a Hamiltonian cycle, then G is called a Hamiltonian graph.

Theorem 3.1 (A necessary condition for a graph to be Hamiltonian). If $G = (V, E)$ is Hamiltonian and if W is any nonempty subset of V, the graph $G - W$ has at most $|W|$ components.

The converse of the above theorem does not hold always. Consider the complete bipartite graph $K_{2,n}$ for $n \geq 2$.

Theorem 3.2 (Ore's Theorem: A sufficient condition for a graph to be Hamiltonian). A simple graph with n vertices (where $n > 2$) is Hamiltonian if the sum of the degrees of every pair of non-adjacent vertices is at least n.

Theorem 3.3 (Dirac's Theorem: A sufficient condition for a graph to be Hamiltonian). A simple graph with n vertices (where $n > 2$) is Hamiltonian if the degree of every vertex is at least $n/2$.

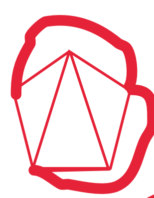
Proof: If each degree is at least $n/2$, the sum of every pair of vertices is at least n. Then the proof follows by Ore's theorem.

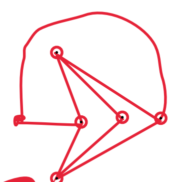
4 Planar Graph

A graph is said to be embedded on a surface S when it is drawn on S so that no two edges intersect, except at end points. A graph is said to be planar if it can be embedded on the plane.

Examples:

1. A tree is embeddable on a plane.
2. Any cycle C_n, $n \geq 3$ is planar.
3. The K_4 is planar.
4. The $K_{2,3}$ is planar.
5. Draw a planar embedding of $K_5 - e$, where e is any edge.
6. Draw a planar embedding of $K_{3,3} - e$, where e is any edge.





Definition 4.1 Consider a planar embedding of a graph G. The regions on the plane defined by this embedding are called faces/regions of G. The unbounded face/region is called the exterior face.

Theorem 4.1 Let G be a connected planar graph with v number of vertices, e number of edges and f number of faces. Then $v - e + f = 2$.

Proof: We use induction on f. Let $f = 1$. Then G cannot have a subgraph isomorphic to a cycle. For, if G has a subgraph isomorphic to a cycle, then in any planar embedding of G, $f \geq 2$. Therefore, G is a tree, and hence $v - e + f = v - (v - 1) + 1 = 2$. Assume that the equation is true for all plane connected graphs having $2 \leq f < n$. Let G be a connected planar graph with $f = n$. Choose an edge that is not a cut-edge, say e. Then, $G - e$ is still a connected graph. Notice that the edge e is incident with two separate faces. So, its removal will combine the two faces, and hence $G - e$ has only $n - 1$ faces. Thus, using the induction hypothesis $v - e + f = 2$. Hence the required result follows.

Corollary 1 If G is a connected planar simple graph with e edges and v vertices, where $v \geq 3$, then $e \leq 3v - 6$.

Proof: Each face has at least 3 edges and each edge is participated in two faces. So, the number of edges $e \geq 3f/2$. Now the proof follows by $v - e + f = 2$.

Exercise: Show that K_5 is non planar.

Corollary 2 If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuit of length three, then $e \leq 2v - 4$. e>=4f/2

Proof: Note that $e \geq 2f$. Then the proof follows by $v - e + f = 2$.

Exercise: $K_{3,3}$ is non planar.

Definition 4.2 If a graph is planar, so will be any graph obtained by removing an edge uv and adding a new vertex w together with edges uw and wv. Such an operation is called an elementary subdivision. The graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are called homeomorphic if they can be obtained from the same graph by a sequence of elementary subdivisions.

Theorem 4.2 (Kuratowski's Theorem) A graph is non planar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5.

Lecture-22-24

Definition: A group is a pair $(G, *)$, where G is a set, $*$ is a binary operation and the following axioms hold:

1. (The associative law)

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in G.$$

2. (Existence of an identity) There exists an element $e \in G$ with the property that $e * a = a$ and $a * e = a$ for all $a \in G$.

3. (The existence of an inverse) For each $a \in G$ there exists an element $b \in G$ such that

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

Remark: Notice that $* : G \times G \to G$ is a binary operation and thus the 'closure axiom': $a, b \in G \implies a * b \in G$ is implicit in the definition.
Definition: We say that a group $(G, *)$ is abelian or commutative if $a * b = b * a$ for all $a, b \in G$.
Proposition:

- (**Uniqueness of the Identity:**) The identity e is the unique element in G : To see this suppose we have another identity f. Using the fact that both of these are identities we see that

$$f = f * e = e.$$

  We will usually denote this element by 1 (or by 0 if the group operation is commutative).

- (**Uniqueness of Inverses:**)The inverse $b \in G$ of $a \in G$ is unique. To see this suppose that c is another inverse to a. Then

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

  We call this unique element b, the inverse of a. It is often denoted a^{-1} (or $-a$ when the group operation is commutative). For simplicity, we write ab for $a * b$.

- (**Cancellation:**) In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.
  Proof: Suppose $ba = ca$. Let a^{-1} be an inverse of a. Then, multiplying on the right by a^{-1} yields $(ba)a^{-1} = (ca)a^{-1}$. Associativity yields $b(aa^{-1}) = c(aa^{-1})$. Then, $be = ce$ and, therefore, $b = c$ as desired. Similarly, one can prove that $ab = ac$ implies $b = c$ by multiplying by a^{-1} on the left.

- (**Socks-Shoes Property:**) For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.
  Proof: Since $(ab)(ab)^{-1} = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, we have by uniqueness of inverses that $(ab)^{-1} = b^{-1}a^{-1}$.

Examples:

- The group of integers $(\mathbb{Z}, +)$ and $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with respect to addition are abelian groups.
- The set $\mathbb{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

if n-j is inverse of j then (j+(n-j))%n=e==0 but 0 is not the identity element for a=n

- The set $\mathbb{Z}_n = \{0, 1, \ldots, n\}$ for $n \geq 1$ is a group under addition modulo n. For any $j \in \mathbb{Z}_n$, the inverse of j is $n - j$. This group is usually referred to as the group of integers modulo n.

(a+b)%n=a...b=e
if b=0, n%n=0!=n,...e???

- The set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime.

e=1 , inverse of a will be 1/a

- The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, whereas the inverse of i is $-i$, and vice versa.
- Let X be a set and let $Sym(X)$ be the set of all bijective maps from X to itself. Then $Sym(X)$ is a group with respect to composition, $\circ$, of maps. This group is called the symmetric group on X and we often refer to the elements of $Sym(X)$ as permutations of X. When $X = \{1, 2, 3, \ldots, n\}$ the group is often denoted S_n and called the symmetric group on n letters.

det=1 thats why inverse exist

- The set of all $n \times n$ matrices with determinant 1 with entries from $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers), or $\mathbb{Z}_p$ (p a prime) is a non-Abelian group under matrix multiplication. This group is called the special linear group of $n \times n$ matrices over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_p$, respectively.

commutative property doesn't holds here

e=Identity matrix and inverse of A is A^-1

- The set of all 2×2 matrices with real number entries is not a group under the matrix multiplication operation. Inverses do not exist when the determinant is 0.
- The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not.
- The set of integers under subtraction is not a group, since the operation is not associative.

Subgroup: Let G be a group with a subset H. We say that H is a subgroup of G if the following two conditions hold:

- $e \in H$,
- If $a, b \in H$ then $ab, a^{-1} \in H$.

Note: One can replace the above conditions with the more economical:

- $H \neq \emptyset$,
- If $a, b \in H$ then $\boxed{a^{-1}b \in H}$.

Remark: It is not difficult to see that one could equivalently say that H is a subgroup of G if H is closed under the group multiplication $*$ and that H with the induced multiplication of $*$ on H is a group in its own right.

Order of a Group: The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of G.
Example: The group $\mathbb{Z}$ of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

Order of an Element: The order of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.
Example:

- Consider $\mathbb{Z}_{10}$ under addition modulo 10. Since $2+2 = 4, 2+2+2 = 6, 2+2+2+2 = 8, 2+2+2+2+2 = 0$, we know that $|2| = 5$. Similar computations show that $|0| = 1, |7| = 10, |5| = 2, |6| = 5$.

Cyclic Group: A group G is called cyclic if there is an element a in G such that $G = \{a^n : n \in \mathbb{Z}\}$. Such an element a is called a generator of G.

Coset of H in G: Let G be a group and let H be a subset of G. For any $a \in G$, the set $\{ah : h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha : h \in H\}$ and $aHa^{-1} = \{aha^{-1} : h \in H\}$. When H is a subgroup of G, the set aH is called the left coset of H in G containing a, whereas Ha is called the right coset of H in G containing a. In this case, the element a is called the coset representative of aH (or Ha). We use $|aH|$ to denote the number of elements in the set aH, and $|Ha|$ to denote the number of elements in Ha.

Properties of Cosets: Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$, e belongs to H -> a*e belongs to aH
2. $aH = H$ if and only if $a \in H$,
3. $aH = bH$ if and only if $a \in bH$
4. $aH = bH$ or $aH \cap bH = \emptyset$,
5. $aH = bH$ if and only if $a^{-1}b \in H$,
6. $|aH| = |bH|$, $= |H|$
7. $aH = Ha$ if and only if $H = aHa^{-1}$,
8. aH is a subgroup of G if and only if $a \in H$.

Suppose G is a group with a subgroup H. We define a relation on G as follows:

$$x\mathcal{R}y \text{ iff } x^{-1}y \in H.$$

y E xH
x E yH
-> if xRy this means xH=yH
->reflexive- aRa iff a^-1*a E H .....when e E H (always as H is a subgroup)
->symmetric - xRy-> xH=yH, yH=xH means y^-1x E H therefore yRx
->transmitive- xRy-> xH=yH, yRz->yH=zH......therefore xH=zH which means x^-1z E H....therefore xRz

x^-1y E H..... y E xH.....xRy so y is the equivalence class of x

This relation is an equivalence relation. Notice that $x\mathcal{R}y$ if and only if $x^{-1}y \in H$ if and only if $y \in xH$. Hence the equivalence class of x is $\boxed{[x] = xH,}$ the left coset of H in G.

for aES , [a] = {x : (a, x) E R}

[x] = {y, xRy}

Lagrange's Theorem: Let G be a finite group with a subgroup H. Then $|H|$ divides $|G|$.
Proof: Using the equivalence relation above, G gets partitioned into pairwise disjoint equivalence classes, say

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

and adding up we get

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r|H|.$$

Notice that the map from G to itself that takes g to a_ig is a bijection (the inverse is the map $g \to a_i^{-1}g$) and thus $|a_iH| = |H|$.

Definition: (**Normal Subgroup**) A subgroup H of G is said to be a normal subgroup if

$$g^{-1}Hg \subseteq H \;\forall g \in G.$$

Definition: Let G be a group with a subgroup H. The number of left cosets of H in G is called the index of H in G and is denoted $[G : H]$.
Examples: abelian->commutative law holds->Hg=gH->
g^-1Hg = g^-1gH = H

- Every subgroup N of an abelian group G is normal.
- The trivial subgroup $\{e\}$ and G itself are always normal subgroups of G. if H=e then g^-1Hg = g^-1eg = g^-1g = e
- If H is a subgroup of G such that $[G : H] = 2$ then H is normal subgroup of G.

Definition: Let $(G, *)$, $(H, \circ)$ be groups. A map $\Phi : G \to H$ is a homomorphism if

$$\Phi(a * b) = \Phi(a) \circ \Phi(b)$$

for all $a, b \in G$. Furthermore Φ is an isomorphism if it is bijective.
Example: Let $\mathbb{R}^+$ be the set of all the postive real numbers. There is a (well-known) isomorphism $\Phi : (\mathbb{R}, +) \to (\mathbb{R}^+, .)$ given by $\Phi(x) = e^x$.

Lecture-25

Definition: A ring R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in R :

1. $a+b=b+a$.
2. $(a+b)+c=a+(b+c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0=a$ for all a in R.
4. There is an element $-a$ in R such that $a+(-a)=0$.
5. Associative Property: $a(bc)=(ab)c$.
6. Distributive Property: $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

The above can be summarize as follows: a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.
Definition: We say that a ring $(R,+,.)$ is commutative if $a.b=b.a$ for all $a,b\in R$.
Definition: A unity (or multiplicative identity) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse.

Theorem: (Rules of Multiplication)- Let a, b, and c belong to a ring R. Then

- $a0=0a=0$.
- $a(-b)=(-a)b=-(ab)$.
- $(-a)(-b)=ab$.
- $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$.
  Furthermore, if R has a unity element 1, then
- $(-1)a=-a$.
- $(-1)(-1)=1$.

Examples:

- The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with respect to usual addition and usual multiplication are rings.
- The set $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$ for $n\geq 1$ under addition and multiplication modulo n is a commutative ring with unity 1.
- The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x)=1$.

- The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.
- The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a noncommutative ring with unity.

Subring: A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

Theorem: (**Subring Test**) A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication that is, if $a - b$ and ab are in S whenever a and b are in S.

Examples:

- $\{0\}$ and R are subrings of any ring R. $\{0\}$ is called the trivial subring of R.
- For each positive integer n, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is a subring of the integers $\mathbb{Z}$.
- The set of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$.

Definition: A field F, containing at least two elements, is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in F :

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all a in R.
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. (Associativity of multiplication) $a(bc) = (ab)c$.
6. (Distributivity of multiplication) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.
7. (Commutativity of multiplication) $ab = ba$.
8. (Existence of a multiplicative identity) There is an element $1 \in F$, such that $1 \neq 0$ and $a.1 = a$.
9. (Existence of a multiplicative inverses) If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $xx^{-1} = 1$.

Examples:

- The sets $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with respect to usual addition and usual multiplication are fields.
- The set $\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$ for $p \geq 2$ under addition and multiplication modulo p is a field, where p is a prime number.
- The set $\mathbb{Z}$ of integers is not a field.