Math Help Centre

MATH1240 Definitions and Theorems

1 Fundamental Principles of Counting

- For an integer $n \geq 0$, n *factorial* (denoted $n!$) is defined by

$$0! = 1,$$
$$n! = (n)(n-1)(n-2)\cdots(3)(2)(1), \quad \text{for} \quad n \geq 1.$$

- Given a collection of n distinct objects, any linear arrangement of these objects is called a *permutation* of the collection.

- If there are n distinct objects and r is an integer with $1 \leq r \leq n$, then by the rule of product, the *number of permutations of size* r for the n objects is

$$P(n,r) = \frac{n!}{(n-r)!}$$

- (*Permutations of objects with indistinguishable object types*): If there are n objects with n_1 indistinguishable objects of a first type, n_2 indistinguishable objects of a second type, ... and n_r indistinguishable objects of an r^{th} type, where $n_1 + n_2 + \cdots n_r = n$, then there are

$$\frac{n!}{n_1!n_2!\cdots n_r!}$$

linear arrangements of the given n objects.

- If we start with n distinct objects, each selection or *combination* of r of these objects (denoted $\binom{n}{r}$ or $C(n,r)$ and read as "n choose r"), with no reference to order, corresponds to $r!$ permutations of size r from the n objects.

- The *number of combinations* of size r from a collection of size n is

$$C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}, \qquad 0 \leq r \leq n.$$

- A *string* is a particular arrangement of of symbols from a prescribed alphabet of symbols.

- The *number of strings* of length n from a given alphabet of k symbols is k^n.

- If $x = x_1x_2\cdots x_k$ is a string, the *weight* of x is $x_1 + x_2 + \cdots + x_k$.

- (*The Binomial Theorem*): If x and y are variables and n is a positive integer, then

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \cdots + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0$$

  In view of this theorem $\binom{n}{k}$ is sometimes referred to as the binomial coefficient.

- For positive integers n and t, the coefficient of $x_1^{n_1}x_2^{n_2}x_3^{n_3}\cdots x_t^{n_t}$ in the expansion of $(x_1 + x_2 + x_3 + \cdots + x_t)^n$ is called the *multinomial coefficient* and is

$$\frac{n!}{n_1!n_2!n_3!\cdots n_t!}$$

- When we wish to select *with repetition, r of n distinct objects*, the number of possible selections is

$$\frac{(n+r-1)!}{r!(n-r)!} = \binom{n+r-1}{r}$$

- The following are equivalent:
  - The number of integer solutions to the equation

$$x_1 + x_2 + \cdots + x_n = r, \qquad x_i \geq 0, \quad 1 \leq i \leq n.$$

  - The number of selections, with repetition, of size r from a collection of size n.
  - The number of ways r identical objects can be distributed among n distinct containers.

2 Fundamentals of Logic

- A verbal assertion is called a statement or proposition that is either true or false, but *not* both. A primitive statement is a statement that can not be broken down into anything simpler.
- If p and q are statements, here are some ways to get new statements from p and q.
- A compound statement is a statement formed by the combination of two or more statements.
  - $\neg p$: The negation of p, read as "Not p".
  - $p \wedge q$: The conjunction of p and q, read as "p and q".
  - $p \vee q$: The disjunction of p and q, read as "p or q". The symbol $\vee$ is used in the inclusive sense. $p \vee q$ is true if p is true, or q is true or both p and q are true. The symbol $\veebar$ is used in the exclusive sense — i.e., $p \veebar q$ is true if p is true, or q is true, but not if both p and q are true.
  - $p \rightarrow q$: The implication of q by p, read as "p implies q".
  - $p \leftrightarrow q$: The biconditional of p and q, read as "p if and only if q" (note: "if and only if" is sometimes abbreviated to "iff"), or "p is necessary and sufficient for q".

  The above symbols, $\neg$, $\wedge$, $\vee$, $\veebar$, $\rightarrow$ and $\leftrightarrow$ are called logical connectives.
- A compound statement is called a tautology if it is true for all truth value assignments for its component statements. If a compound statement is false for all such assignments, then it is called a contradiction. T_0 is used to denote any tautology, and F_0 is used to denote any contradiction.
- Two statements s_1 and s_2 are said to be logically equivalent (and we write $s_1 \iff s_2$) when the statement s_1 is true (respectively, false) if and only if the statement s_2 is true (respectively, false).
- The Laws of Logic:
  For any primitive statements p, q and r, and tautology T_0 and any contradiction F_0,

1	$\neg\neg p \iff p$	Law of Double Negation
2	$\neg(p \vee q) \iff \neg p \wedge \neg q$ $\neg(p \wedge q) \iff \neg p \vee \neg q$	DeMorgan's laws
3	$p \vee q \iff q \vee p$ $p \wedge q \iff q \wedge p$	Commutative laws
4	$p \vee (q \vee r) \iff (p \vee q) \vee r$ $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$	Associative laws
5	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$	Distributive laws
6	$p \vee p \iff p$ $p \wedge p \iff p$	Idempotent laws
7	$p \vee F_0 \iff p$ $p \wedge T_0 \iff p$	Identity laws
8	$p \vee \neg p \iff T_0$ $p \wedge \neg p \iff F_0$	Inverse laws
9	$p \vee T_0 \iff T_0$ $p \wedge F_0 \iff F_0$	Domination laws
10	$p \vee (p \wedge q) \iff p$ $p \wedge (p \vee q) \iff p$	Absorption laws

- Let s be a statement. If s contains no logical connectives other than $\wedge$ and $\vee$, then the dual of s, denoted s^d, is the statement obtained from s by replacing each occurrence of $\wedge$ and $\vee$ by $\vee$ and $\wedge$ respectively, and each occurrence of T_0 by F_0 and F_0 by T_0, respectively.

- The Principle of Duality: Let s and t be statements that contain no logical connectives other than $\wedge$ and $\vee$. If $s \iff t$, then $s^d \iff t^d$.

- Substitution rules:

  1. Suppose that the compound statement P is a tautology. If p is a primitive statement that appears in P and we replace *each* occurrence of p by the *same* statement q, then the resulting compound statement P_1 is also a tautology.
  2. Let P be a compound statement where p is an arbitrary statement that appears in P, and let q be a statement such that $q \iff p$. Suppose that in P we replace one or more occurrences of p by q. Then this replacement yields the compound statement P_1. Under these circumstances, $P_1 \iff P$.

- Given statements p and q, implication, contrapositive, converse and inverse are as follows:
  - The implication: $p \to q$.
  - The contrapositive: $\neg q \to \neg p$.
  - The converse: $q \to p$.
  - The inverse: $\neg p \to \neg q$
- Consider the implication $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$. The statements $p_1, \ldots p_n$ are called the premises, and q is the conclusion. The preceding argument is called valid if whenever each of the premises is true, then the conclusion is true. One way to establish the validity of an argument is to show that $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology.
- If p, q are arbitrary statements such that $p \to q$ is a tautology, then we say that p logically implies q and we write $p \implies q$ to denote this situation. Likewise, is $p \leftrightarrow q$ is a tautology, we write $p \iff q$. $p \not\Longrightarrow q$ is used to indicate that $p \to q$ is not a tautology, and $p \to q$ is not a logical implication.
- Rules of Inference:
  For statements p, q, r and s, and any tautology T_0 and any contradiction F_0, see the table on the next page.

	Rule of Inference	Related Logical Implication	Name of Rule
1	p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	Rule of Detachment
2	$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Law of Syllogism
3	$p \to q$ $\neg q$ $\therefore \neg p$	$[(p \to q) \wedge \neg q] \to \neg p$	Modus Tollens
4	p q $\therefore p \wedge q$		Rule of Conjunction
5	$p \wedge q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \to q$	Rule of Disjunctive Syllogism
6	$\neg p \to F_0$ $\therefore q$	$(\neg p \to F_0) \to p$	Rule of Contradiction
7	$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Rule of Conjunctive Simplification
8	p $\therefore p \vee q$	$p \to (p \vee q)$	Rule of Disjunctive Amplification
9	$p \wedge q$ $p \to (q \to r)$ $\therefore r$	$[(p \wedge q) \wedge [p \to (q \to r)]] \to r$	Rule of Conditional Proof
10	$p \to r$ $q \to r$ $\therefore (p \vee q) \to r$	$[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$	Rule of Proof by Cases
11	$p \to q$ $r \to s$ $p \wedge r$ $\therefore (q \vee s)$	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Rule of the Constructive Dilemma
12	$p \to q$ $r \to s$ $\neg q \vee \neg s$ $\therefore \neg p \vee \neg r$	$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to (\neg p \vee \neg r)$	Rule of the Destructive Dilemma

- A declarative sentence is an open statement if

  1. it contains one or more variables, and
  2. it is not a statement, but
  3. it becomes a statement when the variables in it are replaced by certain allowable choices.

  If the variable in the statement is x, the statement is denoted $p(x)$. If there are multiple variables in the statement, say, x and y, the statement can be denoted $P(x, y)$. The allowable choices for x constitute the universe for the open statement.

- An open statement can have two types of quantifiers which describe the allowable choices for the variable(s) in the statement:

  1. Existential quantifiers: "For some x" is an example of an existential quantifier. It can also be written as "For at least one x", or "There exists an x such that". In symbolic form, it is written as $\exists x$.
  2. Universal quantifiers: "For all x", "For any x", "For each x" etc. Symbolically written as $\forall x$.

- The variable x in an open statement is called a free variable and the truth of the statement varies over the allowable choices of x. When a quantifier is used the statement has a fixed truth value (true) and the variable is bound by the quantifier.

- Let $p(x)$ and $q(x)$ be open statements defined for a given universe. The open statements $p(x)$ and $q(x)$ are called (logically) equivalent and we write $\forall x[p(x) \iff q(x)]$ when the biconditional $p(a) \leftrightarrow q(a)$ is true for each replacement a from the universe. If the implication $p(a) \rightarrow q(a)$ is true for each a in the universe, then we write $\forall x[p(x) \implies q(x)]$ and say that $p(x)$ logically implies $q(x)$.

- For open statements $p(x)$ and $q(x)$ and the universally quantified statement $\forall x[p(x) \rightarrow q(x)]$, we define

  1. The contrapositive of $\forall x[p(x) \rightarrow q(x)]$ to be $\forall x[\neg q(x) \rightarrow \neg p(x)]$.
  2. The converse of $\forall x[p(x) \rightarrow q(x)]$ to be $\forall x[q(x) \rightarrow p(x)]$.
  3. The inverse of $\forall x[p(x) \rightarrow q(x)]$ to be $\forall x[\neg p(x) \rightarrow \neg q(x)]$.

- Let n be an integer. We call n even if n is divisible by 2 — i.e., if there exists an integer r so that $n = 2r$. If n is not even, then we call n odd and find for this case that there exists an integer s where $n = 2s + 1$.

- (Theorem:) For all integers k and l, if k and l are both odd, then $k + l$ is even.

- (Theorem:) For all integers k and l, if k and l are both odd, their product kl is also odd.

3 Set Theory

- A set is a collection of well-defined objects. The objects are called elements and are said to be members of the set. The adjective well-defined implies that for any element we care to consider, we are able to determine whether it is in the set under scrutiny.
- A universe $\mathscr{U}$ is a set from which elements of a given set are considered. For example, if you are considering the set of integers between 1 and 5 (inclusive), the set consists of $\{1, 2, 3, 4, 5\}$, and the universe is the set of integers $\mathbb{Z}$.
- A set is finite if it has a finite number of elements, and infinite if it has infinitely many elements.
- The cardinality of a set A, denoted $|A|$, is the number of elements in the set.
- If C and D are sets from a universe $\mathscr{U}$, we say that C is a subset of D and write $C \subseteq D$ or $D \supseteq C$ if every element of C is an element of D. If, in addition, D contains an element that is not in C, then C is called a proper subset of D, and this is denoted $C \subset D$ or $D \supset C$.
- For a given universe $\mathscr{U}$, the sets C and D (taken from $\mathscr{U}$) are said to be equal, and we write $C = D$, when $C \subseteq D$ and $D \subseteq C$.
- (Theorem:) Let A, B, $C \subseteq \mathscr{U}$.
  1. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
  2. If $A \subset B$ and $B \subseteq C$, then $A \subset C$.
  3. If $A \subseteq B$ and $B \subset C$, then $A \subset C$.
  4. If $A \subset B$ and $B \subset C$, then $A \subset C$.
- The null set, or empty set, is the (unique) set containing no elements. It is denoted by $\emptyset$ or $\{\,\}$.
- (Theorem:) For any universe $\mathscr{U}$, let $A \subset \mathscr{U}$. Then $\emptyset \subseteq A$, and if $A \neq \emptyset$, then $\emptyset \subset A$.
- If A is a set from universe $\mathscr{U}$, the power set of A, denoted $\mathscr{P}(A)$ is the collection (or set) of all subsets of A.
- For any finite set A, with $|A| = n \geq 0$, we find that A has 2^n subsets and that $|\mathscr{P}(A)| = 2^n$.
- A set is closed under an operation (e.g., addition, multiplication, etc.) if the operation produces a member of the same set.
- An operation is binary if there are two operands.
- For $A, B \subseteq \mathscr{U}$, we define the following:
  1. $A \cup B$ (the union of A and B) $= \{x | x \in A \vee x \in B\}$
  2. $A \cap B$ (the intersection of A and B) $= \{x | x \in A \wedge x \in B\}$
  3. $A \triangle B$ (the symmetric difference of A and B) $= \{x | (x \in A \vee x \in B) \wedge x \notin A \cap B\} = \{x | x \in A \cup B \wedge x \notin A \cap B\}$
- Let $S, T \subseteq \mathscr{U}$. The sets S and T are called disjoint, or mutually disjoint when $S \cap T = \emptyset$.

- (Theorem:) If $S, T \subseteq \mathscr{U}$, then S and T are disjoint if and only if $S \cup T = S \triangle T$.
- For a set $A \subseteq \mathscr{U}$, the complement of A denoted $\mathscr{U} - A$, or $\overline{A}$, is given by $\{x | x \in \mathscr{U} \wedge x \notin A\}$.
- For $A, B \subseteq \mathscr{U}$, the (relative) complement of A in B denoted $B - A$, is given by $\{x | x \in B \wedge x \notin A\}$.
- (Theorem:) For any universe $\mathscr{U}$, and any sets $A, B \subseteq \mathscr{U}$, the following statements are equivalent.
  1. $A \subseteq B$.
  2. $A \cap B = A$.
  3. $A \cup B = B$.
  4. $\overline{B} \subseteq \overline{A}$.
- The Laws of Set Theory
  For any sets A, B and C, taken from universe $\mathscr{U}$

1	$\overline{\overline{A}} = A$	Law of Double Complement
2	$\overline{A \cup B} = \overline{A} \cup \overline{B}$ $\overline{A \cap B} = \overline{A} \cap \overline{B}$	DeMorgan's laws
3	$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
4	$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
5	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
6	$A \cup A = A$ $A \cap A = A$	Idempotent laws
7	$A \cup \emptyset = A$ $A \cap \mathscr{U} = A$	Identity laws
8	$A \cup \overline{A} = \mathscr{U}$ $A \cap \overline{A} = \emptyset$	Inverse laws
9	$A \cup \mathscr{U} = \mathscr{U}$ $A \cap \emptyset = \emptyset$	Domination laws
10	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws

- Let s be a (general) statement dealing with the equality of two set expressions. Each such expression may involve one or more occurrences of sets (such as A, $\overline{A}$, B, $\overline{B}$, etc.), one or

more occurrences of $\emptyset$ and $\mathscr{U}$, and only the set operation symbols $\cap$ and $\cup$. The dual of s, denotes s^d, is obtained from s by replacing

1. each occurrence of $\emptyset$ and $\mathscr{U}$ (in s) by $\mathscr{U}$ and $\emptyset$, respectively, and
2. each occurrence of $\cap$ and $\cup$ (in s) by $\cup$ and $\cap$, respectively.

- The Principle of Duality. Let s denote a theorem dealing with the equality of two set expressions (involving only the set operations $\cap$ and $\cup$). Then s^d, the dual of s, is also a theorem.
- When one performs an experiment such as tossing a single fair coin or rolling a single fair die, a set of all possible outcomes for each situation is called a sample space.
- Under the assumption of equal likelihood, let $\mathscr{S}$ by the sample space for an experiment $\mathscr{E}$. Each subset A of $\mathscr{S}$. including the empty subset, is called an event. Each element of $\mathscr{S}$ determines an outcome, so if $|\mathscr{S}| = n$ and $a \in \mathscr{S}$, $A \subseteq \mathscr{S}$, then
  - The probability that $\{a\}$ occurs, $Pr(\{a\}) = \dfrac{|\{a\}|}{\mathscr{S}} = \dfrac{1}{n}$.
  - The probability that A occurs, $Pr(A) = \dfrac{|A|}{\mathscr{S}} = \dfrac{|A|}{n}$.

  Note: We often write $Pr(a)$ for $Pr(\{a\})$.
- For sets A, B, the Cartesian product, or cross product of A and B is denoted by $A \times B$ and equals $\{(a, b) | a \in A, b \in B\}$.

4 Properties of the Integers: Mathematical Induction

- (The Well-Ordering Principle:) Every nonempty subset of $\mathbb{Z}^+$ contains a smallest element. (We often express this by saying that $\mathbb{Z}^+$ is well-ordered.)
- (The Principle of Mathematical Induction:) Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which represents a positive integer.

  1. If $S(1)$ is true; and
  2. If whenever $S(k)$ is true for some (particular, but arbitrarily chosen) $k \in \mathbb{Z}^+$, then $S(k+1)$ is true;

  then $S(n)$ is true for all $n \in \mathbb{Z}^+$.
- (The Principle of Strong Mathematical Induction:) Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which represents a positive integer. Also, let $n_0, n_1 \in \mathbb{Z}^+$ with $n_0 \leq n_1$.

  1. If $S(n_0), S(n_0+1), S(n_0+2), \ldots, S(n_1-1)$ and $S(n_1)$ are true; and
  2. If whenever $S(n_0), S(n_0+1), S(n_0+2), \ldots, S(k-1)$ and $S(k)$ are true for some (particular, but arbitrarily chosen) $k \in \mathbb{Z}^+$, where $k \geq n_1$, then $S(k+1)$ is also true;

  then $S(n)$ is true for all $n \geq n_0$.
- $a_1, a_2, \ldots$ is a recursive sequence if for some positive integer k, $a_1, a_2, \ldots a_k$ are given and $\forall n > k$, $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$.
- If $a, b \in \mathbb{Z}$, and $n \neq 0$, we say that b divides a and write $b|a$ if there is an integer n such that $a = bn$. When this occurs, we say that b is a divisor of a, or a is a multiple of b.
- (Theorem: Properties of Division) For all $a, b, c \in \mathbb{Z}$,

  1. $1|a$ and $a|0$.
  2. $[(a|b) \wedge (b|a)] \implies a = \pm b$.
  3. $[(a|b) \wedge (b|c)] \implies a|c$.
  4. $a|b \implies a|bx$ for all $x \in \mathbb{Z}$.
  5. If $x = y + z$, for some $x, y, z \in \mathbb{Z}$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.
  6. $[(a|b) \wedge (a|c)] \implies a|(bx + cy)$ for all $x, y \in \mathbb{Z}$. (The expression $bx + cy$ is called a linear combination of b, c.)
  7. For $1 \leq i \leq n$, let $c_i \in \mathbb{Z}$. If a divides each c_i, then $a|(c_1x_1 + c_2x_2 + \cdots + c_nx_n)$, where $x_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.
- (Lemma:) If $n \in \mathbb{Z}^+$, and n is composite, then there is a prime p such that $p|n$.

- (Theorem:) There are infinitely many prime numbers.
- (Theorem: The Division Algorithm) If $a, b \in \mathbb{Z}$, with $b > 0$, then there exists unique $q, r \in \mathbb{Z}$ with $a = qb + r$, $0 \leq r \leq b$.
- For $a, b \in \mathbb{Z}$, a positive integer c is said to be a common divisor of a and b if $c|a$ and $c|b$.
- Let $a, b \in \mathbb{Z}$ where either $a \neq 0$ or $b \neq 0$. then $c \in \mathbb{Z}^+$ is called the greatest common divisor of a, b if
  1. $c|a$ and $c|b$ (that is, c is a common divisor of a, b), and
  2. for any common divisor d of a and b, we have $d|c$.
- (Theorem:) For all $a, b \in \mathbb{Z}^+$, there exists a unique integer $c \in \mathbb{Z}^+$ that is *the* greatest common divisor of a, b.
- (Euclidean Algorithm.) Let $a, b \in \mathbb{Z}^+$. Set $r_0 = a$, $r_1 = b$ and apply the division algorithm n times as follows:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4, && 0 < r_4 < r_3 \\
&\vdots && \vdots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2}, && 0 < r_{i+2} < r_{i+1} \\
&\vdots && \vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n.
\end{aligned}$$

  Then r_n, the last nonzero remainder, equals $\gcd(a, b)$.
- If $a, b, c \in \mathbb{Z}^+$, the Diophantine equation $ax + by = c$ has an integer solution $x = x_0$, $y = y_0$ if and only if $\gcd(a, b)$ divides c.
- If $a, b, c \in \mathbb{Z}^+$, c is called a common multiple of a, b if c is a multiple of both a and b. Furthermore, c is called a least common multiple of a, b if it is the smallest of all positive integers that are common multiples of a, b. We denote c by $\operatorname{lcm}(a, b)$.
- Let $a, b, c \in \mathbb{Z}^+$, with $c = \operatorname{lcm}(a, b)$.If d is a common multiple of a and b, then $c|d$.
- For all $a, b \in \mathbb{Z}^+$, $ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$.
- (Lemma:) If $a, b \in \mathbb{Z}^+$ and p is prime, then $p|ab \implies p|a$ or $p|b$.
- (Lemma:) Let $a_i \in \mathbb{Z}^+$ for all $1 \leq i \leq n$. If p is prime and $p|a_1 a_2 \cdots a_n$, then $p|a_i$ for some $1 \leq i \leq n$.

- (Theorem:) Every integer $n > 1$ can be written as a product of primes uniquely, up to the order of the primes. (Here a single prime is considered a product of one factor.)

5 Relations and Functions

- For sets A, B the Cartesian product, or cross product, of A and B is denoted by $A \times B$ and equals $\{(a, b)|a \in A, b \in B\}$.
- For sets A, B any subset of $A \times B$ is called a (binary) relation from A to B. Any subset of $A \times A$ is called a (binary) relation on A.
- For sets $A, B, C \in \mathscr{U}$:
  1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
  2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
  3. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
  4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
- For nonempty sets A, B, a function or mapping, f from A to B, denoted $f : A \to B$ is a relation from A to B in which every element of A appears exactly once as the first component of an ordered pair in the relation.
- For the function $f : A \to B$, A is called the domain of f and B is called the codomain of f. The subset of B consisting of those elements that appear as second components in the ordered pairs of f is called the range of f and is also denoted by $f(A)$ because it is the set of images (of the elements of A) under f.
- A function $f : A \to B$ is one-to-one or injective, if each element of B appears at most once as the image of an element of A.
- If $f : A \to B$ and $A_1 \subseteq A$, then

  $$f(A_1) = \{b \in B | b = f(a), \text{for some } a \in A_1\}$$

  then $f(A_1)$ is called the image of A_1 under f.
- (Theorem:) Let $f : A \to B$, with $A_1, A_2 \subseteq A$. Then
  1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
  2. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
  3. $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ when f is one-to-one.
- If $f : A \to B$ and $A_1 \subseteq A$, then $f|_{A_1} : A_1 \to B$ is called the restriction of f to A_1 if $f|_{A_1}(a) = f(a)$ for all $a \in A$.
- Let $A_1 \subseteq A$ and $f : A_1 \to B$. If $g : A \to B$ and $g(a) = f(a)$ for all $a \in A_1$, then we call g an extension of f to A.
- A function is said to be onto or surjective if $f(A) = B$ — that is, for all $b \in B$, there is at least one $a \in A$ with $f(a) = b$.

- A Stirling number of the second kind is the number of ways to partition a set of m objects into n non-empty subsets and is denoted $S(m,n)$.

$$S(m,n) = \frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$$

- (Theorem:) Let m,n be positive integers with $1 \leq n \leq m$. Then

$$S(m+1,n) = S(m,n-1) + nS(m,n)$$

- For any nonempty sets A, B, any function $f : A \times A \to B$ is called a binary operation on A. If $B \subseteq A$, then the binary operation is said to be closed on A. (When $B \subseteq A$ we may also say that A is closed under f.)

- A function $g : A \to A$ is called a unary, or monary, operation on A.

- Let $f : A \times A \to B$; that is, f is a binary operation on A.

  1. f is said to be commutative if $f(a,b) = f(b,a)$ for all $(a,b) \in A \times A$.
  2. When $B \subseteq A$ (that is, when f is closed), f is said to be associative if for all $a,b,c \in A$, $f(f(a,b),c) = f(a,f(b,c))$.

- $Let f : A \times A \to B$ be a binary operation on A. An element $x \in A$ is called an identity (or identity element) for f if $f(a,x) = f(x,a) = a$ for all $a \in A$.

- (Theorem:) Let $f : A \times A \to B$ be a binary operation. If f has an identity element, then that identity is unique.

- For sets A and B, if $D \subseteq A \times B$, then $\pi_A : D \to A$, defined by $\pi_A(a,b) = a$, is called the projection on the first coordinate. The function $\pi_B : D \to B$, defined by $\pi_B(a,b) = b$, is called the projection on the second coordinate.

- (The Pigeonhole Principle:) If m pigeons occupy n pigeonholes and $m > n$, then at least one pigeonhole has two or more pigeons roosting in it.

- If $f : A \to B$, then f is said to be bijective, or to be a one-to-one correspondence, if f is both one-to-one and onto.

- The function $1_A : A \to A$, defined by $1_A(a) = a$ for all $a \in A$, is called the identity function for A.

- If $f, g : A \to B$, we say that f and g are equal and write $f = g$, if $f(a) = g(a)$ for all $a \in A$.

- If $f : A \to B$ and $g : B \to C$, we define the composite function, which is denoted $g \circ f : A \to C$ by $(g \circ f)(a) = g(f(a))$ for each $a \in A$.

- (Theorem:) Let $f : A \to B$ and $g : B \to C$.

  1. If f and g are one-to-one, then $g \circ f$ is one-to-one.

2. If f and g are onto, then $g \circ f$ is onto.

- (Theorem:) If $f : A \to B$, $g : B \to C$ and $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.
- If $f : A \to A$ we define $f^1 = f$, and for $n \in \mathbb{Z}^+$, $f^{n+1} = f \circ f^n$.
- For sets A, B if $\mathscr{R}$ is a relation from A to B, then the converse of $\mathscr{R}$, denoted $\mathscr{R}^c$, is the relation from B to A defined by $\mathscr{R}^c = \{(b, a) | (a, b) \in \mathscr{R}\}$
- If $f : A \to B$, then f is said to be invertible if there is a function $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.
- (Theorem:) If a function $f : A \to B$ is invertible and a function $g : B \to A$ satisfies $g \circ f = 1_A$ and $f \circ g = 1_B$, then this function g is unique.
- (Theorem:) A function $f : A \to B$ is invertible if and only if it is one-to-one and onto.
- (Theorem:) If $f : A \to B$, $g : B \to C$ are invertible functions, then $g \circ f : A \to C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- If $f : A \to B$ and $B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A | f(x) \in B_1\}$. The set $f^{-1}(B_1)$ is called the preimage of B_1 under f.
- (Theorem:) If $f : A \to B$ and $B_1, B_2 \subseteq B$, then
  1. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;
  2. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;
  3. $f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}$.
- (Theorem:) Let $f : A \to B$ for finite sets A and B, where $|A| = |B|$. Then the following statements are equivalent:
  1. f is one-to-one.
  2. f is onto.
  3. f is invertible.
- A relation $\mathscr{R}$ on a set A is called reflexive of for all $x \in A$, $(x, x) \in \mathscr{R}$.
- A relation $\mathscr{R}$ on a set A is called symmetric if $(x, y) \in \mathscr{R} \implies (y, x) \in \mathscr{R}$ for all $x, y \in A$.
- For a set A, a relation $\mathscr{R}$ on A is called transitive if, for all $x, y, z \in A$, $(x, y), (y, z) \in \mathscr{R} \implies (x, z) \in \mathscr{R}$.
- Given a relation $\mathscr{R}$ on a set A, $\mathscr{R}$ is called antisymmetric if for all $a, b \in A$ ($a \mathscr{R} b$ and $b \mathscr{R} a$) $\implies a = b$.
- A relation $\mathscr{R}$ on a set A is called a partial order or a partial ordering relation if $\mathscr{R}$ is reflexive, antisymmetric, and transitive.

- An equivalence relation $\mathscr{R}$ on a set A is a relation that is reflexive, symmetric, and transitive.
- If A, B and C are sets with $\mathscr{R}_1 \subseteq A \times B$ and $\mathscr{R}_2 \subseteq B \times C$, then the composite relation $\mathscr{R}_1 \circ \mathscr{R}_2$ from A to C defined by $\mathscr{R}_1 \circ \mathscr{R}_2 = \{(x, z) | x \in A, z \in C,$ and there exists $y \in B$ with $(x, y) \in \mathscr{R}_1, (y, z) \in \mathscr{R}_2\}$.
- (Theorem:) Let A, B, C and D be sets with $\mathscr{R}_1 \subseteq A \times B$, $\mathscr{R}_2 \subseteq B \times C$, and $\mathscr{R}_3 \subseteq C \times D$. Then $\mathscr{R}_1 \circ (\mathscr{R}_2 \circ \mathscr{R}_3) = (\mathscr{R}_1 \circ \mathscr{R}_2) \circ \mathscr{R}_3$.
- Given a set A and a relation $\mathscr{R}$ on A, we define the powers of $\mathscr{R}$ recursively by
  1. $\mathscr{R}^1 = \mathscr{R}$;
  2. For $n \in \mathbb{Z}^+$, $\mathscr{R}^{n+1} = \mathscr{R} \circ \mathscr{R}^n$
- An $m \times n$ zero-one matrix $E = (e_{ij})_{m \times n}$ is a rectangular array of numbers arranged in m rows and n columns where each e_{ij}, for $1 \leq i \leq m$ and $1 \leq j \leq n$, denotes the entry in the ith row and jth column of E, and each such entry is 0 or 1. (We can also write $(0, 1)$-matrix for this type of matrix.)
- Let $E = (e_{ij})_{m \times n}$, $F = (f_{ij})_{m \times n}$ be two $m \times n$ $(0, 1)$-matrices. We say that E precedes or is less than F, and we write $E \leq F$ if $e_{ij} \leq f_{ij}$ for all $1 \leq i \leq m$, $1 \leq j \leq n$.
- For $n \in \mathbb{Z}^+$, $I_n = (\delta_{ij})_{n \times n}$ is the $n \times n$ $(0, 1)$-matrix where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

- Let $A = (a_{ij})_{m \times n}$ be a $(0, 1)$-matrix. The transpose of A, written A^{tr}, is the matrix $(A^*_{ji})_{n \times m}$ where $a^*_{ji} = a_{ij}$ for all $1 \leq i \leq m$, $1 \leq j \leq n$.
- Given a set A with $|A| = n$ and a relation $\mathscr{R}$ on A, let M denote the relation matrix for $\mathscr{R}$. Then
  1. $\mathscr{R}$ is reflexive if and only if $I_n \leq M$.
  2. $\mathscr{R}$ is symmetric if and only if $M = M^{tr}$.
  3. $\mathscr{R}$ is transitive if and only if $M \cdot M = M^2 \leq M$.
  4. $\mathscr{R}$ is antisymmetric if and only if $M \cap M^{tr} \leq I_n$.
- Let A be a set and $\mathscr{R}$ be a relation on A. The pair $(A, \mathscr{R})$ is called a partially ordered set, or poset if relation $\mathscr{R}$ on A is a partial order.
- If $(A, \mathscr{R})$ is a poset, we say that A is totally ordered if for all $x, y \in A$, either $x \mathscr{R} y$ or $y \mathscr{R} x$. In this case, $\mathscr{R}$ is called a total order.
- If $(A, \mathscr{R})$ is a poset, then an element $x \in A$ is called a maximal element of A if for all $a \in A$, $a \neq x \implies \not\mathscr{R} a$. An element $y \in A$ is called a minimal element of A if whenever $b \in A$ and $b \neq y$, then $b \not\mathscr{R} y$.

- (Theorem:) If $(A, \mathscr{R})$ is a poset and A is finite, then A has both a maximal and a minimal element.
- If $(A, \mathscr{R})$ is a poset, then an element $x \in A$ is called a least element if $x \mathscr{R} a$ for all $a \in A$. Element $y \in A$ is called a greatest element if $a \mathscr{R} y$ for all $a \in A$.
- (Theorem:) If the poset $(A, \mathscr{R})$ has a greatest (least) element, then that element is unique.
- Let $(A, \mathscr{R})$ be a poset with $B \subseteq A$. An element $x \in A$ is called a lower bound of B if $x \mathscr{R} b$ for all $b \in B$. Likewise, an element $y \in A$ is called an upper bound of B if $b \mathscr{R} y$ for all $b \in B$. An element $x' \in A$ is called a greatest lower bound (glb) of B if it is a lower bound of B, and if for all other lower bounds x'' of B, we have $x'' \mathscr{R} x'$. Similarly, $y' \in A$ is a least upper bound (lub) of B if it is an upper bound of B and if $y' \mathscr{R} y''$ for all other uppers bounds y'' of B.
- (Theorem) If $(A, \mathscr{R})$ is a poset and $B \subseteq A$, then B has at most one lub (gub).
- The poset $(A, \mathscr{R})$ is called a lattice if for all $x, y \in A$, the elements lub$\{x, y\}$ and glb$\{x, y\}$ both exist in A.
- Given a set A and an index set I, let $\emptyset \neq A_i \subseteq A$ for each $i \in I$. then $\{a_i\}_{i \in I}$ is a partition of A if
  1. $A = \bigcup_{i \in I} A_i$,
  2. $A_i \cap A_j = \emptyset$,

  for all $i, j \in I$ where $i \neq j$. Each subset A_i is called a cell or block of the partition.
- Let $\mathscr{R}$ by an equivalence relation on a set A. For each $x \in A$, the equivalence class of x, denoted $[x]$, is defined by $[x] = \{y \in A | y \mathscr{R} x\}$
- (Theorem:) If $\mathscr{R}$ is an equivalence relation on a set A, and $x, y \in A$, then
  1. $x \in [x]$;
  2. $x \mathscr{R} y$ if and only if $[x] = [y]$;
  3. $[x] = [y]$ or $[x] \cap [y] = \emptyset$.
- (Theorem:) If A is a set, then
  1. any equivalence relation $\mathscr{R}$ on A induces a partition of A, and
  2. any partition of A gives rise to an equivalence relation $\mathscr{R}$ on A.
- (Theorem:) For any set A, there is a one-to-one correspondence between the set of equivalence relations on A and the set of partitions of A.

11 An introduction to Graph Theory

- Let V be a finite nonempty set, and let $E \subseteq V \times V$. The pair (V, E) is then called a directed graph or digraph where V is the set of vertices or nodes, and E is its set of (directed) edges or arcs. We write $G = (V, E)$ to denote such a graph.
  When there is no concern about the direction of any edge, we still write $G = (V, E)$. But now E is a set of unordered pairs of elements taken from V, and G is called an undirected graph.
  Whether $G = (V, E)$ is directed or undirected, we often call V the vertex set of G and E the edge set of G.

- If $a, b \in V$ and $(a, b) \in E$, then there is an edge from a to b. Vertex a is called the origin or source of the edge, with b the terminus, or terminating vertex, and we say that b is adjacent from a and that a is adjacent to b. In addition, if $a \neq b$, then $(a, b) \neq (b, a)$. An edge of the form (a, a) is called a loop (at a). When a graph contains no loops, it is called loop-free.

- Let x, y be (not necessarily distinct) vertices in an undirected graph G. An $x - y$ walk in G is a (loop-free) finite alternating sequence

  $$x = x_0, e_1, x_1, e_2, x_2, e_3, \ldots, e_{n-1}, x_{n-1}, e_n, x_n = y$$

  of vertices and edges from G starting at vertex x and ending at vertex y and involving the n edges $e_i = \{x_{i-1}, x_i\}$, where $1 \leq i \leq n$.
  The length of this walk is n, the number of edges in the walk. (When $n = 0$, there are no edges, $x = y$ and the walk is called trivial.)
  Any $x - y$ walk, where $x = y$ and $n > 1$ is called a closed walk. Otherwise the walk is called open.

- Consider any $x - y$ walk in an undirected graph G.

  1. If no edge in the $x - y$ walk is repeated, then the walk is called an $x - y$ trail. A closed $x - x$ trail is called a circuit.
  2. If no vertex of the $x - y$ walk occurs more than once, then the walk is called an $x - y$ path. When $x = y$, the term cycle is used to describe such a closed path.

- (Theorem:) Let $G = (V, E)$ be an undirected graph with $a, b \in V, a \neq b$. If there exists a trail from a to b, then there is a path from a to b.

- Let $G = (V, E)$ be an undirected graph. We call G connected if there is a path between any two distinct vertices in G.

- For any graph $G = (V, E)$, the number of components of G is denoted by $\kappa(G)$.

- Let V be a finite nonempty set. We say that the pair (V, E) determines a multigraph G with vertex set V and edge set E if for some $x, y \in V$, there are two or more edges in E of the form (x, y) (for a directed multigraph), or $\{x, y\}$ (for an undirected multigraph). In either case, we write $G = (V, E)$ to designate the multigraph, just as we did for graphs.

- If $G = (V, E)$ is a graph, then $G_1 = (V_1, E_1)$ is called a subgraph of G if $\emptyset \neq V_1 \subseteq V$ and $E_1 \subseteq E$, where each edge in E_1 is incident with vertices in V_1.

- Given a graph $G = (V, E)$, let $G_1 = (V_1, E_1)$ be a subgraph of G. If $v_1 = V$ then G_1 is called a spanning subgraph of G.

- Let $G = (V, E)$ be a graph. If $\emptyset \neq U \subseteq V$, the subgraph of G induced by U is the subgraph whose vertex set is U and which contains all edges (from G) of either the form (x, y) (when G is directed) or $\{x, y\}$ (when g is undirected) for $x, y \in U$. We denote this subgraph by $\langle U \rangle$. Any subgraph G' of a graph $G = (V, E)$ is called an induced subgraph if there exists $\emptyset \neq U \subseteq V$ where $G' = \langle U \rangle$.

- Let V be a set of n vertices. The complete graph on V, denoted K_n, is a loop-free undirected graph, where for all $a, b \in V$, $a \neq b$, there is an edge $\{a, b\}$.

- Let G be a loop-free undirected graph on n vertices. The complement of G, denoted $\overline{G}$ is the subgraph of K_n consisting of the n vertices in G and all edges that are not in G. (If $G = K_n$, $\overline{G}$ is a graph consisting of n vertices and no edges. Such a graph is called a null graph.)

- Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two undirected graphs. A function $f : V_1 \to V_2$ is called graph isomorphism if

  1. f is one-to-one and onto, and
  2. for all $a, b \in V_1$ $\{a, b\} \in E_1$ if and only if $\{f(a), f(b)\} \in E_2$. When such a function exists, G_1 and G_2 are called isomorphic graphs.

- Let G be an undirected graph or multigraph. For each vertex c of G, the degree of v, written $\deg(v)$ is the number of edges in G that are incident with v. Here a loop at vertex v is considered as two incident edges for v.

- (Theorem:) If $G = (V, E)$ is an undirected graph or multigraph, then $\sum_{v \in V} \deg(v) = 2|E|$.

- (Corollary:) For any undirected graph or multigraph, the number of vertices of odd degree must be even.

- Let $G = (V, E)$ be an undirected graph or multigraph with no isolated vertices. Then G is said to have an Euler circuit if there is a circuit in G that traverses every edge of the graph exactly once. If there is an open trail from a to b in G, and this trail traverses each edge in G exactly once, the trail is called an Euler trail.

- (Theorem:) Let $G = (V, E)$ be an undirected graph or multigraph with no isolated vertices. Then G has an euler circuit if and only if G is connected and every vertex in G has even degree.

- (Corollary:) If G is an undirected graph or multigraph with no isolated vertices, then we can construct an Euler trail in G if and only if G is connected and has exactly two vertices of odd degree.

- Let $G = (V, E)$ be a directed graph or multigraph. For each $v \in V$,

  1. The incoming or in degree of v is the number of edges in G that are incident into v, and this is denoted $id(v)$.
  2. The outgoing or out degree of v is the number of edges in G that are incident from v, and this is denoted $od(v)$.

  For the case where the directed graph or multigraph contains one or more loops, each loop at a given vertex v contributes a count of 1 to each of $id(x)$ and $od(x)$.

- (Theorem:) Let $G = (V, E)$ be a directed graph or multigraph with no isolated vertices. The graph G has a directed Euler circuit if and only if G is connected and $id(v) = od(v)$ for all $v \in V$.

- A graph G is called planar if G can be drawn in the plane with its edges intersecting only at vertices of G. Such a drawing of G is called an embedding of G in the plane.

- A graph $G = (V, E)$ is called bipartite if $V = V_1 \cup V_2$ with $V_1 \cap V_2 = \emptyset$, and every edge of G is of the form $\{a, b\}$ with $a \in V_1$ and $b \in V_2$. If each vertex in V_1 is joined with every vertex in V_2, we have a complete bipartite graph. In this case, if $|V_1| = m$, $|V_2| = n$, the graph is denoted by $K_{m,n}$.

- Let $G = (V, E)$ be a loop-free undirected graph, where $E \neq \emptyset$. An elementary subdivision of G results when an edge $e = \{u, w\}$ is removed from G and then the edges $\{u, v\}$, $\{v, w\}$ are added to $G - e$, where $v \notin V$.
  The loop-free undirected graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are called homeomorphic if they are isomorphic or if they can both be obtained from the same loop-free undirected graph H by a sequence of elementary subdivisions.

- (Kuratowski's Theorem:) A graph is nonplanar if and only if it contains a subgraph that is homeomorphic to either K_5 or $K_{3,3}$

- (Theorem:) Let $G = (V, E)$ be a connected planar graph or multigraph with $|V| = v$ and $|E| = e$. Let r be the number of regions in the plane determined by a planar embedding of G; one of these regions has an infinite area and is called the infinite region. Then $v - e + r = 2$.

- (Corollary:) Let $G = (V, E)$ be a loop-free connected planar graph with $|V| = v$ and $|E| = e > 2$, and r regions. Then $3r \leq 2e$ and $e \leq 3v - 6$.

- Let $G = (V, E)$ be an undirected graph or multigraph. A subset E' of E is called a cut-set of G if by removing the edges (but not the vertices) in E' from G, we have $\kappa(G) < \kappa(G')$, where $G' = (V, E - E')$; but when we remove (from E) any proper subset E'' of E', we have $\kappa(G) = \kappa(G'')$ for $G' = (V, E - E'')$.

- If $G = (V, E)$ is a graph or multigraph with $|V| \geq 3$, we say that G has a Hamilton cycle if there is a cycle in G that contains every vertex V. A Hamilton path is a path (and not a cycle) in G that contains each vertex.

- (Theorem:) Let K_n^* be a complete directed graph — that is, K_n^* has n vertices and for each distinct pair x, y of vertices, exactly one of the edges (x, y) or (y, x) is in K_n^*. such a graph (called a tournament) always contains a (directed) Hamilton path.

- (Theorem:) Let $G = (V, E)$ be a loop-free graph with $|V| = n \geq 2$. If $\deg(x)+\deg(y) \geq n-1$ for all $x, y \in V$, $x \neq y$, then G has a Hamilton path.

- (Corollary:) Let $G = (V, E)$ be a loop-free graph with n (≥ 2) vertices. If $\deg(v) \geq \dfrac{n-1}{2}$ for all $v \in V$, then G has a Hamilton path.

- (Theorem:) Let $G = (V, E)$ be a loop-free undirected graph with $|V| = n \geq 3$. If $\deg(x) + \deg(y) \geq n$ for all nonadjacent $x, y \in V$, then G contains a Hamilton cycle.

- (Corollary:) If $G = (V, E)$ is a loop-free undirected graph with $|V| = n \geq 3$, and if $\deg(v) \geq \dfrac{n}{2}$ for all $v \in V$, then G has a Hamilton cycle.

- (Corollary:) If $G = (V, E)$ is a loop-free undirected graph with $|V| = n \geq 3$, and if $|E| \geq \dbinom{n-1}{2} + 2$, then G has a Hamilton cycle.

- If $G = (V, E)$ is an undirected graph, a proper coloring of G occurs when we color the vertices of G so that if $\{a, b\}$ is an edge in G, then a and b are colored with different colors. (Hence adjacent vertices have different colors.) The minimum number of colors needed to properly color G is called the chromatic number of G and is written $\chi(G)$.

- (Decomposition Theorem for Chromatic Polynomials:) If $G = (V, E)$ is a connected graph and $e \in E$, then
$$P(G_e, \lambda) = P(G, \lambda) + P(G'_e, \lambda)$$

- (Theorem:) For each graph G, the constant term is in $P(G, \lambda)$ is 0.

- (Theorem:) Let $G = (V, E)$ with $|E| > 0$. then the sum of the coefficients in $P(G, \lambda)$ is 0.

- (Theorem:) Let $G = (V, E)$, with $a, b \in V$ but $\{a, b\} = e \notin E$. We write G_e^+ for the graph we obtain from G by adding the edge $e = \{a, b\}$. Coalescing the vertices a and b in G gives us the subgraph G_e^{++} of G. Under these circumstances $P(G, \lambda) = P(G_e^+, \lambda) + P(G_e^{++}, \lambda)$.

- (Theorem:) Let G be an undirected graph with subgraphs G_1, G_2. If $G = G_1 \cup G_2$ and $G_1 \cap G_2 = K_n$ for some $n \in \mathbb{Z}^+$, then
$$P(G, \lambda) = \frac{P(G_1, \lambda) \cdot P(G_2, \lambda)}{\lambda^{(n)}}$$

14 The Integers Modulo n

- Let R be a nonempty set on which we have two closed binary operations, denoted by $+$ and $\cdot$ (which may be quite different from the ordinary addition and multiplication to which we are accustomed). Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in \mathbb{R}$, the following conditions are satisfied.

  1. $a + b = b + a$.
  2. $a + (b + c) = (a + b) + c$.
  3. There exists $z \in \mathbb{R}$ such that $a + z = z + a = a$ for every $a \in \mathbb{R}$.
  4. For each $a \in \mathbb{R}$ there is an element $b \in \mathbb{R}$ with $a + b = b + a = z$.
  5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
  6. $a \cdot (b + c) = a \cdot b + a \cdot c$.
  7. $(b + c) \cdot a = b \cdot a + c \cdot a$.

- Let $(R, +, \cdot)$ be a ring.
  - If $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{R}$, then R is called a commutative ring.
  - The ring R is said to have no proper divisors of zero if for all $a, b \in \mathbb{R}$, $ab = z \implies a = z$ or $b = z$.
  - If an element $u \in \mathbb{R}$ is such that $u \neq z$ amd $a \cdot u = u \cdot a = a$ for all $a \in \mathbb{R}$, we call u a unity or multiplicative identity. of R. Here, R is called a ring with unity.

- Let R be commutative ring with unity. R is called a field if every nonzero element of R is a unit.

- Let $n \in \mathbb{Z}^+$, $n > 1$. For $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n, and we write $a \equiv b (\text{mod } n)$ if $n|(a - b)$, or, equivalently, $a = b + kn$, for some $k \in \mathbb{Z}$.

- (Theorem:) Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

- $\mathbb{Z}_n$ is used to denote $\{[0], [1], [2], \ldots [n - 1]\}$.

- For $n \in \mathbb{Z}^+, n > 1$, $\mathbb{Z}_n$ is a commutative ring with unity $[1]$ (and additive identity $[0]$).

- $\mathbb{Z}_n$ is a field if and only if n is a prime.