Ministry of Transport and Communications of Ukraine
State Department of Communications
Odessa National Academy of Telecommunications
named after A.S.Popov

Department of Higher Mathematics

DISCRETE MATHEMATICS
Textbook

For Students Doing a Course of Higher Mathematics in English

Odessa – 2011

УДК 510(083) План НМВ 2010/2011 уч.г.

Составители:
Доц. В. Н. Гавдзинский, ст. преп. Л. Н. Коробова

Методическое пособие содержит следующие разделы дискретной математики “Теория множеств”, “Отношения”, “Математическая логика”, “Булева алгебра”, “Теория чисел” и предназначено для студентов академии, изучающих математику на английском языке.

Основные теоремы и формулы приведены с доказательством, а также даны решения типовых задач и задания для самостоятельной работы.

Компьютерная верстка ***Корнейчук Е. С.***

Здано в набір 17.06.2011 Підписано до друку 24.06.2011
Формат 60/88/16 Зам. № 4608
Тираж 100 прим. Обсяг: 3,75 ум. друк. арк.
Віддруковано на видавничому устаткуванні фірми RISO
у друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
ОНАЗ, 2011

CONTENTS

1. SET THEORY

1.1. Sets and Elements. Subsets.

Definition. A set is defined as a collection of objects which can be treated as an entity.

This definition implies that the objects have some classifying attributes, and all the objects in the set have the same attributes.

Note also, that object does not necessarily mean material object. We may well talk about the set of transistors in a given circuit, and about the set of all operation frequencies of this circuit.

One usually uses capital letters, *A, B, X, Y,* …, to denote set, and lowercase letters, *a, b, x, y,…,* to denote elements of sets.

Membership in a set is denoted as follows:

$a \in A$ denotes that *a* belongs to a set *A*.

Here $\in$ is the symbol meaning, "is an element of ". We use $\notin$ to mean " is not an element of ".

There are essentially two ways to specify a particular set.

One way, if possible, is to list its elements separated by commas and contained in braces $\{...\}$.

A second way is to state those properties which characterized the elements in the set.

Examples illustrating these two ways are:

$A = \{1, 3, 5, 7, 9\}$ that is A consists of the numbers $1, 3, 5, 7, 9$.

$B = \{x | \ x \text{ is an even iteger}, x > 0\}$ – set, which reads: *B* is the set of x such that x is an even integer and *x* is greater then 0.

Note that the vertical line $|$ is read as "such that" and the comma is read as "and".

Example 1.1.1

1) The set of TV – channels at a given location.
2) The set of all solutions of the equation $\sin x = 1$.

Suppose every element in a set *A* is also an element of a set *B*, that is, suppose $a \in A$ implies $a \in B$. Then a set A is called a **subset** of a set *B*. This relation is written $A \subseteq B$ or $B \supseteq A$.

Definition. Two sets are equal if they both have the same elements. That is: $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

If *A* is not a subset of B , that is, if at least one element of *A* does not belong to *B*, we write $A \not\subset B$.

Example 1.2. Consider the sets

$A = \{1, 3, 4, 7, 8, 9\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{1, 3\}$.

Then $C \subseteq A$ and $C \subseteq B$ since 1 and 3, the elements of C, are also elements of A and B. But $B \not\subset A$ since some of the elements of B, e.g., 2 and 5 do not belong to A. Similarly, $A \not\subset B$.

Some sets will occur very often in the text, and so we use special symbols for them. Some such symbols are:

$\{1, 2, 3, ...\} = \boldsymbol{N}$: the set of natural numbers or positive integers;

$\{..., -2, -1, 0, 1, 2, 3, ...\} = \boldsymbol{Z}$: the set of all integers;

$\boldsymbol{Q}$: the set of rational numbers;

$\boldsymbol{R}$: the set of real numbers;

$\boldsymbol{C}$: the set of complex numbers.

All sets under investigation in any application of set theory are assumed to belong to some fixed large set called the **universal set** which we denote by $\boldsymbol{U}$ unless otherwise stated or implied.

Given a universal set $\boldsymbol{U}$ and a property $\boldsymbol{P}$**,** there may not be any element of $\boldsymbol{U}$ which have property $\boldsymbol{P}$. For example, the following set has no elements:

$$S = \{x \mid x \text{ is a positive integer}, x^2 = 3\}.$$

Definition. A set with no elements is called the **empty set** or null set and is denoted by Ø.

A Venn diagram is a pictorial representation of sets in which sets are represented by enclosed areas in the plane.

The universal set $\boldsymbol{U}$ is represented by the interior of a rectangle, and the other sets are represented by disks lying within the rectangle.

Definition. The set of elements of a set $\boldsymbol{U}$ which do not belong to A is called the **compliment** of the set A, and is denoted by $\overline{A}$

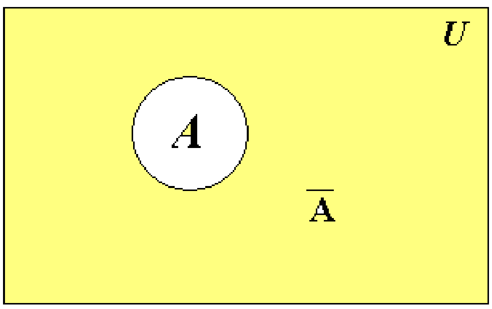


Fig 1.1.1

Definition. The **union** of two sets A and B, denoted by $A \cup B$, is the set of all elements which belong to A or to B. That is

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

Figure 1.1.2 is a Venn diagram in which $A \cup B$ is the shaded region.

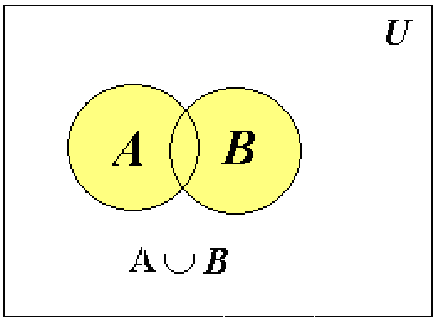


Fig 1.1.2

Definition. The **intersection** of two sets A and B, denoted by $A \cap B$ is the set of elements which belong to both A and B. That is

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

Figure 1.1.3 is a Venn diagram in which $A \cap B$ is the shaded region.

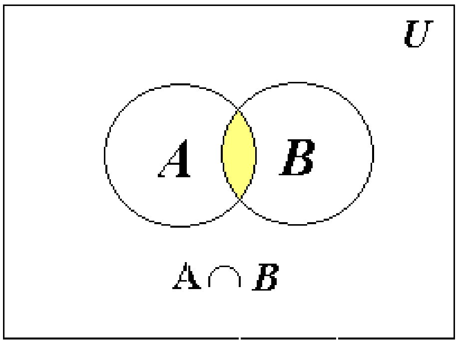


Fig 1.1.3

Definition. The sets A and B are said to be **disjoint** or **nonintersecting** if they have no elements in common.

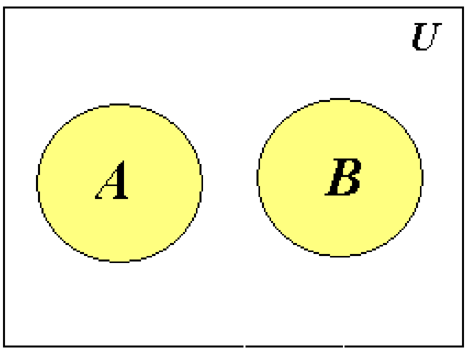


Fig 1.1.4

Definition The **difference** of two sets *A* and *B*, denoted by $A \setminus B$, is the set of elements which belong to A but which do not belong to B. That is

$$A \setminus B = \{x \mid x \in A, x \notin B\}$$

Figure 1.1.5 is a Venn diagram in which $A \setminus B$ is the shaded region.

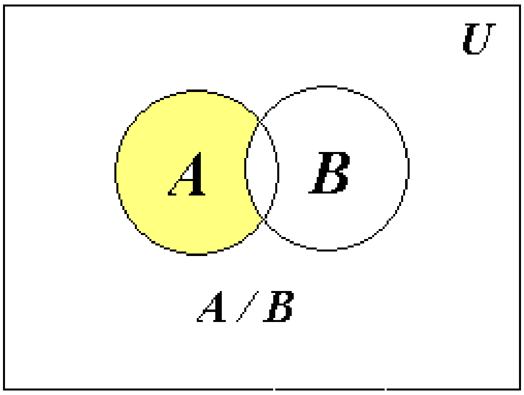


Fig 1.1.5

Definition The **symmetric difference** of two sets *A* and *B*, denoted by $A \oplus B$, consists of those elements which belong to A or B but not to both. That is

$A \oplus B = (A \cup B) \setminus (A \cap B)$ or $A \oplus B = (A \setminus B) \cup (B \setminus A)$

Figure 1.1.6 is a Venn diagram in which $A \oplus B$ is the shaded region.

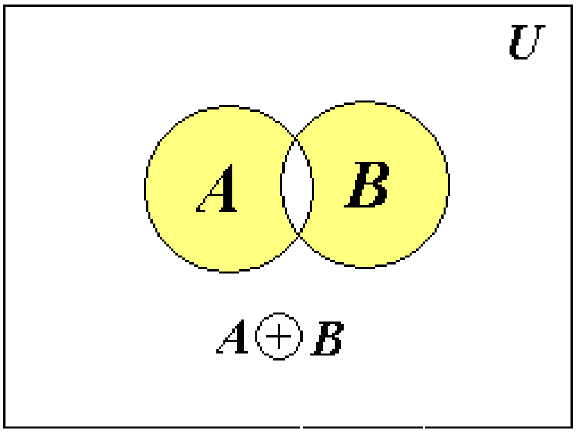


Fig 1.1.6

Example 1,1,3. Let $A = \{1, 3, 4, 5, 8\}$, $B = \{2, 4, 5, 6, 9\}$, then

$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 9\}$;

$A \cap B = \{4, 5\}$;

$A \setminus B = \{1, 3, 8\}$;

$A \oplus B = \{1, 2, 3, 6, 8, 9\}$.

Sets under the operations of union, intersection, and complement satisfy various laws (identities) which are listed in Table 1.1.1

Table 1.1.1 **Laws of the algebra of sets**

1	$A \cup A = A$	$A \cap A = A$	Idempotent laws
2	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$		Associative laws
3	$A \cup B = B \cup A$	$A \cap B = B \cap A$	Commutative laws
4	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$		Distributive laws
5	$A \cup \varnothing = A$ $A \cap U = A$	$A \cap \varnothing = \varnothing$ $A \cup U = U$	Identity laws
6	$\overline{\overline{A}} = A$		Involution law
7	$A \cup \overline{A} = U$ $\overline{U} = \varnothing$	$A \cap \overline{A} = \varnothing$ $\overline{\varnothing} = U$	Complement laws
8	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws

2. RELATIONS

2.1. Product Sets

Definition. A set is called an **ordered set** if to each element there correspons a number $n\ (n \in N)$ and elements are listed in the increasing manner.

Definition. Let two arbitrary sets A and B be given. The set of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is called the **product**, or **Cartesian product**, of the sets A and B. A short designation of this product is $A \times B$, which is read "A cross B".

By definition

$A \times B = \{(a, b) |\ a \in A \text{ and } b \in B\}$.

One frequently writes A^2 instead of $A \times A$.

Example 2.1.1. R denotes the set of real numbers and so $R^2 = R \times R$ is the set or ordered pairs of real numbers. We are familiar with the geometrical representation of R^2 as points in the plane. Each point P represents an ordered pair (a, b) of real numbers and vice versa; the vertical line through P meets the x – axis at a, and the horizontal line through P meets the y – axis at b. R^2 is frequently called the **Cartesian plane**.

This idea of a product of sets can be extended to any finite number of sets. For any sets $A_1, A_2, ..., A_n$ the set of all ordered n – tuples $(a_1, a_2, ..., a_n)$ where $a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n$ is called the **product of sets** $A_1, A_2, ..., A_n$ and is denoted by $A_1 \times A_2 \times ... \times A_n$.

2.2. Binary Relations

Definition. A **binary relation** between elements of the sets A and B is any subset R of the set $A \times B$ that is $R \subset A \times B$.

Suppose R is a relation from A to B. Then R is a set of ordered pairs where each first element comes from A end each second element comes from B. That is, for each $a \in A$ and $b \in B$, exactly one of the following is true:

1) $(a, b) \in R$; we then say "a is $R-$related to b", written aRb;
2) $(a, b) \notin R$; we then say "a is not $R-$related to b", written $a \not R b$

If R is a relation from a set A to itself, that is, if R is a subset of $A^2 = A \times A$, then we say that R is a **relation on** A.

Definition. The **domain** of a relation R is the set of all first elements of the ordered pairs which belong to R, and the **range** is the set of second elements.

Example 2.2.1. Given $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$, and let $R = \{(1, y), (1, z), (3, y)\}$. Then R is a relation from A to B since R is a subset of $A \times B$. With respect to this relation, $1R\,y$, $1R\,z$, $3R\,y$. The domain of R is $\{1, 3\}$ and the range is $\{y, z\}$.

Example 2.2.2. Let us denote in the table the elements belonging to the set $R = \{(a, 1), (b, m), (\Delta, 0)\}$ of the Cartesian product of the sets A and B by the points $(R \subset (A \times B))$:

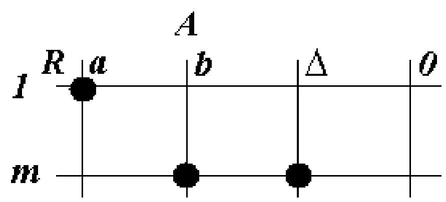


Table 1.2.1

Then we have the binary relation between the sets A and B.

2.3. Pictorial Representatives of Relations

A. Relations on *R*

Let S be a relation on the set $\boldsymbol{R}$ of real numbers. That is, S is a subset of $\boldsymbol{R}^2 = \boldsymbol{R}\times\boldsymbol{R}$. Frequently, S consists of all ordered pairs of real numbers which satisfy some given equation $E(x, y) = 0$ (such that $x^2 + y^2 = 25$).

Since $\boldsymbol{R}^2$ can be represented by the set of points in the plane, we can picture S emphasizing those points in the plane which belong to S. The pictorial representation of the relation in sometimes called the **graph** of the relation. For example, the graph of the relation $x^2 + y^2 = 25$ is a circle having its center at the origin and radius 5.

B. Directed Graphs of Relations on Sets

There is an important way of picturing a relation R on a finite set. First we write down the elements of the set, and then we draw an arrow from each element x to each element y whenever x is related to y. This diagram is called the **directed graph** of the relation.

Let us find the directed graph of the following relation R on the set $A = \{1, 2, 3, 4\}$:

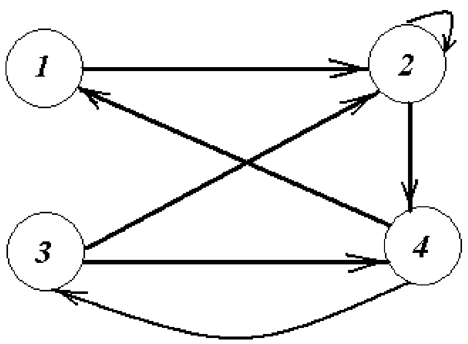


Fig. 1.2.1

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

There is an arrow from 2 to itself, since 2 is related to 2 under R.

C. Pictures of Relations on Finite Sets

Suppose A and B are finite sets. There are two ways of picturing a relation R from A to B.

a) Form a rectangular array (matrix) whose rows are labeled by the elements of A and whose columns are labeled by the elements of B. Put 1 or 0 in each position of the array according as $a \in A$ is or is not related to $b \in B$. This array is called the **matrix of the relation**.

For the relation $R = \{(1, y), (1, z), (3, y)\}$ we have

	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

Fig. 1.2.2

Such matrix is called a Boolean matrix since its elements are only 0 or 1.

b) Let us write down the elements of A and the elements of B in two disjoint disks, and then draw an arrow from $a \in A$ to $b \in B$ whenever a is related to b. This picture will be called the **arrow diagram** of the relation.

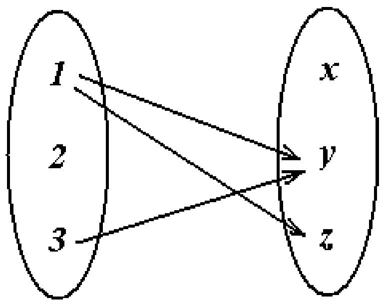


Fig. 1.2.3

D. Composition of Relations

Let A, B and C be sets, and R be a relation from A to B and let S be a relation from B to C. That is, R is a subset of $A \times B$ $(R \subset A \times B)$ and $S \subset B \times C$. Than R and S give rise to a relation from A to C denoted by RS and derived by:

$a(RS)c$ if for some $b \in B$ we have aRb and bSc.

That is, $RS = \{(a, c) \mid \text{there exists } b \in B \text{ for which } (a, b) \in \text{R and } (b, c) \in S\}$.

The relation RS is called the **combination** of R and S.

Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$ and let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$ and $S = \{(b, x), (b, z), (c, y), (d, z)\}$.
Consider the arrow diagrams of *R* and *S*:

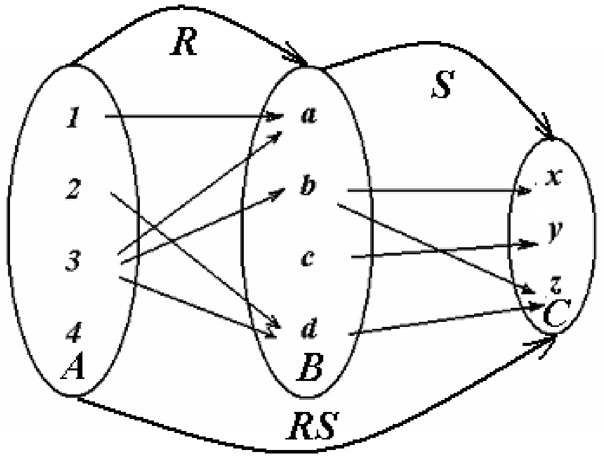


Fig.1.2.4

Observe that there is an arrow from 2 to *d* which is followed by an arrow from *d* to *z*. We can view two arrows as a "path" which "connects" the element $2 \in A$ to the element $z \in C$. Thus $2(RS)z$ since $2Rd$ and *dSz*. Similarly there is a path from 3 to *x* and a path from 3 to *z*. $3(RS)x$ and $3(RS)z$.
Accordingly $RS = \{(2, z), (3, x), (3, z)\}$.

2.4. Inverse Relation

Definition. Let *R* be any relation from a set *A* to a set *B*. The **inverse** of *R*, denoted by R^{-1}, is the relation from *B* to *A* which consists of those ordered pairs, when reversed, belong to *R*; that is,

$$R^{-1} = \{(b, a) | (a, b) \in R\}.$$

For example, let $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$. Then the inverse of $R = \{(1, y), (1, z), (3, y)\}$ is $R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$.
Clearly, if *R* is any relation, then $\left(R^{-1}\right)^{-1} = R$. Also, the domain and range of R^{-1} are equal, respectively, to the range and domain of *R*. Moreover, if *R* is a relation on *A*, then R^{-1} is also a relation on *A*.

2.5. Types of Relations

Definition. A binary relation *R* defined on an unempty set *A* is called **reflexive** if *aRa* for every $a \in A$, that is, if $(a, a) \in R$ for every $a \in A$.

Example 2.5.1. Given the following five relations.

1) Relation $\leq$ (is less than or equal to) on the set $\boldsymbol{Z}$ of integers;
2) Set inclusion $\subseteq$ on a collection C of sets;
3) Relation $\perp$ (perpendicular) on the set L of lines in a plane;
4) Relation $||$ (parallel) on the set L of lines in a plane;
5) Relation $|$ of divisibility on the set $\boldsymbol{N}$ of positive integers. (Recall $x|y$ if there exists z such that $xz = y$.)

Determine which of these relations are reflexive.

Definition. A binary relation R on a set A is called **irreflexive** if $(a,a) \notin R$ for all $a \in A$.

Definition. A binary relation R on a set A is called **symmetric** if whenever aRb then bRa, that is whenever $(a,b) \in R$ then $(b,a) \in R$.

Definition. A binary relation R on a set A is called **antisymmetric** if whenever aRb and bRa then $a = b$, that is, if $a \neq b$ and aRb then $b\cancel{R}a$

Definition. A binary relation R on a set A is called **transitve** if whenever aRb and bRc then aRc, that is, if whenever $(a,b),(b,c) \in R$ then $(a,c) \in R$.

Definition. A binary relation R on a set A is called **complete** if whenever $a \in A$ and $b \in B$ then $a = b$, or $(a,b) \in R.$, or $(b,a) \in R..$

*Example 2.5.2.*Consider the following five relations on the set $A = \{1,2,3\}$:
$R = \{(1,1),(1,2),(1,3),(3,3)\}$, $S = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$
$T = \{(1,1),(1,2),(2,2),(2,3)\}$, $\varnothing$ – empty relation, $A \times A$ – universal relation.
Determine whether or not each of the above relations on A is:
1) reflexive; 2) symmetric; 3) transitive; 4) antysymmetric.

Solution

1) R is not reflexive since $2 \in A$ but $(2,2) \notin R$. T is not reflexive since $(3,3) \notin T$ and, similarly, $\varnothing$ is not reflexive. S and $A \times A$ are reflexive.
2) R is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$, and similarly T is not symmetric. S, $\varnothing$, and $A \times A$ are symmetric.
3) T is not transitive since $(1,2)$ and $(2,3)$ belong to T, but $(1,3)$ does not belong to T. The other four relations are transitive.
4) S is not antisymmetric since $1 \neq 2$ and $(1,2)$ and $(2,1)$ both belong to S. Similarly, $A \times A$ is not antisymmetric. The other three relations are antisymmetric.

2.6. Functional Relations

Definition. A **section** $x = a$ of a set R is a set of elements $y \in B$ for which $(a, y) \in R$.. This section is denoted by $R(a)$.

Definition. Let $c = (a, b)$, where $c \in A \times B$. An element a is called a **projection** of an element c on a set A, and denoted by $\Pr_A c = a$.

Example 2.6.1. Let $A = \{a_1, a_2, a_3, a_4, a_5\}$, $B = \{b_1, b_2, b_3, b_4\}$ and the relation $R = \{(a_1, b_2), (a_1, b_4), (a_2, b_1), (a_2, b_3), (a_3, b_2), (a_3, b_3), (a_3, b_4), (a_5, b_1), (a_5, b_3)\}$ be given. Find:

1) sections $x = a_i$ $\left(i = \overline{1, 5}\right)$;
2) $\Pr_A(a_2, b_3)$ and $\Pr_A R$.

Solution.

Using the definitions of a section and a projection, we have

1) $R(a_1) = \{b_2, b_4\}$; $R(a_2) = \{b_1, b_3\}$; $R(a_3) = \{b_2, b_3, b_4\}$; $R(a_4) = \varnothing$; $R(a_5) = \{b_1, b_3\}$.
2) $\Pr_A(a_2, b_3) = a_2$; $\Pr_A R = \{a_1, a_2, a_3, a_5\}$.

Definition. A relation $R \subset A \times B$ is called a **functional relation** if for each $x \in A$ a section R with respect to x contains not more than one element $y \in B$ or none. Such relation is called a **function** from A into B and denoted by $f : A \to B$ which is read: "f is a function from A into B".

Definition. If the function f is defined on a set $D \subset A$ then this set D is called the **domain** of definition of f, or more briefly the domain of f. A subset $\mathrm{Im} \subset B$, where $\mathrm{Im} = \{f(x) | x \in D\}$ is called the **range** or **image** of f.

Definition. An element $b = f(a)$, where $a \in D$ is called an **image** of the element a, and element a is called a **prototype** of the element b.

Definition. If $D = A$, then a function f is called **everywhere defined**.

Frequently a function can be expressed by means of mathematical formula. For example, consider the function which sends each real number into its square. We can describe this function by writing

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

In the first notation, x is called a **variable** and the letter f denotes the function. In the second notation, x is called the **independent variable** and y is called the **dependent variable** since the value of y will depend on the value of x.

Every function $f : A \to B$ gives rise to a relation from A to B called the **graph** of $\boldsymbol{f}$ and denoted by

Graph of f= $\{(a, b) | a \in A, b = f(a)\}$.

2.7. One-to-one, onto, and Invertible Functions

Definition. A function $f : A \to B$ is said to be **one-to-one** if different elements in the domain *A* have distinct images.

Definition. A function $f : A \to B$ is said to be an **onto** function if each element of *B* is the image of some element of *A*.

In other words, $f : A \to B$ in onto if the image of f is the entire range, i.e. if $f(A) = B$. In such a case we say that *f* is a function from *A* onto *B* or that f **maps** *A* onto *B*.

Definition. A function $f : A \to B$ is **invertible** if its inverse relation f^{-1} is a function from *B* to *A*.

In general, the inverse relation f^{-1} may not be function.

In what follows we use the terms **injective** for one-to-one function, **surjective** for an onto function, and **bijective** for a one-to-one correspondence.

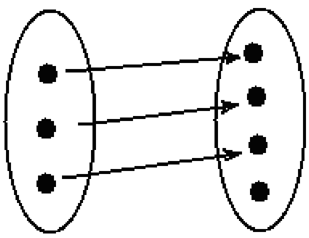


Fig.2.7.1
Injective relation

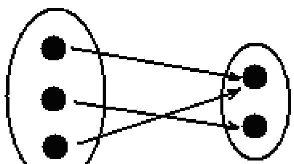


Fig.2.7.2
Surjective relation

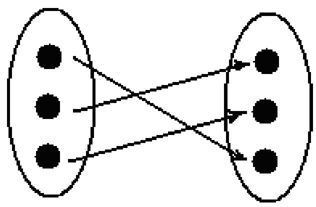


Fig.2.7.3
Bijective relation

Example 2.6.1. Let $\boldsymbol{R}$ – the set of real numbers, $\boldsymbol{R}^+$ – the set of real positive numbers, and a function $f : A \to B$.

1) If $A = B = \boldsymbol{R}$ then the function $f : x \to x^2$ gives the map of *A* onto *B* which is not surjective.
2) If $A = B = \boldsymbol{R}$ then the function $f : x \to 4x - 3$ gives the map of *A* onto *B* which is surjective.
3) If $A = \boldsymbol{R}$, $B = \boldsymbol{R}^+$ then the function $f : x \to 3^x$ gives the map of *A* onto *B* which is injective.

Consider functions $f : A \to B$ and $g : B \to C$; that is, where the range of *f* is the domain of *g*. Then we may define a new function from *A* to *C,* called the **composition** of *f* and *g* and written $g \circ f$ as follows:

$$(g \circ f)a \equiv g(f(a))$$

That is, we find the image of a under f and then find the image of $f(a)$ under *g*.

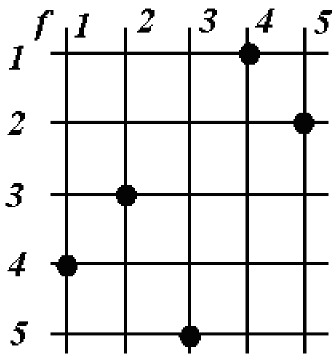
Consider any function $f: A \to B$. Then

$$f \circ I_A = f \text{ and } I_B \circ f = f,$$

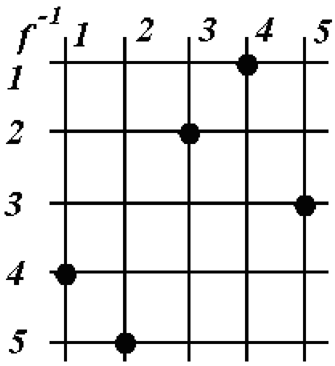
where I_A and I_B are the identity functions on A and B, respectively. The mapping defined by these formulas is called **identical**. Thus

$$I_A = \begin{bmatrix} a_1 \; a_2 \; \dots a_n \\ a_1 \; a_2 \; \dots a_n \end{bmatrix}.$$

Example 2.6.2. Let the mapping f be given by the table



then the mapping $f^{-1} \subset A \times B$ is defined by the table



The functions f and f^{-1} we write in the form

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix}, \quad f^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}.$$

Let us check the fulfillment of the conditions $I_A \circ f = f$ and $f \circ I_A = f$.

$$I_A \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} = f.$$

In the similar way we get $f \circ I_A = f$.

2.8. Ordered Sets

Definition. A binary relation R on a set A is called an **order** relation or partial order relation if it is antisymmetric and transitive.

Definition. A binary relation R on a set A is called an **nonstrict order** relation if it is reflexive, antisymmetric and transitive.

Definition. A binary relation R on a set A is called a **strict order** relation if it is antireflexive, antisymmetric and transitive.

Definition. If an order relation is total then it is called a **totally ordered** or **linearly ordered**.

A nonstrict order relation is denoted by "$\leq$ ", and strict order relation by "$<$ "; and $a \leq b$ is read "a precedes b". $a < b$ means $a \leq b$ and $a \neq b$, and is read "a strictly precedes b" or "b strictly succeeds a ".

Definition. Let A be a subset of a partially ordered set S. An element M in S is called an **upper bound** of A if M succeeds every element of A, i.e. if for every x in A, we have $x \leq M$.

Analogously, an element m in S is called a **lower bound** of a subset A of S.if m precedes every element of A, i.e. if for every y in A, we have $m \leq y$.

2.9. Suplementary Problems

2.9.1. Which of the following sets are equal?

$A = \{x : x^2 - 4x + 3 = 0\}$, $C = \{x : x \in N, x < 3\}$, $E = \{1, 2\}$, $G = \{3, 1\}$,

$B = \{x : x^2 - 3x + 2 = 0\}$, $D = \{x : x \in N, x \text{ is odd}, x < 5\}$, $F = \{1, 2, 1\}$, $H = \{1, 1, 3\}$.

2.9.2. Let $A = \{1, 2, ..., 8, 9\}$, $B = \{2, 4, 6, 8\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{3, 4, 5\}$, $E = \{3, 5\}$.
Which of above sets can equal a set X under each of the following conditions?

(a) X and B are disjont.
(b) $X \subseteq D$ but $X \not\subset B$
(c) $X \subseteq A$ but $X \not\subset C$.
(d) $X \subseteq C$ but $X \not\subset A$.

2.9.3. Let $A = \{a, b, c, d, e\}$, $B = \{a, b, d, f, g\}$, $C = \{b, c, e, g, h\}$,
$D = \{d, e, f, g, h\}$. Find:

(*a*) $A \cap B$
(*b*) $B \cap C$
(*c*) $C \setminus D$
(*d*) $A \cap (B \cup D)$
(*e*) $B \setminus (C \cup D)$
(*f*) $(A \cup D) \cap B$
(*g*) $(A \cup D) \setminus C$
(*h*) $B \cap C \cap D$
(*i*) $(C \setminus A) \setminus D$
(*j*) $A \oplus B$
(*k*) $A \oplus C$
(*l*) $(A \oplus D) \setminus B$

2.9.4. Draw a Venn diagram of sets *A, B, C* where $A \subseteq B$, sets B and C are disjoint, but A and C have elenments in common.

2.9.5. Consider the set $\boldsymbol{Q}$ of rational numbers with the order $\leq$. Consider a subset D of $\boldsymbol{Q}$ defined by $D = \{x | \ x \in \boldsymbol{Q} \text{ and } 8 < x^3 < 15\}$. Find the upper and lower bounds.

3. MATHEMATICAL LOGIC

3.1. Propositions and Compound Statements

Definition. A **proposition** (or **statement**) is a declarative statement which is true or false, but not both.

Consider, for example, the following six sentences:

1) Ice floats in water. 2) China is in Europe.
3) $2+2=4$. 4) $2+2=5$.
5) Where are you going? 6) Do your homework.

The first four are propositions, the last two are not. Also, 1) and 3) are true, but 2) and 4) are false.

With each proposition we associate a logical variable x which takes the value 1 if a proposition is true, and 0 if it is false.

Many propositions are **composite**, that is, composed of **subpropositions** and various connectives. Such composite propositions are called **compound propositions**. A proposition is said to be **primitive** if it can not be broken down into simpler propositions, that is, if it is not composite. For example the following propositions are composite: "Roses are red and violets are blue." "John is smart or he studies every night."

Propositions are denoted by capital letters $X, Y, Z, \ldots$

A compound proposition we get from primitive propositions with the help of logical operations.

Name of operation	Reading	Notation
Negation	Not	$\overline{}$
Conjunction	and	$\wedge$
Disjunction	or	$\vee$
Implication	if … then	$\rightarrow$
Equivalence	if and only if	$\leftrightarrow$
Scheffer's prime	Anticonjunction	$\mid$
Peirce's arrow	Antidisjunction	$\downarrow$
Sum taken absolutely 2	Antiequivalence	$\oplus$

Definition. A **negation** of a proposition X is a proposition $\overline{X}$ which is true when X is false and is false when X is true.

X	$\overline{X}$
0	1
1	0

Definition. A **conjunction** of two propositions X and Y is called a proposition $X \wedge Y$ which is true only in the case if X and Y are both true.

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

Definition. A **disjunction** of two propositions X and Y is called a proposition $X \vee Y$ which is true if at least one of them is true.

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

Definition. An **implication** of two propositions X and Y is called a proposition $X \to Y$ which is false if and only if when X is true and Y is false.

X	Y	$X \to Y$
0	0	1
0	1	1
1	0	0
1	1	1

Definition. An **equivalence** of two propositions X and Y is called a proposition $X \leftrightarrow Y$ which is true if and only if, when X and Y are both true or false.

X	Y	$X \leftrightarrow Y$
0	0	1
0	1	0
1	0	0
1	1	1

*Definition.***Scheffer's prime** $X \mid Y$ by definition is $X \mid Y = \overline{X \wedge Y}$. The truth table is of the form:

X	Y	$X \mid Y$
0	0	1
0	1	1
1	0	1
1	1	0

Definition. **Peirce's arrow** $X \downarrow Y$ by definition is $X \downarrow Y = \overline{X \vee Y}$.

X	Y	$X \downarrow Y$
0	0	1
0	1	0
1	0	0
1	1	0

Definition. A **sum taken absolutely 2** $X \oplus Y$ by definition is $X \oplus Y = \overline{X \leftrightarrow Y}$.

X	Y	$X \oplus Y$
0	0	0
0	1	1
1	0	1
1	1	0

3.2. Basic Laws of Logical Operations

1. Idempotency of disjunction and conjunction:

$$X \vee X \leftrightarrow X, \qquad X \wedge X \leftrightarrow X.$$

2. Commutativity of disjunction and conjunction:

$$X \vee Y \leftrightarrow Y \vee X, \qquad X \wedge Y \leftrightarrow Y \wedge X.$$

3. Associativity of disjunction and conjunction:
$$X \vee (Y \vee Z) \leftrightarrow (X \vee Y) \vee Z,$$
$$X \wedge (Y \wedge Z) \leftrightarrow (X \wedge Y) \wedge Z.$$

4. Double negation $X \leftrightarrow \overline{\overline{X}}$.

5. De Morgan laws:
$$\overline{X} \vee \overline{Y} \leftrightarrow \overline{X \wedge Y}, \qquad \overline{X} \wedge \overline{Y} \leftrightarrow \overline{X \vee Y}.$$

6. Distributivity of disjunction and conjunction operations with respect to each other:

$$X \vee (Y \wedge Z) \leftrightarrow (X \vee Y) \wedge (X \vee Z); \qquad X \wedge (Y \vee Z) \leftrightarrow (X \wedge Y) \vee (X \wedge Z).$$

7. Sewing:

$$(X \vee Y) \wedge (X \vee \overline{Y}) \leftrightarrow X; \qquad (X \wedge Y) \vee (X \wedge \overline{Y}) \leftrightarrow X.$$

8. Absorption:

$$X \vee (X \wedge Y) \leftrightarrow X; \qquad X \wedge (X \vee Y) \leftrightarrow X.$$

9. Operations with logical constants 0 and 1:

$$X \vee 0 \leftrightarrow X; \qquad X \wedge 0 \leftrightarrow 0; \qquad X \wedge \overline{X} \leftrightarrow 0;$$

$$X \vee 1 \leftrightarrow 1; \qquad X \wedge 1 \leftrightarrow X.$$

10. Law of the excluded middle: $X \vee \overline{X} \leftrightarrow 1.$

11. Identity: $X \leftrightarrow X.$

12. Negation of contradiction: $\overline{X \wedge \overline{X}} \leftrightarrow 1.$

13. Contraposition: $(X \to Y) \leftrightarrow (\overline{Y} \to \overline{X}).$

14. Chain rule: $(X \to Y) \wedge (Y \to Z) \leftrightarrow (X \to Z).$

15. Antithesis: $(X \to Y) \leftrightarrow (\overline{X} \leftrightarrow \overline{Y}).$

16. Modus ponens, which means “proposing mode”: $X \wedge (X \to Y) \to Y.$

Example 3.2.1. Suppose that the proposition X is “it is raining” and the proposition Y is “cats and dogs get wet”, then the compound proposition “ it is raining; and if it is raining, then cats and dogs get wet” logically implies that cats and dogs are really wet.

17. Modus tollense, which means “removing mode”:

$$(X \to Y) \wedge (\overline{Y}) \to \overline{X}.$$

As can be seen, it is a counterpart of **modus ponence**. For instance, in the previous example we just used for **modus ponence**, **modus tollense** would state: the compound proposition “ if it is raining; then cats and dogs get wet, and cats and dogs are not wet ” which logically implies that it is not raining.

3.3. Propositional Functions. Quantifiers

Let A be given set. A **propositional function** (or an **open sentence** or **condition**) 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 (with a truth value) whenever any element $a \in A$ is substituted for the variable x. The set A is called the domain of $p(x)$, and the set T_p of all elements of A which $p(a)$ is true is called the **truth set** of $p(x)$. In other words,

$$T_p = \{x \mid x \in A, p(x) \text{ is true}\} \text{ or } T_p = \{x \mid p(x)\}.$$

Frequently, when A is some set of numbers, the condition $p(x)$ has the form of an equation or inequality involving the variable x.

Example 3.3.1. Find the truth set for each propositional function $p(x)$ defined on the set $\boldsymbol{N}$:

1. Let $p(x)$ be "$x+2>7$". Its truth set is $\{6,7,8,...\}$ consisting of all integers greater than 5.
2. Let $p(x)$ be "$x+5<3$". Its truth set is the empty set Ø. That is, $p(x)$ is not true for any integer in $\boldsymbol{N}$.
3. Let $p(x)$ be "$x+5>1$". Its truth set is $\boldsymbol{N}$. That is, $p(x)$ is true for every element in $\boldsymbol{N}$.

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

$$(\forall x \in A)p(x) \text{ or } \forall x p(x) \tag{3.3.1}$$

which reads "For every x in A, $p(x)$ is a true statement" or, simply, "For all x, $p(x)$". The symbol $\forall$ which reads "for all" or "for every" is called the **universal quantifier**. The statement (3.3.1) is equivalent to the statement

$$T_p = \{x \mid x \in A, p(x)\} = A \tag{3.3.2}$$

that is, that the truth set of $p(x)$ is the entire set A.

The expression $p(x)$ by itself is an open sentence or condition and therefore has no truth value. However, $\forall x p(x)$, that is $p(x)$ preceded by the quantifier $\forall$, does have a truth value which follows from the equivalence of (3.3.1) and (3.3.2). Specifically:

If $\{x \mid x \in A, p(x)\} = A$ then $\forall x p(x)$ is true, otherwise, $\forall x p(x)$ is false.

Example 3.3.2.

1. The proposition $(\forall n \in \boldsymbol{N})(n+4>3)$ is true since $\{n \mid n+4>3\} = \{1,2,3,...\} = \boldsymbol{N}$.
2. The proposition $(\forall n \in \boldsymbol{N})(n+2>8)$ is false since $\{n \mid n+2>8\} = \{7,8,9,...\} \neq \boldsymbol{N}$.
3. The symbol $\forall$ can be used to define the intersection of an indexed collection $\{A_i \mid i \in I\}$ of sets A_i as follows:

$$\cap(A_i \mid i \in I) = \{x \mid \forall i \in I, x \in A_i\}.$$

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

$$(\exists x \in A)p(x) \text{ or } \exists x\, p(x) \qquad (3.3.3)$$

which reads "There exists an x in A such that $p(x)$ is a true statement" or, simply, "For some x, $p(x)$". The symbol $\exists$ which reads "there exists" or "for some" or "for at least one" is called the **existential quantifier**. The statement (3.3.3) is equivalent to the statement

$$T_p = \{x \mid x \in A, p(x)\} \neq \varnothing \qquad (3.3.4)$$

i.e., that the truth set of $p(x)$ is not empty. Accordingly, $\exists x\, p(x)$, that is $p(x)$ preceded by the quantifier $\exists$, does have a truth value. Specifically:

If $\{x \mid x \in A, p(x)\} \neq \varnothing$ then $\exists x p(x)$ is true, otherwise, $\exists x p(x)$ is false.

Example 3.3.2.

1. The proposition $(\exists n \in \boldsymbol{N})(n + 4 < 7)$ is true since $\{n \mid n + 4 > 3\} = \{1, 2\} \neq \varnothing$.
2. The proposition $(\exists\, n \in \boldsymbol{N})(n + 6 < 4)$ is false since $\{n \mid n + 6 < 4\} = \varnothing$.
3. The symbol $\exists$can be used to define the union of an indexed collection $\{A_i \mid i \in I\}$ of sets A_i as follows:

$$\cup (A_i \mid i \in I) = \{x \mid \exists i \in I, x \in A_i\}.$$

4. BOOLEAN ALGEBRA

4.1. Boolean Functions

Definintion. A function $f(x_1, x_2, ..., x_n)$ which takes one of two values 0 or 1 of n variables each of those also assumes one of two values 0 or 1 is called a **Boolean function.**

Two Boolean functions are said to be equal if for any tuple of values these two functions take equal values.

We have four Boolean functions of one variable and sixteen functions of two variables. 2^{2^n} is the number of Boolean functions of n variables.

Let us consider truth tables of functions of one and two variables.

x	φ_0	φ_1	φ_2	φ_3
0	0	0	1	1
1	0	1	0	1

Table4.1.1

Functions $\varphi_0(x)$ and $\varphi_3(x)$ are called **constants** respectively 0 and 1.

The function $\varphi_1(x)$ coincides with a variable x and is called **identical**, that is $\varphi_1(x) = x$.

The function $\varphi_2(x)$ takes the values opposite to those of x, and is called a **negation** of x denoted by $\overline{x}$: $\varphi_2(x) = \overline{x}$.

The truth table of a function of two variables is of the form:

x_1	x_2	ψ_0	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6	ψ_7	ψ_8	ψ_9	ψ_{10}	ψ_{11}	ψ_{12}	ψ_{13}	ψ_{14}	ψ_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Operation		0	$\wedge$	$\leftarrow$	x_1	$\overline{x}_1 \wedge x_2$	x_2	$\oplus$	$\vee$	$\downarrow$	$\leftrightarrow$ $\sim$	$\overline{x}_2$	$x_1 \vee \overline{x}_2$	$\overline{x}_1$	$\rightarrow$	$\vert$	1

Table 4.1.2

1. The functions ψ_0 and ψ_{15} are constants.
2. The functions ψ_3, ψ_5, ψ_{10} and ψ_{12} essentially depend on one variable: $\psi_3 = x_1$, $\psi_5 = x_2$, $\psi_{10} = \overline{x_2}$, $\psi_{12} = \overline{x_1}$.
3. The function $\psi_1 = x_1 \wedge x_2$ is called **conjunction**.
4. The function $\psi_7 = x_1 \vee x_2$ is called **disjunction**.
5. The function $\psi_9 = x_1 \leftrightarrow x_2$, or $x_1 \sim x_2$ is called **equivalence**.
6. The function $\psi_6 = x_1 \oplus x_2$ is called the **sum taken absolutely 2**.
7. The function $\psi_{11} = x_2 \rightarrow x_1$ is called **conversion**.
8. The function $\psi_{13} = x_1 \rightarrow x_2$ is called **implication**.
9. The function $\psi_{14} = x_1 | x_2$ is called **Scheffer's prime**.
10. The function $\psi_8 = x_1 \downarrow x_2$ is called **Peirce's arrow**.
11. The functions ψ_2 and ψ_4 are called **exclusion's functions**.

4.2. The Properties of Elementary Boolean Functions

1. The functions: conjunction, disjunction, sum taken absolutely 2, Scheffer's prime, Peirce's arrow are commutative.
2. The functions: conjunction, disjunction, sum taken absolutely 2 are associative, and distributive.
3. De Morgan law: $\overline{x_1 \wedge x_2} = \overline{x_1} \vee \overline{x_2}$, $\overline{x_1 \vee x_2} = \overline{x_1} \wedge \overline{x_2}$.
4. Double negation: $\overline{\overline{x}} = x$.
5. A disjunction expressed in terms of conjunction and sum taken absolutely 2:
$$x_1 \vee x_2 = x_1 \wedge x_2 \oplus x_2 \oplus x_1 .$$
6. A disjunction expressed in terms of implication:

$$x_1 \vee x_2 = (x_1 \to x_2) \to x_2 .$$

7. A negation expressed in terms of Scheffer's prime, Peirce's arrow, sum taken absolutely 2, and equivalence:
$$x \mid x = x \downarrow x = \overline{x} = x \oplus 1 = x \leftrightarrow 0 .$$

8. A conjunction expressed in terms of Scheffer's prime:
$$x_1 \wedge x_2 = (x_1 | x_2) | (x_1 | x_2).$$

9. A disjunction expressed in terms of Peirce's arrow:
$$x_1 \vee x_2 = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2).$$

10. An absorption law: $x_1 \wedge (x_1 \vee x_2) = x_1$.

11. A sewing law: $\overline{x} \vee x = \overline{x} \oplus x = 1$.

12. The following identities for conjunction, disjunction, and sum taken absolutely 2 are valid:

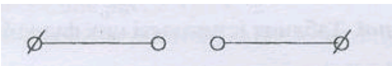
$x \wedge x = x$; $\quad x \vee x = x$; $\quad x \oplus x = 0$;

$\overline{x} \wedge x = 0$; $\quad \overline{x} \vee x = 1$; $\quad x \oplus \overline{x} = 1$;

$x \wedge 0 = 0$; $\quad x \vee 0 = x$; $\quad x \oplus 0 = x$;

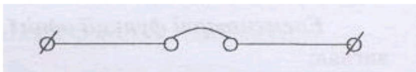
$x \wedge 1 = x$; $\quad x \vee 1 = 1$; $\quad x \oplus 1 = \overline{x}$.

Technical Realization of Functions of One Variable



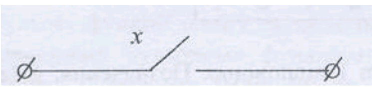
$\varphi_0 = 0$

Constant 0



$\varphi_3 = 1$

Constant 1



$\varphi_1 = x$

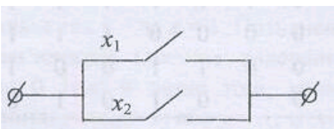
Identical

$\varphi_2 = \overline{x}$

Negation

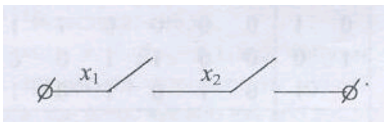
Fig.4.3.1

Technical Realization of Functions of Two Variables



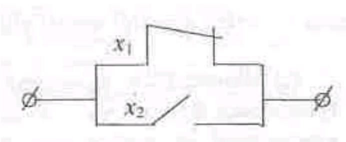
$\psi_7 = x_1 \vee x_2$

Disjunction

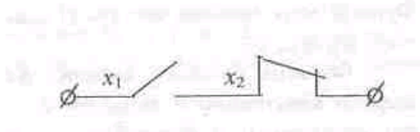


$\psi_1 = x_1 \wedge x_2$

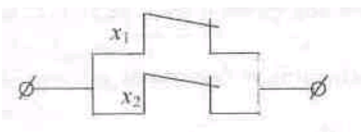
Conjunction



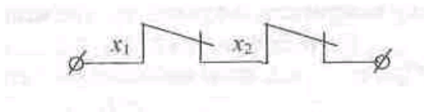
$\psi_{13} = x_1 \to x_2$
Implication



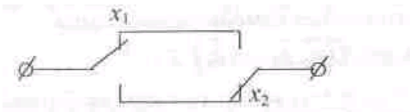
$\psi_2 = x_1 \leftarrow x_2$



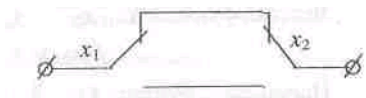
$\psi_{14} = x_1 | x_2$
Scheffer's prime



$\psi_8 = x_1 \downarrow x_2$
Peirce's arrow



$\psi_6 = x_1 \oplus x_2$
Sum taken absolutely 2



$\psi_9 = x_1 \leftrightarrow x_2$
Equivalence

Fig.4.3.2.

4.4. Total Systems of Functions. Basis

Definition. A system of functions of logic algebra $\{\varphi_1, \varphi_2 ..., \varphi_n\}$ is called **total system**, if any function of logic algebra can be expressed in terms of the superposition of these functions.

In addition this system of functions is said to be a **basis** of the logic space.

Definition. A logic function $f^*(x_1, x_2, ..., x_n)$ is called a **duel function** to a function $f(x_1, x_2, ..., x_n)$ if $f^*(x_1, x_2, ..., x_n) = \overline{f}(\overline{x}_1, \overline{x}_2, ..., \overline{x}_n)$.

For example, $\psi_2 = x_1 \wedge x_2$ is duel to $\psi_8 = x_1 \vee x_2$, as $x_1 \wedge x_2 = \overline{\overline{x}_1 \wedge \overline{x}_2}$.

Definition. A function f is called a **self-duel function** if $f^*(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$.

For example the function $f(x_1, x_2, x_3) = x_1 \cdot x_2 + x_3 \cdot x_2 + x_1 \cdot x_3$ is the self-duel function as $x_1 \cdot x_2 + x_3 \cdot x_2 + x_1 \cdot x_3 = \overline{\overline{x}_1 \cdot \overline{x}_2 + \overline{x}_3 \cdot \overline{x}_2 + \overline{x}_1 \cdot \overline{x}_3}$. To check it consider the truth table.

Definition. A function $f(x_1, x_2, ..., x_n)$ is called a **monotonous function** if for any tuples $(x_1', x_2', ..., x_n')$ and $(x_1'', x_2'', ..., x_n'')$ such that $x_i'' \geq x_i', i = \overline{1, n}$ the inequality $f(x_1'', x_2'', ..., x_n'') \geq f(x_1', x_2', ..., x_n')$ takes place .

Definition. A function $f(x_1, x_2, ..., x_n)$ is called a **linear function** if it can be reduced to a polynomial: $f(x_1, x_2, ..., x_n) = c_0 \oplus c_1 x_1 \oplus c_2 x_2 \oplus ... \oplus c_n x_n$, where $c_i = \{0, 1\}, i = \overline{1, n}.$

For example the function $\varphi_7(x_1, x_2) = x_1 \oplus x_2$ is the linear function.

Post's theorem. A system of functions is total if, and only if this system contains at least one function that does not preserve 1, does not preserve 0, not self-dual, not monotonous and is not linear.

For example, Boolean algebra is constructed on the following system of functions $\{\overline{\ \ }, \wedge, \vee\}$ but Zhegalkin algebra on such basis $\{1, \wedge, \oplus\}$.

4.5. Normal Forms of Boolean Functions

Definition. **Elementary conjunction** is a conjunction of any number of Boolean variables taken with negation or without it in which each variable occurs not more than one time.

An elementary conjunction containing none variable we assume the constant 1.

Example 4.5.1. Elementary conjunctions for a function of one variable might be $y, \bar{z}$; for a function of two variables – $\bar{x} \wedge y, x \wedge \bar{z}$.

Definition. By a **disjunctive normal form** (**DNF**) we mean a formula represented in the form of a disjunction of elementary conjunctions.

Example 4.5.2. **DNF** :$(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2}) \vee (x_3 \wedge x_2) \vee \overline{x_3}$.

Definition. An elementary conjunction $x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge ... \wedge x_n^{\sigma_n}$ is called a **constituent** of unit of a function $f(x_1, x_2, ..., x_n)$ if $f(\sigma_1, \sigma_2, ..., \sigma_n) = 1$, that is an interpretation reducing the given elementary conjunction into unit, turns also a function f into 1.

Example 4.5.3. The elementary conjunction $x_1 \wedge \overline{x_2}$ is the constituent of a function of two variables $f(x_1, x_2)$ on the interpretation $(1, 0)$ since $x_1 \wedge \overline{x_2} = x_1^1 \wedge x_2^0$ and $x_1 \wedge \overline{x_2} = 1$.

The elementary conjunction $x_1 \wedge x_2 \wedge x_3$ is the constituent of unit of a function of three variables $f(x_1, x_2, x_3)$ on the interpretation $(1, 1, 1)$ since $x_1 \wedge x_2 \wedge x_3 = x_1^1 \wedge x_2^1 \wedge x_3^1$ and $x_1 \wedge x_2 \wedge x_3 = 1$.

Definition. A formula represented in the form of disjunction of constituents of unit of the given function is called a **perfect disjunction normal form** (**PDNF**).

Definition. An **elementary disjunction** is a disjunction of any number of Boolean variables taken with negation or without it in which, each variable occurs not more than one time.

Elementary disjunction, containing none variables we assume the constant 0.

Definition. A formula represented in the form of a conjunction of elementary disjunctions is called a **conjunction normal form** (***CNF***).

Example 4.5.4. $(\bar{x}_1 \vee x_2 \vee x_3) \vee (x_1 \vee \bar{x}_3) \wedge x_2$ – *CNF*.

Definition. An elementary disjunction $x_1^{\bar{\sigma}_1} \vee x_2^{\bar{\sigma}_2} \vee \ldots \vee x_n^{\bar{\sigma}_n}$ is called a **constituent** of **zero** of a function $f(x_1, x_2, \ldots, x_n)$ if $f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$, that is an interpretation reducing given elementary disjunction into zero turns also a function f into zero.

Example 4.5.5. The elementary disjunction $x \vee \bar{y}$ is a constituent of zero of a function $f(x, y)$on the interpretation $(0, 1)$, since $x \vee \bar{y} = x^1 \vee y^0 = x^{\bar{0}} \vee y^{\bar{1}}$, therefore on interpretation $(x, y) = (0, 1)$we have the equality $x \vee \bar{y} = 0$.

Definition. A formula represented in the form of conjunction of constituents of zero of the given function is called a **perfect conjunction normal form** (***PCNF***).

4.6. Zhegalkin Algebra

Definition. The algebra $(B, \wedge, \oplus, 0, 1)$ formed by the set $B = \{0, 1\}$ together with operations $\wedge, \oplus$ and constants 0, 1 is called **Zhegalkin algebra**.

The basic laws of this algebra are:

1. Commutative laws: $x_1 \oplus x_2 = x_2 \oplus x_1$; $x_1 \wedge x_2 = x_2 \wedge x_1$.
2. Associative laws: $x_1 \oplus (x_2 \oplus x_3) = (x_1 \oplus x_2) \oplus x_3$;
   $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3$.
3. Distributive law: $x_1 \wedge (x_2 \oplus x_3) = (x_1 \wedge x_2) \oplus (x_1 \wedge x_3)$.
4. Idempotent law: $x \wedge x = x$.
5. Operations with constants: $x \wedge 0 = 0$, $x \wedge 1 = x$.

Definition. **Zhegalkin polynomial** is a finite sum taken absolutely 2 mutually distinct elementary conjunctions over a set of variables $\{x_1, x_2, ..., x_n\}$.

Example 4.6.1. 1) Zhegalkin polynomial of constant is equal to this constant.

2) $f(x) = a_0 \oplus a_1 x.$
3) $f(x_1, x_2) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_{12}(x_1 \wedge x_2).$

Theorem. Each Boolean function $f(x_1, x_2, ..., x_n)$ can be represented in the form of Zhegalkin polynomial in a unique way up to order of summands.

Definition Boolean function is called linear if its Zhegalkin polynomial does not contain conjunctions of variables, that is its Zhegalkin polynomial is of the form $a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n$.

4.7. Minimization of Functions

Definition. **Implicant** of a function f is a function g such that on all interpretations on which g is unit, f is also unit.

Definition. A set S consisting of implicants of f is called a **covering** of f if each unit value of f is covered by 1 at least by one implicant of a set S.

Definition. Any elementary conjunction A entering elementary conjunction B and containing less variables than B is called a **fundamental part** of a conjunction B, and it is said that conjunction A is covering a conjunction B.

Definition. A **simple implicant** of a function f is such conjunction implicant, that none of its fundamental part is not implicant of the given function.

A set if all simple implicants forms a covering of the given function.

Definition. The disjunction of all simple implicants of a function is called a **reduced *DNF*.**

Definition. The **disjunctive core** of Boolean function f is such set of its simple implicants which forms a covering of f, but after removal of any implicant it loses this property, that is, ceases to be total system of implicants.

Definition. By a **deadlock *DNF*** we mean a *DNF* of the given Boolean function f consisting only of simple implicants.

Definition. The **minimal *DNF* (*MDNF*)** of the given Boolean function f is called one of its deadlocks *DNF* to which there corresponds the least value of the minimization criterion of *DNF*.

To find a set of simple implicants of the given *PDNF* are used the following operations:

1. The operation of incomplete disjunctive sewing:
$$Ax \vee A\bar{x} = A \vee Ax \vee A\bar{x}.$$
2. The operation of disjunctive absorbtion
$$A \vee Ax = A.$$

In these cases A is some elementary conjunction of variables, x is Boolean variable.

Performing these two operations successively we get so called operation of **total disjunctive sewing**:
$$Ax \vee A\bar{x} = A.$$

Example 4.7.1. Let us have a function *f*, given by *PDNF*
$$f(x,y,z) = xyz \vee \bar{x}yz \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y}\bar{z}.$$
Performing total sewing operations we obtain
$$f(x,y,z) = xyz \vee \bar{x}yz \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y}\bar{z} = (xyz \vee \bar{x}yz) \vee (\bar{x}yz \vee \bar{x}\bar{y}z) \vee (\bar{x}\bar{y}z \vee \bar{x}\bar{y}\bar{z}) =$$
$$= yz \vee \bar{x}z \vee \bar{x}\bar{y}.$$
Working sewing operations in other way we get
$$f(x,y,z) = (xyz \vee \bar{x}yz) \vee (\bar{x}\bar{y}z \vee \bar{x}\bar{y}\bar{z}) = yz \vee \bar{x}\bar{y}.$$
In both cases we have two deadlock *DNF*. The second deadlock *DNF* is simpler than the first one since it contains lesser variables and operations.

4.8. Minimization of Functions by Quine-Mc Cluskey Method

This method was suggested by Quine and improved by Mc Cluskey.

Quien's algorithm consists of following:

1. Write out *PDNF* of the given function.
2. Perform all possible operations of incomplete disjunctive sewing. Resulting formula is a disjunction of all possible implicants of the given function.
3. Perform all possible operations of disjunctive absorbtion. Resulting formula is the reduced *DNF* of the given function.
4. Form an implicant table and find a disjunctive core.
5. Simplify an implicant table by means of removal of rows corresponding to implicants of a disjunctive core and columns corresponding to such constituents of unit which are covered by core implicants.
6. Find all deadlock *DNF* of the given function.
7. Find the minimal *DNF*.

Example 4.7.2. Using Quien's method find the minimal *DNF* of the following function: $f(x,y,z) = xyz \vee x\bar{y}\bar{z} \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee x\bar{y}\bar{z}\bar{}.$

Solution.

Perform all possible operations of disjunctive sewing and absorbtion:
$$xyz \vee \bar{x}yz = yz, \quad x\bar{y}\bar{z} \vee x\bar{y}z = \bar{y}z, \quad xyz \vee x\bar{y}z = xz, \quad x\bar{y}z \vee x\bar{y}\bar{z} = x\bar{y}.$$
Now we get the following formula:

$f(x,y,z) = xyz \vee x\bar{y}\bar{z} \vee \bar{x}yz \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y}\bar{z} = yz \vee \bar{y}\bar{z} \vee \bar{x}z \vee \bar{x}\bar{y}$.

This formula is the reduced *DNF* of the given function. Now let us form an implicant table. Its rows are given by simple implicants, and its columns are given by constituents of unit of the function. Each cell of the table is denoted by asterisk for which implicant of a row is a fundamental part of a constituent of a column.

Implicant table of the function $f(x,y,z)$

	xyz	$x\bar{y}\bar{z}$	$\bar{x}yz$	$\bar{x}\bar{y}z$	$\bar{x}\bar{y}\bar{z}$
yz	*		*		
$\bar{y}\bar{z}$		*			*
$\bar{x}z$			*	*	
$\bar{x}\bar{y}$				*	*

Table 4.7.1.

Find a disjunctive core. It consists of each simple implicant which is unique in the covering by some constituent of unit. In the implicant table the columns contain one sign $*$ corresponding to constituents of unit xyz and $x\bar{y}\bar{z}$ opposite to implicants yz and $\bar{y}\bar{z}$. These simple implicants form the disjunctive core.

Let us form the simplified implicant table. To do this we delete in the implicant table rows corresponding to implicants of the disjunctive core, and columns corresponding to the constituents of unit which are covered by core's implicants. In the given case the core's implicants are covering all constituents of unit, exept one, therefore the simplified implicant table has the following form:

Simplified implicant table

	$\bar{x}\bar{y}z$
$\bar{x}z$	*
$\bar{x}\bar{y}$	*

Table 4.7.2.

From this table we find that the deadlock *DBF's* of the given function include the implicant $\bar{x}z$ or $\bar{x}\bar{y}$ except the disjunctive core.

Thus we get two deadlock *DNF* of the given function:

DNF 1: $f(x,y,z) = yz \vee \bar{y}\bar{z} \vee \bar{x}z$;

DNF 2: $f(x,y,z) = yz \vee \bar{y}\bar{z} \vee \bar{x}\bar{y}$.

In the capacity of the minimal *DNF* we choose *DNF* 1 which contains less signs of negation's operations.

5. GRAPH THEORY

5.1. Definitions.

A graph *G* consists of two things:

1) A finite nonempty set $X = \{x_1, x_2, ..., x_n\}$ whose elements are called **vertices** of a graph.
2) A definite set *U* of unordered pairs of distinct vertices called **edges** of *G*.

We denote such a graph by $G(X, U)$, when we want to emphasize the two parts of *G*.

Definition. A graph *G* is a finite set of points called vertices together with a finite set of edges, each of which joins a pair of vertices.

An edge joining a vertex to itself is called a **loop** (*Fig.5.1.3*).

Vertices are represented by dots, the edges – by straight or curved line segments.

Example 5.1.1. Let a graph $G = (X, U)$ be given, where $X = \{x_1, x_2, x_3, x_4, x_5\}$, $U = \{\{x_1, x_2\}, \{x_2, x_3\}, \{x_3, x_4\}, \{x_4, x_5\}\}$

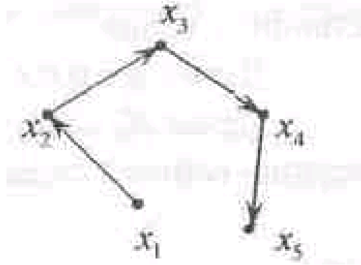


Fig.5.1.1

A pair of vertices in a graph may be joined by more than one edge, In this case we say that we have a **multiple edge**.

Definition. A graph with multiple edges is called a **multigraph** (*Fig.5.1.2*).

Definition. A graph without multiple edges and loops is called a **simple graph** (*Fig.5.1.3*).

Definition. A graph with multiple edges and loops is called a **pseudograph** (*Fig.5.1.5*)

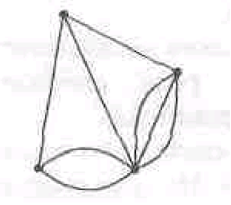


Fig.5.1.2

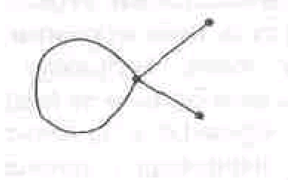


Fig.5.1.3

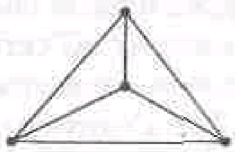


Fig.5.1.4

Fig.5.1.5

Definition. Vertices x and y are said to be **adjacent** if there is an edge $u=(x,y)$.

Definition. The edge $u=(x,y)$ is said to be **incident** on each of its endpoints x and y.

We denote a number of vertices of a graph by n, and number of edges – by m, that is $|X|=n$, $|U|=m$.

Such numbers are called the basic number characteristics of a graph.

Definition. The **degree** of vertex x in a graph G, written $deg(x)$ or $\delta(x)$ is a number of edges in G which are incident on x.

Definition. A vertex of degree zero is called an **isolated** vertex.

Definition. A vertex of degree unit is called an **overhanged** or **terminal** vertex.

Graph with isolated vertex x

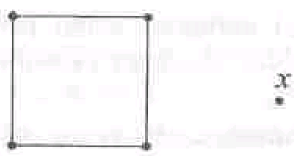


Fig.5.1.6

Graph with terminal vertex x

Fig.5.1.7

Definition. A vertex is said to be **even** or **odd** according as its degree is an even or an odd number.

The following two statements are valid.

Theorem 5.1.1. The sum of the degrees of the vertices of a graph G is equal to twice the number of edges in G.

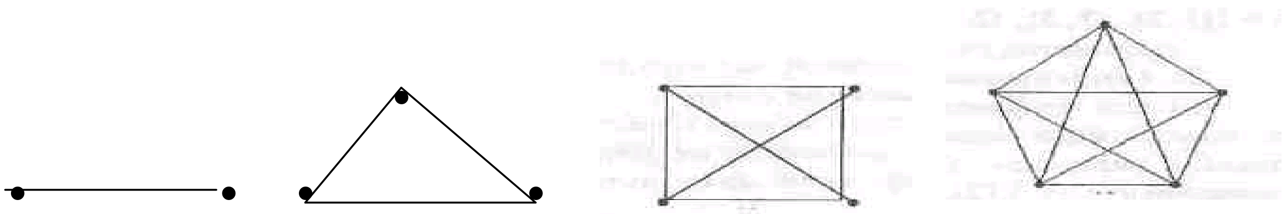
Theorem 5.1.2. The number of vertices which gave an odd degree is even.

These theorems are given without proof.

Definition. A graph which does not have edges is called an **empty graph** and denoted by Ø: U = Ø. All vertices of this graph are isolated.

Definition. A graph G is said to be **complete** if every vertex in G is connected to every other vertex in G.

Examples of complete graphs are given in Fig.5.1.7



K_2 K_3 K_4 K_5

Fig.5.1.7

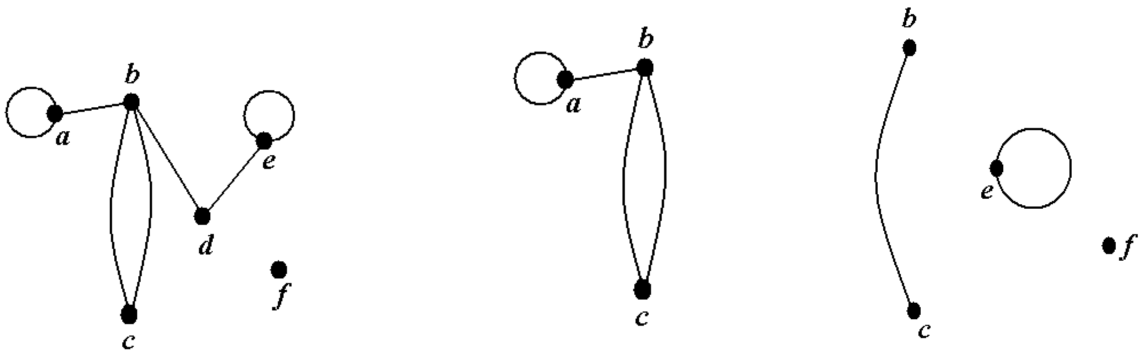
For each vertex of a complete graph we have $\delta(x) = n - 1$.

5.2. Subgraphs

Consider a graph $G = (X, U)$.

Definition. A graph $G_1 = (X_1, U_1)$ is called a **subgraph** of *G* if the vertices and edges of G_1 are contained in the vertices and edges of *G*, that is $X_1 \subseteq X$ and $U_1 \subseteq U$.

Subgraphs of the graph *G:*



Graph *G* Subgraph G_1 Subgraph G_2

Fig.5.2.1

Definition. A graph $G_1 = (X_1, U_1)$ is called an **idgraph** if $X_1 = X$ and $U_1 \subseteq U$.

5.3. Directed Graphs

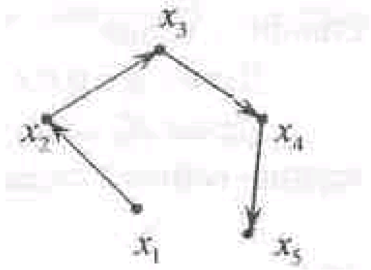
Definition. A **directed graph** or a **digraph** is a graph with directed edges.

In this case a set *U* consists of ordered pairs of vertices. Elements of *U* are called **arcs**.

Example 5.3.1. Let us consider the directed graphs

a) $G_1=(X_1,U_1)$ where $X_1=\{x_1,x_2\}$; $U_1=\{(x_2,x_1)\}$;
b) $G_2=(X_2,U_2)$ where $X_2=\{x_1,x_2,x_3,x_4,x_5\}$; $U=\{(x_1,x_2),(x_2,x_3),(x_3,x_4),(x_4,x_5)\}$.

a) Directed graph G_1



b) Directed graph G_2

Fig.5.3.1

For directed graphs we introduce semidegrees: positive semidegree $\delta_+(x)$ and negative semidegee $\delta_-(x)$.
$\delta_+(x)$ is a number of arcs which go into a vertex *x;*
$\delta_-(x)$ is a number of arcs which go out of a vertex *x*.

5.4. The Ways of Representation of Graphs

1. A finite graph can be given by listing its elements.
 For example,
$G=(X,U)$: $X=\{1,2,3,4,5,6,7,8\}$, $U=\{(1,2),(2,3),(2,4),(1,4),(3,4),(4,5),(6,6),(6,7)\}$.
2. Matrix representation of graph
 Let us consider a digraph $G=(X,U)$, where $X=\{x_1,x_2,\ldots,x_n\}$,
 $U=\{u_1,u_2,\ldots,u_m\}$.

This finite directed graph can be represented by an adjacency matrix.

Definition. By an **adjacency matrix** of a digraph *G* we mean a square matrix $A(G)=(a_{ij})$ of order *n*, where

$$a_{ij}=\begin{cases}1, \text{ if } (x_i,x_j)\in U;\\ 0, \text{ if } (x_i,x_j)\notin U.\end{cases}$$

Definition. By an **incidence matrix** of a digraph *G* we mean a matrix $B(G)=(b_{ij})$ of dimension $n\times m$, where

$$b_{ij}=\begin{cases}1, \text{ if a vertex } x_i \text{ is the end of an arc } u_j;\\ -1, \text{ if a vertex } x_i \text{ is the begining of an arc } u_j;\\ 0, \text{ if a vertex } x_i \text{ is not incidental with an arc } u_j.\end{cases}$$

Example 5.4.1. Consider the digraph G in *Fig.5.4.1.*

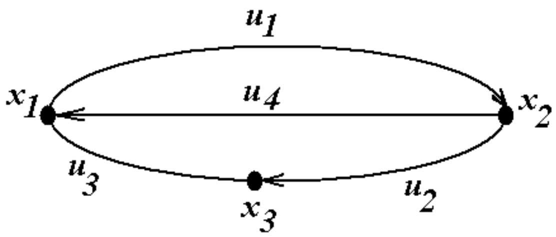


Fig.5.4.1

The adjacency matrix of this graph has the form

$$A(G)=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \end{array}$$

The incidence matrix is of the form

$$B(G)=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \end{array} \\ \begin{pmatrix} -1 & 0 & 1 & 1 \\ 1 & -1 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix} \end{array}.$$

Consider now a finite nondirected graph $G=(X,U)$. $X=\{x_1,x_2,...,x_n\}$, $U=\{u_1,u_2,..., u_m\}$.

Definition. By an **adjacency matrix** of this graph we mean a square matrix $A(G)=(a_{ij})$ of order *n*, where

$$a_{ij}=\begin{cases}1, \text{ if } (x_i,x_j)\in U;\\ 0, \text{if } (x_i,x_j)\notin U.\end{cases}$$

Definition. By an **incidence matrix** of a graph G we mean a matrix $B(G)=(b_{ij})$ of dimension $n\times m$, where

$$b_{ij}=\begin{cases}1, \text{ if a vertex } x_i \text{ is incidental with an edge } u_j;\\ 0, \text{ if a vertex } x_i \text{ is not incidental with an edge } u_j.\end{cases}$$

Example 5.4.2. Consider the graph G in *Fig.5.4.2.*

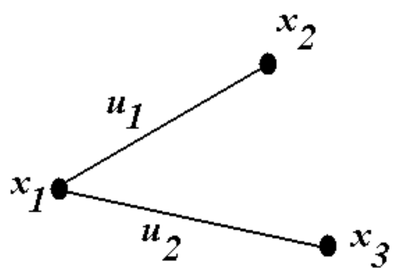


Fig. 5.4.2

The adjacency matrix of this graph is of the form $A(G)= \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$

The incidence matrix has the form $B(G)= \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cc} u_1 & u_2 \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}.$

It is possible to extend the definitions of $A(G)$ and $B(G)$ for multygraphs and pseudographs

Graph	Digraph
Adjacency matrix $A(G)=(a_{ij})$	
$a_{ij}=\begin{cases} 0, \text{if } x_i, x_j \text{ are not adjacent} \\ n, \text{if } x_i, x_j \text{ are adjacent } n \text{ times} \end{cases}$	$a_{ij}=\begin{cases} 0, \text{if } x_i x_j \notin U \\ n, \text{if } x_i x_j \in U \ n \text{ times} \end{cases}$
Incedence matrix $B(G)=(b_{ij})$	
$b_{ij}=\begin{cases} 0, \text{if } x_i \text{ is not incedence with } u_j \\ 1, \text{if } x_i \text{ is incedence with } u_j \\ \alpha, \text{if } u_j \text{ is a loop} \end{cases}$	$b_{ij}=\begin{cases} -1, \text{if } x_i \text{ is initial point of } u_j \\ 1, \text{if } x_i \text{ is end point of } u_j \\ 0, \text{if } x_i \text{ is not incedence with } u_j \\ \alpha, \text{if } u_j \text{ is a loop} \end{cases}$

5.5. Isomorphic Graphs

Definition. Two graphs $G_1 = (X_1, U_1)$ and $G_2 = (X_2, U_2)$ are said to be equal or **isomorphic** if they have the same number of vertices, the same number of edges, and if the vertices (respectively, edges) of G_1 may be put into one-to-one correspondence with the vertices (respectively, edges) of G_2 in such a way that if edge u of G_1 corresponds to edge v of G_2 and the end points of u are x_i and x_j then the end points of v are the vertices corresponding to x_i and x_j.

Example 5.5.1. The graphs represented in *Fig.5.5.1* are isomorphic.

Fig.5.5.1

5.6. Types of Graphs

Definition. A **walk** in a multigraph G is an alternating sequence of vertices and edges of the form

$$x_0 u_1 x_1 u_2 x_2 \ldots x_{n-1} u_n x_n$$

where each edge u_i contains the vertices x_{i-1} and x_i. The number n of edges is called the **length** of the walk.
The walk is said to be **closed** if $x_0 = x_n$.

Definition. A walk in which all edges are distinct is called a **trail**. A closed trail is called a **cycle**. A cycle of k length is called a ***k – cycle***.

Definition. A walk in which all vertices are distinct is called a **simple walk**.
Definition. A cycle in which all vertices (except the end points) are distinct is called a **simple cycle**.
Directed walks are defined by analogy.

Definition. A walk, which does not contain recurring arcs**,** is called a **path**.

Definition. A walk, which does not contain recurring vertices is called a **simple path**.

Definition. A closed path is called a **contour**, and a closed simple path is called a **simple contour**.

Definition. A graph without cycles is called an **acyclic graph (**digraph – **noncounter)** otherwise a graph is called a **cyclic graph** (digraph – **contour**).

Let us agree with the statement: that each vertex joining to itself by a walk of length 0 and this walk is a simple cycle. Such cycle is called a **null cycle**.

The following statements are true:

1. Given a walk *S*. If this walk is not a closed walk then it contains a simple trail with the same ends.

2. Each closed walk *C* contains a simple cycle.

5.7. Connectedness. Connected Components

Consider a nonoriented graph $G(X,U)$.

Definition. A vertex *a* is said to be connected to a vertex *b* if there exists a walk which joins these verteces.

Definition. A graph $G(X,U)$ is said to be **connected** if there is a walk between any two of its vertices.

There exists such decomposition of a set of vertices of X

$(1)\quad X = X_1 \cup X_2 \cup ... \cup X_p, \quad X_i \cap X_j = \varnothing$, if $i \neq j$.

X_i are mutually nonintersecting subsets and all vertices of one set X_i are connected to each other, and vertices of distinct sets X_i are not connected.

$(2)\quad U = U_1 \cup U_2 \cup ... \cup U_p, \quad U_i \cap U_j = \varnothing$, if $i \neq j$.

Then, according to (1) and (2) we have the direct decomposition

$(3)\quad G = G_1 \cup G_2 \cup ... \cup G_p,$

where $G_1 = (X_1, U_1), \quad G_2 = (X_2, U_2), \dots, \quad G_p = (X_p, U_p)$ are nonintersecting connected subgraphs.

These subgraphs are called **connected components** of a graph *G*.

A number p is a **number characteristic** of a graph. Moreover $p = 1$ for a connected graph and $p \geq 2$ for a nonconnected graph.

Theorem. Each nonoriented graph can be decomposed uniquely into a direct sum.

Definition. A digraph is called **strongly connected** if for any pair of vertices *a* and *b* there exists a path from *a* to *b*.

Definition. A **semipath** is the same as a path except the edge v_i may begin at x_{i-1} or x_i and end at the other vertex.

Definition. A graph G is **weakly connected** or **weak** if there is a semipath between any pair of vertices in G.

Example 5.7.1. The graph in *Fig.5.7.1* has three connected components:

Fig.5.7.1

Example 5.7.2. Three connected components G_1, G_2, G_3 of the digraph G are given in *Fig.5.7.2*:

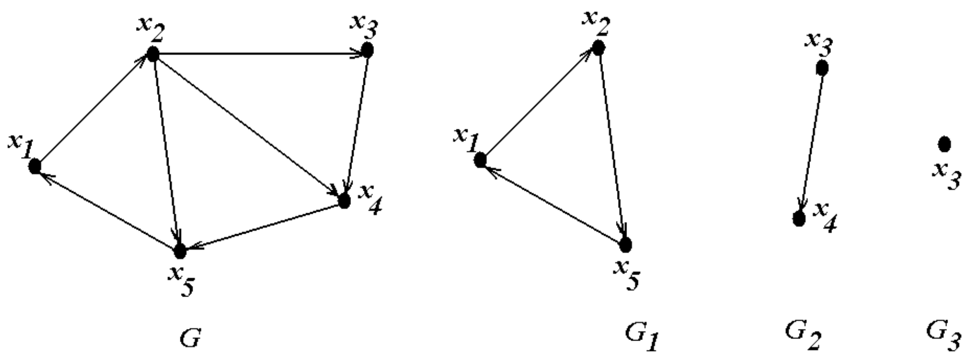


Fig.5.7.2

5.8. Distance and Diameter

Consider a connected graph G. The length of the shortest trail which joins two vertices x and y in a graph G is called a **distance** between these vertices and written $d(x, y)$.

The following metrical axioms are valid:

1. $d(x, y) \geq 0 \ \left(d(x, y) = 0 \Leftrightarrow x = y\right)$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) + d(y, z) = d(x, z)$.

Definition. The diameter of G, written $d(G) = \max\limits_{x,y} d(x, y)$, is the maximum distance between any two points x and y in G.

Let us define for every vertex x in a graph G a quantity $\gamma(x)=\max\limits_{y} d(x,y)$. The minimum of this quantity with respect to all vertices in a graph is called a radius of a graph. That is $d(G)=\min\limits_{x} \gamma(x)=\min\limits_{x} \max\limits_{x,y} d(x,y)$.

A vertex at which this minimum is attained is called a **central vertex**.

5.9.Traversable and Eulerian Graphs

The eighteenth century East Prussian town of Königsberg included two islands and seven bridges as shown in *Fig.5.9.1(a) Question*: Beginning anywhere and ending anywhere, can a person walk through town crossing all seven bridges but not crossing any bridge twice? The people of Königsberg wrote to the celebrated Swiss mathematician L.Euler about this question. Euler proved in 1736 that such a walk is impossible. He replace the islands and the two sides of the river by points and the bridges by curves, obtaining *Fig.5.9.1(b)*.

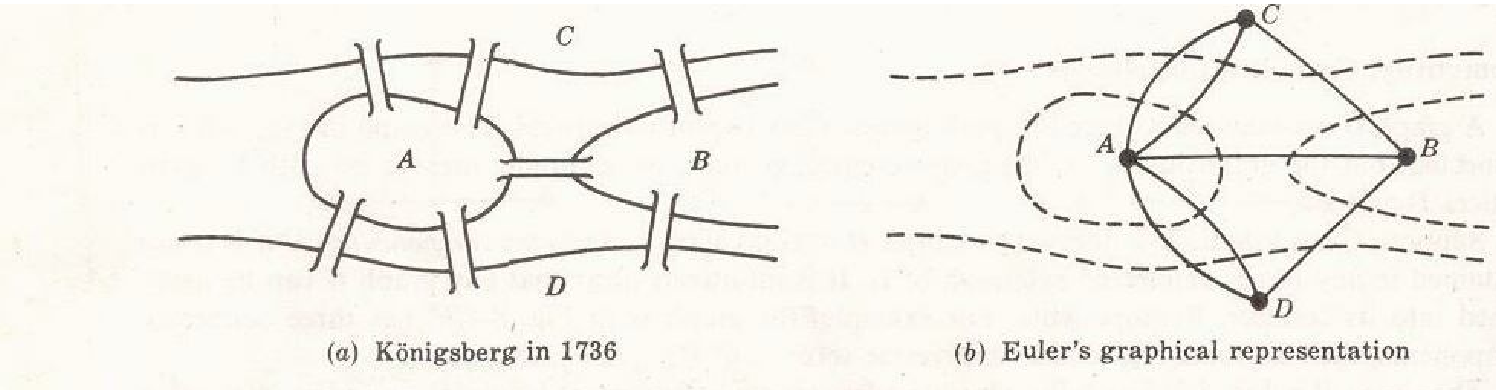


Fig.5.9.1

Observe that *Fig.5.9.1(b*) is a multigraph. A multigraph is said to be **traversable** if it "can be drawn without any breaks in the curve and without repeating any edges", that is: there is a path, which includes all vertices and uses each edge exactly once. Such a path must be a trail (since no edge is used twice) and will be called a **traversable trail.**. Clearly a traversable multigraph must be finite and connected. Figure 5.9.2(b) shows a traversable trial of the multigraph in *Fig.5.9.2(a).* To indicate the direction of the trail, the diagram misses touching vertices which are actually traversed.

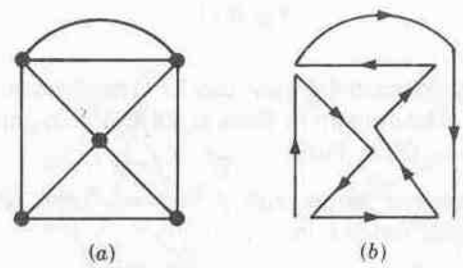


Fig.5.9.2

Now it is not difficult to see that the walk in Königsberg is possible if and only if the multigraph in *Fig.5.9.1(b)* is traversable.

We now show how Euler proved that the multgraph in *Fig.5.9.1 (b)* is not traversable and hence that the walk in Königsberg is impossible.

Recall first that a vertex is **even** or **odd** according as its degree is an even or an odd number. Suppose a multigraph is traversable and that a traversable trial does not begin or end an a vertex *P*. We claim that *P* is an even vertex. For whenever the travesable trail enters *P* by an edge, there must always be an edge not previously used by which the trail can leave *P*. Thus the edges in the trail incident with *P* must appear in pairs, and so *P* is an even vertex. Therefore if a vertex *Q* is odd, the traversable trail must begin or end at *Q*. Consequently, a multigraph with more than two odd vertices cannot be traversable. Observe that the corresponding to the Köningsberg bridge problem has four odd vertices. Thus one cannot walk through Königsberg so that each bridge is crossed exactly once.

Definition. A graph is called an **Eulerian graph** if there exists a closed traversable trail, called an Eulerian trial.

Theorem 5.9.1. A finite connected graph is Eulerian if and only if each vertex has even degree.

5.10. Hamiltonian Graphs

A Hamiltonian **circuit** in a graph *G*, named after the nineteenth – century Irish mathematician William Hamilton (1803 – 1865), is a closed path that visits every vertex in *G* exactly once. (Such a closed path must be a cycle.) If *G* does admit a Hamiltonian circuit, then *G* is called a **Hamiltonian graph**.

Note that an Eulerian circuit traverses every edge exactly once, but may repeat vertices, while a Hamiltonian circuit visits each vertex exactly once but may repeat edges. *Fig.5.10.1* gives an example of a graph which is Hamiltonian but not Eulerian, and vice versa.

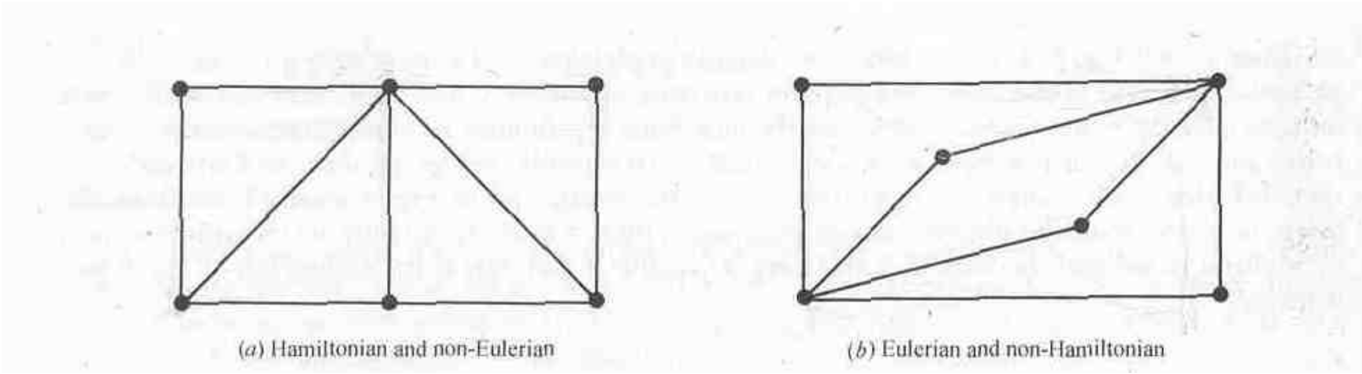


Fig.5.10.1

Although it is clear that only connected graphs can be Hamiltonian, there is no simple criterion to tell us whether or not a graph is Haviltonian as there is for Eulerian graphs. We do have the following sufficient condition which is due to G.A.Dirac.

Theorem5.10.1. Let G be a connected graph with n vertices. Then G is Hamiltonian if $n \geq 3$ and $n \leq \deg(x)$ for each vertex x in G.

5.11. Cyclomatic Graphs. Trees

Let us consider a graph $G = (X, U)$.

Definition. A graph edge through which at least one cycle passes is called a **cyclic edge**.

Definition. An edge which does not belong to any cycle is called an **isthmus**.

Example 5.11.1. In *Fig. 5.11.1* we have the graph with isthmuses u_1 and u_2:

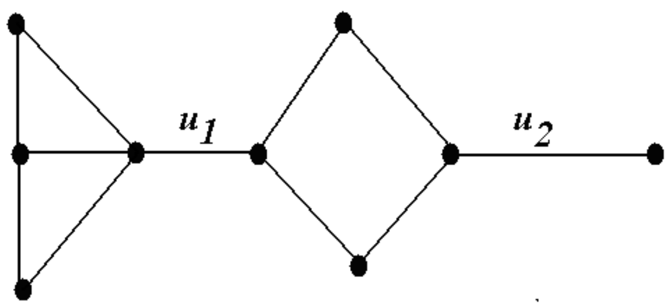


Fig. 5.11.1

Definition. Let $|X| = n$ is a number of vertices, $|U| = m$ is a number of edges, p is a number of connected components of a graph. A quantity $\lambda = m - n + p$ is called a **cyclomatic number**.

It is possible to prove that $\lambda \geq 0$.

5.12. Tree Graphs

Definition. A graph *T* is called a **tree** if *T* is connected and *T* has no cycles. Examples of trees with six vertices are shown in *Fig. 5.12.1.*

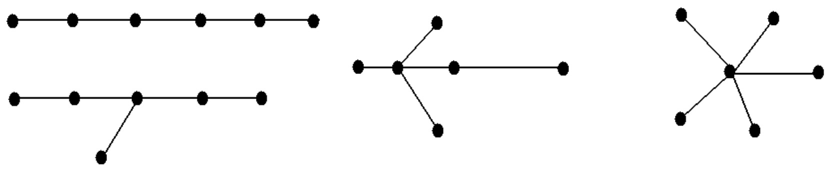


Fig. 5.12.1.

Example of a forest which is a tree is shown in *Fig. 5.12.2.*

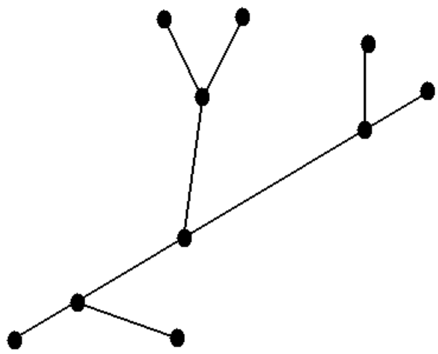


Fig. 5.12.2

Definition. A **forest** is a graph with no cycles; hence connected components of a forest *G* are trees. Note, that a forest can be a tree.

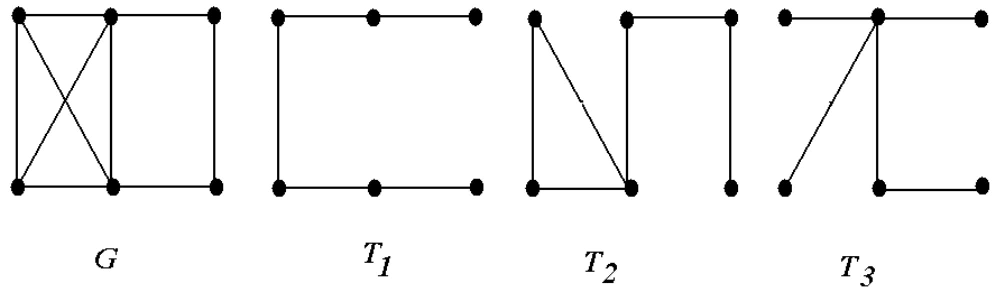
The following definitions of a tree are equivalent:

a) a tree is a connected graph with no cycles;
b) a tree is a connected graph in which each edge is an isthmus;
c) a tree is a connected graph with a cyclomatic number equals zero.

5.13. Spanning Trees

Definition. A subgraph *T* of a connected graph *G* is called a **spanning tree** of *G* if *T* is a tree and *T* includes all the vertices of *G*.

Fig.5.13.1 shows a connected graph *G* and spanning trees T_1, T_2 and T_3 of *G*.



5.14. Transport Networks

Definition. S **transport network** is a directed graph $G = (X, U)$ in which

1) there corresponds a non-negative number $c(u)$ to every arc u called an **arc capacity**;
2) To vertices *s* and *t* are separated. The graph *G* does not include arc which enters *s* and leaves *t*.

These two vertices are called a **source** (s) and a **sink** (t).

Example 5.14.1. In *Fig.5.14.1* the following transport network is given:

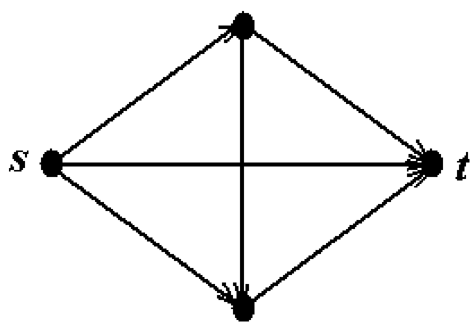


Fig.5.14.1

s is a source, *t* is a sink *a* and *b* are intermediate vertices.

We denote by U_x^+ a set of all arcs which enter *x* and by U_x^- which leave *x*.

For vertices s and t we have $U_s^+ = U_t^- = 0$.

Definition. A function φ which is defined on arc of a network, and takes nonnegative values is called a **flux** if the following conditions are satisfied

(1) $\varphi(u) \geq 0, \quad u \in U$;

(2) $\sum\limits_{u \in U_x^+} \varphi(u) - \sum\limits_{u \in U_x^-} \varphi(u) = 0, \; x \in U, x \neq s, x \neq t$;

(3) $\varphi(u) \le c(u)$.

A flux is a scheme of a transport organization $\varphi(u)$ which means an amount of load passing through an arc in a unit time and does not exceed a capacity of an arc.

The conditions (2) are called **conditions** of **conservation**.

The total quantity of load, which leaves s, equals the total quantity which enters *t*. This total quantity is called a **flux quantity** and denoted by Φ, that is

$$\Phi = \sum_{u \in U_t^+} \varphi(u) = \sum_{u \in U_s^-} \varphi(u).$$

Let $A \subseteq X$ be a subset of network vertices which satisfies the condition $s \in A, t \notin A$.

We denote $\overline{A} = X \setminus A$, then $s \in A, t \in \overline{A}$.

Consider a set $\left(A, \overline{A}\right)$ of all network arcs, which start in the set *A* and end in the set $\overline{A}$:

$$\left(A, \overline{A}\right) = \left\{(x, y) : x \in A, y \in \overline{A}\right\}.$$

Definition. A set of arcs $\left(A, \overline{A}\right)$ is called a **cutset** caused by a set of vertices of *A*. A **capacity** of **cutset** $C\left(A, \overline{A}\right)$ is a sum of capacities of all arcs belonging to the cutset.

6. ELEMENTS OF NUMBER THEORY

6.1. Fundamental Concepts

If m is a natural number then for any integer number a there exists a pair of integer numbers q and r such that

$$a = m \cdot q + r, \quad 0 \le r < m.$$

A number q is called a **quotient**, and a number r is called a **remainder.** If a can be divided by m without remainder then we denote $m|a$.

Definition. The least common multiple (LCM) of two (or more) nonzero whole numbers is the smallest nonzero whole number that is the multiple of each all of the numbers. LCM of a and b is written $[a,b]$.

Example 6.1.1. Find $[24,36]$.

Solution.

Step1: Express the numbers 24 and 36 in their prime factor exponential form:

$$24 = 2^3 \cdot 3, \quad 36 = 2^2 \cdot 3^2.$$

Step 2: The LCM will be the number $2^3 \cdot 3^2$.

Definition. The greatest common factor (GCF) of two (or more) nonzero whole numbers is the largest nonzero whole number that is a factor of both (all) of the numbers. GCF of a and b is written (a,b).

If $(a_1,a_2,...,a_n)=1$ then numbers $a_1,a_2,...,a_n$ are called **mutually prime numbers**.

Theorem. If $a = b \cdot q + r$, then $(a,b)=(b,r)$.

Proof. If $d|b$ and $d|r$ then $d|a$. If $d|a$ and $d|b$ then $d|r$. Therefore a set of divisors of b and r coincides with a set of divisors of a and b. Hence their greatest common factors are equal.

6.2. Euqludean Algorithm

Let a and b be positive integers, and $a > b$. We can find

$$a = b \cdot q_1 + r_1, \quad 0 < r_1 < m_1;$$
$$b = r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1;$$
$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad 0 < r_n < r_{n-1};$$
$$r_{n-1} = r_n \cdot q_n.$$

As a result we have

$$(a,b) = (b,r_1) = (r_1,r_2) = \ldots = (r_{n-1},r_n) = r_n.$$

Example 6.2.1. Find $(525,231)$.

$$\begin{array}{r|l} 525 & \underline{231} \\ \underline{462} & 2 \end{array}$$

$$\begin{array}{r|l} 231 & \underline{63} \\ \underline{189} & 3 \end{array}$$

$$\begin{array}{r|l} 63 & \underline{42} \\ \underline{42} & 1 \end{array}$$

$$\begin{array}{r|l} 42 & \underline{\underline{21}} \\ \underline{42} & 2 \\ 0 & \end{array}$$

Therefore $(525,231) = 21$.

6.3. Congruences and Their Properties

Definition. Let m be a positive integer. We say that ***a* is congruent to *b* modulo *m***, written $a \equiv b(\operatorname{mod} m)$ if m divides the difference $a - b$. The integer m is called the **modulus**.

For example

1. $87 \equiv 23(\operatorname{mod} 4)$ since 4 divides 87 – 23 = 64,
2. $67 \equiv 1(\operatorname{mod} 6)$ since 4 divides 67 – 1 = 66,
3. $72 \equiv -5(\operatorname{mod} 7)$ since 7 divides $72 - (-5)$ = 77,
4. $27 \not\equiv 8(\operatorname{mod} 9)$ since 9 does not divide 27 – 8 = 19.

Remark: Suppose m is positive, and a is any integer then there exist integers q and r with $0 \le r \le m$ such that $a = mq + r$. Hence

$$mq = a - r \text{ or } m|(a - r) \text{ or } a \equiv r(\operatorname{mod} m).$$

Accordingly:

1) Any integer a is congruent modulo m to a unique integer in the set $\{0,1,2,...,m-1\}$. The uniqueness comes from the fact that m cannot divide the difference of two such integers.
2) Any two integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

Now we consider some properties of congruences.

1. Suppose $a \equiv c(\operatorname{mod} m)$ and $b \equiv d(\operatorname{mod} m)$. Then $a + b \equiv c + d(\operatorname{mod} m)$ and $a \cdot b \equiv c \cdot d(\operatorname{mod} m)$.

Let $a = b + km, \quad c = d + lm$, then $a + c = b + d + (k + l)m$ or $a + c \equiv b + d(\operatorname{mod} m)$; $a \cdot c \equiv b \cdot d + m(kd + bl + klm) = bd + mn$.

2. Both sides of a congruence and modulus it is possible to divide by some common divisor.

Let $a \equiv b(\bmod m)$; $a = a_1 d, b = b_1 d, m = m_1 d$, then $a_1 d = b_1 d + k m_1 d$. Hence $a_1 = b_1 + k m_1$ and $a_1 \equiv b_1 (\bmod m_1)$.

3. Both sides of a congruence we can divide by their common divisor if the latter and the modulus of the congruence are mutually prime.

Let $a \equiv b(\bmod m)$; $a = a_1 d, ba = b_1 d, (m,d) = 1$, then $(a_1 - b_1)d = km$. Since $(m,d) = 1$, then $m | (a_1 - b_1)$ and $a_1 \equiv b_1 (\bmod m_1)$.

4. If $a \equiv b(\bmod m)$, then $(a,b) = (b,m)$.

Really, if $a \equiv b(\bmod m)$, then $a = b + lm$ and $(a,b) = (b,m)$.

Example 6.3.1. Observe that $2 \equiv 8(\bmod 6)$ and $5 \equiv 41(\bmod 6)$. Then:

1) $2 + 5 \equiv 8 + 41(\bmod 6)$ or $7 \equiv 8 + 49(\bmod 6)$;
2) $2 \cdot 5 \equiv 8 \cdot 41(\bmod 6)$ or $10 \equiv 328(\bmod 6)$.

6.4 Residue Classes

Since congruence modulo *m* an equivalence relation, it partitions the set $\boldsymbol{Z}$ of integers into disjoint equivalence classes called the **residue classes modulo *m***. A residue class consists of all those integers with the same remainder when divided by *m*. Therefore, there are *m* such residue classes and each residue class contains exactly one of the integers in the set of possible remainders, that is $\{0,1,2,...,m-1\}$.

Generally speaking, a set of *m* integers $\{a_1, a_2, ..., a_m\}$ is said to be a **complete system modulo *m*** if each a_i comes from a distinct residue class. Thus the integers from 0 to *m* – 1 form a complete residue system. The notation $[x]_m$ or simply $[x]$ is used to denote the residue class (modulo *m*) containing an integer *x*, that is, those integers which are congruent to *x*. In other words, $[x] = \{a \in \boldsymbol{Z} | \, a \equiv x(\bmod m)\}$.

Accordingly, the residue classes can be denoted by $[0]$, $[1]$, $[2]$,…,$[m-1]$ or by using any other choice of integers in a complete residue system.

Example 6.4.1. The residue classes modulo *m* = 6 follow:

$$[0] = \{...,-18,-12,-6,0,6,12,18,...\}, \quad [1] = \{...,-17,-11,-5,1,7,13,19,...\},$$
$$[2] = \{...,-16,-10,-4,2,8,14,20,...\}, \quad [3] = \{...,-15,-9,-3,3,9,15,21,...\},$$
$$[4] = \{...,-14,-8,-2,4,10,16,22,...\}, \quad [5] = \{...,-13,-7,-1,5,11,17,23,...\}.$$

6.5. Euler Function

Definition. A function of natural argument $\varphi(n)$ which defines the number of integers between 1 and *n* (exclusive) which are relatively prime to *n* is called the Euler function .

*Example 6.5.1.*By definition we have

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$. If p is a prime number, then $\varphi(p)=p-1$. We shall show that $\varphi(p^n)=p^{n-1}(p-1)$, where n is a natural number.

Solution. Really, among p^n natural numbers there is $\frac{p^n}{p}=p^{n-1}$ numbers which can be divided by p. Others, p^n-p^{n-1} coprime to p^n, that is $\varphi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1)$.

It is possible to prove that Euler function is multiplicative, that is $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$ as $(n,m)=1$. If a natural number N is expanded into prime factors: $N=p_1^{m_1}\cdot p_2^{m_2}\cdot\ldots\cdot p_k^{m_k}$, then we have

$$\varphi(N)=\varphi\left(p_1^{m_1}\right)\cdot\varphi\left(p_2^{m_2}\right)\cdot\ldots\cdot\varphi\left(p_k^{m_k}\right)=$$

$$=p_1^{m_1}\left(1-\frac{1}{p_1}\right)p_2^{m_2}\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)p_k^{m_k}=N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Example 6.5.2. Calculate $\varphi(28)$.

Solution. $\varphi(28)=\varphi\left(2^2\cdot 7\right)=28\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)=12.$

Theorem (Euler). If $(a,m)=1$ then $a^{\varphi(m)}\equiv 1(\operatorname{mod} m)$.
If $m=p$ is a prime number, then $\varphi(p)=p-1$ and we get, according to Euler's theorem, Fermat's little theorem

$$a^{p-1}\equiv 1(\operatorname{mod} p).$$

6.6. Congruence Equations

A **polynomial congruence equation** or, limply, a **congruence equation** (in one unknown *x)* is an equation of the form

$$a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1 x+a_0\equiv 0(\operatorname{mod} m) \qquad (6.6.1)$$

Such an equation is said to be of **degree** n if $a\neq 0(\operatorname{mod} m)$. Suppose $s\equiv t(\operatorname{mod} m)$. Then s is a solution of (6.6.1) if and only if t is a solution of (6.6.1). Thus the **number** of **solutions** of (6.6.1) is defined to be the number of incongruent solutions or, equivalently, the number of solutions in the set $\{0,1,2,\ldots,m-1\}$.

Of course, these solutions can always be found by testing, that is, by substituting each of the m numbers into (6.6.1) to see if it does indeed satisfy the equation.

The **complete set** of **solutions** of (6.6.1) is a maximum set of incongruent solutions whereas the **general** solution of (6.6.1) is the set of all integral solutions of (6.6.1). The general solution of (6.6.1) can be found by adding all the multiples of the modulus m to any complete set of solutions.

Example 6.6.1. Consider the equations:

1. $x^2 + x + 1 \equiv 0(\mathrm{mod}\,4)$, **2.** $x^2 + 3 \equiv 0(\mathrm{mod}\,6)$, **3.** $x^2 - 1 \equiv 0(\mathrm{mod}\,8)$.

Here we find the solutions by testing.

1. There are no solutions since 0, 1, 2, and 3 do not satisfy the equation.
2. There is only one solution among 0, 1,…,5 which is 3. Thus the general solution consists of the integers $3 + 6k$ where $k \in \boldsymbol{Z}$.
3. There are four solutions: 1, 3, 5 and 7. This shows that a congruence of degree n can have more then n solutions.

Now we consider the following linear congruence equation

$$ax \equiv b(\mathrm{mod}\,m) \tag{6.6.2}$$

If a and m are relatively prime, then equation (6.6.2) has a unique solution. Moreover, if s is a unique solution to $ax \equiv 1(\mathrm{mod}\,m)$, then the unique solution to $ax \equiv b(\mathrm{mod}\,m)$ is $x = bs$.

Example 6.6.2.

1. Consider the congruence equation $3x \equiv 5(\mathrm{mod}\,8)$.

Since 3 and 8 are coprime, the equation has the unique solution. Testing the integers 0, 1,…,7, we find that

$$3 \cdot 7 = 21 \equiv 5(\mathrm{mod}\,8).$$

Thus $x = 7$ is the unique solution of the given equation.

2. Consider the linear congruence equation

$$33x \equiv 38(\mathrm{mod}\,280) \tag{6.6.3}$$

Since $GCF(33,280) = 1$, the equation (6.6.3) has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 280$ is relatively large. We apply the Euclidean algorithm to first find a solution to

$$33x \equiv 1(\mathrm{mod}\,280). \tag{6.6.4}$$

We find $x_0 = 17$ and $y_0 = 2$ to be a solution of

$$33x_0 + 280y_0 = 1.$$

This means that $s = 17$ is a solution of the equation (6.6.4). Then $sb = 17 \cdot 38 = 646$ is a solution of (6.6.3). Dividing 646 by $m = 280$, we obtain the remainder $x = 86$, which is the unique solution of (6.6.3) between 0 and 280. The general solution is $86 + 280k$ with $k \in \boldsymbol{Z}$.

6.7. Chinese Remainder Theorem

An old Chinese riddle asks the following question: “Is there a positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 5 it yields a remainder 4, when x is divided by 7 it yields a remainder 6?”
In other words, we seek a common solution of the following three congruence equations:

$$x \equiv 2(\bmod 3), \qquad x \equiv 4(\bmod 5), \qquad x \equiv 6(\bmod 7). \tag{6.7.1}$$

Theorem. Given the system

$$\begin{cases} x \equiv r_1(\bmod m_1), \\ x \equiv r_2(\bmod m_2), \\ \text{.....................}, \\ x \equiv r_k(\bmod m_k), \end{cases} \quad \text{where } m_i\left(i = \overline{1,k}\right) \text{ are}$$

pairwise relatively prime. Then the system has the unique solution modulo $M = m_1 m_2 ... m_k$.

Proof. Consider the integer $x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + ... + M_k s_k r_k$, where $M_i = M|m_i$ and s_i is the unique solution of $M_i x \equiv 1(\bmod m_i)$. Let j be given. For $i \neq j$, we have $m_j | M_i$ and hence $M_i s_i r_i \equiv 0(\bmod m_j)$.

On the other hand, $M_j s_j \equiv 1(\bmod m_j)$ and hence $M_j s_j r_j \equiv r_j(\bmod m_j)$.

Accordingly, $x_0 \equiv 0 + ... + 0 + r_j + 0 + ... + 0 \equiv r_j(\bmod m_j)$.

In other words, x_0 is a solution of each of the equations in (6.7.1). It remains to show that x_0 is the unique solution of the system (6.7.1) modulo M.

Suppose x_1 is another solution of all the equations in (6.7.1). Then $x_0 \equiv x_1(\bmod m_1)$, $x_0 \equiv x_1(\bmod m_2)$, ..., $x_0 \equiv x_1(\bmod m_k)$. Hence $m_i | (x_0 - x_1)$, for each i. Since the m_i are relatively prime, $M | (x_0 - x_1)$. That is $x_0 \equiv x_1(\bmod M)$. Thus the theorem is proved.

Example 6.7.1. Solve the system of congruence equations

$$\begin{cases} x \equiv 2(\bmod 3), \\ x \equiv 3(\bmod 5), \\ x \equiv 1(\bmod 7). \end{cases}$$

Solution. We find $M_1 = 35, M_2 = 21$, $M_3 = 15$. On using the congruences $35 s_1 \equiv 1(\bmod 3)$, $21 s_2 \equiv 1(\bmod 5)$, $15 s_3 \equiv 1(\bmod 7)$ we get $s_1 = 2, s_2 = 1, s_3 = 1$. Then $x = 2 \cdot 25 \cdot 2 + 3 \cdot 21 + 15 \equiv 281(\bmod 105)$ or $x \equiv 8(\bmod 105)$.

Answer: $x \equiv 8(\bmod 105)$.

7. GROUPS. RINGS. FIELDS

7.1. Operarions

Definition. Let S be an nonempty set. An **operation** on S is a function $*$ from $S \times S$ into S. In such a case, instead of $*(a,b)$, we write $a * b$ or sometimes ab.

An operation $*$ from $S \times S$ into S is usually called a **binary operation**.

Definition. An operation $*$ on a set S is said to be **associative** if, for any elements $a, b, c,$ in S, we have $(a * b) * c = a * (b * c)$.

Definition. An operation $*$ on a set S is said to be **commutative** if, for any elements a, b in S, we have $a * b = b * a$.

Definition. An element e in S is called an **identity** element for $*$ if, for any element a in S, we have $a * e = e * a = a$.

Definition. The **inverse** of an element a in S is an element b such that $a * b = b * a = e$. The inverse of an element $a \in S$ is usually denoted by a^{-1}.

7.2. Groups

Let G be an nonempty set with binary operation. Then G is called a **group** if the following axioms hold:

1. Associative Law: For any $a, b, c,$ in G, we have $(ab)c = a(bc)$.
2. Identity element: There exists an element e in G such that $ae = ea = a$ for every a in G.
3. Inverses: For each a in G, there exists an element a^{-1} in G (the inverse of a) such that $aa^{-1} = a^{-1}a = e$.

A group G is said to be **abelian** or (**commutative**) if $ab = ba$ for every $a, b \in G$, That is, if G satisfies the Commutative Law.

When G is abelian, the binary operation is denoted by + and G is said to be written **additively**. In such a case the identity element is denoted by 0 and is called the **zero** element; and the inverse is denoted by $-a$ and it is called the **negative** to a.

The number of elements in a group G denoted by $|G|$, is called the **order** of G. In particular, G is called a **finite group** if its order is finite.

Example 7.2.1.

a) The nonzero rational number $Q \setminus \{0\}$ form an abelian group under multiplication. The number 1 is the identity element and $\frac{q}{p}$ is the multiplicative inverse of the rational number $\frac{p}{q}$.

b) Let S be the set of 2×2 matrices with rational entries under the operation of matrix multiplication. Then S is not a group since inverse do not always exist. However, let G be the subset of 2×2 matrices with a nonzero determinant. Then G is a group under matrix multiplication. The identity element is
$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and the inverse of A is A^{-1}.

7.3. Subroups. Homomorphisms

Let H be a subset of a group G. Then H is called a **subgroup** of G if H is itself a group under the operation of G.

A subset H of a group G is a subgroup of G if :

1. The identity element $e \in H$.
2. H is closed under the operation of G, i.e. if $a, b \in H$ then $ab \in H$.
3. H is closed under inverse, that is, $a \in H$, then $a^{-1} \in H$.

Every group G has the subgroups $\{e\}$ and G itself. Any other subgroup of G is called a **nontrivial subgroup**.

Theorem (Lagrange). Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

Example 7.3.1. Consider the group G of 2×2 matrices with rational entries and nonzero detearminants. Let H be the subset of G consisting of matrices whose upper-right entry is zero, that is, matrices of the form $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$. Then H is a subgroup of G since H is closed under multiplication and inverses and $I \in H$.

Definition. A mapping f from a group G into a group G' is called a **homomorphis** if, for every $a, b \in G$, $f(ab) = f(a)f(b)$.

In addition, if f is one-to-one and onto, then f is called an **isomorphism**; and G and G' are said to be **isomorphic**, written $G \cong G'$.

If $f : G \to G'$ is a homomorphism, then the kernel of f, written $Ker\, f$ is the set of elements whose image is the identity e' of G'; that is,

$$Ker\, f = \{a \in G \mid f(a) = e'\}.$$

Recall that the image of f, written $f(G)$ or $\operatorname{Im} f$, consists of the images of the elements under f; that is, $\operatorname{Im} f = \{b \in G' \mid \text{there exists } a \in G \text{ for which } f(a) = b\}$.

Example 7.3.2. a) Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. The mapping $f : G \to G'$ defined by $f(a) = 2^a$ is a homomorphism because $f(a+b) = 2^a \cdot 2^b = f(a)f(b)$. In fact, f is also one-to-one and onto; hence G and G' are isomorphic.

c) Let a be any element in a group G. The function $f : \boldsymbol{Z} \to G \;\; G'$ defined by $f(n) = a^n$ is a homomorphism since $f(m+n) = a^{m+n} = a^m \cdot a^m = f(m) \cdot f(n)$.

7.4. Rings. Fields

Let R be a non-empty set with two binary operations: an operation of addition and an operation of multiplication. Then R is called a **ring** if the following axioms are satisfied:

1) For any $a, b, c \in R$, we have $(a+b)+c = a+(b+c)$.
2) There exists an element $0 \in R$, called the **zero element**, such that for every $a \in R$, $a + 0 = 0 + a = a$.
3) For each $a \in R$ there exists an element $-a \in R$, called the **negative** of a, such that $a + (-a) = (-a) + a = 0$.
4) For any $a, b \in R$, we have $a + b = b + a$.
5) For any $a, b, c \in R$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6) For any $a, b, c \in R$, we have **(i)** $a \cdot (b+c) = ab + ac$, and **(ii)** $(b+c)a = ba + ca$.

Observe that the axioms 1) through 4) may be summarized by saying that R is an abelian group under addition.

Subtraction is defined in R by $a - b = a + (-b)$.

A subset S of R is a **subring** of R if S itself is a ring under the operations in R. We note that S is a subring of R if : **(i)** $0 \in S$, and **(ii)** for any $a, b \in S$, we have $a - b \in S$ and $a \cdot b \in S$.

Definition. R is called a **commutative ring** if $ab = ba$ for every $a, b \in R$.

Definition. R is called a **ring with** an **identity element** 1 if the element 1 has the property that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$. In such a case, an element $a \in R$ is called a **unit** if a has a multiplicative inverse, that is, an element a^{-1} in R such that $a^{-1} \cdot a = a \cdot a^{-1} = 1$.

Definition. R is called a **ring with zero divisors** if there exist nonzero elements $a, b \in R$ such that $ab = 0$. In such a case, a and b are called **zero divisors**.

Definition. A commutative ring R is an **integral domain** if R has no zero divisors, that is, $ab = 0$ implies $a = 0$ or $b = 0$.

Definition. A commutative ring R with an identity element 1 (not equal to 0) is a **field** if every nonzero $a \in R$ is a unit, that is, has a multiplicative inverse.

A field is necessarily an integral domain, for if $ab = 0$ and $a \neq 0$, then $b = 1$.
We remark that a field may also be viewed as a commutative ring in which the nonzero elements form a group under multiplication.

Example 7.4.1.

a) The set $\boldsymbol{Z}$ integers with the usual operations of addition and multiplication is the classical example of an integral domain (with an identity element). The units in $\boldsymbol{Z}$ are only 1 and -1, that is, no other element in $\boldsymbol{Z}$ has a multiplicative inverse.
b) The rational numbers $\boldsymbol{Q}$ and real numbers $\boldsymbol{R}$ each forms a field with respect to the usual operations of addition and multiplication.
c) Let R be any ring. Then the set $R[x]$ of all polynomials over R is a ring with respect to the usual operations of addition and multiplication of polynomials. Moreover, if R is an integral domain then $R[x]$ is also an integral domain.

Definition. A subset I of a ring R is called an **ideal** in R if the following three properties hold:

1) $0 \in I$.

2) For any $a, b \in I$ we have $a - b \in I$.

3) For any $r \in R$ and $a \in I$, we have $ra, ar \in I$.

Now let R be a commutative ring with an identity element. For any $a \in R$, the following set is an ideal:

$$(a) = \{ra \mid r \in R\} = aR.$$

Example 7.4.2. Let R be any ring. Then $\{0\}$ and R are ideals. In particular, if R is a field, then $\{0\}$ and R are the only ideals.

7.5. Polynomials over a Field

Let K be an integral domain or a field. Formally a polynomial f over K is an infinite sequence of elements from K in which all except a finite number of them are 0; that is, $f = (\ldots, 0, a_n, \ldots, a_1, a_0)$ or, equivalently, $f(x) = a_n x^n + \ldots + a_1 x + a_0$ where the symbol x is used as an undetermined. The entry a_k is called the kth coefficient of f. If n is the largest integer for which $a_n \neq 0$, then we say that the degree of f is n, written $\deg(f) = n$. We also call a_n the leading coefficient of f. If $a_n = 1$, we call f a **monic** polynomial.

A scalar $a \in K$ is a **root** of a polynomial $f(x)$ if $f(a) = 0$.

Theorem. Let $f(x)$ and $g(x)$ be polynomials over a field K with $g(x) \neq 0$. Then there exist polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)\, g(x) + r(x)$ where either $r(x) \equiv 0$ or $\deg(r) < \deg(g)$, (without proof).

Corollary 1. Suppose $f(x)$ is divided by $g(x) = x - a$. Then $f(a)$ is the remainder. The proof follows from the previous theorem. That is, dividing $f(x)$ by $x - a$ we get

$$f(x) = q(x)\,(x-a) + r(x)$$

where $\deg(r) < \deg(x-a) = 1$. Hence $r(x) = r$ is a scalar. Substituting $x = a$ in the equation for $f(x)$ yields

$$f(a) = q(a)\,(a-a) + r = r.$$

Thus $f(a)$ is the remainder.

Corollary 2. The scalar $a \in K$ is a root of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Theorem. Suppose $f(x)$ is a polynomial over a field K, and $\deg(f) = n$. Then $f(x)$ has at most n roots.

Proof. The proof is by induction on n. If $n = 1$, then $f(x) = ax + b$ and $f(x)$ has the unique roor $x = -\frac{b}{a}$. Suppose $n > 1$. If $f(x)$ has no roots, then the theorem is true. Suppose $a \in K$ is a root of $f(x)$. Then

$$f(x) = (x-a)\, g(x) \qquad (7.5.1)$$

where $\deg(g) = n - 1$. We claim that any other root of $f(x)$ must also be a root of $g(x)$.

Suppose $b \neq a$ is another root of $f(x)$. Substituting $x = b$ in equation (7.5.1) yields $0 = f(b) = (b-a)\, g(b)$.

Since K has no zero divisors and $b - a \neq 0$ we must have $g(b) = 0$. By induction $g(x)$ has at most $n - 1$ roots. Thus $f(x)$ has at most $n - 1$ roots other than a. Thus $f(x)$ has at most n roots.

The theorem has been proved.

Theorem. Suppose a rational number $\frac{p}{q}$ is a root of the polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

where all the coefficients $a_n, a_{n-1}, \ldots a_1, a_0$ are integers. Then p divides the constant term a_0 and q divides the leading coefficient a_n. In particular, if $c = \frac{p}{q}$ is an integer, then c divides the constant term a_0. (Without proof).

Example 7.5.1. Suppose $f(x) = x^3 + x^2 - 8x + 4$. Assuming $f(x)$ has a rational root, find all the roots of $f(x)$.

Solution.

Since the leading coefficient is 1, the rational roots of $f(x)$ must be integers from among

$\pm 1, \pm 2, \pm 4$.

Note $f(1) \neq 0$ and $f(-1) \neq 0$. Dividing by $x - 2$, we get that $x = 2$ is a root and

$$f(x) = (x-2)(x^2 + 3x - 2).$$

Using the quadratic formula for $x^2 + 3x - 2 = 0$, we obtain the following three roots:

$$\left[\begin{array}{l} x_1 = 2, \\ x_2 = \dfrac{-3-\sqrt{17}}{2}, \\ x_3 = \dfrac{-3+\sqrt{17}}{2} \end{array}\right.$$

FOR NOTES