Tran Viet Dung

LECTURE ON MATHEMATICS I

For HEDSPI Students

Hanoi University 2008

COMTENTS

Chapter I

SYMBOLIC LOGICS

1. Propositions

Definition 1.

A Proposition is a statement which is either true or false, although we may not know which. Propositions are denoted by lower letters as p, q, r… The truth or falsity is called truth value of the proposition. The truth value of the proposition p is denoted by V(p).

If p is true then V(p) = 1 or T. If p is false then V(p) = 0 or F.

Example 1.

The proposition p is given by p = " The sun rises in the east " and the proposition q is given by q = " The sun rises in the west". Then V(p) = 1 and V(q) = 0.

However, for several propositions we do not know the truth values.

Example 2.

The proposition r = " There exists life outside the earth." Up to now we can not know the truth value of the statement r.

2. Logical operations

Negation operator NOT

Definition 2.1.

The negative proposition of a proposition p is the proposition $\overline{p}$ defined by its truth table as follows

p	$\overline{p}$
1	0
0	1

Table 1.NOT truth table

Note : For a proposition p we have V(p) = V$\left(\overline{\overline{p}}\right)$.

Example 3.

Given a proposition p = " Hanoi is the capital of Vietnam ". Then NOT p is the proposition $\overline{p}$ = " Hanoi is not the capital of Vietnam".

Example 4.

The proposition q is " The equation f(x) = 0 has solutions ", then the negative proposition is " The equation f(x) = 0 has no solution ".

Conjunction operator AND ($\wedge$)

Definition 2.2.

Given two propositions p and q . The proposition $p \wedge q$ is true only both p and q are true propositions. The AND operator is defined by a truth table which lists of possible combinations of the truth values of p andq :

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

TABLE 2 . AND truth table

Example 5.

If p = " Pigs are mammals" and q = "Pigs fly " , then $p \wedge q$ is interpreted as " Pigs are flying mammals ".

Disjunction operator OR ($\vee$)

Definition 2.3.

For propositions p and q the proposition $p \vee q$ is false only when both p and q are false. The OR operator is defined by the following truth table

p	Q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Table 3. OR Truth Table

Theorem 1. (De Morgan 's Law)

For any two propositions p and q we have

1) $V(\overline{p \wedge q}) = V(\bar{p}) \vee V(\bar{q})$,

2) $V(\overline{p \vee q}) = V(\bar{p}) \wedge V(\bar{q})$,

Corollary 2.

The disjunction operator OR may be defined by NOT and AND operators:

$$V(p \vee q) = V(\overline{\bar{p} \wedge \bar{q}}).$$

Theorem 3.(Distributive Laws).

For any three propositions p, q, r, we have

1) $V(p\wedge(q\vee r)) = V((p\wedge q)\vee(p\wedge r))$

2) $V(p\vee(q\wedge r) = V((p\vee q)\wedge(p\vee r))$

Theorem 4.(commutative and associative Laws**)**

For propositions p, q, r, we have

1) $V(p\wedge q) = V(q\wedge p)$,

2) $V(p\vee q) = V(q\vee p)$,

3) $V((p\wedge q)\wedge r)=V(p\wedge q(\wedge r))$,

4) $V((p\vee q)\vee r))= V(p\vee(q\vee r))$.

Implication operator IMP (□)

Definition 2.4.

For two propositions p, q, the proposition p□q is defined by its truth table

p	q	P□q
1	1	1
1	0	0
0	1	1
0	0	1

TABLE 4. IMP truth table

Thus, the proposition p□q is false only when p is true and q is false.

Assertion 5.

If p, q are propositions then we have

1) the proposition $p \rightarrow (p \vee q)$ *is true,*

2) The proposition $(p \wedge q) \rightarrow p$ *is true.*

Theorem 6.

The implication operator IMP may be built from the negation operator NOT and the conjunction operator AND:

$V(p \rightarrow q) = V(\overline{p \wedge \bar{q}})$.

Equivalence operator IFF (↔)

Definition 2.5.

Given two propositions p, q. The proposition p↔q is true only when the truth values of p and q are the same.

p	**q**	P↔q
1	1	1
1	0	0
0	1	0
0	0	1

TABLE 5. IFF Truth Table

Theorem 7.

For propositions p, q we have

$V(p \leftrightarrow q) = V((p \rightarrow q) \wedge (q \rightarrow p))$.

Theorem 8.

The equivalence operator may be built from the negation operator NOT and the conjunction operator AND:

$V(p\leftrightarrow q) = V((\overline{p \wedge \overline{q}})\wedge(\overline{q \wedge \overline{p}}))$.

Tautologies, contradictions

Definition 3.1.

A proposition composite by atomic propositions is called a tautology if it is always true regardless truth values of atomic components.

Example 5.

a)The proposition (p∧q)□p is a tautology. Actually, we have the truth table of this proposition

p	q	p∧q	(P∧q)□p
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

b)((p∨q)∧ $\overline{p}$)□q is a tautology. The truth table is

p	q	p∨q	(P∨q)∧ $\overline{p}$	((P∨q)∧ $\overline{p}$)□q
1	1	1	0	1
1	0	1	0	1
0	1	1	1	1
0	0	0	0	1

Definition 3.2.

A proposition composite by atomic propositions is called a contradiction if it's values are always false regardless truth values of atomic components.

Example 6.

a) The proposition $p \wedge \overline{p}$ is a contradiction. Actually, the truth table of this proposition is

p	$\overline{p}$	$p \wedge \overline{p}$
1	0	0
0	1	0

b)The proposition $(p \wedge q)$□$\overline{p}$ is a contradiction because the truth values of this are always false:

p	q	$\overline{p}$	$\overline{q}$	$p \vee \overline{p}$	$q \wedge \overline{q}$	$(p \vee \overline{p})$□$q \wedge \overline{q}$
1	1	0	0	1	0	0
1	0	0	0	1	0	0
0	1	1	1	1	0	0
0	0	1	1	1	0	0

2. Generation of operators

4.1 Binary operator XOR (↕)

Definition 4.1.

For two propositions p and q, the proposition p□q is defined by the truth table

p	q	p $\updownarrow$ q
1	1	0
1	0	1
0	1	1
0	0	0

Assertion 9.

The XOR operator is the negation of the IFF operator:

$V(p \updownarrow q) = V(\overline{p \leftrightarrow q})$.

4.2 Binary operator NOR ($\uparrow$)

Definition 4.2.

Given two proposition p, q. The proposition $p\uparrow q$ is the proposition defined by the truth table

p	q	$p\uparrow q$
1	1	0
1	0	0
0	1	0
0	0	1

This means neither p nor q.

Assertion 10.

The operator NOR is negation of OR:

$V(p\uparrow q) = V(\ \overline{p \vee q}\ ).$

4.3 Binary Operator NAND (↓)

Definition 4.3.

Given two propositions p and q. The proposition $p\downarrow q$ is defined by the truth table

p	q	$p\downarrow q$
1	1	0
1	0	1
0	1	1
0	0	1

Assertion 11.

The operator NAND is the negation of AND:

$V(p\downarrow q) = V(\overline{p \wedge q}).$

3. Propositions with quantifiers $\forall, \exists$.

Definition 5.1.

Let $p(x)$ is a statement for $x \in X$. Then

$\forall x \in X, p(x)$ is a proposition that is true if for every x in the set X, $p(x)$ is true. $\exists x \in X, p(x)$ is a proposition that is true if there is an element x in X such that $p(x)$ is true.

Analogously, we have propositions as $\forall x \exists y, P(x,y)$; $\exists x \exists y, P(x,y)$ or $\forall x \forall y, P(x,y)$.

In general, we have propositions containing $\exists, \forall$ and a statement $P(x_1,\dots,x_n)$.

Example 7.

a)The proposition **“**$\forall x \in \mathbf{R}$, $x^2+1 \geq 0$.“ is true.

b)The proposition **“**$\forall x \in \mathbf{R}$, $x^2-1 \geq 0$.“ is false.

c)The proposition **“**$\exists x \in \mathbf{R}$, $x^2-1 \geq 0$“ is true.

d) The proposition “ $\forall x \in \mathbf{R}, \exists y \in \mathbf{R}$, $x + y \geq 0$“ is true

e)The proposition “$\exists y \in \mathbf{R} \, \forall x \in \mathbf{R}$, $x + y \geq 0$“ is false.

Example 8.

The function $f(x)$ is continuous at the point x_0 if “ $\forall \varepsilon > 0$, $\exists \delta > 0$, $\forall x, ((|x-x_0| < \delta) \Rightarrow |f(x)-f(x_0)| < \varepsilon)$“.

Note.

To receive the negation of a proposition containing qualifiers $\forall, \exists$ and statement $P(x_1,\dots, x_n)$, we change $\forall$ by $\exists$, change $\exists$ by $\forall$ and change $P(x_1,\dots, x_n)$ by $\overline{P}(x_1,\dots, x_n)$.

Example 9.

In Example 8, using the above note we have that a function $f(x)$ is not continuous at the point x_0 if

“$\exists \varepsilon > 0, \forall \delta > 0, \exists x(((|x-x_0| < \delta) \wedge (|f(x)-f(x_0)| > \varepsilon)$”.

Chapter II

SETS

1. Sets and elements

1.1 Some definitions and notations

Definition 1.

A set is a collection of elements. Let a be and element of a set A. Then we say that the element a is be long to A and denote by a $\in$ A. If the element a is not belong to A then denote by a $\notin$ A.

Let a and b be two element of a set A. If a and b are the same then denote by a $\neq$ b.

The set containing no any element is called the empty set and denoted by $\varnothing$.

Definition 2.

The set A and the set B are called equal and denoted by A = B if an element a $\in$ A $\leftrightarrow$ a $\in$ B.

1.2 The ways to determine a set

Method 1. *Listing of all elements of the set*.

Example 1.

a) $A = \{ 1,2,3,4,5,6,7,8,9,10 \}$.

b) $B = \{ 1, 3, 5, ..., 2n+1,...\}$

However in several cases we can not know exactly elements of a set or can not list all elements of a set.

c) We usually use some number sets as follows:

N is the set of natural numbers,

Z is the set of integer numbers,

Q is the set of rational numbers,

R is the set of real numbers.

Example 2.

a) Let A be the set of real roots of the equation $x^9 - 3x^8 + 4x^3 - 100 = 0$. Then it is difficul to us to collect elements of A.

b) Let **R** be the set of real numbers. We can not list all elements of **R.**

Hence a set is also defined by the following method.

Method 2.

Poiting out the characteristic properties of elements of the set.

Example 3.

In Example 2a) an element of A is a real root of given equation. Then we can denote

$$A = \{ x\in \mathbf{R} \mid x^9 - 3x^8 + 4x^3 - 100 = 0 \}.$$

In Example 2b) an element of R is a real numbers.

Example 4.

a) $A = \{ 1,2,3,4,5,6,7,8,9,10 \}$ can be expressed as

$$A = \{ x\in \mathbf{N} \mid 1 \leq x \leq 10 \}.$$

b) $B = \{ 1, 3, 5, ...\} \qquad = \{ k \in N \mid k = 2n +1, n \in N \}$.

1.3 Subsets

Definition 3.

We say that a set A is a subset of a set B or that A is included in B and denote by $A \subset B$ if all elements of A are also belong to B. That is

$A \subset B$ if and only if ($a \in A \Rightarrow a \in B$).

Example 5. a) $\{ 1, 3, 5 \} \subset \{ 1, 2, 3, 5, 8, 13 \}$.

b) $\mathbf{N} \subset \mathbf{Z}$, $\mathbf{Z} \subset \mathbf{Q}$, $\mathbf{Q} \subset \mathbf{R}$.

Note. a) A set is a subset of itself.

b) For two sets A, we have

$A = B$ iff $A \subset B$ and $B \subset A$.

2. Set operations

Intersection and union of sets

Definition 4.

The *intersection* of a set A and a set B is the set $A \cap B$ given by

$$A \cap B = \{ x \mid x \in A \wedge x \in B \}.$$

Definition 5.

The *union* of a set A and a set B is the set $A \cup B$ given by

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

Example 6.

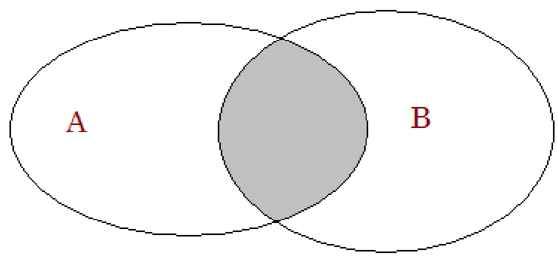
a)If A = {1,2,3,4.5,6 }, B = { 1,3,5,7,9 } then $A \cap B = \{ 1,3,5\}$, $A \cup B = \{ 1,2,3,4,5,6,7,9 \}$.

b) $A = \{ x \in R \mid f(x)= 0 \}$ $B = \{ x\in R \mid g(x) = 0 \}$

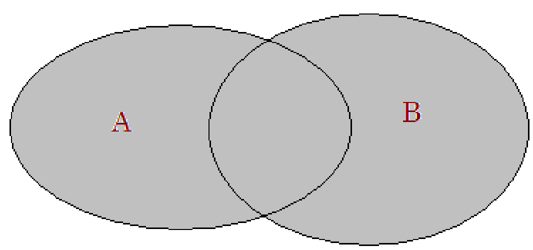
then $A \cap B = \{ x\in R \mid f(x) = 0 \wedge g(x) = 0 \}$.

If $A \cap B = \varnothing$ then we say that A, B are disjoint .

Venn diagrams



$A \cap B$



$A \cup B$

Difference of sets, compliment of a subset

Definition 5.

The difference of a set A and a set B is the set A\B defined by

$$A\backslash B =\{ x \in A \mid x \notin B \}.$$

Let U be the universal set the compliment of a set A denoted by

$$\overline{A} = U \backslash A.$$

Example 7.

a) A = { 1,2,3,4,5 }, B = { 1,3,5,7,9 }, A\B = { 2,4 }.

b) A = { $x \in R \mid f(x) = 0$ }, B = { $x \in R \mid g(x) = 0$ }

The set $\{ x \in R \mid \dfrac{f(x)}{g(x)} = 0 \}$ is equal to A\B.

Properties

Theorem 1.

For sets A, B, C, we have

1) $A \cup B = B \cup A, \ A \cap B = B \cap A,$

2) $A \cup (B \cup C)) = (A \cup B) \cup C, \qquad A \cap (B \cap C) = (A \cap B) \cap C,$

3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$

4) $\varnothing \cap A = \varnothing, \quad \varnothing \cup A = A,$

5) $A \subset B \Leftrightarrow A \cap B = A$

6) $A \subset B \Leftrightarrow A \cup B = B$.

Notations : $\bigcap_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n,$

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

Theorem 2.

For sets X, $A_1,\ldots, A_n$, we have

1) $X \setminus \bigcap_{i=1}^{n} A_i = \bigcup_{i=1}^{n} (X \setminus A_i)$,

2) $X \setminus \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (X \setminus A_i)$,

3) $\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$,

4) $\overline{\bigcap_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$.

The Cartesian product of sets

Definition 6.

The cartesean product of a set A and a set B is the set $A\times B$ of all ordered pairs whose first coordinates in A and whose second coordinate is in B, i.e $A\times B = \{ (a, b) \mid a\in A, b \in B \}$.

Example .

If $A = \{ 1,2,3 \}$, $B = \{2,4 \}$ then $A\times B = \{ (1,2), (1,4), (2,2), (2,4), (3,2), (3,4)\}$.

In General

$A_1\times A_2\times\ldots \times A_n = \{(x_1,x_2,\ldots,x_n) \mid x_1\in A_1\ldots,x_n\in A_n\}$,

$A^n = \{(x_1,x_2,\ldots,x_n) \mid x_1\in A\ldots,x_n\in A \}$.

3. Some properties of finite sets

Assume that the number of elements of a set X is finite. Denote by N(X) the number of elements of X.

Theorem 3.

Let A and B be finite sets . Then we have

$$N(A \times B) = N(A).N(B).$$

Theorem 4.

a)*For two disjoint sets A, B we have*

$N(A \cup B) = N(A) + N(B).$

b) For A, B are arbitrary , we have

$N(A \cup B) = N(A) + N(B) - N(A \cap B).$

Theorem 5.

For arbitrary finite sets $A_1, A_2, ...A_m$, the number of elements of their union is counted by the formula

$N(A_1 \cup ... \cup A_m) = N_1 - N_2 + N_3 +... + (- 1)^{m-1} N_m ,$

where $N_1 = N(A_1)+...+N(A_m), ..., N_k = \sum_{1 \le i1 \langle i2 \langle ... \langle ik \le m} N(A_{i1} \cap A_{i2} \cap ... A_{ik})$

Example .

$N(A_1 \cup A_2 \cup A_3) = N_1 - N_2 + N_3$, where

$N_1 = N(A_1) + N(A_2) + N(A_3)$,

$N_2 = N(A_1 \cap A_2) + N(A_1 \cap A_3) + N(A_2 \cap A_3)$

$N_3 = N(A_1 \cap A_2 \cap A_3)$.

Chapter III

MAPPINGS

1. Basic concepts

Definition 1.

Let X and Y be two sets. A mapping (map or function) f from X to Y is an assignment of every element in X to an unique element in Y.

Let f be a mapping from X to Y. If $x \in X$, the element of Y to which x assigned by f and denoted by f(x). Denote by

$$f: X \to Y, x \mapsto f(x).$$

If f(x) = y, we say that x is mapped to y by f and y is the image of x under f.

Definition 2.

Two mappings f, g from X to Y are called equal if they are the same way on every element of X, i.e

$$f = g \text{ iff for all } x \in X, f(x) = g(x).$$

Example 1.

a) A mapping $f: X \to R$ for a subset X in R is a real function.

b) The map $Id_X: X \to X$ given by $Id_X(x) = x$ for every $x \in X$ is called the identity on X.

Definition 3.

Let $f: X \to Y$ be a map

a) For a set $A \subset X$, the set $f(A) = \{ f(x) | x \in A \}$ is called the image of A under f.

b) For $B \subset Y$ the set $f-1(B) = \{ x \in X | f(x) \in B \}$ is called the preimage of B under f.

If $A = X$, $f(X)$ is denoted by Im(f). If $B = \{b\}$, we write $f-1\{b\}$ instead of $f-1(\{b\})$.

2. Injective,surjective, bijective mappings

Definition 4.

Let $f: X \to Y$ be a map.

a) The map f is called injective if for $x1, x2 \in X$, $f(x1) = f(x2)$ implies $x1 = x2$.

b) The map f is called surjective if for every $y \in Y$ there exists an element $x \in X$ such that $f(x) = y$.

c) The map f is called bijective if it is both injective and surjective.

Example 2.

a) $f : R \to R$, $f(x) = 2x +1$ is bijective.

b) $g: R \to R$, $g(x) = ex$ is injective not surjective

c) $h: R \to R$, $h(x) = x2$ is neither injective nor surjective.

Remark.

X and Y are finite sets. We have

a) If $f: X \to Y$ is injective then $N(X) \leq N(Y)$

b) If $f: X \to Y$ is surjective then $N(X) \geq N(Y)$

c) If $X \to Y$ is bijective then $N(X) = N(Y)$.

3. Composition of maps, inverse maps

Definition 5.

Given three sets X, Y, Z and maps

$$f: X \to Y,\ g: Y \to Z.$$

The composition of f and g is the map

$$g \circ f: X \to Z$$

given by $(g \circ f)(x) = g(f(x))$ for $x \in X$.

Example 3.

If $f,g: R \to R$, $f(x)= x^2$, $g(x) = \sin(x)$ then

$(g \circ f)(x)= \sin(x^2)$, $(f \circ g)(x)= \sin^2(x)$.

Proposition 1.

For maps $f:X \to Y$, $g:Y \to X$, $h:Z \to W$, we have

a) $h \circ (g \circ f) = (h \circ g) \circ f$,

b) $f \circ Id_X = f$; $Id_Y \circ f = f$.

Proposition 2.

Let $f:X \to Y$, $g: Y \to Z$ be maps.

a) If f and g are injective then $g \circ f$ is injective

b) If f and g are surjective then $g \circ f$ is surjective

c) If f and g are bijective then $g \circ f$ is bijective.

Proposition 3.

Let $f : X \to Y$ be a bijection. Then there is a map $g: Y \to X$ $g(y) = x$ if $f(x) = y$.

$\sqcup$

Definition 6.

Given a bijection f: $X \to Y$, the map

$g : Y \to X$ for which $g(y) = x$ if $f(x) = y$ is called the inverse of f and denoted by $g = f^{-1}$.

Proposition 4.

Let $f : X \to Y$, $g: Y \to Z$ be bijections , Id_X be the identity on X. Then

a) $Id_X^{-1} = Id_X$,

b) $(f^{-1})^{-1} = f$,

c) $f^{-1} \circ f = Id_X$, $f \circ f^{-1} = Id_Y$,

d) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Example 4.

a) $f : \mathbf{R} \to \mathbf{R}$, $y = f(x) = 2x + 1$, then $x = f^{-1}(y) = \frac{y-1}{2}$

b) $f : R \to (0; \infty)$, $y = f(x) = e^x$, then $x = f^{-1}(y) = \ln y$.

4. Restriction, characteristic functions

Definition 7.

Let $f : X \to Y$ be a map, A be a subset of X . The restriction of f to A is a map $f|_A : A \to Y$ given by $f|_A(x) = f(x)$ for all $x \in A$.

Definition 8.

Let g is the restiction of f to A. Then f is called a extension of g to X.

Definition 9.

Let $A \subset X$, the map $\chi_A : X \to \{0, 1\}$ given by

$\chi_A(x) = 1$ if $x \in A$; $\chi_A(x) = 0$ if $x \notin A$

is called the characteristic function of the set A.

Definition 10.

Given $X = X_1 \times X_2$.

a) The map $p_1 : X_1 \times X_2 \to X_1$ defined by $p_1(x_1, x_2) = x_1$ is called the canonical projection on X_1.

b) The map $p_2 : X_1 \times X_2 \to X_2$ defined by $p_2(x_1, x_2) = x_2$ is called the canonical projection on X_2

5. Substitutions

Definition 11.

A bijection from a finite set X into itself is called a substitution (or permutation) of X.

Let $X = \{ 1, 2, ..., n \}$, $f : X \to X$ be a bijection. Then we can write

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

where the first row contains elements of X and the second row containes images of corresponding elements.

Proposition.

a) *Composition of substitutions of X is a substitution of X.*

b) The inverse map of a substitution of X is a substitution of X

c) If X contains n elements then there are n! (n factoral) substitutions of X.

Example 5.

Given two substitution

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

Find substitutions $g_o f$ and f^{-1}.

Solution. $g_o f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$, $f^{1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$.

Definition.

A substitution f is called a *cycle* of length k and denoted by $(i_1, i_2, \ldots, i_k)$ if $f(i_1) = i_2$, $f(i_2) = i_3, \ldots, f(i_k) = i_1$, $f(j) = j$ for $j \notin \{i_1, i_2, \ldots, i_k\}$.

Example 6.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 5 \end{pmatrix}$$ is a cycle of length 3 and can be writen by $f = (1, 2, 4)$.

A cycle f of length 2 is called a *transposition* i.e $f = (i_1, i_2)$. That means $f(i_1) = i_2$, $f(i_2) = i_1$, $f(j) = j$ for $j \neq i_1, i_2$.

Proposition.

a) Any substitution is a product of cycles

b) Any substitution is a product of transpositons

Definition.

Given a substitution $\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$,

a) (i, j) is called an inversion for f if $i < J$ and $f(i) > f(j)$.

b) f is called even if the number of inversions for f is even

c) f is called odd if the number of inversion for f is odd.

d) If N(f) is the number of inversions for f then the sign of f denoted by sign(f) is given by $\mathrm{sign}(f) = (-1)^{N(f)}$.

Example 7.

a) For f $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 6 & 5 & 7 & 2 & 1 \end{pmatrix}$, N(f) = 12, f is an even substitution, sign(f) = 1.

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 5 \end{pmatrix} = (1,2,4) = (2,4)\,(1,4).$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 6 & 5 & 7 & 2 & 1 \end{pmatrix} = (1,4,5,7)(2,3,6) =$

$= (5,7)(4,7)(1,7)(3,6)(2,6)$

Denote S_n the set of substitutions of X = {1,2, ..., n}.

Proposition.

For f, g $\in S_n$, we have

a) $sign(f \circ g) = sign(f).sign(g)$,

b) $sign(f)\ \ sign(f^{1})$,

c) *If f is a cycle of length k then* $sing(f) = (-1)^{k+1}$.

d) $sign(f) = -1$ *is f is a transposition*

6. Collections

Collection of sets

In several cases we consider a set that its elements are sets. For example,the set of strigth lines on the plane, where a line is an element of the set but it is a set of points.

Definition.

Given a set X. A set C consists of some subsets of X is called a collection of subsets of x.

Let **C** is collection of subsets of X. The *intersection* of collection **C** is given by

$$\bigcap \mathbf{C} = \bigcap_{A \in C} A = \{ x \mid x \in A, \text{fof all } A \text{ in } \mathbf{C} \}.$$

The *union* of **C** is given by

$$\bigcup \mathbf{C} = \bigcup_{A\in C} A = \{\ x \mid x\in A \text{ for some } A \text{ in } \mathbf{C}\ \}$$

Example 8.

$$X = \{\ n\in N \mid n < 25\ \}$$

$O = \{\ n\in X \mid n \text{ is odd}\ \}$

$S = \{\ n\in X \mid n \text{ is square}\ \}$

$P = \{\ n\in X \mid n \text{ is prime}\ \}$

$\mathbf{C} = \{\ O, S, P\ \}$; then $\bigcap \mathbf{C} = \varnothing$,

$\bigcup \mathbf{C} = \{1,2,3,4,5,7,9,11,13,15,16,17,19,21,23\}$

Definition.

Given a set X the power set P(X) of X is defined by $P(X) =\{\ A \mid A$ is a subset of $X\ \}$.

Example 9.

$X = \{1), P(X) = \{\varnothing, \{1\}\ \}$.

Collection of maps

Definition.

Let X and Y be two sets . A set that its elements are maps from X to Y is a collection of maps from X to Y.

The collection of all maps from X to Y is denoted by

$$F(X,Y) = \{\ f \mid f : X \to Y\ \}.$$

Example 10.

If $X = \{\ x, y\ \}$, $Y = \{\ 1, 2\ \}$ then

$F(X,Y) = \{\ f_1, f_2, f_3, f_4\ \}$ where

$f_1 : x\mapsto 1\ ,\ \ y\mapsto 1,$

$f_2 : x\mapsto 1,\ \ \ y\mapsto 2\ ,$

$f_3 : x\mapsto 2\ ,\ \ y\mapsto 1,$

$f_4 : x\mapsto 2\ ,\ \ y\mapsto 2.$

Let X be a set, T = { 0, 1}.

Proposition.

For a set X there is a bijection from the power set P(X) to the collection F(X,T).

proof. Consider g : P(X) $\to$ F(X,T) as follows

A$\subset$ X, put g(A) = $\chi_A \in$ F(X,T), where χ_A is the characteristic function of A,. We show that g is a bijective map.

Assume that A, B in X, A $\neq$ B . Then There exists a$\in$A\B or b$\in$B\A. If a $\in$A\B then χ_A(a) = 1, χ_B(a) = 0. So $\chi_A \neq \chi_B$ and g is injective.

Let f $\in$F(X,T) . Put A = { x$\in$X | f(x) = 1 } then f = χ_A . Hence g(A) = f and g is surjective. Thus, g is bijective. The proposition is proved.

Chapter IV

RELATIONS

1. On relation Concepts

Definition 1 .

Let X be a set, a relation R on X is subset of the Cartesean product $X \times X$. If $(a,b) \in R$, we say that a is related to b and may write aRb.

Example 1.

Denote by X the set of all inhabitances of some island.

Let U be the subset of $X \times X$ given by $(a, b) \in U$ iff a is the uncle of b. Then U is a relation on X.

Let N be the subset of $X \times X$ given by $(x, y) \in N$ iff x is the niece of y. Then N is also a relation of X.

Example 2 .

X is the set of of real numbers. The subset $S \subset X \times X$ given by $(a, b) \in S$ iff $a \leq b$. Then S or $\leq$ is a relation on X.

Definition 2 .

Let R be a relatrion on X . We say that R is

a) reflexive if aRa for all $a \in X$,

b) symmetric if $aRb \Leftrightarrow bRa$,

c) antisymmetric if $(aRb)\wedge(bRa)\Rightarrow a = b$,

d) transitive if $(aRb)\wedge(bRc) \Rightarrow(aRc)$.

Example 3.

a) In Example 2, the relation S is reflexive, antisymmetric, transitive.

b)X the set of all students in a class. The subset $S \subset X\times X$ given by xSy iff x, y have the same old years. Then S is reflexive, symmetric, transitive.

2. Order relation

Concepts on order relation

Definition 3.

A relation R on X is called an (partly) oder relation if R is reflexive, antisymmetric and transitive. It is usualy denoted by $\leq$. That means $\leq$ is an order relation if

a) $a \leq a$ for all $a\in X$,

b) If $a \leq b$ and $b \leq a$ then $a = b$,

c) If $a\leq b$ and $b \leq c$ then $a \leq c$.

An order relation $\leq$ on X is called total order if for all a, b in X either $a \leq b$ or $b \leq a$.

Example 4.

a) We consider the set **R** of all real numbers. The relation $\leq$ is understood as usual mean ‘’ less than or equal to “. Then $\leq$ is a total order relation on **R** .

b)N is the set of positive integers. Let the relation R on N defined by aRb if b is a multiple of a. Then R is an order relation but not a total order relation.

Notation

Let $\leq$ be an order relation on X. If $x \leq y$ and $x \neq y$ then denote $x < y$.

Definition 4.

An order relation $\leq$ is given on X. Let $A \subset X$.

a) If $x \in X$ such that $a \leq x$ for all $a \in A$ then x is called an upper bound of A.

b) If $y \in X$ such that $y \leq a$ for all $a \in A$ then y is called a lower bound of A.

c) An element x_o is called the greatest element of A if $x_o \in A$ and x_o is an upper bound of A.

d) An element y_o is called the least element of A if $y_o \in A$ and y_o is a lower element.

Note.

1) The least element of A is unique,

2)The greatest of A is unique.

3)Maybe there not exist the least element and the greatest element.

Definition.

Let $\leq$ be an order relation on X, $S \subset X$. An element $x^* \in S$ is called a maximal element of S if for $a \in S$, $x^* \leq a$ implies $x^* = a$. An element $y^* \in S$ is called a minimal element of S if for $a \in S$, $a \leq y^*$ implies $y^* = a$.

Example 5.

Let N be the set of natural numbers N = {0,1,2,... }. The order relation $\leq$ on N given by $x \leq y$ if y is a multiple of x (i.e $y = kx$ for some natural number k. Let S = {2, 4, 5, 6, 9, 12, 16}. Then 2, 3. 5 are minimal elements and 5, 9, 12, 16 are maximal elements.

Lexicographical order.

Definition.

Given a total order relation $\leq$ on X. We defind a order relation on X^n as follows we sat that

$(x_1 ,..., x_n) < (y_1, ..., y_n)$ if there is an idex k , $0 \leq k \leq n-1$ such that $x_i = y_i$, and $x_{k+1} < y_{k+1}$, and we say that

$(x_1 ,..., x_n) \leq (y_1, ..., y_n)$ if $(x_1 ,..., x_n) = (y_1, ..., y_n)$ or

$(x_1 ,..., x_n) < (y_1, ..., y_n)$.

Note. The relation $\leq$ on X^n is a total order relation and called the lexicographical relation on X^n.

Example 6.

X ={0,1} with the total order $\leq$ as $0 \leq 0$, $0 \leq 1$, $1 \leq 1$. In the lexicographical order , compare elements x =(1,1,0,1,0,1,1) ,
y= (1,0,1,1,0,0,0), z = (1,0,1,0,1,1,1) .

Solution

- **y** < x because we take k = 1 and test the above condition .

Where $y_1 = x_1$, $y_2 < x_2$.

- z < y because we take k = 2 , $z_1 = y_1$, $z_2 = y_2$, $z_3 < y_3$.

- **z** < x by using the transitive propertiy of the order relation.

3. Equivalence relation

3.1 Definitions and examples

Definition.

A relation R on a set X is called an equivalence relation if R is reflexive, symmetric and transitive and usually denoted by $\sim$. So a relation $\sim$ is an equivalence relation of X if

a) $x \sim x$ for all $x \in X$

b) if $x \sim y$ then $y \sim x$,

c) If $x \sim y$, $y \sim z$ then $x \sim z$.

Example 7.

a) X is the set of all students of HUT. Put xRy if x and y are in the same class. Then R is an equivalence relation.

b) Let **Z** be the set of integers n be a fix positive integer. Put xRy if x – y is a multiple of n. Then R is an equivalence relation on **Z.**

3.2 Equivalence classes.

Definition .

Consuder an equivalence $\sim$ on X. For a x$\in$ X The set

$\bar{x}$ = { y$\in$X | x$\sim$y } is an equivalence class containing x.

Example 8.

In Example 7 b), take n = 4, the relation $\sim$R defined by xRy if x – y is a multiple of 4. Then equivalence classes are

$\bar{0}$ = { z = 4k | k$\in$ Z },

$\bar{1}$ = { z = 4k+1 | k$\in$ Z },

$\bar{2}$ = { z = 4k +2 | k$\in$ Z },

$\bar{3}$ ={ z = 4k+ 3 | k$\in$ Z }.

Proposition .

Let $\sim$ be an equivalence relation on X. We have

1) *If $y \in \bar{x}$ then $\bar{x} = \bar{y}$,*
2) *Two equivalence classes are either distint or equal.*

Proof .

1) Let y $\in \bar{x}$ then y$\sim$x and x$\sim$y , where $\sim$ is the given equivalence relation. Take an element z. We have

z$\in \bar{x}$ $\Leftrightarrow$ z$\sim$x $\Leftrightarrow$ z$\sim$y $\Leftrightarrow$ z$\in \bar{y}$. Thus, $\bar{x} = \bar{x}$.

2) Assume that $\bar{x} \cap \bar{y} \neq \varnothing$. Take an element z $\in \bar{x} \cap \bar{y}$.

Then $\bar{x} = \bar{z} = \bar{y}$.

Proposition.

Let $\sim$ be an equivalence on X . Then the collection of all equivalence classes is a partition on X.

Proof.

For $x \in X$, xRx and implies $x \in \bar{x}$. Thus, $\bigcup_{x \in X} \bar{x} = X$.

On the other hand, if $\bar{x} \neq \bar{y}$ then $\bar{x} \cap \bar{y} = \varnothing$. This complete the proof.

Note that a partition of a set X induces an equivalence relation on X. Actually, If $X = \bigcup_{i \in I} A_i$ is a partition . $A_i \cap A_j = \varnothing$. We defind a relation $\sim$ on X as follows. For $x, y \in X$, $x \sim y$ if x, y are in the same a subset A_i. We can check that $\sim$ is an equivalence relation.

Definition.

Let $\sim$ be an equivalence relation on X. The set of all equivalence classes $X/\sim \; = \{ \bar{x} \mid x \in X \}$ is called the quotient set of X by the relation $\sim$.

3.3 Partitions induced by maps

Let $f : X \to Y$ be a map. then f induces an equivalene relation on X as follows.

Proposition.

Let f be a map from X to Y. The relation R on X is defined by aRb if f(a) = f(b). Then R is an equivalence relation on X.

Proof.

- for $a \in X$ clearly, f(a) = f(a) , Hence, aRa.
- If aRb then f(a) = f(b) . It follows f(b) = f(a) and therefore, bRa.

● If aRb, bRc then f(a) = f(b), f(b) = f (c). We have f(a) = f(c) and therefore aRc.

The relation is equivalence and the proof is copleted.

Note . By the above proposition a map from X to Y induces an equivalence relation on X and therefore a partition on X .

Example. a) f : **R** □ **R** given by $f(x) = x^2$.

The corresponding equivalence relation $\sim$ defined by $x \sim y$ if $|x| = |y|$.

c) f : **Z** □ **Z** , $f(n) = (-1)^n$. Then the corresponding equivalence relation $\sim$ defined by $x \sim y$ if $x - y$ is even. The corresponding partition is $\mathbf{Z} = Z_1 \cup Z_2$, where $Z_1 = \{ 2n+1 \mid n \in \mathbf{Z} \}$

and $Z_2 = \{ 2n \mid n \in z \}$.

Chapter V

ALGEBRAIC STRUCTURES

1. Binary operators

Definitions and examples

Definition 1.

A binary operator on a set x is a map T : $X \times X \rightarrow X$. For $(x,y) \in X \times X$, T(x, y) is an element of X an denoted by T(x,y) = xTy. Binary operations usually denoted by +, . , * , ∘ or other notations.

Example 1.

The addition (+) on the set of real numbers **R,** (**Q, Z, N**) is a binary operator

The multiplication (.) on the set **R** , (**Q, Z, N**)

c) Let Sym(X) be the set of bijecctions from X into itself. The composition operation (∘) : for f, g∈ Sym(X) , g∘f is the composition of maps f, g. Then (∘) is a binary operator.

d) Let P(X) be the power set of X. Then ∪, ∩ are binary operators on P(x).

Definition 2.

Let * be a binary operator on X and A be a subset of of X. We say that A is closed under the operator * if for every x, y ∈ A

$a*b \in A$

Example 2.

Let Z be the set of integers , Z_1 be the subset of all odd integers, Z_2 the set of all even integers.

a) Under the addition Z_2 is closed,

b) The set Z_1 is not closed under the addition.

Actually, If a,b are in Z_2 (even) then a + b is in Z_2 (even) . If a,b are in Z_1 (odd) then a + b is even . Hence a + b is not in Z_1

Example 3.

Let Q be the set of rational numbers,

B $=\{ a + b\sqrt{2} \mid a, b \in Q \}$. Then Q is closed under addition and multiplication.

Actually, $a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) =$

$= (a_1+ a_2)+(b_1 + b_2)\sqrt{2}$

and $(a_1 + b_1\sqrt{2})(a_1 + b_1\sqrt{2}) =$

$= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1) \sqrt{2}$.

Example 4.

For $X \subset Y$, the power set P(X) is closed under the operations of union and intersection on the power set P(Y).

Properties of binary operators

Definition 3.

Consider a binary operator $(*)$ on X.

a) We say that $*$ is commutative if for every $a, b \in X$,

$$a * b = b * a,$$

b) We say that $*$ is assiciative if for $a, b, c \in X$,

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

c) we say that an element e is an identity for $*$ if for every $a \in X$,

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

Note. If $*$ has an identity element then it is unique.

Actually, if e, f are identity elemens then e = e$*$ f = f . It follows e = f.

Definition 2.

Soppose * has the identity e. Let x$\in$ X. An element x'$\in$ X is called the inverse element for x if x$*$ x' = x' $*$x = e.

If every element of X has the inverse element, we say that $*$ is an invertible oerator.

Note. If * is associstive the inverses are unique.

Notations

a) If a binary operator denoted by + then the identity is usually denoted by 0and the inverse of x is denoted by – x

b) If a binary denoted by . then the identity is denoted by 1 (or e) and the inverse of x is denoted b x^{-1}.

Example 5.

a) On **R** the addition is commutative, associative, has the identity element 0, for x the inverse element is –x.

b) On R the multiplication is commutative, associative, has the identuty 1, for x $\neq$ 0, the inverse is $x^{-1} = \frac{1}{x}$

Example 6.

The multiplication on **Z** has commutative, asoociative properties , has the identity 1. For x $\neq$ 1, -1, there is not the inverse element.

Example 7.

Let Sym(X) be the set of all bijections of X. The composition operation $\circ$ has the following properties

a) $(f\circ g)\circ h = f\circ(g\circ h)$,

b) The identity is Id_X,,

c) For $f \in Sym(X)$, the iverse element is the inverse map f^{-1}.

d) The operation $\circ$ is not commutative , in gerneral $f\circ g \neq g\circ f$.

2. Groups

Semigroups

Definition 3.

A set X with a binary operator is called a sugroup if the operator is associative.

Example 8.

a) **N** with the addition,
b) **Z** with the multiplication,
c) **P(X)** with the union operation,
d) **P(X)** with the intersection operation,
e) **R, Q, Z** with the addition or with the multiplication**.**

Concepts on groups

Definition 4.

Given a binary operator $*$ on a set G. Then G is called a group if the operator has folloing properties

1) Associativity : for a,b, c $\in$ G, $a * (b *c) = (a *b) * c$,
2) Idetity element : there is an element e such that for all x$\in$ G. $e *x = x* e = x$,
3) Inverse element: for each x$\in$ g, there exists x' such that $x *x' = x' *x = e$.

The inverse element for x is denoted by x^{-1}.

If the operator of a group G is commutative then G is called a commutative group (or Abelian group).

Example 9.

a) **Z**, **Q**, **R** with the addition are Abelian Groups,
b) **Q\{0}, R\{0}** with the multiplication are Abelian groups,
c) Sym(X) with the coposition of maps $\circ$ is a noncommutative group.

Some properties

Proposition 1.

In a group, the identity is unique, foe an element x the inverse element is unique.

Proposition 2.

Let (G, .) be a group. For a,b are given in G. We have

1) *The equation ax = b has unique solution*

2) *The equation $xa = b$ has unique solution.*

Proof.

1) $ax = b \Leftrightarrow a^{-1}(ax) = a^{-1}(ax) \Leftrightarrow (a^{-1}a)x = a^{-1}b \Leftrightarrow$

$ex = a^{-1}b \Leftrightarrow x = a^{-1}b$, where e is the identity.

2) Analogously, $xa = b \Leftrightarrow x = ba^{-1}$.

Proposition 3.

Let (G,.) be a group. Then

1) If $ax = ay$ then $x = y$,
2) If $xa = ya$ then $x = y$,
3) $(xy)^{-1} = y^{-1}x^{-1}$.

3. Subgroups, normal subgroups

Subgroups

Definition 5.

Let $(G, *)$ be a group, a subset H in G is called a subgroup of g if H is also a group under the operator $*$.

Example 10.

a) **Z** is a subgroup of (**Q**,+) or (**R**, +),
b) 2**Z =** $\{ 2n \mid n\in$ **Z** $\}$ is a subgroup of (Z, +),
c) H = $\{ 2n+1 \mid n\in$ **Z** $\}$ is not a subgroup of (**Z** , +),
d) **Z** is not a subgroup of (**Q***, .) , where **Q***= **Q**\{0}, the operator is the multiplication.

Proposition 5.

Given a group (G,.) and a nonempty subset H of G. Then H is a subgroup of G if two conditions hold:

1) For all$x, y \in H$, $xy \in H$,

2) For all $x \in H$, the inverse $x^{-1} \in H$.

Note. A nonempty subset H of a group G is a subgroup if for all $x, y \in H$, $xy^{-1} \in H$.

Proposition 6.

Intersection of a collection of subgroups of G is a subgroup of G

Normal subgroups

Definition 6.

Let H be a subgroup of a group (G,.). The left and the right cosets of H containing g are

$gH = \{ gh \mid h \in H \}$; $Hg = \{ hg \mid h \in h \}$

respectively.

Proposition 7.

Assume that H ios a subgroup of G. Then

1) For $x \in G$, $x \in xH$,

2) If $y \in xH$ then $xH = yH$,

3) The cosets of H form a partition of G.

4) $xH = yH$ if and only if $x^{-1}y \in H$.

Definition 7.

A subgroup H of a group G is called a normal subgroup of G if for all $x \in G$, $h \in H$, $xhx^{-1} \in H$. If H is a normal subgroup of g we denote by

H G.

Example 11.

a) G is a group, e is the identity element of G. Then G and {e} are normal subgroups.

b) If G is an Abelian group then any sugroup H of G is a normal subgroup.

Proposition 8.

Let H be a subgroup of a group G. Then H is a normal subgroup if and only if for all $a \in G$ $aH = Ha$.

Let H be a normal subgroup of (G, .). Put $\overline{x} = xH$ for $x \in G$.

On the set $G/H = \{ xH \mid x \in G \} = \{ \overline{x} \mid x \in G \}$ we define a operator as follows

$$\overline{x} . \overline{y} = \overline{x.y} .$$

Then this is a binary operator.

Proposition 9.

Assume that H is a normal subgroup of G. G/H with the above operator is a group called the quotien group.

Example 12.

Z is the of integers, m is a fix natural number, $m\mathbf{Z} = \{ mn \mid n \in$ Z }. Then m**Z** is a nomal subgroup of the additive group **Z** and the quotient group $\mathbf{Z}/m\mathbf{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1} \}$, where $\bar{k} = \{mn + k, n \in Z \}$.

4. Rings and fiels

Rings

Definition 8.

Let V be a set with two binary operators usually as addition and multiplication (+ and .). Then we V is a ring if

1) (V, +) is a Abelian group with the identity 0.
2) For $x,y, z \in V$, $(xy)z = x(yz)$,
3) For $x,y,z \in V$, $x(y + z) = xy + xz$,
4) For $x,y,z \in V$, $(x + y) z = xz + yz$.

If ring V has the property : $xy =yx$ for $x, y \in V$ then the ring is called commutative.

If ring V has the identity for the multiplication , V is called a ring with identity.

Example 13.

a) (Z, +, .), (Q, +, .), (R, +, .) are commutative rings with identity.
b) Let P[x] be the set of all polynomials . With the addition of polynomials and multiplication of polynomials P[x] becomes a commutative.

Fields

Definition 9.

Let F be a ring. We say that F is a field if

1) F is a commutative ring with identity 1.

2) For $x \neq 0$, $y \neq 0$, we have $xy \neq 0$

3) For every $x \neq 0$, there exists the inverse element x^{-1} such that $x.x^{-1} = 1$.

Remark. If F is a field , $F^* = F\backslash\{0\}$ is group under the multiplication.

Example 14.

a) (R, + , .) is a field,

b) (Q, + , .) is a field.

c) $\mathbf{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, where $\bar{0} = \{ 3n \mid n \in Z \}$, $\bar{1} = \{ 3n+1 \mid n \in Z \}$, $\bar{2} = \{ 3n+2 \mid n \in Z \}$. Defind addition and multiplication operations as follows $\bar{i} + \bar{j} = \overline{i+j}$, $\bar{i} . \bar{j} = \overline{i.j}$. Then Z_3 is a field.

Notation.

Let F be a field, x is an element of F the sum

$x + x + ... + x$ (k terms) is denoted by kx.

Definition 10.

Let F be a field, e be the identity element of F. If p is the smallest natural number such that $pe = 0$ then p is called the characteristic of the field F. If $ke \neq 0$ for every natural number k then the characteristic is zero.

Example 15.

a) $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, $\bar{1} + \bar{1} + \bar{1} = 3.\bar{1} = \bar{0}$. Characteristic of Z_3 is 3.

b) Field **R** of real numbers has the characteristic zero.

c) Field Q of rational numbers has the characteristic zero.

Theorem 10.

Assume that p is the characteristic of a field. If $p \neq 0$ then p is a prime number.

Proof

If $p = r.s$ then $pe = 0$ and $(re)(se) = 0$. It follows $re = 0$ or $se = 0$. This is a contradiction.

Ring of integers

Definition 11.

Let m and n be integers . We say that m divides n and write $m | n$ if there exists an integer k such that $n = km$. Then m is a divisor of n and n is a multiple of m.

Example 16.

3 is a divisor of 6, and 6 is a multiple of 3. We denote $3 | 6$.

Definition 12.

If a, d are natural numbers , d is a nonzero then there exist unique unique integers q and r such that

$a = qd + r, \quad 0 \leq r < d.$

The number q is called the quotient.

If $r = 0$ then d is a divisor of a and a is a multiple of d.

Definition 13.

Two integers a, b are said to be congruenct modulo n if $a - b$ is an integer multiple of n .

Remark. Two integers a, b are congruent modulo m if and only if they have the same remander after dividing by the modolus m.

Denote $a \equiv b \bmod m$

Example 17

a) $3 \equiv 8 \bmod 5$,

b) $-3 \equiv 17 \bmod 10$.

Proposition 11.

The congruence modulo m relation is an equyvalence relation

Proof.

1) For an integer $a \in Z$, $a \equiv a \bmod m$,

2) If $a \equiv b \bmod m$ then $b \equiv a \bmod m$,

3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

Proposition 12.

If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then

$$(a + c) \equiv (b + d) \bmod m,$$

$$(a - c) \equiv (b - d) \bmod m,$$

$$a.c \equiv b.d \bmod m.$$

Definition 14.

The set of integers congruent to an integer i modulo m is called the congruence class of i modulo m. This class is denote by $\bar{i}$.

The set of congruence class modulu m is denoted by $\mathbf{Z}_m$ o r $\mathbf{Z}/m\mathbf{Z}$.

Thus $Z_m = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1} \}$.

Now we difine the addition and multiplication on Z_m as follows

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a}.\bar{b} = \overline{a.b}.$$

Proposition 13.

Z_m with the above addition and multiplication becomes a ring.

Euclidean Algorithm

Definition 15.

Given two natural integers a, b. The greatest common divisor is the largest number that divides both a and b without living a remader.

Denote the greatest common divisor of a, b by GCD(a, b).

Definition 16.

If GCD(a, b) = 1 then a, b are said to becoprime.

Example 18.

a) GCD(6 , 9) = 3,
b) GCD(180, 315) = 45
c) GCD (315, 143) = 1. So 315 and 143 are copime.

Proposition 14.

If $GCD(a , b) = d$ *then there exist integers* m, n *such that* $am + bn = d$.

Definition 17.

For two natural numbers a, b the lowest common denominator (LCD) is the least common multiple of a and b.

Example 19.

a) LCD(6, 9) = 18,
b) LCD(180, 315) = 1260.

Proposition 15.

For natural numbers a, b we have

$$a.b = GCD(a,b).\ LCD(a,b).$$

Proposition 16.

Suppose that natural numbers a, b, q, r satisfy the formula

$$a = bq + r.$$

Then $$GCD(a, b) = GCD(b, r).$$

Steps of Euclidean Algorithm.

Using the above proposition one can obtain a method of finding GCD of a,b called Euclidean algorithm.

Each step k begins with two natural numbes i and j and the goal is to find two new nonegative integers q_k, r_k :

$i = q_k.j + r_k$, $0 \le r_k < j$.

q_k, r_k are called the qoutient and the remainder of step k. In step 1 the numbers i and j are taken to be the numbers a, b.

Step 1. Express $a = q_1.b + r_1$,

Step2. $b = q_2.r_1 + r_2$

Step 3. $r_1 = q_3.r_2 + r_3$

... ...

Step k . $r_{k-2} = q_k.r_{k-1} + r_k$

... ...

The last step $r_{n-1} = q_{n+1}. r_n$.

Then $r_n = GCD(a, b)$.

Example 20.

Find GCD of 1071 and 1029.

Solution

$1071 = 1 \times 1029 + 42,$

$1029 = 24 \times 42 + 21,$

$42 = 2 \times 21.$

The greatest common divisor of 1071 and 1029 is 21.

Presentation of integers

We usually integers as form 10-adic. For example,

$$2139 = 2.10^3 + 1.10^2 + 3.10^1 + 9.10^0.$$

Remark.

Given a positive integer b . For a natural number n we have the expression

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1.b + a_0,\ \ 0 \leq a_j < b\ ,\ a_k \neq 0. \qquad (*)$$

Then the presentation (*) is said to be the expansion of n by base b.

Denote $n = (\ a_k\, a_{k-1} ... a_1\, a_0)_b$

If b = 2 the presetation (*) is called the binary expansion of n.

Example 21.

a) The binary expansion of 35 is

$$35 = 1\times 2^5 + 0\times 2^4 + 0\times 2^3 + 0\times 2^2 + 1\times 2^1 + 1\times 2^0$$

$$35 = (100011)_2$$

b) The expansion of 135 by base 4 is

$$135 = 2\times 4^3 + 0\times 4^2 + 1\times 4^1 + 3\times 4^0$$

$$135 = (2013\ )_4\ .$$

Algorithm for expantion of n by base b.

on the step k we find the numbers q_k, a_k satisfy

$$q_{k-1} = b.q_k + a_k, \qquad 0 \leq a_k < b.$$

Step 1. $n = b.q_0 + a_0$

Step 2. $q_0 = b.q_1 + a_1$

Step 3. $q_1 = b.q_2 + a_2$

... ...

The last *step* is $q_{m-1} = b.q_m + a_m$ if $q_m = 0$.

Then $n = (a_m a_{m-1} \ldots a_1 a_0)_b$.

Example 22.

Represent 1397 by base 8.

$1397 = 8.\ 174 + 5$

$174 = 8.21 + 6$

$21 = 8.2 + 5$

$2 = 8.0 + 2$

Hence, $1397 = (2565)_8$

Chapter VI

FIELD OF COMPLEX NUMBERS

1. Concepts on complex numbers

Canonical form of complex numbers

Definition 1 .

Let **R** be the fiel of real numbers . Put **C** = **R**×**R** . We define addtion and multiplication operators on **C** as follows .

For $z_1 = (a, b)$, $z_2 = (c, d)$ in **C**,

$z_1 + z_2 = (a + c, b + d)$,

$z_1 . z_2 = (ac – bd, ad + bc)$.

Proposition 1.

The set C with the above addition and multiplication operators is a field called the fiedl of complex numbers.

Proof. We can check following properties

1) $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$,
2) $z_1 + z_2 = z_2 + z_1$,
3) There is an identity element $0 = (0,0)$ for addition , $0 + z = z + 0 = z$ for $z \in$ **C**.
4) For $z =(a, b)$, $-z = (-a, -b)$,
5) $z_1(z_2z_3) = (z_1z_2)z_3$,
6) $z_1.z_2 = z_2.z_1$
7) $z_1(z_2 + z_3) = z_1z_2 + z_1z_3$

8) The identity for multiplication is e = (1, 0), ez = ze = z.

9) z = (a, b) ≠ 0 , the inverse element is z^{-1} = ($\frac{a}{a^2+b^2}$, $\frac{-b}{a^2+b^2}$),

$z.z^{-1} = z^{-1}.z = e$.

We say that an element of C is a complex number.

Note.

For complex numbers of form (a, 0), we have

(a, 0) + (c, 0) = (a + c, 0)

(a, 0)(c, 0) = (ac, 0).

We can identify a complex number (a, 0) as the real number a∈**R** (a ,0) ≡ 0 . Then the identity e = (1, 0) ≡ 1.

Put i = (0, 1). We have i^2 = (0, 1)(0, 1) = (-1, 0) = -1. This ellement i is called the imaginary unit. For z = (a, b) , it can be expressed as z = (a, b) = a + b.i, a.b ∈ **R.**

Definition 2.

For a complex number z ∈ C,

$$z = a + bi , \qquad (1.1)$$

where a, b∈ R, and $i^2 = -1$. The above form of z is called the canonical form of z. The real number a is called the real part of z and denoted by a = Re(z). The real number b is called the imaginary part of z denoted by b = Im(z).

Note that for z_1 ,z_2 ∈ C,

$$z_1 = z_2 \text{ iff } Re(z_1)=Re(z_2), \quad Im(z_1)= Im(z_2). \qquad (1.2)$$

Operations of complex numbers in canonical form

Addition : $(a + b.i) + (c + d.i) = (a + c) + (b + d)i$,

Substraction: $(a + b.i) - (c + d.i) = (a - c) + (b - d)i$,

Multiplication : $(a + b.i)(c + d.i) = (ac - bd) + (ad + bc)i$,

Division is defined by $\frac{z_1}{z_2} = z_1 . z_2^{-1}$ for $z \neq 0$.

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,\mathrm{i}.$$

Example1

a) $(2 + 3i) + (-1 + 4i) = 1 + 7i$,

b) $(2 + 3i) - (5 + i) = (-3) + 2i$,

c) $(2 + 3i)(1 + i) = -1 + 5i$,

d) $\frac{2+3i}{1+i} = \frac{(2+3i)(1-i)}{(1+i)(1-i)} = \frac{5+i}{2} = \frac{5}{2} + \frac{i}{2}$,

e) $(2 + 3i)^3 = -46 + 9i$

Modulus, conjugation of complex numbers

Definition 3.

For a complex number $z = a + bi$, where $a, b \in \mathbf{R}$.

Modulus $|z|$ of z is given

$$|z| = \sqrt{a^2 + b^2}\,, \qquad (1.3)$$

Conjugate of z = a + bi is defined to be the complex number a – bi usualy denoted by z* or $\bar{z}$

$$\bar{z} = a - bi \quad . \qquad (1.4)$$

Proposition 1.

For complex numbers we have

1) $|z| \geq 0$, *and* $|z| = 0$ *iff* $z = 0$,

2) $|z + w| \leq |z| + |w|$,

3) $|z.w| = |z|\,|w|$

4) $|1| = 1$, $\left|\dfrac{z}{w}\right| = \dfrac{|z|}{|w|}$,

5) $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{z.w} = \bar{z}\,.\,\bar{w}$,

6) $\overline{\left(\dfrac{z}{w}\right)} = \dfrac{\bar{z}}{\bar{w}}$, $\bar{\bar{z}} = z$,

7) $\bar{z} = z$ *if and only if z is a real number,*

8) $\bar{z} = -z$ *if and only if z is purely imaginary,*

9) $Re(z) = \dfrac{1}{2}(z + \bar{z})$, $Im(z) = \dfrac{1}{2i}(z - \bar{z})$,

10) $|z| = |\bar{z}|$, $|z|^2 = z.\,\bar{z}$.

2. Polar form of complex numbers

Definitions and examples.

A complex number z can be wiewed as a point or a vector in two-dimension cartesean coordinate system called the complex plane.

The number z = x + yi can be considered as the poin z(x, y) in the plane Oxy and Oxy is called the complex plane.

So the modolus of z is the distance from O to z, the number x is x-coordinate of z and y is the y-coordinate of z.

If $z = x + 0i$ then z is a real number and it lies on x-axis. Therefore, Ox is called the real axis. If $z = 0 + yi$ then z is purely imaginary and lies on Oy . Then Oy is called the imaginary axis.

In the complex plane , for a point $z = (x, y)$, we put $r = |z|$, and φ the angle beween Ox and Oz.

We have

$$z = x + yi = r(\cos\varphi + i.\sin\varphi) \qquad (2.1)$$

The expantion (2.1) is called the polar form (or trigonometric form) of z. Here we recall that r is the modulus of z. The value φ is called argument of z. The argument of z is unique modulo 2π.

Put $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Then

$$z = r(\cos\varphi + i\sin\varphi) = r\, e^{i\varphi} \qquad (2.2)$$

The form (2.2) is called the exponential form of z.

Some operations of complex numbers in the polar form

We can show the following formulas

Multiplication:

If $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ and $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$ then

$$z_1.z_2 = r_1.r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) \qquad (2.3)$$

Division:

If $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ and $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, $z_2 \neq 0$, then

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)) \qquad (2.4)$$

Exponentiation:

If $z = r(\cos\varphi + i.\sin\varphi)$ then

$$z^n = r^n(\cos n\varphi + i.\sin n\varphi) \qquad (2.5)$$

Here we pove the formula (2.3):

$$z_1.z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1)\, r_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= r_1r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1 .\sin\varphi + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)$$

$$= r_1r_2((\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) \quad .$$

Moiver's formula :

$$(\cos\varphi + i.\sin\varphi)^n = (\cos n\varphi + i.\sin n\varphi) \qquad (2.6)$$

Example 2.

Express the complex number $(1 + i)^{99}$ in the canonical form.

Solution. $z = (1 + i) = \sqrt{2}\,(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}),$

$$z^n = (\sqrt{2})^{99}(\cos 99\frac{\pi}{4} + i\sin 99\frac{\pi}{4}) =$$

$$= (\sqrt{2})^{99}(\cos 3\frac{\pi}{4} + i\sin 3\frac{\pi}{4}) = 2^{49}(-1 + i)$$

$$= -2^{49} + 2^{49}.i$$

Example 3.

Express sinnx, cosnx in term of cosx sinx

Solution. We have

$$(\cos\varphi + i.\sin\varphi)^n = (\cos n\varphi + i.\sin n\varphi).$$

On the other hand, by binomial formula

$$(\cos\varphi + i.\sin\varphi)^n = \sum_{k=0}^{n} C_n^k (\cos x)^k (i.\sin x)^{n-k}.$$

here

$$C_n^k = \frac{n(n-1)\ldots(n-k+1)}{k(k-1)\ldots2.1}.$$

Then express $(\cos\varphi + i.\sin\varphi)^n =$ $A + Bi$, where A, B are polynomials of cosx, sinx. It follows

$A = \cos nx$, $B = \sin nx$. That are formulas we need.

Example 4.

$(\cos x + i\sin x)^3 = \cos 3x + i\sin 3x$,

Other hand, $(\cos x + i\sin x)^3 =$

$= \cos^3 x + 3\cos^2 x.(i\sin x) + 3\cos x(i\sin x)^2 + (i\sin x)^3$

$= (\cos^3 x - 3\cos x \sin^2 x) + i(3\cos^2 x \sin x - \sin^3 x)$.

Hence, $\cos 3x = \cos^3 x - 3\cos x \sin^2 x$,

$\sin 3x = 3\cos^2 x \sin x - \sin^3 x$.

n-roots of a complex number

Definition 4.

If c is a complex number, n is a positive integer, then any complex number z satisfying the formula $z^n = c$ is called an n-th root of the coplex number c.

Example 5.

a) The numbers 1, -1 are square roots of 1,

b) The numbers 1, -1, i, -i are fouth roots of 1.

c) $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ is a square root of i.

For c = 0 the n-th root of 0 is 0.

For a complex number c , the set of all n-th roots of c is denoted by $\sqrt[n]{c}$.

Thus, $\sqrt[n]{c} = \{ z \in \mathbf{C} \mid z^n = c \}$.

Proposition 2.

If $c = r(\cos\varphi + i.\sin\varphi)$ is nonzero then the set of all n-th roots contains n elements z_k given by

$$z_k = \sqrt[n]{r}\,(\cos\frac{\varphi+2k\pi}{n} + i.\sin\frac{\varphi+2k\pi}{n}),\ k = 1,2,...,n-,. \qquad (2.7)$$

where $\sqrt[n]{r}$ represents the usual (positive) n-th root of the positive number r.

Proof. Let $z = \rho(\cos\theta + i\sin\theta)$ be an n-th root of c. Then

$$z^n = \rho^n(\cos n\theta + i\sin n\theta) = r(\cos\varphi + i.\sin\varphi).$$

We have $\rho^n = r$; $n\theta = \varphi + 2k\pi$, $k\in \mathbf{Z}$. It follows

$$\rho = \sqrt[n]{r},\ \theta = \frac{\varphi+2k\pi}{n},\ k\in\mathbf{Z}.$$

However, we have only n distint values of z corresponding to n values of k =0, 1,..., n-1 that denoted by $z_k = \sqrt[n]{r}\,(\cos\frac{\varphi+2k\pi}{n} + i.\sin\frac{\varphi+2k\pi}{n}$.

The proposition is proved.

Example 6.

Find the set of all n-th roots of 1.

Solution. We have $1 = 1(\cos 0 + i\sin 0)$. By the for mula (2.7), there are n values of n-th roots that are

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i.\sin\frac{2k\pi}{n},\ \text{where } k = 0, 1, ..., n-1.$$

Example 7.

The 6^{th} roots of 1 are

$$\varepsilon_0 = 1,\quad \varepsilon = \varepsilon_1 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3},$$

$$\varepsilon_2 = \cos 2\frac{\pi}{3} + i \sin 2\frac{\pi}{3}, \quad \varepsilon_3 = \cos 3\frac{\pi}{3} + i\sin 3\frac{\pi}{3},$$

$$\varepsilon_4 = \cos 4\frac{\pi}{3} + i\sin 4\frac{\pi}{3}, \quad \varepsilon_5 = \cos 5\frac{\pi}{3} + i\sin 5\frac{\pi}{3}.$$

3. Quadratic equations on C

Quadratic equations of real coefficients

Let us consider quadratic equations

$$ax^2 + bx + c = 0, \qquad (3.1)$$

where a, b, $c \in R$, $a \neq 0$ and x is the variable.

Recall that to **find the real solutions** of the equation (3.1) we have

1) If $\Delta = b^2 - 4ac > 0$ then the equation has two real root

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \; x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}. \qquad (3.2)$$

2) If $\Delta = b^2 - 4ac = 0$ then the equation (3.1) has a double solution

$$x_1 = x_2 = \frac{-b}{2a}, \qquad (3.3)$$

3) If $\Delta = b^2 - 4ac < 0$ then the equation has no real solutions.

To **find complex solutions** of the equation (3.1) we have

1) If $\Delta \geq 0$ solutions as in (3.2), (3.3).
2) If $\Delta < 0$ the equation has two conjugate complex roots

$$x_{1,2} = \frac{-b \pm i\sqrt{|\Delta|}}{2a}. \qquad (3.4)$$

Example 8.

Solve the equation $x^2 - 2x + 10 = 0$.

Solution. $\Delta = b^2 - 4ac = -36 < 0$. We have two conjugate complex roots $x_1 = 1 + 3i$, $x_2 = 1 - 3i$.

Quadratic equations of complex coefficients

Let us consider the equation

$$ax^2 + bx + c = 0, \qquad (3.5)$$

where a, b, c are complex coefficients , $a \neq 0$

The equation always has complex roots

$$x_{1,2} = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad , \qquad (3.6)$$

where $\sqrt{b^2 - 4ac}$ in the sense of square roots of a complex number. So $\sqrt{b^2 - 4ac}$ contains two values.

Remark that when consider the equations in **C** we can see the case of real coefficients as special case of complex coefficients.

Example 9.

Solve the equation $x^2 + 2ix - 10 = 0$.

Solution. $x_1 = -i + 3$, $x_2 = -i - 3$

Example 10. Solve the equation

$$x^2 - 2(1 + i)x - 14i = 0,$$

Solution. $x_{1,2} = (1+i) + \sqrt{(1+i)^2 + 14i} = (1+i) + \sqrt{16i}$

$$= (1+i) + 4\sqrt{i} = (1+i) \pm 4\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i\right).$$

Thus, $x_1 = (1+2\sqrt{2}) + (1+2\sqrt{2})i$; $x_2 = (1 - 2\sqrt{2}) + (1- 2\sqrt{2})i$.

4. Polynomials of complex variables

Consider a polynomial of degree n on **C**

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \quad , \qquad (4.1)$$

where $a_0, a_1, ..., a_n \in C$, $a_n \neq 0$ and x is complex variable.

Definition 5.

A complex number α is said to be a root of the polynomial

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

if $p(\alpha) = 0$ i.e $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0$.

Proposition 3.

*Every polynomial of degree n on **C** has exactly n complex roots (counting multiple roots according to their multiplicity).*

Proposition 4.

If $x_1, x_2, ..., x_n$ are roots of the polynomial $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ then $p(x)$ can be represented in the form

$$p(x) = a_n(x - x_1)(x - x_2)...(x - x_n). \qquad (4.2)$$

Now we consider the polinomial of real coefficients

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \;, \qquad (4.3)$$

where $a_0, ..., a_n$ are real numbers.

Proposition 5.

If α is a complex root of $p(x)$ in (4.3) then the conjugate complex number $\overline{\alpha}$ of α is also a root of $p(x)$.

Proof. From $p(\alpha) = 0$ we have $p(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0$ and

$$\overline{p(\alpha)} = \overline{a_0 + a_1\alpha + ... + a_n\alpha^n} = 0.$$

Hence, $a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + ... + a_n\overline{\alpha}^n = 0$. Thus, $p(\overline{\alpha}) = 0$ and $\overline{\alpha}$ is a root of p(x). The proof is complete.

Proposition 6.

Let p(x) be a polynomial of real coefficients . Then p(x) can be expressed as a product of binomials and quadratic polynomials of negative discriminant.

Proof. Let $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, $a_i \in \mathbf{R}$. Suppose that $x_1, ..., x_n$ are n complex roots of p(x). Then

$$p(x) = a_n(x - x_1)(x - x_2)...(x - x_n). \qquad (4.4)$$

If x_k is a real root then $(x - x_k)$ is a real binomial factor of p(x).

If x_k is a complex root (noreal) then $\overline{x_k}$ is also a root of p(x). We have

$(x - x_k)(x - \overline{x_k}) = x^2 - (x_k + \overline{x_k})x + x_k\overline{x_k}$ is a factor of p(x). Moreover, $(x_k + \overline{x_k})$ and $x_k\overline{x_k}$ are real numbers. So this factor is a quadratic polynomial that has no real roots and therefore, the discrimant Δ of this factor is negative.